



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 1

Friday 7 November 2003

Contents

- [Credit agencies sending our files abroad](#)
[David Lazarus via Paul Saffo](#)
- [Crypto screwup: Sensitive Israeli missile test inadvertently broadcast](#)
[Craig S. Bell](#)
- [A new risk for electronic voting](#)
[Jeremy Epstein](#)
- [California Halts E-Vote Certification](#)
[Kim Zetter via Monty Solomon](#)
- [Touch screen voting -- like Web site maintenance?](#)
[William Nico](#)
- [Irish Labour Party urges suspension of e-voting until flaws addressed](#)
[Patrick O'Beirne](#)
- [E-ZPass, UPS, and Newark Airport](#)
[Susan Landau](#)
- [Microsoft puts a price on the heads of virus writers](#)
[NewsScan](#)
- [Microsoft patches their patched patches](#)
[Robert Bruce Thompson via Dave Farber](#)
- [Remember those jokes about "if AT&T built cars?"](#)
[Daniel P.B. Smith](#)

- [Duh! an electronic signature!](#)
[Geoff Kuenning](#)
 - [Paying employees is not rocket science](#)
[Paul Robinson](#)
 - [Another victim of the d__n bad-word filter!](#)
[Adam Abrams](#)
 - [REVIEW: "High Integrity Software", John Barnes](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Credit agencies sending our files abroad (via Dave Farber's IP)

<Paul Saffo <psaffo@iftf.org>>
Fri, 07 Nov 2003 08:47:57 -0800

David Lazarus <dlazarus@sfchronicle.com>,
San Francisco Chronicle, 7 Nov 2003 [PGN-ed]
sfgate.com/article.cgi?file=/c/a/2003/11/07/MNG4Q2SEAM1.DTL
IP Archives at: <http://www.interesting-people.org/archives/interesting-people/>

Two of the three major credit-reporting agencies (Equifax, Experian and TransUnion, each holding detailed files on about 220 million U.S. consumers) are in the process of outsourcing sensitive operations abroad, and a third may follow suit shortly. Privacy advocates say the outsourcing of files that include Social Security numbers and complete credit histories could lead to a surge in identity theft because U.S. laws cannot be enforced overseas. For their part, the credit agencies say the trend is a necessary cost-cutting move in light of new legislation that would allow all consumers to obtain free copies of their credit reports. (TransUnion

states that
would cost them as much as \$350 million a year.)

"The application of American law in a foreign country is difficult, if not impossible," said Sen. Dianne Feinstein. "Therefore, the more companies move overseas, the less American law can control the uses for which personal data is put. And this can only represent an increasing threat to the privacy of our citizens."

Sen. Barbara Boxer said she would ensure that the matter was raised as senators and House members completed changes to the Fair Credit Reporting Act. "This information is very significant, and I intend to make sure that the conferees who are finalizing the bill are aware of the *Chronicle*'s investigation in hopes that they will protect Americans from such outrageous invasions of privacy," Boxer said.

✶ Crypto screwup: Sensitive Israeli missile test inadvertently broadcast

<"Craig S. Bell" <craig@runbox.com>>
Thu, 06 Nov 2003 22:38:47 GMT

A security lapse by Israel Aircraft Industries apparently permitted an internal screening of a missile test to be accessible by satellite dish, unencrypted.

<http://www.haaretz.com/hasen/spages/357662.html>

[PGN-ed; also

<http://www.newsday.com/news/nationworld/wire/sns-ap-israel-missile-test,0,409849.story?coll=sns-ap-nationworld-headlines>

]

A new risk for electronic voting

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Thu, 6 Nov 2003 15:56:08 -0500

The RISKS of electronic voting have been discussed often enough in this forum that I won't repeat them further (cf. Rebecca Mercuri's piece in [RISKS-22.96](#)).

Last week's election in Fairfax County (Virginia) had a new risk I haven't seen covered before. They use WinVote machines, made by Advanced Voting Solutions of Frisco, Tex. These are essentially Windows laptops with a touchscreen and an 802.11 wireless net. (More about that in another RISKS article one of these days.)

Seems that during the election, at least eight of the machines failed (out of almost 1000 in use county-wide), and were taken out of the polling places to a central repair facility, and then brought back after some form of "repair" was made (a reboot at the polling place did not solve the problem). The seals were broken, but the voting officials in the precincts were told to resume using them. The result was a lawsuit by the Republican party

seeking to invalidate the votes from those machines. There aren't enough votes at stake that it would change any of the election results.

Of course, the real problem is that without any sort of physical (paper) record, it's impossible to prove what really happened when the machines were being "repaired".

In addition, the "hi tech" vote counting (which was supposed to occur by uploading the results from every precinct to a central computer over a dial-up line) overloaded the servers, and "More than half of precinct officials resorted to the old-fashioned telephone to call in their numbers or even drove the results to headquarters, elections officials said. A handful of precincts went back to paper ballots."

The only thing that's surprising here is that the election officials were surprised.

See <http://www.washingtonpost.com/wp-dyn/articles/A1397-2003Nov5.html>

California Halts E-Vote Certification (Kim Zetter)

<Monty Solomon <monty@roscom.com>>

Tue, 4 Nov 2003 19:16:59 -0500

Kim Zetter, Wired.Com, 3 Nov 2003

SACRAMENTO, California -- Uncertified software may have been installed on

electronic voting machines used in one California county, according to the secretary of state's office. Marc Carrel, assistant secretary of state for policy and planning, told attendees Thursday at a panel on voting systems that California was halting the certification process for new voting machines manufactured by Diebold Election Systems. The reason, Carrel said, was that his office had recently received "disconcerting information" that Diebold may have installed uncertified software on its touch-screen machines used in one county. He did not say which county was involved. However, Secretary of State spokesman Douglas Stone later told Wired News that the county in question is Alameda. ...

<http://www.wired.com/news/politics/0,1283,61068,00.html>

⚡ Touch screen voting -- like Web site maintenance?

<William Nico <nico@mcs.csu Hayward.edu>>

Wed, 5 Nov 2003 09:02:54 -0800 (PST)

The 4 Nov 2003 election in Pleasanton, CA had only a School Board choice on the ballot. However, the "Instructions", which comprised the opening page on the touch screen voting machine, were wholly focused in detail on the gubernatorial recall election of 7 Oct 2003!

⚡ Irish Labour Party urges suspension of e-voting until flaws

addressed

<"Patrick O'Beirne" <pob2002@sysmod.com>>

Mon, 03 Nov 2003 19:39:55 +0000

<http://www.labour.ie/press/detail.tml?SKU=20031103143251>

Press Release

Gilmore urges suspension of e-voting until flaws addressed

Eamon Gilmore TD, Labour Spokesperson on Environment and Local Government

Issued on Monday 03 November, 2003

The Labour Party has called for the suspension of plans to extend electronic voting until the e-voting system has been changed.

The call was made today (Monday) by the Labour Party Spokesperson on Local Government and the Environment, Eamon Gilmore TD, at a Press Conference to launch a study of electronic voting system which was commissioned by the Labour Party. The report was prepared by two Labour Party members, Shane Hogan and Robert Cochran who are both experienced IT specialists.

Deputy Gilmore said:

"The report identifies a number of major flaws and deficiencies in the electronic voting system which the Government plans to extend to all areas of the country for the Local and European Elections next year.

The major defects are:-

* No integrated end-to-end test of the entire system has been conducted to date. The testing of the Integrated Election Software (IES) software was

carried out by the UK based Electoral Reform Society in 2002. However for

this test the random mix feature of the IES was disabled. An integrated end-to-end test would generally be considered a key part of the implementation of any new technology.

* Formal Methods were not used to prove the accuracy of the software.

Formal Methods refer to a set of mathematically based techniques that are used in the development of safety-critical software such as airplane

navigation or life support machines. The Department of the Environment has

not made the actual source code publicly available but it is clear from

the technology used and source code review that formal methods were not

used and that therefore there are bugs in the software.

* It is possible that the data-base on the Count Centre PC which is

Microsoft access, could be overridden by a replacement pre-prepared data

base, which could be designed to give a specific result by a single "copy"

command. In addition vote information is transferred between PCs at the

Count Centre on floppy discs. It would not be difficult to exchange discs.

* Unauthorised persons could produce a version of the NEDAP voting machine

software and/or the IES which could be designed to give an election result

biased in favour of a particular Party or Candidate.

"These threats are possible because the proposed electronic voting system

lacks the transparency of the current paper ballot system. The voter has no

way of being certain that the vote which he/she casts is

accurately recorded
by the voting machine and software and is thereafter not
overridden by a
corruption of the Count Centre software. The voter is expected
to have blind
trust in the technology.

"The Labour Party is proposing a number of reforms which will be
necessary
if the proposed electronic voting system is to be reliable, free
from
interference and if it is to enjoy the confidence of the public.

"The reforms proposed by the Labour Party are as follows:-

1. The introduction of a Voter Verifiable Audit Trail (VVAT)
which would
create a parallel paper record of votes cast which could be
stored and
checked in the event of a dispute over an election outcome.
2. The use of Formal Methods to ensure that the software used in
both the
election machines and in the vote counting is totally reliable.
3. The adoption of formal procedures to prevent interference
either with the
machines software or counting process.
4. The carrying out of an integrated end-to-end test of the
entire system.
5. The establishment of an independent audit and supervisory
role over
electronic voting for the Standards In Public Office Commission.

"The complete changeover to electronic voting next June will be
the biggest
single change in the country's electoral practice since
Independence.

"It is essential that electronic voting has the confidence of
the public and

of the participants in elections. The system which the Government intends to use next June is seriously flawed. No democracy should proceed with a new electoral system which opposition Parties fear may lead to election rigging.

"It is essential for continuing confidence in the electoral system that the proposed electronic voting be changed. The Government should suspend plans for the extension of electronic voting until the reforms proposed by the Labour Party have been implemented."

✶ E-ZPass, UPS, and Newark Airport

<Susan Landau <susan.landau@sun.com>>

Mon, 3 Nov 2003 10:16:03 -0400

[This appeared in the Metropolitan Diary section of *The New York Times*,
3 Nov 2003. It is yet another example of what can happen when perfectly plausible actions are combined in unexpected ways. Fortunately this one is humorous. Susan Landau]

Dear Diary:

After moving to Nashville from New York recently, it occurred to me that I no longer had a pressing use for my E-ZPass. Following the E-ZPass instructions, I filled out a few forms and dropped my pass off at United Parcel Service, destination Staten Island service center.

Two weeks passed, and I received my normal E-ZPass e-mail

statement. I entered my account and, lo and behold, my recently surrendered pass had been used by someone to go from Newark Airport to Exit 18 on the New Jersey Turnpike.

I was incensed.

I immediately called E-ZPass and informed them that someone had stolen my pass. I explained that I had mailed the pass and that now someone was running up and down the turnpike using it.

Very calmly, the E-ZPass representative said, "Sir, your E-ZPass was not stolen, it is in the UPS truck, and every time that truck goes through an E-Z Pass toll booth, it is going to register another toll."

Microsoft puts a price on the heads of virus writers

<"NewsScan" <newsscan@newsscan.com>>

Thu, 06 Nov 2003 08:58:12 -0700

Microsoft is using an old-fashioned tactic to fight new-fangled viruses -- it's created a \$5-million Anti-Virus Reward Program and is offering \$250,000 bounties for information leading to the arrest and conviction of the people behind last summer's Blaster worm and Sobig virus. Together, those attacks are blamed for \$2 billion in losses by businesses and consumers, according to consulting firm Computer Economics Inc. Security experts are split on

whether the new initiative will prove successful, but Microsoft senior security strategist Philip Reitingger says, "What we hope to accomplish is to give people an incentive to do the right thing." [*Los Angeles Times*, 6 Nov 2003; NewsScan Daily, 6 Nov 2003]

<http://www.latimes.com/technology/la-fi-bounty6nov06,1,4082881.story?coll=la-headlines-technology>

[The sad part is that for \$5M, MS cannot fix its deeper computer security problems, so that expenditure will not solve their problems. On the other hand, if MS spent \$2B rearchitecting and reimplementing their software, think what might be done! (On the other hand, I recall the period in the 1970s when IBM reportedly spent \$40M on improving its mainframe computer security. The old joke at the time was that they spent \$39M on public relations and \$1M on travel.) PGN]

🔥 Microsoft patches their patched patches (IP)

<Robert Bruce Thompson>

Mon, 03 Nov 2003 11:34:47 -0500

(via Dave Farber's IP, with an addition forward from Mark Luntzel)

For years, the conventional wisdom has been that one can't trust Microsoft software until version 3.0, and that apparently is true for their security patches as well.

The middle of last month, with much fanfare, Microsoft went to their new scheme of releasing patches in batches once a month. A week or so later, they released batches of patches to those batches of patches. Now, they're releasing batches of patches to the batches of patches to the batches of patches.

For details, see:

<<http://www.esecurityplanet.com/prodser/article.php/3101901>>

These batches and batches of patched patched patches are critical, so don't ignore them. And, the way things are going, look for batches and batches of patched patched patched patches sometime next week.

Robert Bruce Thompson <thompson@ttgnet.com>

<http://www.ttgnet.com/thisweek.html> <http://forums.ttgnet.com/ikonboard.cgi>

Remember those jokes about "if AT&T built cars?"

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

Sat, 01 Nov 2003 14:38:40 -0500

... those humorous pieces that point out the ludicrous unusability of computer user interfaces by speculating on what a car with a similar user interface might be like? Well, don't laugh too hard... *The Boston Globe* auto writer Royal Ford just published an article headed: "For drivers,

electronic overload."

The Boston Globe, 1 Nov 2003

"To start the heater or air conditioning in the [a 2-year old Acura] MDX, you start with the dashboard navigation screen, then make your way through a series of baffling electronic menus, through climate control and beyond.... 'It's a distraction while you're driving,' [owner Stuart Schneiderman] said.... The system in the [BMW] 7 Series... remains a landmark in complexity, using a dial between the front seats to reach eight "points" of control. Each point then controls a multilayered system of options that many drivers have found to be like peeling an electronic onion.... the system proved so complicated that Web sites have offered "cheats," hidden shortcuts like those used by video gamers.... the Lexus LS430 [has] one of the most manageable electronic... but the manual for the system runs to 178 pages."

To anyone who's ever had the window of a rental car frost up in traffic, while leaving an airport, with no place to pull over and no companion handy to dig out the owner's manual and locate the right button... the RISKS should be obvious.

Daniel P. B. Smith, dpbsmith@world.std.com alternate:
dpbsmith@alum.mit.edu

⚡ Duh! an electronic signature!

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

Mon, 3 Nov 2003 23:39:07 -0800 (PST)

I just finished submitting a reference letter to the Hertz Foundation for a student. This process is done through a Web form. The foundation requires an electronic signature on the recommendation. The signature is collected by presenting the recommender with a Web page reading something like this:

I certify that I am the person named below:

(type name in box)

Even my wife, who is a musician by profession, reacted with "Oh, yeah, *that's* real secure!"

I suggest that instead, the foundation should simplify my life by simply providing a check box labeled "This recommendation is forged."

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

✶ Paying employees is not rocket science

<Paul Robinson <postmaster@paul.washington.dc.us>>

Tue, 28 Oct 2003 23:31:25 GMT

WBIG radio reported Friday that there was a protest by employees of the Prince George's County [Maryland] School District over payroll problems.

The School District has installed a new computer system and

apparently is unable to generate payroll checks for quite a number of employees including school bus drivers. This is also causing problems with their health insurance as well. Some of the employees report that they have not been paid since the start of the school year. A School District spokesperson reportedly said they are working with Oracle to find where the problem is.

My own comment is that something is really strange here. I used to do payrolls myself, by hand. Generally you do them by computer because it's cheaper than using lots of clerks and because it scales better. But as this article's title noted, payrolls are not some arcane subject, the method to do them is pretty much cut and dried and has been probably since the 1970s or 1980s with the standard accounting rules in effect. The only issue is for the number of employees that the computer system will scale properly.

Let's presume PG county has perhaps 30,000 employees at the school district. If it takes an average of 10 seconds - obviously more than it actually takes - to do all required calculations for each check, such as what deductions, what payments, and how salary is computed, then they need 300,000 seconds to calculate payroll, or roughly about 84 hours. Split this onto 10 PCs and it takes 1 day. Probably 4 hours on a mainframe.

Basically the most labor intensive part of this is keeping the laser printers full of check stock. There's something wrong with the picture

here.

✂ Another victim of the d__n bad-word filter!

<Adam Abrams <adamabrams@shaw.ca>>

Mon, 03 Nov 2003 11:04:59 -0800

I tried to register as a user at collectorcartraderonline.com in order to save a search. Filled out everything, clicked "submit", and got this odd message: "This e-mail address has been flagged as inadmissible and you are unable to place an ad."

This could mean any number of things ranging from benign (I'd already registered and forgotten about it) to downright unsettling (I'm on some secret government hit list). OK, maybe the second one is unlikely, but it was still disturbing...

An e-mail cleared it all up: I'm the latest victim of the "bad word filter".

As they put it: "The reason that you are unable to create an account is due to your e-mail address containing a vulgar word that has been flagged by our bad word table."

I had to call their toll free line to have an actual human sign me up. While on hold, I studied my e-mail address with fresh and suspicious eyes. It's my full name + provider, "adamabrams@shaw(dot)ca". Even before the days of e-mail, I'd never noticed anything even slightly vulgar about my name. Could

it be "bra"? They might have me flagged as a ladies-undergarment fetishist.

"rams"? Maybe the L.A. football team has had an obscenely bad season. No, it was "dam". That's right, even misspelled bad words set off the alarm. So I'm also being punished for other people's illiteracy.

I guess the RISK is mainly that they'll lose customers due to an overzealous data filter that flags letter combinations that appear in many everyday words.

(Turns out the rep entered part of my address incorrectly, but when I logged in to correct my profile, my e-mail triggered the same bad-language flag again! OK... I give up.)

⚡ REVIEW: "High Integrity Software", John Barnes

<Rob Slade <rslade@sprint.ca>>

Mon, 3 Nov 2003 07:08:12 -0800

BKHISTSA.RVW 20030913

"High Integrity Software", John Barnes, 2003, 0-321-13616-0

%A John Barnes

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

%D 2003

%G 0-321-13616-0

%I Addison-Wesley Publishing Co.

%O 416-447-5101 fax: 416-443-0948 800-822-6339 bkexpress@aw.com

%O <http://www.amazon.com/exec/obidos/ASIN/0321136160/>

robsladesinterne

<http://www.amazon.co.uk/exec/obidos/ASIN/0321136160/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0321136160/>

[robsladesin03-20](#)

%P 430 p. + CD-ROM

%T "High Integrity Software: The SPARK Approach to Safety and Security"

Once upon a time, a group set out to build a language which would allow you to write programs that could be formally verified. Formal analysis and proof can be used to determine that a program will work the way you want it to, and not do something very weird (usually at an inopportune time). First came the attempt to build the Southampton Program Analysis Development Environment (or SPADE) using a subset of the Pascal programming language. When it was determined that Pascal wasn't really suitable, research was directed to Ada, and the SPADE Ada Kernel, or (with a little poetic licence) SPARK, was the result.

SPARK can be considered both a subset and extension to Ada, but is best seen as a separate language in its own right. SPARK forbids language structures such as the infamous GOTO statement of Fortran and BASIC (which cannot be formally verified). Support for some object-oriented features has been included in SPARK, but not for aspects like polymorphism which would make formal proof problematic. A great deal of the security of SPARK lies in the idea of contracts and the use of data specifications (usually referred to as interfaces) that prevent problems such as the unfortunately all-too-ubiquitous buffer overflow.

Part one is an overview of the background and features of

SPARK. Chapter

one reviews some of the problems of unproven software, and the major

components of SPARK. Support for the formal proof functions, such as

abstraction (the elimination of details not essential to the fundamental

operation of the concept or function) are discussed in chapter two. The

various analysis tools are listed in chapter three.

Part two outlines the SPARK language itself. Chapter four describes the

structure of SPARK and the lexical items it contains. Language elements are

covered in chapters five, six, and seven, successively dealing with the type

model and operators, control and data flow, and packages and visibility

(local, global, etc.) which also reviews the object-oriented aspects of

SPARK. Interfacing of the various parts of SPARK, and also of SPARK and

other languages, is in chapter eight.

Part three looks at the various analytical utilities in SPARK and the proof

process. Chapter nine concentrates on the main Examiner tool. A mathematical discussion of data flow analysis, in chapter ten, is not

necessary to the operation of SPARK, but provides background and explanation. Verification, and the instruments that support it, are

reviewed in chapter eleven. Chapter twelve examines the rather vague

practice of design, and proposes the INFORMED (INformation Flow Oriented

METHOD of Design) process, although it seems to be limited to some

admittedly useful principles. A list of similar precepts makes up the

eponymous programming "Techniques" of chapter thirteen. Chapter fourteen

retails a number of case studies of the possible use of SPARK for various applications: the simpler ones also contain source code.

Both the writing in the book, and the explanations of SPARK, are clear.

Formal methods of architecture and programming are not well understood, and

this text does provide some justification for the exercise, although more

evidence and support would be welcome. I recommend this work not only to

those interested in more secure applications development, but also to those

needing more information about formal methods in composition and system

architecture.

copyright Robert M. Slade, 2003 BKHISTSA.RVW 20030913
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu

victoria.tc.ca/techrev/mnbksc.htm sun.soci.niu.edu/~rslade/
secgloss.htm



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 2

Weds 12 November 2003

Contents

- [Eurofighter Typhoon brake fault](#)
[Peter B. Ladkin](#)
- [Computers in cars: "When you add complexity you add risks"](#)
[NewsScan](#)
- [Mail-order price-listing typo cost company over \\$2 million](#)
[Chiaki Ishikawa](#)
- [New election to be held due to technical glitch](#)
[Kim Alexander](#)
- [Vanishing votes; wireless security experts](#)
[Rebecca Mercuri](#)
- [Fairfax County electronic voting: the saga continues](#)
[Jeremy Epstein](#)
- [Thwarted Linux backdoor](#)
[Douglas W. Jones](#)
- [Talk of wiretaps rattles Hollywood](#)
[Bernard Weinraub via Monty Solomon](#)
- [Update: Fun with stolen credit-card numbers](#)
[Jonathan Kamens](#)
- [Re: SPARK Ada in "High Integrity Software"](#)
[Peter B. Ladkin](#)

- [Re: goto in Slade's review of "High Integrity Software"](#)
[Martin Cohen](#) [Andrew Dalke](#)
 - [Marcus Ranum: The Myth of Homeland Security](#)
[PGN](#)
 - [REVIEW: "The GSEC Prep Guide", Mike Chapple](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ Eurofighter Typhoon brake fault

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Wed, 12 Nov 2003 10:08:58 +0100

Flight International reported a braking problem occurring on a Eurofighter Typhoon aircraft on 9 Oct 2003 that led to the suspension of all flights (*Flight International*, 21-27 October 2003, p4, article by Julian Moxon). A cockpit warning light came on during landing, the pilot deployed the braking parachute, but the brakes could be used to bring the aircraft to a halt.

The furlough lasted three weeks, and the aircraft were to return to flight operations last week. Apparently 15 days have been lost from the flight test program. The braking problem centered on a faulty microchip in the landing gear computer (*Flight International*, 4-10 Nov 2003, p6).

Peter B. Ladkin, University of Bielefeld, Germany
<http://www.rvs.uni-bielefeld.de>

Computers in cars: "When you add complexity you add risks"

<"NewsScan" <newsscan@newsscan.com>>

Wed, 12 Nov 2003 07:35:15 -0700

The computer systems in today's luxury cars are wonderful when they work right, but not so wonderful when something goes wrong. Donald Buffamanti of AutoSpies.com (self-described as "the ultimate insider guide to the world's best automobiles") says of one automaker's cars: "People have reported total electronic shutdowns to us attributed to the network in the 7-series." One luxury car owner, whose onboard computer gave monitoring information that sent him off to the service station every few days to check his tire pressure, complains: "Why does it have a computer that reads the problems if they can't fix them?" Responding to complaints such as these, a BMW executive says: "There is a not-uncommon shakedown period of one to two years with technology this new," and a Honda executive admits: "When you're adding complexity, you are adding risks." The BMW exec adds: "The good news is that if it's working right after four years, it will continue to work for a long time after that. Electronics have a much longer life than mechanical parts." [**USA Today**, 11 Nov 2003; NewsScan Daily, 12 Nov 2003] http://www.usatoday.com/tech/news/2003-11-11-carrepairs_x.htm

[See [RISKS-22.02,03,73,74](#) for other recent items on the 7-Series.

Interesting statement that if it works for four years, it will continue

to do so; RISKS readers are familiar with various reasons why

this might
not be true. PGN]

✦ Mail-order price-listing typo cost company over \$2 million

<Chiaki Ishikawa <ishikawa@yk.rim.or.jp>>

Tue, 11 Nov 2003 09:08:21 +0900

It is widely reported in the Japanese press that a mail order web page's typo cost a company more than two million dollars.

One "0" was missing from the price of a PC sold by Marubeni, a large trading company's mail order web site. Before the error was caught, about one thousand people ordered 15 hundred units. (The real price was 198, 000 Japanese Yen. It was listed initially as 19, 800 Yen.)

After the error was spotted, and trying to cancel the selling contract with many customers had strong resistance from the said buyers and failed, the company decided to bite the bullet and announced that it would sell the PC at the incorrect list price to the customers who ordered the PC in order to "keep its trust among the customers" or whatever.

I read that a lawyer offered a comment that in Japanese law a notion of "clear misunderstanding nullifying a contract" (not sure what the right English translation is.) exists, and so the contract to sell the goods (which was deemed as being established by the automatic response sent to the buyer after the order at the web site was submitted) can be

scrapped due to
this principle in court.

However, Marubeni obviously decided to honour the contract to
protect its
name.

Another commented in a newspaper article that mail order
companies should be
aware of anomalies such as sudden surge of orders on one product
to spot
this kind of error. (Intriguing problem. This is similar to
input
validation problem and no amount of "intelligence" would be
enough to
eliminate such errors, but a common sense check that puts a
lower limit on
the price of a category of product, say, of PC, printer, etc.
could have
caught this particular case.)

⚡ New election to be held due to technical glitch

<Kim Alexander <kimalex@calvoter.org>>

Tue, 11 Nov 2003 12:12:28 -0800

A revote will be held in Grant Parish, Louisiana after a
candidate, Barney
Durand contested the results after being told he lost the race
for police
jury. He was running against an incumbent, Julius Scott, who
was reported
to have won the race by an 8-vote margin. Turns out one of the
election
technicians had doubled either some or all of the absentee count
(it's not
clear which is the case), adding an additional 20 votes, five
for Durand and

15 for Scott.

The new count showed Durand won the election by only a few votes. I phoned Mr. Durand last week. He told me that the Secretary of State agreed he had won the election, but the losing candidate filed a lawsuit that resulted in a judge ordering the revote to take place.

[http://www.nola.com/newsflash/louisiana/index.ssf
?/base/news-5/1066890841145171.xml](http://www.nola.com/newsflash/louisiana/index.ssf?/base/news-5/1066890841145171.xml)

[Vanishing votes; wireless security experts \(Re: Epstein, RISKS-23.01\)](#)

<"Rebecca Mercuri" <notable@mindspring.com>>

Sat, 08 Nov 2003 14:47:38 -0500

As a follow-up to Jeremy Epstein's posting in [RISKS-23.01](#), it seems that the WinVote machines also had the mysterious capability of subtracting around one in every hundred votes for a particular Republican candidate. This was confirmed by post-election testing (when county officials examined one of the machines after complaints were filed by voters in three different precincts). The Washington Post reported Thursday that for School Board candidate Rita S. Thompson "the machines initially displayed an "x" next to her name but then, after a few seconds, the "x" disappeared." The fact that these votes may not have been recorded on the (so-called) audit trail created internally on the machines underscores the need for

voter verified
paper ballots in electronic voting systems.

I would like to bring readers' attention to the fact that the current IEEE voting system draft allows for wireless (and other transmission) technology to be used with precinct electronic balloting systems. We need some individuals with the ability to provide a detailed explanation of security issues with wireless to assist with the current debate on this subject. Anyone who has technical expertise in this area should contact me immediately at: mercuri@acm.org

✶ Fairfax County electronic voting: the saga continues

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Tue, 11 Nov 2003 09:59:33 -0800

As I reported in [RISKS-23.01](#), the Fairfax County (Virginia) election last week, which used new electronic WinVote systems, was marred by problems. It seems that some of them are more serious than I noted previously.

The Washington Post reports that in one local race, "Voters in three precincts reported that when they attempted to vote for [a local candidate], the machines initially displayed an 'x' next to her name but then, after a few seconds, the 'x' disappeared." The "county officials tested one of the machines in question yesterday and discovered that it seemed to subtract a vote for [the candidate] in about 'one out of a hundred tries,'

said

Margaret K. Luca, secretary of the county Board of Elections."
[Incidentally, this is the same county official who told me in writing that the "Electoral Board is taking every step to ensure a secure and successful election...".]

If we assume that the one in a hundred number is accurate, the fact that the election was decided by a margin of about 1% should leave everyone a bit nervous. The real problem is now that they're trying to "inspect" the voting logs to see what happened. But as we all know, the voting logs, being electronic, may not represent anything at all.

Last night I had a discussion with someone in a position of knowledge, who told me that this "1% vote" problem is of more concern to the county staff than the eight failed machines I referenced in [RISKS-23.01](#). In the case of those failed machines, the county staff is confident that they know what went wrong, and they understand what the vote totals should have been. [Not that their confidence gives me much confidence!] However, for the 1% vote problem, the county staff apparently don't know what caused the problem. And that makes them, and me, that much more nervous.

As a co-worker called it, this is "electronic hanging chad".

<http://www.washingtonpost.com/wp-dyn/articles/A6291-2003Nov5.html>

⚡ Thwarted Linux backdoor

<"Douglas W. Jones" <jones@cs.uiowa.edu>>

Tue, 11 Nov 2003 09:21:16 -0600

On 5 Nov 2003, an attempt to insert a very cleverly crafted backdoor into Linux was averted. This is a really good example of the subtle kinds of hacks a source code examiner must be waiting to catch if we want genuinely secure voting systems under the current model of proprietary DRE systems with a closed-door source code examination.

Someone broke into a server at kernel.kbits.net and inserted the following code into the Linux kernel:

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
    retval = -EINVAL;
```

This was done in the code `sys_wait4()`. Larry McVoy caught the fact that the change had been made, and was annoyed because it wasn't logged properly.

Matthew Dharm asked "Out of curiosity, what were the changed lines." Zwane Mwaikambo responded "That looks odd", and Andries Brouwer responded "Not if you hope to get root."

So, an annoying violation of the software change logging requirements turned out to be an attempt to install a backdoor in Linux. At least two very experienced programmers looked at it and saw just slightly odd code, before the serious nature of the threat was actually discovered.

This particular attack, by the way, is ruled out by the current voting system standards, not because they require a comprehensive security

analysis, but because of their C-centered coding rules. Embedded assignment is forbidden. Current source code checks are good at finding embedded assignments and flagging them (as long as the code is written in C). No doubt, a hacker of the sophistication suggested by the attack illustrated above would strictly adhere to the coding guidelines in formulating their attack.

For the complete story of this attack on Linux, including the actual E-mail exchange documenting the discovery of the attack, see:

<http://kerneltrap.org/node/view/1584>

Linux: Kernel "Back Door" Attempt

This attack has only made the mainstream media in one place, so far:

<http://www.smh.com.au/articles/2003/11/07/1068013371170.html>

Bid to backdoor Linux kernel detected - smh.com.au

This is a pity, because I think this story is really important.

⚡ Talk of wiretaps rattles Hollywood

<Monty Solomon <monty@roscom.com>>

Tue, 11 Nov 2003 04:12:35 -0500

[Source: Bernard Weinraub, *The New York Times*, 11 Nov 2003; PGN-ed]

<http://www.nytimes.com/2003/11/11/business/media/11wire.html>

The case began with a dead fish and a rose in an aluminum pan, left on the

hood of a car parked on a Los Angeles street. Taped to the windshield of the car, which belonged to a reporter for the *Los Angeles Times*, was a piece of cardboard with a single word: "Stop." The discovery in June 2002 -- for which an ex-convict was later arrested -- unleashed a chain of events that has suddenly entwined many of the Hollywood elite and threatens to turn into the kind of scandal that the show business world has not faced in decades. Managers, actors, businessmen and lawyers are being questioned, and in some cases subpoenaed, by the federal government in a widening grand jury investigation of suspected illegal wiretapping that has moved beyond Los Angeles to New York, according to entertainers, producers, lawyers and others involved in the inquiry.

This involves Anthony Pellicano, a private investigator for numerous Hollywood celebrities. An FBI raid netted many transcripts of taps.

✶ Update: Fun with stolen credit-card numbers ([RISKS-22.93](#))

<Jonathan Kamens <jik@kamens.brookline.ma.us>>
Sun, 26 Oct 2003 21:29:57 -0500

RISKS readers might appreciate the following update to my experience with the theft of my AmEx card number....

Over a month after I canceled the stolen number and got a new one, two charges

I did not make from America On-Line showed up on my statement.

According to AOL, my number was used to open two AOL accounts, but by the time AOL tried to bill the number, I had canceled it. AmEx's policy for this situation is not what you would expect, i.e., to reject a charge to a number canceled due to fraud, but rather TO TRANSMIT THE NEW NUMBER TO THE MERCHANT. Yes, that's right, AmEx gave AOL my replacement card number, and AOL turned around and rebilled me using the new number. According to AOL, other card issuers handle this situation more sanely, but AmEx is "notorious" about correcting card numbers for merchants when they shouldn't.

AOL assured me that once a number has entered their system, users can't see it, so even after AmEx sent the new number to AOL, whoever opened the accounts would not have been able to use them to find out my new number.

AmEx denied that they would ever transmit a replacement number to a merchant. However, their denial is not credible, because:

- * AmEx confirmed that the charges from AOL were made using my new card number;
- * The AOL accounts were opened before my replacement number was issued, so it's impossible that they could have been opened using the replacement number; and
- * AOL told me exactly when they billed AmEx with the old number, when AmEx sent them the new one, and when they rebilled successfully using it.

I told the AmEx rep. that since he and AOL were giving me different stories, I wanted him to call AOL and figure out the truth. He said only the AmEx "fraud department" could do that, but he could hand the matter over to the fraud department only by initiating a fraud dispute and canceling my new number. I refused to allow him to do this, because I did not believe my new number had been compromised, and I did not intend to waste more time changing all of my recurring transactions to a new number twice in two months. He said there was no way I could speak to the fraud department directly. I finally got him to give me a U.S. Mail address which I could use to write to them.

Needless to say, I have written them a rather strongly worded letter demanding a credible explanation for how AOL got my new card number. It'll have to be a very good explanation indeed to convince me not to take my business elsewhere.

As if all this weren't bad enough, AOL gave me one more piece of very disconcerting information. One of the AOL accounts was opened using my name, and the other was opened using MY FIVE-YEAR-OLD DAUGHTER'S NAME. This elevates the situation from a simple stolen credit-card number to something potentially much more serious (and scary). Therefore, I'll be spending tomorrow making phone calls to various law-enforcement agencies trying to find someone willing to initiate an investigation. I am pessimistic about my chances of success.

✈ Re: SPARK Ada in "High Integrity Software" (Slade, [RISKS-23.01](#))

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

Wed, 12 Nov 2003 10:40:24 +0100

I should like to add a few comments to Rob Slade's generally positive review of John Barnes's book on SPARK Ada in [RISKS-23.01](#).

The main characteristics of the SPARK Ada language is that it is an unambiguous subset of Ada with a rigorous semantics. I understand that its developers felt that such characteristics were minimal necessary for guaranteeing the behavior of compiled code. "Unambiguous" means that all compilers compile source to object code which behaves exactly the same with respect to the program variables as other object code compiled from the same source, and it is necessary to achieve this that the semantics of the subset be precise.

They also chose the subset to be as far as possible amenable to static analysis, partly through use of code annotation. The goal was, as I understand it, to ensure that the behavior of all programs written in the language would be completely predictable, not just in theory, but also in practice. SPARK Examiner is the static analysis tool which comes with SPARK Ada.

Proponents of SPARK Ada argue that these properties are necessary in languages used for the development of critical systems, and I am inclined to accept such arguments.

SPARK Ada has achieved measurable success in the development of avionics software by Lockheed Martin for their C130J new-generation Hercules transport aircraft, which has been bought by the UK military. UK military procurement regulations make requirements on development methods which are likely most easily met through methods involving the use of programming languages with SPARK Ada's characteristics. There is a collection of papers on SPARK Ada and its use at www.sparkada.com

If one needs a language with the characteristics mentioned above -- and who doesn't, even for non-critical systems? -- then SPARK Ada is the most experienced game in town. (There are other tools, such as Perfect Developer from Escher Technologies, also a UK company, which claim identical or similar properties, are younger, therefore less tried, but likely also worth a look.)

Barnes's book is *the* book on SPARK Ada. It was first published in 1997 and Slade reviewed the recently-published Second Edition.

I have no connection with Praxis Critical Systems, the provider of SPARK Ada, other than that of general admiration for their sterling work.

Peter B. Ladkin, University of Bielefeld, Germany
<http://www.rvs.uni-bielefeld.de>

Re: goto in Slade's review of "High Integrity Software" ([RISKS-23.01](#))

<Martin Cohen <mjcohen@acm.org>>

Sun, 09 Nov 2003 11:19:37 -0800

In Rob Slade's review of "High Integrity Software" in [RISKS-23.01](#), he says that

"SPARK forbids language structures such as the infamous GOTO statement of

Fortran and BASIC (which cannot be formally verified)."

To the contrary (as I learned back in the 1970's), the semantics of gotos and labels are quite simple: At any label, the conditions that hold there are the union of the conditions that hold at all the gotos that have the label as their destination together with the conditions that hold at the end of the statement preceding the label. The conditions that hold (textually) following a goto are null (i.e., nothing is true, since you can't get there).

I remember when I first read this and thought "Of course!" It's the kind of thing that is obvious after seeing it, but not obvious to come up with it. I do not know who first thought of this, but I admire their clear thinking.

✶ Re: goto in Slade's review of "High Integrity Software" ([RISKS-23.01](#))

<"Andrew Dalke" <adalke@mindspring.com>>
 Sat, 8 Nov 2003 00:08:43 -0700

A GOTO can be emulated with a loop and a set of if statements. Reaching back into my now rusty BASIC, the following

```
10 PRINT "What is your name?",
20 A$ = INPUT$( )
30 IF A$ = "END" THEN GOTO 60
40 PRINT "Hello, ", A$
50 GOTO 10
60 PRINT "Okay, bye-bye!"
70 END
```

can be translated into inefficient (and untested) Python as

```
line_number = 1
while line_number < 100:
    if line_number == 10:
        print "What is your name?",
    elif line_number == 20:
        a = raw_input("")
    elif line_number == 30:
        if a == "END":
            line_number = 60
    elif line_number == 40:
        print "Hello,", a
    elif line_number == 50:
        line_number = 10
    elif line_number == 60:
        print "Okay, bye-bye!"
    elif line_number == 70:
        break
    else:
        line_number = line_number + 1
```

Or does SPARK also forbid combining loops and if statements because there is

no way to formally verify them?

✦ Marcus Ranum: The Myth of Homeland Security

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

Mon, 10 Nov 2003 12:32:50 PST

Marcus Ranum
The Myth of Homeland Security
Wiley, 2004
xviii+244

This book could not be more timely or more relevant. It is extraordinarily important for all RISKS readers, as it reinforces so many themes that we have discussed here, including the reality that many critical problems (especially low-tech threats) do not necessarily have technologically based solutions (especially high-tech fixes). Common sense abounds, along with a lot of very practical insights.

The front jacket flap tells it like it is:

"Writing with anger, honesty, and true patriotism, Ranum reveals the truth about 'feel-good' security policies and boondoggle spending programs that mask the real threats and do nothing tangible to improve public safety."

This book has huge platters of food for thought. Intellectually, you won't go hungry reading it, and there is much on which to chew. However, if the book leaves a bad taste in your mouth, it is not Marcus Ranum's fault. He

is simply and compellingly telling it like it is, and we all need to listen.

[Despite the publication date of 2004, the book is out now. PGN]

🔥 REVIEW: "The GSEC Prep Guide", Mike Chapple

<Rob Slade <rslade@sprint.ca>>
Mon, 10 Nov 2003 07:46:26 -0800

BKGSECPG.RVW 20030918

"The GSEC Prep Guide", Mike Chapple, 2003, 0-7645-3932-9,
U\$60.00/C\$90.99/UK#41.95

%A Mike Chapple

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2003

%G 0-7645-3932-9

%I John Wiley & Sons, Inc.

%O U\$60.00/C\$90.99/UK#41.95 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0764539329/>

robsladesinterne

<http://www.amazon.co.uk/exec/obidos/ASIN/0764539329/>

robsladesinte-21

%O <http://www.amazon.ca/exec/obidos/ASIN/0764539329/>

robsladesin03-20

%P 448 p. + CD-ROM

%T "The GSEC Prep Guide: Mastering SANS GIAC Security Essentials"

The SANS (System administrators, Audit, Network, Security) Institute

GIAC (Global Information Assurance Certification) Security Essentials

Certification (GSEC) is supposed to be the "core" program for the various GIAC courses and exams.

Chapter one covers some basic, but random, security concepts and topics. A list of sample questions, intended to help the student/candidate prepare for the GSEC exam, is given at the end of every chapter. If these truly represent the level and type of questions on the exam then getting the GSEC is a snap: quick, which type of situation is worse, one that has low threat and low vulnerability or high threat and high vulnerability? (On the other hand, you may have to know the party line: one question insists that you credit SANS with the concept of defence in depth, and there is a concept of "separation of privilege" that seems to be what everyone else refers to as separation of duties.) Security policies are discussed in a verbose but almost "content-free" manner in chapter two. Virtually nothing is said about the policy process and different functional types of policies. Again, there is a demand for idiosyncratic jargon: high level policies are "program" policies, whereas detailed policies (mostly procedural, given the list discussed) are "issue-specific." One term that might be worth adopting is "system-specific policy": those who deal with policies know that it is difficult to have exceptions documented. Using this term for deviations, as SANS does, may reduce the resistance to noting the irregularities. There are some basic ideas about risk assessment and management in chapter three, but most of the text reviews network scanning tools. Chapter four contains network nomenclature, Cisco equipment filtering command arguments, and miscellaneous IP (Internet Protocol) protocols in varying depth. There are a brief list of the titular "Incident Handling" factors contained in chapter five, as well

as random legal terms. The discussion of cryptography in chapter six is reasonable up to the point of symmetric block ciphers, but subsequent material has errors (keystream data should *not* repeat during the course of a message), confusing diagrams, and unhelpful mathematics. There is no deliberation about the usage of public key cryptography, hashes, and digests until chapter seven, which, despite the title, has absolutely nothing to say about "Applications Security." Chapter eight provides a simple overview of firewalls and intrusion detection systems (IDSs) but is not overly detailed: no distinction is made between application and circuit-level proxies, and some of the statements made are clearly incorrect for circuit devices. There is a grab bag of malware, cryptanalysis, attack methods and more in chapter nine. The content on operations security is limited to assorted aspects and tools of Windows and UNIX that might be related to secure processing, in chapters ten and eleven respectively. Chapter twelve is a practice exam. It's pretty easy.

The GSEC is sometimes said to be adequate preparation for the CISSP (Certified Information Systems Security Professional) exam, but there are significant gaps in GSEC's coverage of the security topic. Although risk assessment and policy are discussed, management issues and access controls get limited substance in GSEC. Security architecture, applications security, physical security, and business continuity are all missing, while operations are restricted to Windows and UNIX.

This book does provide some useful direction in regard to

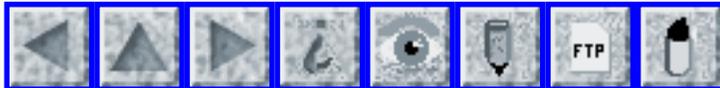
information

systems security, but readers should be warned that the missing pieces will probably be very important at some point.

copyright Robert M. Slade, 2003 BKGSECPG.RVW 20030918
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu

Computer Security Day, November 30 <http://www.computersecurityday.com/>

victoria.tc.ca/techrev/mnbksc.htm sun.soci.niu.edu/~rslade/secgloss.htm



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 3

Friday 14 November 2003

Contents

- [Whirled-Wide Web](#)
[Bertrand Meyer](#)
- [TAB operator error in punter's favour](#)
[David Shaw](#)
- [Astonishing electronic voting "glitch"](#)
[Steve Summit](#)
- [The computer is ALWAYS right](#)
[Charles Lamb](#)
- [Re: California halts e-vote certification](#)
[David E. Ross](#)
- [More on Diebold installing uncertified software in California](#)
[PGN](#)
- [Re: A new risk for electronic voting](#)
[Steven M. Bellovin](#)
- [Report raises more questions about voting machines](#)
[EPIC](#)
- [Belkin: Another protocol-violation-to-sell-products risk](#)
[Tim Bradshaw](#)
- [New definition of "Fish 'N Chips"](#)
[Jim Schindler](#)

- [Minnesota CriMNet shutdown](#)
[Steven Hauser](#)
 - [FBI's reach into records is set to grow](#)
[Monty Solomon](#)
 - [High-tech microscopes expose Americans' private lives](#)
[Monty Solomon](#)
 - [A heavily used RISKY website: France Telecom](#)
[Peter Kaiser](#)
 - [Holes found in online job search privacy](#)
[Brian Berstein via Monty Solomon](#)
 - [Security patching: a story from the trenches](#)
[Rex Black](#)
 - [Bank scam with spaces in trick URL](#)
[Mark Brader](#)
 - [Computers in cars: "When you add complexity you add risks"](#)
[Richard I Cook](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Whirled-Wide Web

<Bertrand Meyer <Bertrand.Meyer@inf.ethz.ch>>

Sun, 09 Nov 2003 11:50:46 +0100

Source: Le Monde, 30 October 2003,

<http://www.lemonde.fr/txt/article/0,1-0@2-3228,36-340095,0.html>

Spiders are not new to the RISKS bestiary (see [18.46](#) and [18.58](#)) but I don't recall seeing this particular issue. On 28 Oct 2003, the local listeners of two national radio stations were surprised to hear that it was snowing in Dinard. That's a town in Brittany, which has a mild oceanic climate; snow in October would be exceptional. The error, corrected after half an hour,

was due to early-morning frost on the web woven by a spider on one of the weather station's sensors. "The computer" interpreted frost as snow, enabling the regional management of Meteo France to claim that the sensor functioned correctly. (It did detect the frost!) They added that that the system has been working "perfectly" since its installation, to the great satisfaction of its users.

Before that system was put in place, the airport employed three people to gather weather data. They have now been replaced by sensors. The resulting information, collected 24x7, is updated every 30 minutes and made publicly available, in particular for pilots.

Daytime weather reports are checked by a human, but not those issued at night.

Bertrand Meyer, ETH, Zurich <http://se.inf.ethz.ch>
Eiffel Software, Santa Barbara <http://www.eiffel.com>

[Subject line PGN-spun]

⚡ TAB operator error in punter's favour

<David Shaw <dshaw@avaya.com>>
Fri, 14 Nov 2003 16:42:09 +1100

A punter [US: gambler] collected AUD\$2.6 million after a TAB operator incorrectly entered his trifecta bet on the 2003 Melbourne Cup, Australia's most prestigious horse-race. It seems this system offers the

punter the choice as to whether their bets are read back to them. He phoned in a \$6 trifecta 20 times for the winning combination of the Melbourne Cup. However, the TAB operator mistakenly entered the bet 203 times, resulting in the huge windfall. He had elected not to have the bets read back and was unaware of the error at the time. On discovering the windfall in his bank account, he called the TAB, expecting this to have been a mistake. The TAB rules state that if you do not have your bets read back to you, you are forced to honor the bet, win or lose. So, he was forced to accept the winnings! Quite a remarkable tale! [PGN-ed]

⚡ Astonishing electronic voting "glitch"

<Steve Summit <scs@eskimo.com>>

Wed, 12 Nov 2003 12:42:51 -0500

The *Indianapolis Star*

<http://www.indystar.com/articles/6/091021-1006-009.html>

reported on the latest case of anomalous e-voting results. Last Tuesday's

Boone County election, using MicroVote software returned about 144,000

votes, with only 19,000 registered voters. After further review, the 5,352

votes were claimed to have been recorded. With yet another mistake, does

anyone still trust closed-source electronic voting? [PGN-ed]

[<http://yro.slashdot.org/article.pl?sid=03/11/12/1320208>

It's interesting to wonder what might have happened if the

initial

inaccurate result had not been so glaringly obvious ...

⚡ The computer is ALWAYS right

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

Thu, 13 Nov 2003 01:06:52 -0500

According to an article in the Newark NJ **Star-Ledger**, the town of Southington, CT was testing the Avante International Vote-Trakker machine in an actual election. It had a special feature which displays a printout of the cast vote for voter confirmation. This feature was nullified by the registrar who refused to do anything about a voter's claim her confirmation printout didn't match her vote.

<http://www.nj.com/search/index.ssf>

[?/base/news-11/1068444794272720.xml?starledger?ntop](http://www.nj.com/base/news-11/1068444794272720.xml?starledger?ntop)

⚡ Re: California halts e-vote certification

<"David E. Ross" <david@rossde.com>>

Sat, 08 Nov 2003 17:03:56 -0800

While the reported problem in Alameda County was that uncertified software was loaded into the voting terminals, this is really far more serious. The security of Diebold's touch-screen voting system is so weak that someone outside of Alameda County's election office (someone working for

Diebold)

had access to make unauthorized changes to the vote-counting software.

David E. Ross <<http://www.rossde.com/>>

More on Diebold installing uncertified software in California

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

Thu, 13 Nov 2003 12:13:54 PST

The *Los Angeles Times* today has an article relating to Diebold's Accuvote touchscreen voting machines, by Allison Hoffman and Tim Reiterman, entitled "Secretary of State Orders Audit of All Counties' Voting Systems: Review of upgraded touchscreen software leads to discovery that two registrars installed it without state's OK." Los Angeles Registrar Conny McCormack is quoted as saying, "All of us have made changes to our software -- even major changes -- and none of us have gone back to the secretary of state. But it was no secret we've been doing this all along. [Secretary of State Kevin Shelley] knew we were making changes."

<http://www.latimes.com/news/local/la-me-voting13nov13,1,531224.story?coll=la-headlines-california>

Shelley's news release announcing the investigation is online at http://www.ss.ca.gov/executive/press_releases/2003/03_100.pdf

It must be noted (by PGN) that the Federal Election Commission standards

against which these systems have been certified are so weak that all sorts of serious problems can remain despite certification. But patching is apparently commonplace AFTER certification. In some cases, the software actually has to be CHANGED to accommodate each different ballot face, and think of what Trojan horses might be able to sneak in as a result of that!

⚡ Re: A new risk for electronic voting

<"Steven M. Bellovin" <smb@research.att.com>>
Sat, 08 Nov 2003 15:32:10 -0500

It's worth remembering that mechanical voting machines have their own risks. The "programming" of the traditional lever machines still used in New York is an arcane art, and in some ways less susceptible to auditing than electronic machines -- each machine is set up individually, so every machine is in some sense configured independently. The write-in mechanisms are, to say the least, arcane, and it's very hard for election officials to read votes scrawled in a too-small space, with a blunt pencil, written at an improbable angle. (In my town a few years ago, there was a massive (and successful) write-in campaign a few years ago, when it was discovered that only three candidates were running for the three vacant seats on the school board and one of the three was from a seriously fringe party.)

Me -- I avoided my county's touch screen machines by voting

absentee -- I

was out of down last Tuesday, which let me qualify for a mark sense ballot.

Of course, I have no idea if it was actually readable, since there was no check machine in the county clerk's office...

Report raises more questions about voting machines

<EPIC Info <info@epic.org>>

Thu, 13 Nov 2003 17:20:30 -0500

(From EPIC Alert 10.23:)

The Congressional Research Service (CRS) of the Library of Congress has presented to Congress a report entitled, "Election Reform and Electronic Voting Systems: Analysis of Security Issues." The report was written in response to rising concern and questions regarding new electronic voting systems after recent allegations that these systems use software that is subject to alarming security vulnerabilities. The report analyzes the controversy surrounding direct recording electronic (DRE) voting machines - the first fully computerized voting system - while putting it in the larger context of election practices and voting machine development. It details the types of threats and vulnerabilities that could jeopardize the voting process, as well as the specific complaints broached by security experts.

While the CRS took pains not to take a position in the debate,

it does recognize that recent analysis demonstrates the existence of security flaws in DREs, which are cause for concern. As the report states, "at least some current DREs clearly exhibit security vulnerabilities. Those vulnerabilities pose potential ... risks to the integrity of elections." It goes on to list a number of different proposals being advocated to address these vulnerabilities, including ensuring that security protocols are followed, improving the standards and certification process for voting machines, use of open source computer code, and improvements in verifiability and transparency. The last point is one that computer scientists and voting activists have been pushing for, specifically by requiring voter-verifiable paper print-outs of vote selection for voters to review. The CRS stops short of issuing any recommendations, but does indicate that further investigation and action should be taken regarding this matter.

The CRS Report on electronic voting is available at:

<http://www.epic.org/privacy/voting/crsreport.pdf>

For background information, see EPIC's Voting page at:

<http://www.epic.org/privacy/voting>

⚡ Belkin: Another protocol-violation-to-sell-products risk

<Tim Bradshaw <tfb@cley.com>>

Wed, 12 Nov 2003 13:33:42 +0000

The Register (<http://www.theregister.co.uk/content/69/33858>).

[html](#)) has been reporting a Belkin wireless router which, once every 8 hours, picks an HTTP request and redirects it to a web page advertising Belkin's parental-control system. Belkin seem to have now (<http://www.theregister.co.uk/content/6/33918.html>) promised a firmware upgrade which disables this feature. How many people will install it is another question.

Other than the obvious offensiveness of this kind of thing, there are horrible dangers involved. I could be half way through some transaction over the web, and have my *router* unilaterally, decide to redirect my requests somewhere else. Worse, a *program* could be doing it, and it might not even spot that something odd had happened. Any cache this side of the router will get randomly poisoned, and so on. This is just a stupid, dangerous thing to do.

Together with the recent Verisign `Site Finder' service reported in [RISKS-22.91](#), this seems to be the beginning of something new and, I think, worrying: important protocols (such as routing or DNS) are being usurped to sell advertising. Both of the cases mentioned here are sufficiently clumsy that they're likely to have hurt the usurper more than the users of these protocols, but I suspect things will be more subtle and insidious in due course. There's nothing wrong with advertising as such, but if it results in an infrastructure where no one can trust anything to actually work the way it is meant to, I think there's a significant problem.

🔥 New definition of "Fish 'N Chips"

<Jim Schindler <Jimschin@pacbell.net>>

Wed, 12 Nov 2003 22:56:36 -0800

Chips in Fish Help Net Australian Cod Poachers, 6 Nov 2003

<http://story.news.yahoo.com/news>

[?tmpl=story&cid=1516&ncid=1516&e=5&u=](http://story.news.yahoo.com/news?tmpl=story&cid=1516&ncid=1516&e=5&u=)

[/afp/20031106/od_afp/australia_fish_offbeat_031106194455](http://story.news.yahoo.com/news?tmpl=story&cid=1516&ncid=1516&e=5&u=/afp/20031106/od_afp/australia_fish_offbeat_031106194455)

Australian fisheries investigators have wrapped up [with fish wrap?] an illegal poaching operation after inserting microchips into fish then tracking them to the culprits' freezer, officials said. Victoria state Fisheries Minister Bob Cameron said the hi-tech sting began when officers in his department found an illegal fishing net in a creek in the state's northwest. The officers inserted microchips under the skin of the golden perch and murray cod caught in the net then returned them and waited for the poachers to turn up. The fish had disappeared a day later and when officers stopped the poachers' vehicle they could find no trace of the animals. However, a subsequent search of their home uncovered fillets in the freezer, complete with microchips still emitting signals to the fisheries officers' tracking devices. [...]

[Thus restoring cod peace to its perch in the "inter" net?
PGN]

✶ Minnesota CriMNet shutdown

<Steven Hauser <hause011@tc.umn.edu>>

Sat, 8 Nov 2003 12:00:24 -0600 (CST)

Minnesota has a large database of millions of records of police activity and incident data compiled on its citizens. The data is not owned by the government but an extra-legal private entity, the Minnesota Chiefs of Police Association. This alone is scary, no recourse for inaccuracy, no way to assure data is not leaked or used for political or commercial purposes. News articles show it may have been used in political demonstrations to target citizens.

Good "death squad" database.

It was also hacked by an unidentified whistleblower who gave State Representative Mary Liz Holberg supposedly private data about herself. The cops are pressuring the Representative to turn over the whistleblower for prosecution, but the Representative has not yet squealed. This incident caused the system to be shut down.

Google search on CriMNet or MJNO to get more articles.

[The Internetted system is of course thought to be secure because it is password protected! There's a LONG article by Patrick Howe. PGN]

<http://www.twincities.com/mld/pioneerpress/news/politics/7154217.htm>

⚡ FBI's reach into records is set to grow

<Monty Solomon <monty@roscom.com>>

Thu, 13 Nov 2003 01:12:31 -0500

A little-noticed measure approved by both the House and Senate would significantly expand the FBI's power to demand financial records, without a judge's approval, from securities dealers, currency exchanges, car dealers, travel agencies, post offices, casinos, pawnbrokers and any other institution doing cash transactions with "a high degree of usefulness in criminal, tax or regulatory matters."

[Source: Eric Lichtblau, *The New York Times*, 12 Nov 2003; PGN-ed]

<http://www.nytimes.com/2003/11/12/politics/12RECO.html>

⚡ High-tech microscopes expose Americans' private lives

<Monty Solomon <monty@roscom.com>>

Thu, 13 Nov 2003 00:51:20 -0500

Don Campbell, USA Today, 10 Nov 2003

Too many of us [accept] the argument that the concept of personal privacy in the Internet era is as outdated as the Model T.

Americans can get pretty upset about the ways in which modern technology drives us nuts - such as telemarketers who disrupt our dinner

and spam
e-mailers who make pornographic sales pitches.

But a more insidious invasion of Americans' privacy quietly has taken root in Florida. It has received little attention from the media except in Florida and a handful of other states being recruited to join the enterprise. The project underscores how our fascination with technology blinds us to violations of our privacy - and highlights the inadequacy of today's mishmash of federal and state privacy laws.

"MATRIX," an acronym for Multistate Anti-Terrorist Information Exchange, is, according to its creator, the largest database on the planet, with more than 20 billion records. Working with the Florida Department of Law Enforcement (FDLE) and \$12 million in federal funding, a company called Seisint designed MATRIX with the objective of compiling an electronic dossier on every citizen in the nation.

Not surprisingly, the cover story is that MATRIX is needed to fight terrorism. If that doesn't ping the strings of your patriotic heart, it's also being touted as the cat's meow when it comes to catching kidnappers and child molesters. ...

http://www.usatoday.com/news/opinion/editorials/2003-11-10-campbell_x.htm

⚡ A heavily used RISKY website: France Telecom

<Peter Kaiser <la--a@p-k.ch>>

Thu, 13 Nov 2003 18:29:40 +0100

I am not in France at the moment, but I need to order telephone service in France, so I went to France Telecom's web site, which advertises itself as secure. One eventually finds a button for the order page: a popup window with minimal decoration and no outward indication of security -- that is, no "locked/unlocked" symbol. The page asks for exactly the kind of information you don't want to become public, including bank details, etc.

It isn't secured. The information isn't encrypted before being sent. I informed France Telecom of this by e-mail, including mentioning that the page appears to violate European law on the protection of personal information. A customer service representative replied:

"Thousands of orders are placed on francetelecom.com every day, we have not been informed of problems encountered as a result of orders made on our site." [P-K's translation. PGN]

I'm not reassured by this glib response, traditional though it may be.

The customer rep gave a number to call to order service by telephone, but that number -- as she knows, just as she knows I am not in France -- is unusable outside France, which places added pressure to use the unsecured website. If France Telecom left the security symbol on the order page, at least people would have the information to make an informed choice of

whether to proceed, but it has been deliberately hidden. And the informed choice is irrelevant to the laws protecting personal information; those are an obligation on the business, not a choice by the client.

Directing "thousands" of such orders daily, unencrypted, to a well-known Internet destination is a risk for both the customers and France Telecom. Perhaps France Telecom considers identity theft a uniquely American crime, but I wonder if anyone at a responsible level is aware of the legal issues under European law of protecting exactly this kind of information. European courts seem to take these issues seriously, I'm glad to say.

🔪 Holes found in online job search privacy (Brian Berstein)

<Monty Solomon <monty@roscom.com>>

Wed, 12 Nov 2003 08:41:05 -0500

Brian Bergstein, AP Online, 11 Nov 2003

<http://finance.lycos.com/home/news/story.asp?story=36422485>

Some career Web sites, recruitment services and automated job-application kiosks offer flimsy privacy protections and might even violate employment and credit laws, a report released Tuesday asserts. Many job sites still let too much information from resumes posted online get into the hands of third parties through online "cookies" that monitor Web surfing, according to the report, led by Pam Dixon, formerly of the University of

Denver's

Privacy Foundation and now head of her own group, the World Privacy Forum.

The report also faults self-service job application computers commonly used

by chain stores. It says they almost always demand social security numbers

and perform background checks on applicants without clearly stating who will

see the information. Dixon is urging job seekers to demand more stringent

privacy protections. She also wants the Federal Trade Commission and the

Equal Employment Opportunity Commission to look more closely at how job

sites and recruitment services handle information. ...

✶ Security patching: a story from the trenches

<Rex Black <rexblack@ix.netcom.com>>

Sat, 08 Nov 2003 13:53:00 -0600

I have a Dell Latitude running Windows 2000 with service pack 2 (I believe).

It is my back-up laptop. While on a business trip to Denver, my regular

laptop suffered a failure due to a poorly-designed and poorly-tested power

connector on the motherboard (another story). No problem, thought I, I'll

use the Dell laptop. I had about five days between my return from Denver

and my departure on my next trip to Tel Aviv.

Given all the security nonsense going on, I felt compelled to install the

latest security patches from Microsoft's Web site. During the course of the

first attempt to do so, my system was infected by the Blaster

Worm.

Fortunately, I have Symantec's Ghost utility running on the system, and I could revert to the old OS install and start all over.

This time, I resolved to install--and update--Norton Internet Security and Norton Antivirus prior to loading the security patches. During the course of updating the security and virus definitions, my system was again infected by the Blaster Worm. However, this time around, with the help of information and a free utility on Symantec's Web site, I was able to remove the worm.

I then went to apply the security patches again. This time, one of the patches did something untoward to my system and it started crashing. Since three days had passed at this point and I was due to leave for Tel Aviv soon, I didn't have time to isolate the bug. My guess is that the patch was not compatible with my particular system configuration.

So, I reinstalled Windows 2000 from the Ghost image yet again, reloaded all my applications yet again (including Norton Internet Security and Norton Antivirus), updated the security and virus definitions yet again (escaping infection this time), and skipped the security patches. I'm going to trust Norton Internet Security, Norton Antivirus, and daily updates to those programs to protect me, because I can't trust the Microsoft security patches to be adequately tested.

Salient points:

1. One major quality risk for patches of any kind is regression

(the failure of what heretofore worked). For any emergency patch, there is simply no time to repeat all the tests run against the regular release. Since security patches might well involve code deep within the operating system, it's no surprise to me that this failure to adequately regression test the patches resulted in a major incompatibility bug escaping to the field.

2. Regression bugs, particularly those where new code breaks existing functionality, can easily result in a maintenance release or patch resulting in a lower (rather than higher) level of system quality. Regression bugs might be relatively rare, but, as this case points out, they can be very dangerous.

3. It was already frustrating to have to spend about a day moving all my data and applications from my primary laptop to my backup laptop. Almost all of that time was spent installing applications on the backup system.

4. Add to that frustration the fact that I had to go through the "install OS-reinstall apps-update apps" process three times--twice more than had the problem not occurred in the first place.

All told, rack up three lost days of productivity to security bugs and general clunkiness in the Microsoft OS. At my usual consulting rates, that's thousands of dollars of lost time. Will Microsoft reimburse me for that? No way. Does that experience make me receptive to the idea of

switching to some other desktop platform (Linux, Mac, whatever)? You bet.

Am I more-than-ever convinced of the importance of thorough testing, including regression testing, of any software release? Absolutely.

Rex Black Consulting Services, Inc., 31520 Beck Road, Bulverde, TX 78163 USA
+1 (830) 438-4830 www.rexblackconsulting.com

✶ Bank scam with spaces in trick URL

<msb@vex.net (Mark Brader)>

Thu, 13 Nov 2003 17:23:45 -0500 (EST)

We have previously seen examples of scams involving a trick URL, where the part immediately after "http://" not the real domain name. But here now is a variant that I haven't heard of before -- making cleverly deceptive use of spaces.

A former co-worker, Donald Teed, reports receiving what at first looked like one more normal message from an Internet-aware company. He describes it as follows: "The e-mail will appear to come from the bank, using the correct domain, and the link in the e-mail will appear to be a link to the bank, using the correct URL." The bank in this case was Capital City Trust

<<http://www.capcity.ab.ca/>>. But the actual URL was like this:

```
<a href="http://www.capcity.ab.ca
```


<Richard I Cook <ri-cook@uchicago.edu>>

Thu, 13 Nov 2003 07:36:58 -0600

The reporter noted a consumer asking, "Why does it have a computer that reads the problems if they can't fix them?"

Although it makes me a bit of an old geezer to admit it, Bill Karcher framed this idea in the early 1970's. One of the systems software heavies from Control Data Corporation (the original 'supercomputer' maker), Karcher's Law was "Don't check for error conditions you are not prepared to handle." This was particularly important when memory and processor cycles were at a premium.

The problem described by this reporter is a common one, namely, "punt to the user" style systems. The idea that the user will be able to manage all the fault conditions that the computer can detect leads, inexorably, to unusable systems. Of course, even if the history of such a system is that it produces lots of false or misleading information or behaves strangely or unintelligibly, whenever an over failure does occur, the user will be blamed for having ignored the warning.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 23: Issue 4

Friday 28 November 2003

Contents

- [Sony to recall 550,000 CD Walkman battery packs](#)
[Monty Solomon](#)
- [Amber Alert, Coming to the Inbox Nearest You](#)
[Rebecca Mercuri](#)
- [Southern draws thwart voice recognition for police](#)
[Ken](#)
- [California to require voting machine receipts and stricter auditing](#)
[Steve Bellovin](#)
- [E-Votes must leave a voter-verified paper audit trail](#)
[PGN](#)
- [Diebold ATMs hit by Nachi worm](#)
[Steve Summit](#)
- [Proposed reason for electronic voting mess](#)
[John Bechtel](#)
- [Re: Astonishing electronic voting "glitch"](#)
[Martin Ward](#)
- [Whois bug at www.tucows.com](#)
[Tony Toews](#)
- [Man arrested wardriving child porn](#)
[Walter Roberson](#)

- [Old Nigerian scam nets \\$400,000](#)
[Arthur J. Byrnes](#)
 - [In-Security clearance](#)
[Name withheld by request](#)
 - [Human Error Leads to AT&T's Anti-Spam Gaffe](#)
[Ryan Naraine via Fuzzy Gorilla](#)
 - [Books of Interest: End of the World; Human Factor](#)
[Mike Smith](#)
 - [REVIEW: "Practical Cryptography", Bruce Schneier/Niels Ferguson](#)
[Rob Slade](#)
 - [REVIEW: "Wireless Security Essentials", Russell Dean Vines](#)
[Rob Slade](#)
 - [Re: SANS, GSEC, and Chapple book review](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **Sony to recall 550,000 CD Walkman battery packs**

<Monty Solomon <monty@roscom.com>>

Wed, 19 Nov 2003 07:56:34 -0500

Reuters, 19 Nov 2003: Sony Corp said on Wednesday it would recall about 550,000 external battery packs for its CD Walkman worldwide because of a defect in the connector cord that could cause the pack to heat up and partially melt. A Sony spokeswoman said there had been one reported instance of the battery pack damaging the CD player's nylon carrying case.

<http://finance.lycos.com/home/news/story.asp?story=36534151>

⚡ Amber Alert, Coming to the Inbox Nearest You

<Rebecca Mercuri" <notable@mindspring.com>>

Tue, 25 Nov 2003 20:29:01 -0500

The latest in the spam wars -- Amber Alert! This one promises to clog your email box with photos of children who may or may not have vanished, probably for years even after they've (hopefully) been found. It's so much more convincing than those "estate of Nigerian millionaire deposit account" messages. Makes you nearly want to cry. Hey, if it was my kid, I'd spam the universe. But it's still spam. So when you reply to the sender (who is inevitably going to be some kindhearted soul that you know who received this from a long chain of other friends whose email addresses they've included to prove it's "authentic") with a "this is spam" message you're just going to appear to be heartless. There's no good way out of this one other than to immediately redirect all messages with the subject phrase "Amber Alert" into your trashbin, pray you never need to do this for your own kid or someone you really do know **FIRSTHAND**, and don't look back.

⚡ Southern draws thwart voice recognition for police

<Ken>

Sun, 23 Nov 2003 09:47:03 -0600

[PGN-ed from an AP item]

<http://www.cnn.com/2003/US/South/11/16/southern.drawl.ap/>

Southern drawls ("lazy mouth") have thwarted voice recognition equipment used by the Shreveport, Louisiana, Police Department to route non-emergency calls to persons or departments. Switching to a more conventional voice menu touch-tone response system is planned.

⚡ California to require voting machine receipts and stricter auditing

<Steve Bellovin <smb@research.att.com>>

Fri, 21 Nov 2003 18:09:04 -0500

According to the Associated Press, California's Secretary of State Kevin Shelley has ordered that by 2006, all electronic voting machines in the state must provide a "voter verified paper audit trail". He also introduced stricter requirements for testing and auditing the software used for both recording and tabulating votes.

Steve Bellovin, <http://www.research.att.com/~smb>

[See also Kim Zetter, wired.com, 21 Nov 2003. PGN]

<http://www.wired.com/news/evote/0,2645,61334,00.html>

⚡ E-Votes must leave a voter-verified paper audit trail

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

Sun, 23 Nov 2003 13:12:19 PST

CA SoS Shelley has apparently taken the recommendations of some of the members of his review panel seriously, in light of recent strange events previously recorded here.

As RISKS readers are aware, this is in essence an approach recommended by Rebecca Mercuri, in which voters verify that the paper record is identical to what is on the touch-screen. The machine- and human-readable audit trail would remain within the voting system. In the pure Mercuri Method, the machine-readable audit trail would be the official ballot, although the California wording seems to suggest that the electronic version would be the official version unless irregularities had to be resolved by comparing the electronic and paper versions. Clearly, any discrepancies detected during the voting process should result in the machine being taken out of service.

⚡ Diebold ATMs hit by Nachi worm

<Steve Summit <scs@eskimo.com>>

Tue, 25 Nov 2003 13:14:28 -0500

Astonishingly, several Diebold Automatic Teller machines were infected by the "Nachi" worm last August, and the company has confirmed this. These

were an "advanced line of Diebold ATMs built atop Windows XP Embedded", and were therefore vulnerable. They weren't on the public Internet, but of course many recent worms have displayed remarkable potency in their ability to hop over firewalls and infect private intranets.

Full story at <http://www.theregister.co.uk/content/55/34175.html> .

To me, this incident reinforces a worrisome trend. On the one hand, everyone knows that critical functions shouldn't be implemented using less-than-rugged components such as "consumer grade" operating systems. But the ubiquity of the market leader's products and the resulting convenience of using them means that the temptation to do so, even when it's formally inadvisable, is quite often irresistible. Such decisions are always papered over with superficially plausible rationalizations such as "this component performs a non-critical function of the otherwise critical system" (e.g. "these computers are involved with nonessential railway communication functions, not signalling") or "these computers are not connected to the public Internet in any way" (as in the present incident), but as we know all too well, in complex, interconnected systems, those convenient assumptions have a way of breaking down.

✶ Proposed reason for electronic voting mess

<John Bechtel>

Sat, 15 Nov 2003 19:23:35 +0000

Reading RISKS, there are endless stories of badly designed and implemented electronic voting machines. The authors are passionately committed to the democratic process, and hate to see even a chance of voter disenfranchisement. The authors elicit dismay at the "authorities" callous disregard for due process and good engineering. The authors care.

A comparison comes to mind: Much of modern art is, frankly, rubbish. The artists will say that its purpose isn't to be beautiful, its purpose is to make us think. Question. Have an opinion. Care.

Maybe, just maybe, "they" are doing the same thing with the voting machines?

Putting bad products in the field to make "us" care, to think, to act... even, as a last resort, vote. Voter apathy and low voter turnout is well known. Begging people to vote hasn't worked. Perhaps there is no better way to make people cherish their vote, and use it, than to make them think it is being taken away.

Nothing like an even bigger conspiracy theory, is there?

John Bechtel, Maidenhead, UK

⚡ Re: Astonishing electronic voting "glitch" ([RISKS-23.03](#))

<Martin Ward <Martin.Ward@durham.ac.uk>>

Tue, 18 Nov 2003 10:34:03 +0000

> It's interesting to wonder what might have happened if the
initial
> inaccurate result had not been so glaringly obvious ... [PGN]

Perhaps I am too paranoid, but it looks as though "someone" is
testing to
see just how big a "glitch" they can get away with, while at the
same time
getting the punters accustomed to regular "glitches" in e-voting
software
(just as MS has got people accustomed to desktops which
regularly crash,
freeze or scramble documents).

How many other results were there that were *not* so glaringly
obvious? How
do you know that the results of this "test" were not: "Just keep
the total
number of votes less than the total number of voters, and people
won't
notice a thing"?

Martin.Ward@durham.ac.uk <http://www.cse.dmu.ac.uk/~mward/>

Whois bug at www.tucows.com

<Tony Toews <ttoews@mvps.org>>

Fri, 14 Nov 2003 22:21:19 -0700

I went to run a whois inquiry on a domain at www.tucows.com. I
get a
screen which asks me to validate a number which appears on a
graphic. And
it doesn't take the entered number. It displays another number
in
graphical format. Which it also doesn't take. Repeat until
frustrated.

I later reread the screen and decided to check my browser's cookie settings -- which I manually set for each Web site I visit. If I see anything suspicious in the cookie site I tell IE to not save that Web site cookies. Turns out that was the problem.

- 1) I complained a week ago and have not received a response.
- 2) A sentence along the lines of "If the system doesn't accept the number you enter double check your cookie settings." would've saved a lot of frustration on my part.

Tony Toews, Microsoft Access MVP
Microsoft Access Links, Hints, Tips & Accounting Systems at
<http://www.granite.ab.ca/accmstr.htm>

Man arrested wardriving child porn

<Walter Roberson <roberson@ibd.nrc.ca>>
Sat, 22 Nov 2003 11:57:04 -0600 (CST)

In Toronto, Canada, this week:

After pulling the man over, Sgt. Don Woods discovered the man was naked

from the waist down as he downloaded images on a laptop computer of a

young girl involved in a sex act with an adult. Investigation showed the

man had hooked into a wireless computer network at a nearby house to gain

access to a resident's Internet connection and download images from child

pornography Web sites.

<http://www.canoe.ca/NewsStand/LondonFreePress/News/2003/11/22/264890.html>

✶ Old Nigerian scam nets \$400,000

<"Arthur J. Byrnes" <arthurb@ajb.com>>

Wed, 19 Nov 2003 21:11:14 -0500

[For those of you who wonder why you keep getting variants of the confidential scam spams asking you to help launder millions of dollars,

here is one of the reasons why: There are still suckers falling for them.

PGN]

The *Daytona Beach News Journal* (13 Nov 2003) reported that a local man had fallen for the Nigerian 419 e-mail scam to the tune of \$400,000. Even after being informed it was a scam, he continued to send money. He had mortgaged his house and used up his life savings. [PGN-ed]

<http://www.news-journalonline.com/NewsJournalOnline/News/Headlines/03NewsHEAD01111303.htm>

The Risk? With no spam regulations and no cooperation between national governments con-men are getting away with many people's hard earned money.

Some folks think that the greedy get what they deserve, but falling for this type of scam, may also be a sign of mental illness.

[Gambling is addictive behavior. Perhaps so are Nigerian-type

scams .
PGN]

✶ In-Security clearance

<[Name withheld by request]>
Sat, 22 Nov 2003

I am in the process of getting a DoD security clearance in connection with my job. My contact in my employer's security office claimed to have sent me the information I needed to apply for the clearance by e-mail, but I never got it. When I talked to this person by phone she said that she had sent me "the program" several times. The following exchange ensued:

Me: The program? You mean, you sent me an executable attachment?

She: That's right.

Me: Well, no wonder I didn't get it! It was deleted by my virus protection program, which deletes all e-mails with executable attachments.

She: No problem, I'll just send you a URL where you can download it.

Me: OK. Er, isn't there any other way for me to submit my application, like on paper for example?

She: No.

The URL she sent me was:

<http://www.dss.mil/epsq/index.htm>

Note it's http, not https.

It is quite a challenge to find the right link on that page, but when you do you eventually get lead to:

<https://sclient.dss.mil/download/>

Thankfully a secure page, but one whose certificate is not signed.

From there you are lead to a page where you "certify" (by clicking on a button that says, "I certify that the above answers are true") that you are in the U.S. and promise not to export the program outside the U.S. (because it contains encryption technology).

Finally, you get to the download page, where you have the following choices of operating systems:

1. Windows 95, 98, NT or 2000
2. Windows 3.x

Mac and Linux users like me are out of luck.

Fortunately, I have a dual-boot Linux/Win2000 machine at home, so I tried running the program on that machine. The executable I got from the site turned out to be an installer, which installed 212 different files (that I could find) on my disk.

The punch line, of course, is that when I tried to run it, it didn't work.

The cursor changed into an hourglass, then back to an arrow, and nothing else happened. God only knows what it did. I'll probably have

to wipe the
disk and reinstall the OS before I can trust this machine again.

The degree of cluelessness on the part of the people who are responsible for guarding our country's military secrets that this episode reveals is truly scary. Think about it: the only way to get a security clearance is to agree to 1) run a program whose pedigree you have no way of verifying 2) on an operating system that is notoriously insecure and 3) (presumably -- I never got a chance to find out) give that program sensitive personal information. To my mind, anyone who agrees to this ought to be summarily denied a clearance, but of course, that fate is probably reserved for troublemakers like me who raise these kinds of issues.

✶ Human Error Leads to AT&T's Anti-Spam Gaffe

<Fuzzy Gorilla <fuzzygorilla@SoftHome.net>>

Sun, 16 Nov 2003 20:57:15 -0500

After seeing a rush of spam, and brainstorming possible remedies, AT&T sent out a mass e-mailing to business partners and customers asking for the IP addresses of all outbound SMTP servers (to be used for a white list), threatening to cut off e-mail access of nonresponders. Subsequently, they sent a follow-up apology, with a request to disregard the first e-mail, claiming that the original notices went out as a result of "human error".
[Source: Ryan Naraine, 22 Oct 2003, Jupitermedia Corporation;

PGN-ed]

<http://boston.internet.com/news/article.php/3097171>

🔥 Books of Interest: End of the World; Human Factor

<"Smith, Mike" <msmith@adga.ca>>

Fri, 28 Nov 2003 08:33:59 -0500

I thought RISKS readers might be interested in two books I came across recently.

The first is "The End of the World: The Science and Ethics of Human Extinction" by John Leslie. It's focus is the so-called Doomsday Argument, first described by cosmologist Brandon Carter.

The argument assumes that human population growth will continue to be exponential up to the point where some unspecified disaster wipes out the species. Therefore, most of the humans who will have ever lived will live in the one or two generations before Doomsday. If you take yourself as a random human, you must conclude that you are most likely to be in the last couple of generations. In other words, Doom is more likely to come sooner rather than later. About half the book defends the argument. Apparently mathematicians and philosophers have been trying to find an error in the reasoning for about twenty years, without success.

Mr. Leslie goes on to discuss some of the ways in which we might become

extinct, from nuclear war to plague to technology run amok to asteroid impact. He discusses whether we should, from an ethical perspective, try to preserve ourselves if we can't eliminate human misery. Some of these philosophical discussions are pretty tough reading.

Ultimately, Mr. Leslie's point is that not only are the risks obvious, but they are also higher than we might otherwise think.

The second book is "The Human Factor" by Kim Vicente. This very readable book is about why we need to consider the "human factor" in designing socio-technological systems. Without considering the way people use technology, we run the risk of our technological systems moving outside their "safety envelopes" and causing disasters. He uses a wide array of case studies, from the Reach toothbrush to the Aviation Safety Reporting System, to show how human factor engineering and systems approaches to design benefit everyone. Mr. Vicente also gives many examples of poor system design that led to disaster, including preventable accidental hospital deaths (which outnumber traffic accident deaths in the U.S.) and the Walkerton, Ontario, contaminated water tragedy.

Mike Smith, Senior IT Security Engineer, AEPOS Technologies Corporation
819-772-8522 ext. 230 www.aepos.com

★ REVIEW: "Practical Cryptography", Bruce Schneier/Niels Ferguson

<Rob Slade <rslade@sprint.ca>>
Mon, 17 Nov 2003 07:42:08 -0800

BKPRCCRP.RVW 20030918

"Practical Cryptography", Bruce Schneier/Niels Ferguson, 2003,
0-471-22357-3, U\$50.00/C\$76.95/UK#34.95
%A Bruce Schneier schneier@counterpane.com
%A Niels Ferguson niels@macfergus.com
%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8
%D 2003
%G 0-471-22357-3
%I John Wiley & Sons, Inc.
%O U\$50.00/C\$76.95/UK#34.95 416-236-4433 fax: 416-236-4448
%O [http://www.amazon.com/exec/obidos/ASIN/0471223573/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0471223573/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/0471223573/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0471223573/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/0471223573/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0471223573/robsladesin03-20)
%P 410 p.
%T "Practical Cryptography"

The preface points out that cryptography has done more harm than good in terms of securing information systems, not because cryptography fails in and of itself, but, rather, due to the improper use or implementation of the technology. This book is intended to provide concrete advice to those designing and implementing cryptographic systems. As such, it is not the usual introduction to cryptography, and is aimed at a fairly limited group.

Chapter one asserts that we should be engineering for security, rather than speed or bells and whistles. Security is only as strong as the weakest

link, we are told in chapter two, and (following from the idea of defence in depth) we need to have engineering in depth (and probably breadth, as well). The issues are important, but there is some lack of clarity to the organization and flow of the text and arguments: the reader may start to wonder what the essence of the message is. (I see that I should have trademarked "professional paranoia" when I started using it years ago, but it is nice to note that the point is being taken.) Chapter three is a rather unusual "Introduction to Cryptography" (and the mathematical format of the text doesn't make it easier for the math-phobic to concentrate on the meaning), but focussing on the applications and problems, the cryptanalytic attacks, and repeating the injunctions against complexity and the sacrifice of security for performance is a reasonable position.

Having come this far, it is interesting to note that we are only starting part one, reviewing message security. Chapter four compares and reviews various existing block ciphers. The modes, and attacks against specific modes, of block algorithms are described in chapter five. (This material appears to be what would, in a more traditional book, be the introduction to cryptography.) Hash functions are explained, compared, and assessed in chapter six, while seven extends the concept to message authentication codes, which ensure not only detection of accidental alteration, but are also resistant to outsider modification attacks on the data or transmission.

We therefore have the basic tools that we need to consider a

channel that is secure from eavesdropping and manipulation by anyone not party to the communications, in chapter eight. Implementation, and the engineering or software development considerations, are examined in chapter nine.

Part two deals with key negotiation, partly by introducing the concept of asymmetric (more commonly, if less accurately, referred to as "public key") cryptography, the major strength of which involves the handling of keys. Chapter ten raises the issue of randomness, which is vital in the choice of keys, and also talks about the components of the Fortuna system for generating pseudo-random numbers. Prime numbers are explained in chapter eleven, due to their importance in asymmetric cryptography. The venerable Diffie-Hellman algorithm is reviewed, along with the math that makes it work, in chapter twelve. (If you want to follow the material all the way, you'll have to be good at mathematics, but the discussion, while interesting, is not vital to the use of the system.) A similar job is done on RSA in chapter thirteen. Chapter fourteen is entitled an "Introduction to Cryptographic Protocols" but really talks about trust, risk, and more requirements for the secure channel. The high level design of a key negotiation protocol is incrementally developed in chapter fifteen. Implementation issues specific to asymmetric systems are reviewed in chapter sixteen.

Part three looks at key management, and various approaches to the problem.

Chapter seventeen discusses the use, and risks of using, clocks and time in cryptosystems. The idea of the key server is illustrated by Kerberos in chapter eighteen, but almost no detail is included. A quick introduction to PKI (Public Key Infrastructure) is given in chapter nineteen, followed by a philosophical review of other considerations in twenty, and additional practical concerns in twenty one. (While the division is not unreasonable, these three could, without seriously distorting the book, have been one big chapter.) Storing secrets, important for key and password reliability, is contemplated in chapter twenty two.

Part four contains miscellaneous topics, including the futility of standards (twenty three), the questionable utility of patents (twenty four), and the need for involving real experts (twenty five).

As noted, this book is not simply another introduction to cryptography. The content is for those involved in the guts of a cryptosystem, and the material provides significant guidance for the concerns of people in that position.

copyright Robert M. Slade, 2003 BKPRCCRP.RVW 20030918
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
victoria.tc.ca/techrev/mnbksc.htm sun.soci.niu.edu/~rslade/
secgloss.htm

★ REVIEW: "Wireless Security Essentials", Russell Dean Vines

<Rob Slade <rslade@sprint.ca>>

Fri, 21 Nov 2003 07:31:38 -0800

BKWLSCES.RVW 20031018

"Wireless Security Essentials", Russell Dean Vines, 2002,
0-471-20936-8, U\$40.00/C\$62.50

%A Russell Dean Vines

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2002

%G 0-471-20936-8

%I John Wiley & Sons, Inc.

%O U\$40.00/C\$62.50 416-236-4433 fax: 416-236-4448

%O [http://www.amazon.com/exec/obidos/ASIN/0471209368/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0471209368/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0471209368/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0471209368/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0471209368/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0471209368/robsladesin03-20)

%P 345 p.

%T "Wireless Security Essentials"

The introduction asserts, as a statement on the rapid pace of technological innovation, that wireless security may have changed between the writing and the publication of the book. It may be an interesting comment on security that the book is still relevant and that wireless security is unchanged in the two years since the book's completion. It may also be a measure of the good job that Vines did on his subject.

Part one deals with the foundational aspects of the technology. Chapter one covers computing technology, with a basic but brief look at computer architecture and some network architecture (but mostly protocols). Both wireless LAN and cellular telephone are discussed, but the LAN

material

predominates. Wireless theory, including radio communication and transmission protocols, is examined in chapter two. The explanations are

good: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread

Spectrum (FHSS) are much better than in other related works, although the

text could still use some improvement on details such as DSSS chipping and

the mapping of bits to the frequency signals. Wireless reality, in chapter

three, is an odd mix of the security portions of wireless LAN protocols

(except for Bluetooth, which has a number of functions explained in detail),

the Infrared Data Association (IrDA), wireless operating systems and

devices, and wireless services.

Part two covers security essentials. Chapter four outlines security

concepts and methodologies in a well-chosen (with the signal exception of

cryptography) but not well-structured list. (Given Vines' participation in

"The CISSP Prep Guide" [cf. BKCISPPG.RVW] this is not surprising.)

According to chapter five, security technology primarily encompasses

cryptographic aspects of wireless LAN protocols. There is a very comprehensive examination of a broad range of attacks against wireless

devices (Personal Digital Assistant [PDA] viruses, for example) and

transmissions (there is an extremely detailed analysis of WEP weaknesses,

backed up by even more details in appendices B and C), as well as recommended countermeasures, in chapter six.

Although not perfect, this book is an extremely useful guide to the security

issues surrounding the use of wireless devices. Of the various

books

reviewed on the topic of wireless LANs and security, it is the best work seen to date.

copyright Robert M. Slade, 2003 BKWLSCES.RVW 20031018
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu
victoria.tc.ca/techrev/mnbksc.htm sun.soci.niu.edu/~rslade/secgloss.htm

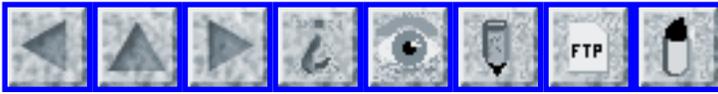
Re: SANS, GSEC, and Chapple book review ([RISKS-23.02](#))

<Rob Slade <rslade@sprint.ca>>

Sat, 22 Nov 2003 22:27:57 -0800

In my recent review of "The GSEC Prep Guide" by Mike Chapple, I probably did not sufficiently stress the point that the faults of the book are not necessarily to be imputed to the GSEC program itself. I have been asked by Stephen Northcutt to note that Chapple has no association with SANS, and that Northcutt has (in a review under the book's listing on Amazon.com) noted that the material in Chapple's book does not adequately reflect the breadth of the material tested for in the GSEC exam.

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu
victoria.tc.ca/techrev/mnbksc.htm sun.soci.niu.edu/~rslade/secgloss.htm



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 5

Weds 3 December 2003

Contents

- [Two loose screws killed Disneyland rider](#)
[PGN](#)
- [US railroad uses Wi-Fi to run 'driverless' trains](#)
[Lars Kongshem](#)
- [Nuclear plan shut down by lightning strike](#)
[Fuzzy Gorilla](#)
- [Tanker Truck Shutdown Via Satellite](#)
[Fuzzy Gorilla](#)
- [Microsoft Windows, Auto Edition](#)
[Andrew Whitby](#)
- [What Bill Gates Says About Security \(from InformIT\)](#)
[Dawn Cohen](#)
- [Another large gas bill](#)
[Amos Shapir](#)
- [UK MoD scraps 120-million-pound computer project](#)
[Fuzzy Gorilla](#)
- [How Much Is Privacy Worth?](#)
[Monty Solomon](#)
- [Government e-mails apparently sent to hairdresser](#)
[Neil Youngman](#)

- ['Master' and 'slave' computer labels unacceptable, LA officials say](#)
[Henry Baker](#)
 - [Security subtleties](#)
[identity withheld by request](#)
 - [Man trapped for hours by payphone](#)
[Mark Brader](#)
 - [Debian security breach and forensic analysis](#)
[Gerrit Muller](#)
 - [Re: Security patching: a story from the trenches](#)
[Walter Dnes](#)
 - [Dangerous looking e-mail from quickbooks](#)
[Kyle York](#)
 - [Re: In-Security clearance](#)
[Peter H. Coffin](#)
 - [Re: Amber Alert, Coming to the Inbox Nearest You](#)
[Timothy Knox](#)
 - [Re: Cehck tihs out!](#)
[Rodney Hoffman](#)
 - [ANNOUNCE: New mailing list for secure application development, SC-L](#)
[Kenneth R. van Wyk](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Two loose screws killed Disneyland rider

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

Wed, 26 Nov 2003 15:17:15 -0800 (PST)

Improper maintenance and inadequate operator training are being blamed for the death of the rider of the Big Thunder Mountain Railroad roller coaster at Disneyland on 5 Sep 2003. The lead car lost its rear-wheel assembly and hit the tunnel roof, causing the following passenger car to go underneath it. The train had just been returned to service after routine

maintenance

three days earlier. Unusual noises were noted on the first 12 trips of the day, and operators had planned to take the train off line after the 13th

ride -- which never finished. Subsequent analysis showed that two screws

had not been properly tightened. [PGN-ed from cnn.com]

<http://www.cnn.com/2003/US/West/11/26/disneyland.accident.ap/index.html>

US railroad uses Wi-Fi to run 'driverless' trains

<Lars Kongshem <lars.kongshem@kongshem.com>>

Fri, 21 Nov 2003 11:52:30 -0800

"The Burlington Northern and Santa Fe Railway Company (BNSF) has found a novel use for Wi-Fi. It has started using the wireless networking technology to control trains remotely. BNSF locomotives carry freight across the continental US. However, it is using wireless technology to move units around its rail yards.... (Drivers) operate a control panel that mirrors what they'd see if they were sitting in the cab. Their instructions are relayed to each loco via the 'industrial strength' WLAN."

Given Wi-Fi's security problems, this novel use of 802.11 certainly gives a new meaning to the word "loco"!

[Source: *The Register*, Nov 20 2003]

<http://www.theregister.co.uk/content/69/34101.html>

Lars Kongshem, 2220 Taylor St. Suite D, San Francisco, CA 94133

1-415.606.5277 lars.kongshem@kongshem.com + <http://www.kongshem.com>

[Of course, if they were carrying fruit, it would be PLUM LOCO. PGN]

✶ Nuclear plan shut down by lightning strike

<Fuzzy Gorilla <fuzzygorilla@SoftHome.net>>

Sun, 16 Nov 2003 21:30:42 -0500

A 15 Sep 2003 lightning strike in Chester County, Pennsylvania, shut down a pair of nuclear reactors 36 miles away at the Peach Bottom Atomic Power Station. Early that morning, lightning struck a PECO power line in East Bradford Township, near West Chester. A circuit breaker failed to isolate the damaged power line, cutting off electricity to more than 100,000 PECO customers and three PECO/Exelon plants -- Peach Bottom, Conowingo (Md.) Hydroelectric Station and Muddy Run Pumped Storage Facility in Holtwood. ... At least two complications occurred at Peach Bottom as the reactors were shutting down, according to a preliminary report issued by the NRC. One of four emergency generators failed, and a safety relief valve used to control steam pressure initially stuck open. The NRC has decided to penalize Exelon because the September shutdown was the fourth at Unit 2 in less than a year.

The reactor tripped off unexpectedly 21 Dec 2002, when a

computer failure
caused steam isolation valves to close. On 21 Apr, the valves
closed and
shut the reactor again because of instrument problems on an air
line. The
unit also was down from 22 Jul to 1 Aug because of generator
problems.

[Source: Article by Rebecca J. Ritzel, (Lancaster)

Intelligencer Journal,

date not available, but prior to 19 Nov, anticipating a public
meeting of

Nuclear Regulatory Commission officials; PGN-ed, but URL no
longer valid.]

<http://www.yorkdispatch.com>

✶ Tanker Truck Shutdown Via Satellite

<Fuzzy Gorilla <fuzzygorilla@SoftHome.net>>

Sun, 16 Nov 2003 21:05:12 -0500

[The obvious RISKS -- when mandated by law, that a terrorist
would be
unaware of the need to disable the system; and that no cracker
would ever
find out the needed signal and shut down a truck for 'fun'; and
that no GPS
or other systems failure might cause a truck to be shut down
incorrectly by
law enforcement -- are probably obvious to any RISKS reader.]

Satellite Security Systems (S3), in cooperation with the
California Highway
Patrol (CHP) and InterState Oil Company, dramatically
demonstrated the first
wireless remote shutdown of a fully loaded moving petrochemical
tanker
truck. From S3's headquarters in San Diego (530 miles away),
"satellite

communications were used to disable the truck in seconds, proving S3's GlobalGuard and FleetGuard a viable solution to the challenge of controlling rogue hazardous waste vehicles that could pose a threat to homeland security."

While the California state government may be voting as early as January on Assembly Bill (AB) 575 (requiring truck disabling devices, global positioning or other "location reporting systems" on hazardous material haulers), the CHP has been tasked with researching various technologies to support these regulatory initiatives. [PGN-ed from *SpaceDaily*, 4 Nov 2003]
<http://www.spacedaily.com/news/gps-03zn.html>

Microsoft Windows, Auto Edition

<Andrew Whitby <s358831@student.uq.edu.au>>
Tue, 2 Dec 2003 12:44:07 +1000 (GMT+1000)

The Associated Press reports:

First Microsoft set out to put a computer in every home. Now the software giant hopes to put one in every vehicle, too. "We'd like to have one of our operating systems in every car on Earth," said Dick Brass, the vice-president of Microsoft's automotive business unit. "It's a lofty goal." Cars with the Microsoft software will speak up when it's time for an oil change. They'll warn drivers about wrecks on the road ahead and

scout alternative routes. They will pay freeway tolls automatically. The software running their brakes will upgrade itself wirelessly.

I can see it now. "A security update is available for your braking system. Press okay to begin installation."

Apparently the RISKS are not obvious to everyone.

⚡ What Bill Gates Says About Security (from InformIT)

<"Dawn Cohen" <COHEND@wyeth.com>>

Mon, 17 Nov 2003 11:48:34 -0500

InformIT, 13 Nov 2003: What Bill Gates Says About Security

"You don't need perfect code to avoid security problems. There are things we're doing that are making code closer to perfect, in terms of tools and security audits and things like that. But there are two other techniques: one is called firewalling, and the other is called keeping the software up to date. None of these problems (viruses and worms) happened to people who did either one of those things. If you had your firewall set up the right way * when I say firewall I include scanning E-mail and scanning file transfer -- you wouldn't have had a problem.

"But did we have the tools that made that easy and automatic and that you could really audit that you had done it? No. Microsoft in particular and the industry in general didn't have it. "The second is just the updating

thing. Anybody who kept their software up to date didn't run into any of those problems, because the fixes preceded the exploit. Now the times between when the vulnerability was published and when somebody has exploited it, those have been going down, but in every case at this stage we've had the fix out before the exploit.".... "Actually, all the forms of Unix (as well as Linux) have had more vulnerabilities per line of code. They don't propagate as much because they're not as dense as our system is, so the things that prevent the propagation are particularly important for our world."

<http://www.informit.com/content/index.asp>

[?product_id=3D%7BEF1DDC0F-F7BB-47F2-A1AC-00FCB4BCCC39%7D&111603](http://www.informit.com/content/index.asp?product_id=3D%7BEF1DDC0F-F7BB-47F2-A1AC-00FCB4BCCC39%7D&111603)

✶ Another large gas bill

<amos083@walla.co.il>

Mon, 1 Dec 2003 13:31:32 +0200

Commenting on a complaint from a Mr Arthur Purdey about a large gas bill, a spokesman for North Westgas said, "We agree it was rather high for the time of year. It's possible Mr Purdey has been charged for the gas used up during the explosion that destroyed his house." (*The Daily Telegraph*)

✶ UK MoD scraps 120-million-pound computer project

<Fuzzy Gorilla <fuzzygorilla@SoftHome.net>>

Sun, 16 Nov 2003 20:46:03 -0500

Sources: John Leyden, 6 Nov 2003, The Register,
<http://www.theregister.co.uk/content/7/33831.html>

Sara Arnott, 5 Nov 2003,
<http://www.computing.co.uk/News/1147382>

Also

[http://www.femail.co.uk/pages/standard/article.html
?in_article_id=201440&in_page_id=2p](http://www.femail.co.uk/pages/standard/article.html?in_article_id=201440&in_page_id=2p)

Britain's Ministry of Defence squandered 118 million pounds on a computer system that was axed before ever being used. The Defence Stores Management Solution was designed to modernise the MoD's inventories of equipment. (Hardware valued at 12.2 million pounds was salvaged and not included in the 118M figure.) The system had been expected to save 650 million pounds in its first ten years. A report on the collapse of the project (begun in 1999) was released in mid-November. Reasons given included "developments in defence logistics" had rendered the project obsolete, but also indicated management weaknesses at every level: "The MoD had no framework to assess and manage deliverability once projects were launched; the DLO lacked effective change management support and co-ordination; and the BCP suffered from poor financial governance, weak benefits management, poor communications and a failure to establish an effective programme management organisation. ... The review also noted weaknesses in the scrutiny and approvals process. Although BCP projects, including the DSMS, did not meet the Department's requirements in important areas -- especially on

affordability and benefits management -- the projects were not rejected,"

✶ How Much Is Privacy Worth?

<Monty Solomon <monty@roscom.com>>

Wed, 3 Dec 2003 09:01:22 -0500

The Supreme Court will hear oral arguments today over whether the federal government should reimburse individuals whose sensitive data was disclosed illegally, even if no harm can be proven. The Privacy Act of 1974 prohibits the government from disclosing private information intentionally, without the individual's consent, and provides for a \$1,000 minimum fine if the individual is "adversely affected." In the case, known as Doe v. Chao, the Department of Labor distributed the Social Security number of a coal miner who was appealing for black lung benefits. Since 1969, the Labor Department has used miners' Social Security numbers as their case numbers on documents shared with coal companies, insurance companies and lawyers for all sides. Those documents also were published in court filings that later ended up in legal databases. [Ryan Singel, wired.com, 3 Dec 2003; PGN-ed]

<http://www.wired.com/news/privacy/0,1848,61439,00.html>

✶ Government e-mails apparently sent to hairdresser

<Neil Youngman <n.youngman@ntlworld.com>>

Sun, 16 Nov 2003 21:21:40 +0000

According to this BBC article, a hairdresser called Ronnie Campbell received e-mails apparently intended for a Member of Parliament (MP), called Ronnie Campbell. Usual RISKS apply.

<http://news.bbc.co.uk/1/hi/uk/3267221.stm>

✶ 'Master' and 'slave' computer labels unacceptable, LA officials say

<Henry Baker <hbaker1@pipeline.com>>

Thu, 27 Nov 2003 23:09:22 -0800

FYI -- In Tinseltown, bus 'slaves' must go to the end of the line... This gives a whole new meaning to 'PC' language. Please update your cable labels.

Los Angeles officials have asked that manufacturers, suppliers, and contractors stop using the terms "master" and "slave" on computer equipment, saying such terms are unacceptable and offensive -- after someone had filed a discrimination complaint with LA County's Office of Affirmative Action Compliance. "Based on the cultural diversity and sensitivity of Los Angeles County, this is not an acceptable identification label," Joe Sandoval, division manager of purchasing and contract services, said in a memo sent to

County vendors. [PGN-ed from Reuters item]

<http://www.cnn.com/2003/TECH/ptech/11/26/master.term.reut>

Security subtleties

<[identity withheld by request]>

Thu, 9 Jan 2003

I work at a large institution which shall remain nameless. I was recently involved in the evaluation of a product from a company which I will call Company X. The product consists of a Linux server that is sealed in a way that it is impossible to open the box without leaving evidence of tampering. During the course of the normal operation of the product it was installed behind our firewall, and it made copies of sensitive data accessible on our intranet.

The loan agreement stipulated that before the box could be returned, our sensitive data had to be deleted from the disks. The box had a built-in "self-destruct" feature that was supposed to accomplish this. Unfortunately, self-destruct was a little too thorough: it not only erased all the data, but it erased the operating system as well, leaving the box unbootable.

The problem with this is no doubt immediately obvious to long-time Risks readers: if the box is unbootable then we have no way of verifying that the data is in fact gone. For all we know, self-destruct only

erases the boot
sector.

I raised this objection with representatives of Company X. They suggested that instead of running self-destruct that I use the standard Web-based control interface to erase the data. No, this wouldn't work either, I explained, because again there is no way to verify that the data has actually been erased. For all we know, the only thing that is actually erased is a symlink.

They suggested "running a big magnet over the box." Same problem of course.

I pointed out that the only way for us to verify that the data was in fact gone would be to examine the disk, which meant one way or another obtaining either root or physical access. They refused to allow this because (they said) they were concerned about us stealing the software.

We went back and forth about this literally for months, and I was astonished how hard it was for people to grasp the concept that just because you can't see the data through an HTTP interface doesn't mean it's not there. We finally arrived at the following compromise: Company X would send a representative to our site where the rep would witness the invocation of the self-destruct feature, after which we would open the box, remove the disks, and install them on another machine where they could be examined and/or further wiped.

The big day finally arrived, and we ran self-destruct according

to the directions. Oddly, there was no indication when the process was finished. We waited five minutes (the prescribed amount of time). At that point the company rep said he wanted to log in to the machine to make sure that it had worked properly. I was shocked, shocked! to discover that in fact self-destruct seemed to have done absolutely nothing. All the files were still there, both our data and those of Company X.

At that point the rep typed "rm -rf /". He then proceeded to open the box, take out the disk (turned out there was only one), and give it to me. He then took the box (sans disk) with him and left.

This story is fraught with subtle ironies, not least of which is the amount of trouble Company X went through to prevent us from stealing their software, only to leave it with us in a pretty easily recoverable form (to say nothing of the fact that in the interim we had actually purchased the product, so if we wanted to open it up and steal their software nothing would have prevented us from doing so).

But the most worrisome aspect of this story is that apparently, among many dozens of customers who evaluated the product, I was the only one to raise any security concerns. Company X's attitude throughout the whole affair was, essentially, "Gee, we never thought of that. No one else ever complained." (And Company X has a reputation for technical savvy.)

So I'm off to go through Company X's dumpsters. I expect to be

able to
retire off what I find there.

✶ Man trapped for hours by payphone

<msb@vex.net (Mark Brader)>
Tue, 18 Nov 2003 14:36:33 -0500 (EST)

A man in East St. Louis got his middle finger stuck in a payphone's coin-return slot. Fortunately, this also meant that when he realized he needed to call 911, there was a payphone conveniently... *at hand*. Eventually the phone was removed and taken, with the victim, to a hospital emergency room where doctors managed to pry them apart.

See e.g. <<http://www.guardian.co.uk/uslatest/story/0,1282,-3402400,00.html>>.

[This is known as giving him the finger back. An overzealous knee-jerk response to this episode might be to get rid of the few payphones that remain. PGN]

✶ Debian security breach and forensic analysis

<Gerrit Muller <gerrit.muller@embeddedsystems.nl>>
Wed, 03 Dec 2003 12:41:24 +0100

The text below was send to me by Auke Jilderda. The original e-mail is from the debian mailing list.

This is a very readable and interesting case description of an intrusion of a software repository.

The Debian Project
[debian.org/](http://www.debian.org/)

<http://www.>

Debian Investigation Report
press@debian.org
December 2nd, 2003

Debian Investigation Report after Server Compromises

The Debian administration team and security experts are finally able to pinpoint the method used to break-in into four project machines. However, the person who did this has not yet been uncovered. The package archives were not altered by the intruder.

The Debian administration and security teams have checked these archives (security, us, non-us) quite early on in the investigation and re-installation process. That's why the project was able to open up the security archive again and confirm that the stable update (3.0r2) wasn't compromised.

[Truncated for RISKS. See <<http://www.debian.org/>> for the complete report. PGN]

[Re: Security patching: a story from the trenches \(Rex Black, R-23.03\)](#)

<Walter Dnes <waltdnes@waltdnes.org>>
Sat, 15 Nov 2003 16:49:17 -0500

A more accurate subject would be "Risks of updating Internet-insecure computers via the Internet". Rex Black had a computer that was not secure to connect to the Internet. So he connected to the Internet in order to download patches secure the computer; what's wrong with this picture ?

Browsing through my router logs, I see approximately 3 hits per minute on port 135 today, i.e. approximately one every 20 seconds. The Blaster patch is 918576 bytes, which would take 3 minutes to download on a v90 dialup. A 33.6 dialup will take approximately 4 minutes. During this timespan he would get 9 to 12 hits on port 135, and be COM-promised (sorry) long before the download was complete.

This is prime example of why he needed yet another computer, preferably with a different enough OS that it is not vulnerable at the same moment. I downloaded the Blaster patch from Microsoft's website using Mozilla Firebird on a linux Machine. A Mac running Safari would probably have worked just as well. The patch is small enough to fit on a floppy and could have been moved to the laptop that way.

Even if the patch was too large for a floppy, he could've used another computer to check Norton's and/or Microsoft's website, and find out which ports to block to temporarily protect himself whilst downloading the patch.

So much for criticism, what solution do I offer? I suggest a "safe mode"

Internet connection option be available for these situations. It would require stateful firewalling that would, by default, reject *ANY* packets from IP addresses and ports that the machine had not initiated a connection with. Actually, it wouldn't be a bad idea for the average home user 100% of the time. The only holes normally necessary to allow in the firewall would be for...

- * NETBEUI for other *LOCAL* machines; *NOT* including machines on the Internet side of the connection
- * Active-mode mode FTP initiates a second connection back to the client. Stateful firewalling can handle this.

Other exceptions would be to allow file-sharing over a VPN. If the user feels *REALLY* confident and adventurous, allow external connections for P2P applications.

⚡ Dangerous looking e-mail from quickbooks

<Kyle York <kyork@cisco.com>>
Wed, 19 Nov 2003 16:00:46 -0800

I just received an e-mail from quickbooks that my credit card information was soon to expire and I should immediately call a toll-free number to renew it. A quick look at the headers made me immediatly suspicious:

```
Received: from mta1.primary.ddc.dartmail.net ([146.82.220.34])
  by **my machine** with esmtp (Exim 3.35 #1 (Debian))
  id 1ALnfP-0005xu-00
  for <**me*>; Mon, 17 Nov 2003 10:00:03 -0800
```

X-MID: <Kilauea73191-16006-99081021-3@flonetwork.com>
Date: Mon, 17 Nov 2003 13:01:21 -0500 (EST)
Message-Id: <Kilauea73191-16006-99081021-3@flonetwork.com>
From: QuickBooks Payroll Services
<quickbookspayrollservices@offers.quickbooks.com>
To: **me**

Subject: QuickBooks Critical Notice - Credit Card Expiration
Reminder

Note the two relays, and how the From: line doesn't match the
Message-Id.

Both flonetwork.com and ddartmail.net are aliases for doubleclick.
net which

made me even more suspicious. In the body of the e-mail was a
toll-free
number that doesn't appear anywhere on www.quickbooks.com.

It turns out this was legitimate e-mail, but given the number of
scams how

many people would really pay attention if it wasn't? And how
many spam

filters would have kicked it out due to the problems noted?

Re: In-Security clearance ([RISKS-23.04](#))

<hellsop@ninehells.com (Peter H. Coffin)>

Fri, 28 Nov 2003 19:50:32 -0600

I would be greatly interested to learn if this installer
referenced by the
unknown submitter is the same "Netopsystems FEAD Recomposer"
which is used

to package Adobe Acrobat Reader version 6. There are a
nontrivial number of
reports (both on the web and on USENET) of the installer failing
to work on

many Windows 2000 machines, usually with the same "hourglass
then nothing

apparently has happened" symptoms, but has also various other reported issues, such as leaking memory and creating CPU loops sufficient to require hardware resets of the computers running the installer, in addition to more trivial assumptions like listing Windows 2000 as supported but only actually supporting Service Pack 2 of Windows 2000.

If it is this same installer, this would be extremely interesting for use as an installer for a security clearance application submitter for the US. The FEAD system is published by Netopsystems AG, Berlin, Germany.

http://www.netopsystems.com/site/english/fead_e.html

[Added in archive: The program in question is reportedly called the Electronic Personnel Security Questionnaire (EPSQ). PGN]

Re: Amber Alert, Coming to the Inbox Nearest You (Mercuri, R-23.04)

<Timothy Knox <tdk@thelbane.com>>
Fri, 28 Nov 2003 15:55:54 -0800

One other response, that I have used to some good effect, is to find the hoax details on an urban legends website (I personally recommend <<http://www.snopes.com/>>) and reply-to-all with the URL. It may not stop them all (there are none so blind as those who will not see), but it does help some. At least one person wrote me back, thanking me for pointing them to the site.

🔥 Re: Cehck tihs out! ([RISKS-22.91](#))

<"Rodney Hoffman" <rodney@oxy.edu>>

Fri, 28 Nov 2003 14:59:16 -0800

Matt Davis at Cambridge has posted a response to this:

"Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mtt aer in waht oredr the ltteers in a wrod are, ..."

See <http://www.mrc-cbu.cam.ac.uk/~matt.davis/Cmabrigde/>

where Davis says, "I've written this page, to try to explain the science

behind this meme. There are elements of truth in this, but also some things

which scientists studying the psychology of language (psycholinguists) know

to be incorrect. ... To my knowledge, there's no-one in Cambridge UK who is currently doing research on this topic."

The page also includes samples in many other languages.

🔥 ANNOUNCE: New mailing list for secure application development, SC-L

<"Kenneth R. van Wyk" <Ken@KRvW.com>>

Sun, 30 Nov 2003 16:22:57 -0500

I would like to announce the availability of a new and free resource to the

software security community, the SC-L e-mail discussion forum. The moderated

forum is open to the public. The group's purpose is, "to further the state of the practice of developing secure software, by providing a free and open, objectively moderated, forum for the discussion of issues related to secure coding practices throughout a software development lifecycle process (including architecture, requirements and specifications, design, implementation, deployment, and operations)." (The complete text of the group's charter, including its acceptable and unacceptable usage policies, can be found at <http://www.securecoding.org/list/charter.php>.)

To subscribe to the list, simply connect to <http://www.securecoding.org/list> and follow the directions on the form. Submissions should be sent (by subscribers only) to sc-l@securecoding.org.

Ken van Wyk, Moderator, SC-L mailing list ken@securecoding.org



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 6

Tuesday 9 December 2003

Contents

- [Electronic car doors trap man in Australian flood, nearly drown him](#)
[Tony Healy](#)
- [New official self-service litigation system available in England/Wales](#)
[Tony Ford](#)
- [Software paraphrases sentences](#)
[Justine Roberts](#)
- [The Eight Fallacies of Distributed Computing](#)
[Peter Deutsch via Roger Z](#)
- [Human Factor?](#)
[Dave Brunberg](#)
- [This number's ready for prime time](#)
[NewsScan](#)
- [Re: Another large gas bill](#)
[Tom Hayhurst](#)
- [Big money on the line, but no source code...](#)
[D G Rossiter](#)
- [Nevada to apply slot-machine security to e-voting hardware?](#)
[David Brunberg](#)
- [Re: Diebold ATMs hit by Nachi worm](#)
[Russ Cooper](#) [Elinor Mills Abreu via Lillie Coney](#)

- [Voter-verified breadcrumb trail?](#)
[Dave Brunberg PGN](#)
 - [Voting machines](#)
[William Ehrich](#)
 - [Re: "In-Security clearance"](#)
[Eric Dobbs](#)
 - [Re: Real purpose behind In-Security clearance program](#)
[Daniel Suthers](#)
 - [Nigerian scams](#)
[Ted Lemon](#)
 - [The Internet and the right to communicate](#)
[Monty Solomon](#)
 - [The Structure of an Accident](#)
[William Langewiesche via Monty Solomon](#)
 - [REVIEW: "Linux Security Cookbook", Barrett/Silverman/Byrnes](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Electronic car doors trap man in Australian flood, nearly drown him**

<Tony Healy>

Thu, 4 Dec 2003 12:06:39 +1100

The driver of a Honda CRV 4WD found himself trapped in his stranded vehicle in recent floods in Melbourne, Australia. The electrically driven windows would not wind down since the electrical system was underwater and, for some reason, he couldn't open the doors either. This might have been due to the pressure of the water outside or to other artifacts of the electrical system failing.

http://www.news.com.au/common/story_page/0,4057,8052562%

[255E1702,00.html](#)

✶ New official self-service litigation system available in England/Wales

<Tony Ford <tony.ford@net.ntl.com>>

Sat, 26 Jan 2002 15:43:09 +0000

Today's **Daily Telegraph** carries a **potentially** disturbing report describing a new service, "Money Claim Online", whereby individuals and law firms (solicitors) can issue most simple legal proceedings (where a sum less than UK pounds 100,000 is claimed, = US\$140K)) and enforce judgments via a Web browser. The new service has been set up without publicity by the Lord Chancellor's Department, which runs the courts system in England and Wales. It seems that the system is accessible to the public now, although it has not been officially launched.

People using the service are (oddly) referred to as "customers" and there is a Customer Help Desk ...

The newspaper report is also viewable at this Daily Telegraph link on-line:

<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2002/01/26/nsue26.xml&sSheet=/news/2002/01/26/ixhome.html>

The service can be seen on-line at:

<http://www.courtservice.gov.uk/mcol/>

[CORRECTION IN ARCHIVE COPY RESULTED FROM on-line **Telegraph** change,

thanks to Trevor Zacks via Lindsay.Marshall. PGN]

No details are apparent of what measures are taken to validate the identity of the claiming party or prevent other gross miscarriages of justice but it would appear that the potential exists for significant trouble even though the site warns that "vexatious litigants" are not allowed to us it (these are people who have abused the litigation system in the past to such an extent that they have been declared "vexatious litigants", restricting their ability freely to issue legal proceedings).

PS: I am a lawyer myself, although I don't practise in this area .. but do work in-house for a large IT company ... these comments are offered purely in a personal capacity.

Tony Ford, Guildford, Surrey, UK MailTo:tony.ford@net.ntl.com

Software paraphrases sentences

<Justine Roberts <jr4939@itsa.ucsf.edu>>

Fri, 05 Dec 2003 07:48:00 -0800

"Software paraphrases sentences" is the headline of a long story by Kimberly Patch in the 3/10 Dec 2003 issue of Technology Research News. Worth a look. Although the research is presented as entirely benign and useful, I find its implications & goals rather scary, starting, perhaps, with the problem of student plagiarizers.

[http://www.trnmag.com/Stories/2003/120303/
Software_paraphrases_sentences_120303.html](http://www.trnmag.com/Stories/2003/120303/Software_paraphrases_sentences_120303.html)

⚡ The Eight Fallacies of Distributed Computing

<"r z" <roger@darkhorsemail.net>>
Tue, 09 Dec 2003 09:33:10 -0800

The Eight Fallacies of Distributed Computing
Peter Deutsch

Essentially everyone, when they first build a distributed application, makes the following eight assumptions. All prove to be false in the long run and all cause big trouble and painful learning experiences.

1. The network is reliable
2. Latency is zero
3. Bandwidth is infinite
4. The network is secure
5. Topology doesn't change
6. There is one administrator
7. Transport cost is zero
8. The network is homogeneous

[http://web.archive.org/web/20030208015752/http://java.sun.com/
people/jag/Fallacies.html](http://web.archive.org/web/20030208015752/http://java.sun.com/people/jag/Fallacies.html)

⚡ Human Factor?

<Dave Brunberg <DBrunberg@FBLEOPOLD.com>>
Wed, 3 Dec 2003 09:35:42 -0500

Seeing Mike Smith's review of "The Human Factor" reminded me of a phrase we have in the municipal water and wastewater treatment industry-- we refer to "The Bubba Factor."

Bubba is not merely human, he is the incarnation of Murphy's Law. Bubba doesn't bother to check that the tank's too full. Bubba caps off a pneumatic control line to a valve because he likes to operate it manually. Bubba figures that it's a good idea to change the plant's operating rate from 10% of capacity to 95% by manually making a step change in the feed pump setpoint. Bubba forgets that when the clarifier sludge overflows into the reverse osmosis system that you can't just let the daylight shift take care of it.

Most water/wastewater plants are not yet highly automated, and frequently, operators resist the trend to automate. Bubba's clever, and he always finds a way to break the fail-safe. In these situations, you walk a very fine line between making the plant so inflexible that operators cannot respond to unforeseen problems and giving Bubba a little too much latitude.

✶ This number's ready for prime time

<"NewsScan" <newsscan@newsscan.com>>
Wed, 03 Dec 2003 09:08:52 -0700

Michigan State University grad student Michael Shafer has

succeeded in identifying the largest known prime number to date, using a distributed computer network of more than 200,000 computers located around the world. The new number is 6,320,430 digits long and is only the 40th Mersenne prime to have ever been discovered (Mersenne primes are an especially rare breed that take the form of 2-to-the-power-of-P minus one, where P is also a prime number). Shafer was taking part in the Great Internet Mersenne Prime Search (GIMPS) project, when the new number popped up. "I had just finished meeting with my advisor when I saw the computer had found a new prime. After a short victory dance, I called up my wife and friends involved with GIMPS to share the great news," said Shafer. [*New Scientist*, 2 Dec 2003; NewsScan Daily, 3 Dec 2003] <http://www.newscientist.com/news/news.jsp?id=ns99994438>

[I suppose all of the contributors of machine time would be known as Mersenne-aries -- oxymoronically, because they were most likely unpaid.
PGN]

[Typo fixed in archive copy. PGN]

✦ Re: Another large gas bill (Shapir, [RISKS-23.05](#))

<tom.hayhurst@reuters.com>
Thu, 04 Dec 2003 13:25:52 +0800

> It's possible Mr Purdey has been charged for the gas used up

> during the explosion that destroyed his house." (*The Daily Telegraph*)

Good joke, but sadly not true. While there are many web pages that attribute this story to the *Telegraph*, it doesn't appear in their archives. A search of the Factiva news archives finds six references to Arthur Purdey in print, all in the comedy clippings sections of newspapers ("Girl floats out to sea on inflatable teeth; is rescued by man on giant lobster" and the like). The earliest reference, from a York local paper, in February 2003, gives no source, although the same publication attributes it to an unnamed Lancashire newspaper three months later. Subsequent appearances give the original source as the *Telegraph* three times and the *Bangkok Post* once.

[So it got more Bangkok for the buck in the latter paper. PGN]

⚡ Big money on the line, but no source code...

<D G Rossiter <drossite@twcny.rr.com>>

Thu, 4 Dec 2003 08:10:04 +0000

Not quite as important as electronic voting programs, but still with big consequences.

"In the College Bowl Race, the Crucial Players Are the Programmers".

Apparently, the Bowl Championship Series rankings, which determine which

lucrative post-season games a college can play, are partly determined by

computer rankings. The programmers refuse to give their

algorithms, let
alone their source code. One complains: "Now you want to look
under the
hood of my car" when asked about this; another says "The more
you specify,
the more you annoy the readers."

[*The New York Times*, 04 Dec 2003]

<http://www.nytimes.com/2003/12/04/technology/circuits/04foot.html>

⚡ Nevada to apply slot-machine security to e-voting hardware?

<David Brunberg <brunberg@zoominternet.net>>

04 Dec 2003 19:43:27 -0500

According to *The Reno Gazette-Journal* (link below), Nevada
Secretary of
State Dean Heller "plans to enlist the expertise of the Nevada
Gaming
Control Board to ensure the machines are secure and accurate."
The state
maintains strict control and oversight of slot machines,
presumably because,
as the state's most visible industry, gambling must be seen by
the public to
be untainted. One hopes that people will consider that getting
a fair shake
at the election box is at least as important as whether the
quarter slots
are on the up-and-up. Avi Rubin (Johns Hopkins University) said
he found
major security flaws with the system used by one of the
companies that is in
the running for a contract to provide voting machines across
Nevada.

<http://www.rgj.com/news/stories/html/2003/12/02/58202.php?sp1=3Drgj>

du=mbrella&sp3=3Dumbrella&sp5=3DRGJ.com&sp6=3Dnews&sp7=3Dnews_front

Re: Diebold ATMs hit by Nachi worm ([RISKS-23.04](#))

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

Sat, 29 Nov 2003 00:31:01 -0500

Lest we forget, this is the "Risks Forum", not some weekday morning kids show.

Steve Summit is "astonished" that a commercial product running on a Windows platform was affected by Nachi. This after how many months? This despite the fact that I could attribute problems with an infinite number of commercial IT products to the effect Nachi created? Oh, I'm sorry, but this is the "Risks Forum".

Are many here surprised that Diebold sold "default installations" of its product on a Windows platform which was improperly designed? Are many here surprised that people bought the equivalent of the "off-the-shelf" version?

Since they affirm the ATM was "infected", that means it accepted an inbound connection to TCP135. Now maybe some don't know, but I can see no reason why anything should be querying an ATM, for any reason, least of all via such a sensitive protocol. Now if you didn't know before, you may have learned from recent discussions about the August 2003 blackout, you don't query the

endpoint. It either tells you its status, or you assume its dead. Either way, you're in control. Do I want to control an ATM's status, or do I want it to explain its status to me? If I'm not getting expected information from such a front line device, I, as a backend server, am simply going to stop listening to it and page a tech. Not sending expected info, or sending unexpected info, denote a problem...send the technician. I can't think of a reasonable design that involves the backend sending uninitiated queries to the ATM, ergo, there's no reason the ATM was left listening for inbound TCP135 queries. That's a design problem, not a problem with the OS or its components.

That such devices are now placed on the same network as devices to which can be attached Nachi infected systems is, well, a problem. Its one thing to shut down ATMs because their backend servers can't be reached due to network congestion, its another thing to have an ATM compromised directly. Diebold's designed default installation clearly isn't intended to minimize risk, its intended to minimize support problems from customers who attempt to implement their product insecurely.

Imagine if they disabled inbound TCP135 attempts. During implementation they'd get a surge of support calls from less than qualified implementers claiming they couldn't connect to the ATM remotely in order to configure it...;-]

Bottom line, is the risk here just not the unfortunately common

risk that if
I'm stupid I can blame someone else for not telling me I was
stupid? If that
isn't the risk, then the risk is that commercial vendors still
allow me to
shoot myself in the foot, and the media could make such wounds
fester.

Russ - NTBugtraq Editor

⚡ Re: Diebold ATMs hit by Nachi worm ([RISKS-23.04](#))

<Lillie Coney <lillie.coney@acm.org>>

Tue, 09 Dec 2003 11:00:36 -0500

Computer security experts predicted more problems to come as
Windows
migrates to critical systems consumers rely on. Bruce Schneier
is quoted:
"Specific purpose machines, like microwave ovens and until now
ATM machines,
never got viruses. Now that they are using a general purpose
operating
system, Diebold should expect a lot more of this in the
future." John
Pescatore, an analyst at Gartner, agreed. "It's a horrendous
security
mistake," he said, of specific-purpose machines like ATMs
running Windows,
written for general purpose computers and for which Microsoft
Corp. releases
security fixes on a regular basis. "I'm a lot more worried about
my money
than I was before this." Diebold switched from using IBM's OS/2
on its ATMs
because banks were requesting Windows, said Steve Grzymkowski,
senior
product marketing manager at Diebold. [Source: Experts Worried

After Worm

Hits Windows-Based ATMs, Elinor Mills Abreu, Reuters, 8 Dec 2003; PGN-ed]

⚡ Voter-verified breadcrumb trail?

<Dave Brunberg <DBrunberg@FBLEOPOLD.com>>

Wed, 3 Dec 2003 09:23:42 -0500

The subject of e-voting has been hot of late (for very good reason) and many have pressed for the voter-verified paper trail. This may be a good first step, but could also be a serious insecurity of the false-sense-of-security type. When one votes for Joe Blow and gets a paper saying her vote went to Joe Schmo, she knows something went wrong. Neglecting the fact that election officials may not be required to address the discrepancy, this at least gives the voter the knowledge that the system is broken.

But what happens when you vote for Joe Blow and get a paper that says "Joe Blow"? Is there any guarantee that the vote for J.B. is registered on the disk, or over the network? What guarantee is there that no alterations occurred between the touchscreen station and the recording station? Or that the software in the station hasn't been compromised to change 10% of the votes for J.B. to J.S. before recording but after printing?

Once you get out of the actual voting station and the printer, what, if anything, guarantees that votes aren't swapped or dropped? And, for areas

where physical intimidation may be a factor, how can the voter be assured of anonymous voting when the printer spits out the name of their selections for anyone to see?

The next obvious solution will be to require independent auditing of open operating code for all voting systems. Can we do this without ensuring that we must have one programmer from each political party (and there are many) go over every single voting system? Can we be sure that the auditors are honest? Can we have multiple vendors or should we have a single, open design for every precinct in the country?

Why not just admit that e-voting cannot be made secure without adding in so much complexity that it becomes prohibitively expensive or self-defeating?

For simple punch-card systems, you could have a reader on site through which the electors would feed their cards. The reader would report their choices back to them through a private interface (e.g., the video replays used at U.S. football games). If there was a problem, the voter would be given a new card to punch again. Certainly, the readers could be compromised as well, but they could not actually change the punched votes. If enough voters found discrepancies, that precinct would be deactivated until the cause was found.

Voter-verified breadcrumb trail? (Re: Dave Brunberg, [RISKS-23.06](#))

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

Wed, 3 Dec 2003 14:42:46 PST

Responding to the above message by Dave Brunberg:

ONE. COUNT THE PAPER, and let the electronics appease the media only for an

UNOFFICIAL PRELIMINARY count. The official count would be paper.

(Vendor arguments that paper is unreliable are largely bogus. Vendor

arguments that their systems CANNOT have erroneous results are of

course COMPLETELY BOGUS, ignoring insider fraud, programming screwups,

and configuration errors. Instead, they tend to argue that no

"hackers" can break in, which is not the primary concern for polling

place voting -- although it would be a serious concern for Internet

voting.)

TWO. IF THERE IS A DISCREPANCY, the machine should be IMMEDIATELY DISABLED

for the duration of the election. No fooling around with machines

that indicate on the screen that your vote has been recorded for a

candidate you did not vote for, where you are told that it is an error

on the screen but is correct in memory -- as happened in Florida in

2002.)

THREE. Why have electronic voting machines at all? GOOD QUESTION. The

most compelling arguments are providing a nice voter

interface and
avoiding overvotes -- although we have reported cases of
blank
positions being counted as votes by miscalibrated optical
scanners (or
tampered ballots?), and there are also reports of chad
knocked out of
punchcards because of too-deeply-prescored chad slots,
suggesting that
some of the card-system overvotes are not the voters'
faults. But see
the next message from William Ehrich, which has been said
before but
is worth saying again. PGN

Voting machines

<William Ehrich <ehrich@mninter.net>>

Tue, 2 Dec 2003 02:59:53 -0600

All the technical people seem to agree that a voting machine has
to produce
a piece of paper for audit trail, and some feel that that piece
of paper
should be the primary record of the vote.

It seems an obvious extension of this idea to have the voter
simply mark the
piece of paper with a felt marker.

That is in fact how we have been voting here. [Minnesota. PGN]
It works well.

There is a counting machine at the voting place to count the
ballots. If I
don't trust that machine I can (in principle) recount them with
a different
machine or count them by hand.

There is a RISK in using a computer where it is not needed and can do more harm than good.

✶ Re: "In-Security clearance" ([RISKS-23.04](#))

<"Eric Dobbs" <edobbs@freemod.net>>

Tue, 2 Dec 2003 15:23:20 -0500 (EST)

Since I've had to use the EPSQ program that the author of the "In-Security clearance" article talks about, I understand his frustration. The process of finding, downloading and installing the program is rather Byzantine. In its defense, though, there's some rather carefully-thought-out access control and encryption used to protect the personal data that's entered into the program - see the link below for details.

<http://www.dss.mil/epsq/epsqfaq/epsqfaq13.htm>

It's a pain to use, however; the interface was designed using 16-bit Windows controls, so it looks horrid on anything newer than Windows 3.11, it can be rather unstable under Windows NT 4.0 and 2000 (better under XP), and the whole rigamarole of a website is a classic example of government IT in action.

✶ Re: Real purpose behind In-Security clearance program ([RISKS-23.04](#))

<Daniel Suthers <db_s__usenet@tanj.com>>

Sun, 30 Nov 2003 12:59:45 -0800

An unknown poster detailed the process for applying to the US government for a security clearance. After he followed all the steps, he was required to run a program on his PC which did... nothing.

It's not too hard to imagine that the program was assisting the clearance process by scanning the hard drive for signs of illicit activity or setting up a back door so the Feds could check it later. Of course, one would have to be paranoid to even imagine the US government doing such a thing in the name of national security.

I've noticed this trend in Federal programs. They expect us to accept the risk of running unverified programs on our PCs as a requirement for doing business with them. They have produced several "infection detection" programs that were released in executable form only.

Since the Patriot Act was passed, there is a very real risk that some of the computer programs supplied by government agencies are, in some way, spyware. I can imagine wording in the "acceptance agreement" that would waive your rights to privacy upon installation of the various programs.

I don't have a security clearance, and don't expect to need one, so you can include my name. :-)

⚡ Nigerian scams

<Ted Lemon <mellon@nominum.com>>

Sat, 29 Nov 2003 23:03:28 -0600

I think that many of the younger readers of RISKS are unaware that there is no need for an "addiction" or "mental illness" in the usual sense for someone to fall prey to these scams. All you really need is to be old, and to have the maladies of old age. A stroke, incipient Alzheimer's, whatever, and suddenly your mom or dad has been taken by the scammers, probably for everything they're worth. This really could happen to someone you love, and it's no joke.

⚡ The Internet and the right to communicate

<Monty Solomon <monty@roscom.com>>

Mon, 1 Dec 2003 22:51:18 -0500

by William J. McIver, Jr., William F. Birdsall, and Merrilee Rasmussen

The development of the Internet challenges traditional conceptions of information rights. The discourse surrounding these rights and the Internet typically deals with each right in isolation and attempt to adapt long established understandings of each right to the new technological environment. We contend there is a need to address information rights within a comprehensive human rights framework, specifically, a right to

communicate. This paper examines the development of a right to communicate and how it can be defined and implemented.

Contents

Introduction

Basis for a human right to communicate

Satellites and communication rights

Mass media mentality

UNESCO and the right to communicate

Politics and policy

Definition

National initiatives

Soft law

Communicative law

Opposition to a right to communicate

Conclusion

http://firstmonday.org/issues/issue8_12/mciver/index.html

The Structure of an Accident

<Monty Solomon <monty@roscom.com>>

Sun, 30 Nov 2003 04:30:47 -0500

The Structure of an Accident

Atlantic Unbound, 22 Oct 2003

William Langewiesche, the author of "Columbia's Last Flight," talks

about the fundamental problems within NASA that led to the space shuttle's demise.

<http://www.theatlantic.com/unbound/interviews/int2003-10-22.htm>

REVIEW: "Linux Security Cookbook", Barrett/Silverman/Byrnes

<Rob Slade <rslade@sprint.ca>>

Tue, 9 Dec 2003 08:31:39 -0800

BKLNSCCB.RVW 20031019

"Linux Security Cookbook", Daniel J. Barrett/Richard E. Silverman/Robert G. Byrnes, 2003, 0-596-00391-9, U\$39.95/C\$61.95
%A Daniel J. Barrett dbarrett@oreilly.com
%A Richard E. Silverman res@oreilly.com
%A Robert G. Byrnes byrnes@oreilly.com
%C 103 Morris Street, Suite A, Sebastopol, CA 95472
%D 2003
%G 0-596-00391-9
%I O'Reilly & Associates, Inc.
%O U\$39.95/C\$61.95 707-829-0515 fax: 707-829-0104 nuts@ora.com
%O <http://www.amazon.com/exec/obidos/ASIN/0596003919/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0596003919/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/0596003919/robsladesin03-20>
%P 311 p.
%T "Linux Security Cookbook"

In the introduction, the authors state that this is not a security text, but a list of practical and individual pointers for improving security in specific areas.

Chapter one covers how to take system snapshots with Tripwire, in order to detect changes that might indicate an intrusion or a virus. The establishment of a firewall, using the iptables and ipchains utilities, is dealt with in chapter two. Chapter three examines the control of access to various network services. Authentication techniques and infrastructures are detailed in chapters four and five. Protecting outgoing network

connections, files, and e-mail are described in chapters six, seven, and eight respectively. The material on testing and monitoring, in chapter nine, is the most extensive in the book, and provides a good introduction to Snort as well.

This is good, practical advice, and makes an excellent reference for anyone dealing with the security of Linux in a networked environment. In one sense the authors are right, for they stick to the nuts and bolts, without discussing security frameworks or theories. In another sense they are wrong: this text does what the "hacking" books only pretend to do. The authors of the genre of "Teach Total Idiots How to Hack and They Will Automatically Turn Into Security Experts" texts all imagine that they teach you how to harden/secure a system, but don't. This does.

copyright Robert M. Slade, 2003 BKLNSCCB.RVW 20031019
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

Volume 23: Issue 7

Thursday 18 December 2003

Contents

- [Remote-controlled trains](#)
[Bill Tolle](#)
- [Over-reliance on PowerPoint leads to simplistic thinking](#)
[NewsScan](#)
- [Japan's Mars probe goes off course](#)
[PGN](#)
- [Risk of a test message: Heated Training Session](#)
[Patrick Lincoln](#)
- [Voter information up for grabs](#)
[NewsScan](#)
- [Voting machine maker dinged](#)
[Lillie Coney](#)
- [Convicted felons worked for electronic voting companies](#)
[Susan Marie Weber](#)
- [Re: Diebold ATMs hit by Nachi worm](#)
[Drew Dean](#)
- [Re: Why have electronic voting machines at all?](#)
[Russ Cooper](#)
- [Proper understanding of "The Human Factor"](#)
[Don Norman](#)

- [April Fool's e-mail freed detained kidnapper](#)
[Lillie Coney](#)
 - [This number's ready for prime time](#)
[Mark Brader](#)
 - [Correction for RISKS-23.06](#)
[Trevor Zacks](#)
 - [Free lunch? Or double-or-nothing?](#)
[Rob Slade](#)
 - [REVIEW: "Effective Security Management", Charles A. Sennewald](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Remote-controlled trains

<Bill Tolle <Bill3849094@A-Buyers-Realty.com>>

Mon, 08 Dec 2003 16:10:19 -0600

A railroad worker was struck and killed by one of the locomotives he was operating by remote control from the Union Pacific rail yards in San Antonio, TX. [Source: AP item, *Houston Chronicle*, 8 Dec 2003]
<http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/2279855>

✶ Over-reliance on PowerPoint leads to simplistic thinking

<"NewsScan" <newsscan@newsscan.com>>

Mon, 15 Dec 2003 08:42:21 -0700

NASA's Columbia Accident Investigation Board has fingered the agency's over-reliance on Microsoft PowerPoint presentations as one of the elements

leading to last February's shuttle disaster. The Board's report notes that NASA engineers tasked with assessing possible wing damage during the mission presented their findings in a confusing PowerPoint slide so crammed with bulleted items that it was almost impossible to analyze. "It is easy to understand how a senior manager might read this PowerPoint slide and not realize that it addresses a life-threatening situation," says the report. NASA's findings are echoed in a pamphlet titled "The Cognitive Style of PowerPoint," authored by information presentation theorist Edward Tufte, who says the software forces users to contort data beyond reasonable comprehension. Because only about 40 words fit on each slide, a viewer can zip through a series of slides quickly, spending barely 8 seconds on each one. And the format encourages bulleted lists -- a "faux analytical" technique that sidesteps the presenter's responsibility to link the information together in a cohesive argument, according to Tufte, who concludes that ultimately, PowerPoint software oozes "an attitude of commercialism that turns everything into a sales pitch." [*The New York Times*, 14 Dec 2003; NewsScan Daily, 15 December 2003]

<http://partners.nytimes.com/2003/12/14/magazine/14POWER.html>

✶ Japan's Mars probe goes off course

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

Tue, 9 Dec 2003 13:48:28 PST

Nozomi ("hope"), Japan's first interplanetary explorer, went off course in attempting to orbit Mars, culminating a five-year journey. Efforts to salvage the mission have failed and the probe has almost run out of fuel, although the probability of a collision with Mars has reportedly been reduced from 1% to 0%.

<http://www.cnn.com/2003/TECH/space/12/09/japan.mars.ap/index.html>

⚡ Risk of a test message: Heated Training Session

<Patrick Lincoln <lincoln@csl.sri.com>>

Thu, 18 Dec 2003 07:34:38 -0800

According to an advisory issued on 17 Dec 2003 by the National Weather Service, "... the Earth has left its orbit and is hurtling towards the sun." The post on the National Oceanic & Atmospheric Administration's Web site continued: "Unusually hot weather will occur for at least the next several days as the Earth draws ever nearer to the sun. Therefore, an excessive heat watch has been posted." The release was a test message, erroneously posted by during a training session. The statement has since been removed.

<http://www.informationweek.com/story/showArticle.jhtml?articleID=17000138>

⚡ Voter information up for grabs

<"NewsScan" <newsscan@newsscan.com>>

Thu, 11 Dec 2003 10:23:45 -0700

Unbeknownst to most citizens, state officials are selling their voter-registration information to political candidates, nonprofit groups and data collectors who then combine it with census data, purchasing histories, credit reports and magazine subscription lists in order to fine-tune their messages or marketing pitches to specific constituencies, such as pickup truck drivers who subscribe to "Soldier of Fortune" or SUV drivers who buy lacy underwear at Victoria's Secret. And while some states limit sales to political groups, 22 states lack any criteria restricting who may purchase the information. "Voters fill out these forms in good faith, thinking the information they're providing is needed for the purpose of administering elections," says California Voter Foundation founder Kim Alexander. "Then they get phone calls or a knock on the door from campaign strangers who have a list of their personal data." Alexander says the information requested by many states, such as Social Security numbers and mother's maiden names, could easily be used for identity theft. The situation has become especially troubling since Congress passed the Help America Vote Act last year, which required that states develop a centralized, statewide voter-registration database, making it possible for third parties to collect huge amounts of data very easily. Alexander says the reason there's been no outcry against the practice is that "the people who ultimately decide how voter

data should
be allowed to be used are the politicians... Politicians need to
rein in
the laws, yet they're the biggest consumers of data." [Wired.
com, 11 Dec
2003; NewsScan Daily, 11 Dec 2003]
[http://www.wired.com/news/business/0,1367,61507,00.html?
tw=wn_tophead_2](http://www.wired.com/news/business/0,1367,61507,00.html?tw=wn_tophead_2)

⚡ Voting machine maker dinged

<Lillie Coney <lillie.coney@acm.org>>
Thu, 18 Dec 2003 09:53:56 -0500

California Secretary of State Kevin Shelley has said that
Diebold Elections
Systems could lose the right to sell electronic voting machines
in
California. State auditors found that Diebold distributed
software versions
in 17 counties that had not been certified by the state, and
that in 3 of
those counties (including Los Angeles County) the systems had
not been
approved by the Federal Election Commission. [Source: Voting
machine maker
dinged, Auditor says software wasn't approved Elise Ackerman,
*San Jose
Mercury News*, 17 Dec 2003; PGN-ed]

[And as noted here on various occasions, the FEC standards are
very weak
to begin with. Even the California certification process does
not require
any MEANINGFUL assurance that electronic machines record cast
votes
correctly. PGN]

✶ Convicted felons worked for electronic voting companies

<"SusanMarieWeber" <susanmarieweber@earthlink.net>>

Tue, 16 Dec 2003 22:30:58 -0800

Voter advocate Bev Harris alleged Tuesday that managers of a voting-machine subsidiary of Diebold Inc. included at least five convicted felons, among them a cocaine trafficker, a man who conducted fraudulent stock transactions, and a programmer jailed for falsifying computer records. The programmer, Jeffrey Dean, wrote and maintained a proprietary code used to count hundreds of thousands of votes as senior vice president of Global Election Systems Inc. Ohio-based Diebold purchased GES in January 2002. According to a court document released before GES hired him, Dean served time in a Washington correctional facility for stealing money and tampering with computer files in a scheme that "involved a high degree of sophistication and planning."

In January, Senator Barbara Boxer, D-Calif., will submit a bill requiring stringent background checks on all electronic voting company employees who work with voting software. The bill, which Boxer plans to introduce in January, would toughen security standards for voting software and hardware, and require touch-screen terminals to include printers and produce paper backups of vote counts by the 2004 presidential election.

[Source: Critics: Convicted felons worked for electronic voting companies

Rachel Konrad, Associated Press, 16 Dec 2003; PGN-ed]

<http://www.bayarea.com/mld/mercurynews/news/local/7507193.htm>

Also see

<http://www.wired.com/news/evote/0,2645,61640,00.html>

[And this story does not even mention Phil Foster, employee of Sequoia

Pacific, indicted for vote fraud, who was working in the back rooms

during the elections of Riverside County, November, 2000. smw]

[... or a bunch of other felony convictions related to voting. Of

course the risks of undetected errors and malicious misdeeds in voting

machines have been discussed for years in RISKS. It is encouraging

that more people are beginning to understand the risks. PGN]

✶ Re: Diebold ATMs hit by Nachi worm (Cooper, [RISKS-23.06](#))

<Drew Dean <ddean@csl.sri.com>>

Tue, 09 Dec 2003 15:50:42 -0800 (PST)

I find Russ Cooper's contribution to be symptomatic of the security

community's world view: security über alles. Yes, it may be more secure

if an ATM always initiates contact with the outside world, but it has major

impacts in manageability, and also opens up new threats.

Consider the following scenario: There's an ATM, indirectly connected to the

Internet, sitting in a shopping mall. It's 3am (local time -- always true

somewhere in the world), the mall is locked up tight, and there's a worm on the loose. Said worm is programmed to look for vulnerable ATMs, and cause them to dispense all the cash they hold. It would be a Bad Thing (tm) if the mall opens the next morning with cash scattered all over the floor. Observe that sending a service technician out is extremely expensive, and logistically difficult/impossible. It's both faster and cheaper for the bank's data center to remotely patch the ATMs from a central location.

Now, you can argue that the ATM should be polling the data center for patches, but that opens up an equivalent vulnerability: once the polled machine is compromised, it sends the patch(es) of the attacker's choice to the ATM, and we end up in the same situation. Of course, if the ATM is compromised, it might stop listening for updates. Partial failure of systems is always difficult to design for, and this example is no different.

I think a fair summary is that the real world is a messy place, with many different threats, and while sound bites may be satisfying to pronounce, they rarely solve the problem.

Drew Dean, Computer Science Laboratory, SRI International
[Similar comment from Ray Blaak. PGN]

⚡ Re: Why have electronic voting machines at all? ([RISKS-23.06](#))

<"Russ" <Russ.Cooper@rc.on.ca>>
Wed, 10 Dec 2003 05:09:05 -0500

Maybe I missed the comment, but it seems to me that one of the most compelling reasons for e-voting, getting more people out to vote, is being missed in these threads. Maybe voter turnout in the States is always >50%, it isn't here (Canada).

If an eligible voter can sit at home, take a couple of minutes, and register their preference in an election, there's a belief that a lot more people will vote. I fail to see how anything else could be as likely to increase voter participation.

I'm not minimizing the risks or cost involved in making such a scheme work securely, but in a country such as ours where people are broadly distributed, reducing the need for people to go to a polling station is highly desired.

Russ - NTBugtraq Editor

⚡ Proper understanding of "The Human Factor"

<"Don Norman" <don@jnd.org>>

Thu, 11 Dec 2003 12:15:00 -0600

[Warning: This is not a posting of some news item. It is an essay -- well, a lecture -- triggered by two recent RISKS postings, particularly because the second posting completely misunderstood the purpose of the first and

didn't bother to read the book which was being recommended.
And exhibited

an attitude on the part of designers that is the biggest risk
of all risks

-- because it is the kind of attitude that causes the very
problems the

RISKS group is designed to eliminate. DN]

If we assume that the people who use technology are stupid
("Bubbas") then

we will continue to design poorly conceived equipment,
procedures, and

software, thus leading to more and more accidents, all of which
can be

blamed upon the hapless users rather than the root cause -- ill-
conceived

software, ill-conceived procedural requirements, ill-conceived
business

practices, and ill-conceived design in general. This appears to
be a lesson

that must be repeated frequently, even to the supposedly
sophisticated

reader/contributor to RISKS.

It is far too easy to blame people when systems fail. The result
is that

over 75% of all accidents are blamed on human error. Wake up
people! When

the percentage is that high, it is a signal that something else
is at fault

-- namely, the systems are poorly designed from a human point of
view. As I

have said many times before (even within these RISKS mailings),
if a valve

failed 75% of the time, would you get angry with the valve and
simply

continual to replace it? No, you might reconsider the design
specs. You would

try to figure out why the valve failed and solve the root cause
of the

problem. Maybe it is underspecified, maybe there shouldn't be a
valve there,

maybe some change needs to be made in the systems that feed into

the valve.

Whatever the cause, you would find it and fix it. The same philosophy must apply to people.

Item. I predict that the municipal water and wastewater treatment industry is in for a series of serious accidents. Why? Because of postings like that of Dave Brunberg ([RISKS-23.06](#)). He was triggered by Mike Smith's recommendation for the book "The Human Factor" ([RISKS-23.04](#)), but without bothering to read the book. So he tells us of the "Bubba factor" in his industry, namely, the belief that operators (named "Bubba") are characterized by stupidity, laziness, and general ineptness. Brunberg complains that he must make his software work despite the incompetence of his operators: "you walk a very fine line between making the plant so inflexible that operators cannot respond to unforeseen problems and giving Bubba a little too much latitude."

No wonder we continue to have problems. It is this attitude of developers that cause the very problems they complain about. The book, the Human Factor, is in fact an excellent argument against Brunberg's point of view. In it, the author (Kim Vicente) points out that procedural demands, business practices that reward productivity and punish safety, and the inability of system designers to understand the real requirements on the plant operators are what leads to failure. Poor Bubba is yelled at by his bosses for slowing up production, penalized if he raises questions about safety. If he follows procedures, he can't meet production requirements. If he violates them --

which is what everyone is forced to do -- he is punished if an accident occurs. No matter that lots of other Bubbas have warned about that likelihood.

Let me also recommend the excellent "Field Guide to Human Error Investigations." Here, the author (Sidney Dekker) points out that the old view of human error is that it is the cause of accidents whereas the new view is that it is a symptom of trouble deeper inside a system. Alas, the "old" view is in actuality the current view, whereas the "new" view is still seldom understood. (The "new" view has only been around for 50 years, so I suppose we need to give it more time.). The Field Guide is about aviation, but it is very applicable to the waste industry as well -- and to hospitals, and emergency crews, and manufacturing plants, and any situation where accidents are being blamed on people.

The most serious RISK in all this is that people take the easy way out, blame the operator for incompetence, and then smile smugly from their air-conditioned office, far away from the plant. As long as this attitude persists, we will have bigger and bigger accidents.

DISCLAIMER (MILD). My strong recommendation for "The Human Factor" appears on the back jacket of that book and on my website. My equally strong recommendation for the "Field Guide" will appear on my website Real Soon Now.

Dekker, S. (2002). The field guide to human error investigations. Burlington

VT: Ashgate.

Vicente, K. J. (2003). The human factor: revolutionizing the way people live with technology. Toronto: A. A. Knopf Canada.

Don Norman, Nielsen Norman Group and Northwestern University
norman@nngroup.com <http://www.jnd.org>

[Two typos fixed in archive. PGN]

April Fool's e-mail freed detained kidnapper

<Lillie Coney <lillie.coney@acm.org>>

Thu, 04 Dec 2003 12:42:14 -0500

A Homeland department employee's prank e-mail prompted the release of an immigration agency detainee who had been convicted of kidnapping, according to the department's Inspector General. The unidentified detainee turned himself in to Immigration and Customs Enforcement deportation officers two days after his improper release. The employee sent an April Fool's e-mail to 16 ICE detention officers and supervisors advising them that the detainee's citizenship had been established with a Puerto Rican birth certificate, which authorized his release. At the end of the e-mail, the employee wrote, "Now about that bridge I'm selling. April Fools!" Nine minutes later, the employee sent a second e-mail that began by saying, "In case you didn't get to the end of my previous message, here's what really

happened today." The second message said that the detainee had been ordered deported to the Dominican Republic. A homeland officer who read the first prank e-mail but did not note the April Fools reference, and did not read the second e-mail, processed paperwork that authorized the detainee's release from a county jail on 2 Apr. [Source: Wilson P. Dizard III, Government Computer News (gcn.com), 28 Nov 2003; PGN-ed]

✦ This number's ready for prime time ([RISKS-23.06](#))

<msb@vex.net (Mark Brader)>
Tue, 9 Dec 2003 20:14:06 -0500 (EST)

Primes of the form 2-to-the-power-of-P would be *exceedingly* rare.
[Yes, ONLY ONE for P>0. PGN]
Fortunately, that's not what the New Scientist article actually says.
[MINUS ONE was inadvertently omitted from the parenthetical, and
has been added to the archive copy. Noted by many of you.
TNX. PGN]
[ANOTHER TYPO CORRECTED IN archive copy of THIS one. P>0.
Sorry. PGN]

✦ Correction for [RISKS-23.06](#) (via Lindsay Marshall)

<Trevor Zacks>
15 Dec 2003

New official self-service litigation system available in England/
Wales

link is (now) not

<https://www.moneyclaim.gov.uk/csmco/index.html>

but

<http://www.courtservice.gov.uk/mcol/>

corrected in the on-line version of the Telegraph at the
specified link.

[Also corrected in RISKS archives. PGN]

✶ Free lunch? Or double-or-nothing?

<Rob Slade <rslade@sprint.ca>>

Mon, 15 Dec 2003 13:11:27 -0800

Leave your cards in the car when you walk into McQuickFood, lest
you end up
paying for your neighbour's lunch. (We've already seen this
with SpeedPass,
have we not?)

CREDIT CARDS DO THE WAVE (From NewsScan)

MasterCard and American Express have been testing "contactless"
versions of
their credit cards that use an embedded RFID chip rather than a
magnetic
strip to store financial data. The cards can simply be waved in
front of a
reader to complete the purchase. "In some instances it's faster
than cash.
You're eliminating the fumble factor," says a MasterCard VP. The
company
plans to roll out its PayPass system next year, beginning in
fast food
joints and other venues where customers tend to be in a hurry.
Forrester

Research predicts it will take several years for the contactless cards to go mainstream, citing consumers' security concerns and unfamiliarity with the technology as impediments to change. (AP/Wired.com 14 Dec 2003)

http://www.wired.com/news/technology/0,1282,61603,00.html?tw=wn_tophead_7

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: "Effective Security Management", Charles A. Sennewald

<Rob Slade <rslade@sprint.ca>>
Tue, 16 Dec 2003 08:28:19 -0800

BKEFSCMN.RVW 20031006

"Effective Security Management", Charles A. Sennewald, 2003, 0-7506-7454-7, U\$49.95/C\$72.50

%A Charles A. Sennewald

%C 225 Wildwood Street, Woburn, MA 01801

%D 2003

%G 0-7506-7454-7

%I Butterworth-Heinemann/CRC Press/Digital Press

%O U\$49.95/C\$72.50 800-366-BOOK fax 800-446-6520 www.bh.com/bh/

%O <http://www.amazon.com/exec/obidos/ASIN/0750674547/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0750674547/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0750674547/>

[robsladesin03-20](#)

%P 395 p.

%T "Effective Security Management"

The preface makes clear that the author's major background is in the field of physical security. This is evident in places throughout the rest of the book, but much of the material is more broadly applicable.

The introduction presents a wonderful statement about management, that it is "the ability to create an environment in which other individuals willingly participate to achieve objectives."

Part one deals with general security management. Chapter one outlines some principles of organization, and provides an excellent overview of the basics of management. The physical security background shows in, for example, the assumption that demonstrating a "contribution to profits" is relatively straightforward and easy to quantify. The review questions at the end of the chapter are an adequate summary of the material, but provide no more than a simple reading check. Organizational structure, in chapter two, is based on the real world rather than theory. Sennewald notes the difference between formal and informal arrangements, as well as both the good and bad reasons that the two exist. Security's role in the organization emphasizes physical security, but chapter three also addresses non-traditional functions such as training, internal consulting, and executive protection. Chapters four, five, and six deal with the roles of, respectively, the security director, supervisor (emphasizing the chain of command), and employee (mostly stressing personal character and integrity).

Part two addresses security personnel management. Chapter seven, on hiring, is reasonable, but fails to provide useful guidance on avoiding common pitfalls in reviewing resumes and interviewing candidates. There is, for example, a heavy reliance on open-ended questions, which often backfire on interviewers since the responses tend to be so different that it makes the difficult task of judging between people even harder. The creation of a job description, in chapter eight, provides good pointers and a helpful outline. There are more complaints about how training is done poorly than suggestions about how to fix the problem in chapter nine. The material on discipline, in chapter ten, is good but not great. In regard to the motivation of employees, Sennewald presents the classic "Theory X and Theory Y" model, but chapter eleven is more concerned with pointing out the disadvantages of punishment and control (X) than with suggesting how to support employees (Y). Chapter twelve, on promotions, repeats many of the points of chapter seven. The vague look at communications, in chapter thirteen, is not necessarily helpful. The classic debate between employment of, or contracting out, security personnel is presented in chapter fourteen.

Part three considers operational management. Budgeting, in chapter fifteen, is a good start for those without a financial background, but gets bogged down in specific forms. The basics of risk management (albeit limited to physical security situations) is introduced in chapter sixteen.

Some expansion is given in chapter seventeen, but the content is generally duplicated, and I wonder why the chapters were split. Review and audit, renamed the security survey, is important, but chapter eighteen seems to be a not-completely-recycled magazine article. It seems odd to cover office administration, in chapter nineteen, but many physical security officers may have limited office background, so this might be quite useful. The discussion of policy and procedures, in chapter twenty, primarily deals with procedures. Chapter twenty one, on computers and security management, is the longest in the book, but is only a computer literacy article and addresses no specific security applications. Sennewald argues that statistics can be useful, but chapter twenty two does not provide much direction in their manipulation.

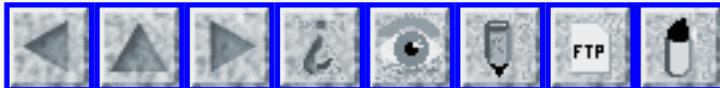
Part four deals with public relations. A pedestrian selling job for security is in chapter twenty three. The relationship with law enforcement, in chapter twenty four, emphasizes what the police can provide. Chapter twenty five promotes cooperation with those in the same industry and the importance of trade groups, as well as community service. This latter topic is expanded in twenty six. Chapter twenty seven is a very recognizable list of thirty two "jackass traits" for managers, pointing out all kinds of mistakes people can make. How to improve your performance gets less space, and it is hard to know where to draw the line between opposing problems,

such as "the Despot" and "The Popularity Kid."

Despite specific problems, this book provides some extremely valuable advice for security managers of all kinds, not just the physical security officers at whom it is aimed.

copyright Robert M. Slade, 2003 BKEFSCMN.RVW 20031006
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

Volume 23: Issue 8

Monday 22 December 2003

Contents

- [Railroad accident results from deactivated crossing gates](#)
[PGN](#)
- [Chats led to Acxiom hacker bust](#)
[Kevin Poulsen via Monty Solomon](#)
- [Moderation and Immoderation](#)
[PGN](#)
- [Re: Tragedy of the Commons](#)
[Douglas W. Jones](#)
- [Re: Proper Understanding of the Human Factor](#)
[Peter B. Ladkin](#)
- [Poor writing is the problem, not PowerPoint](#)
[Simson L. Garfinkel](#)
- [Why have electronic voting machines at all?](#)
[Finn Poschmann Sander Tekelenburg](#)
- [CFP: CyberCrime and Digital Law Enforcement Conference, Mar 2004](#)
[Michel E. Kabay](#)
- [Info on RISKS \(comp.risks\)](#)

➤ **Railroad accident results from deactivated crossing gates**

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

Mon, 22 Dec 2003 14:56:11 PST

An upgrade to the Caltrain guarded crossing system was designed by SRI many years ago, and has been very effective at diminishing road-rage by re-opening up the forward gates when trains are stopped in the station. For the past few years, the Caltrain folks have been upgrading the tracks, adding sidings to enable high-speed trains to pass. To do so, they have shut down passenger service altogether on weekends, turning off the crossing controls. However, the rails have been used to move the needed construction materials (roadbed, ties, rails, etc.), with flagmen posted as needed. However, at 11:30pm on Sunday, 14 Dec 2003, just a few blocks from SRI in Menlo Park, a truck struck a slow-moving train already 3/4 of the way through the crossing. Why this happened was not known.

[Source: *San Jose Mercury News* (Peninsula Edition), 16 Dec 2003, page 3B.]

🔥 Chats led to Acxiom hacker bust

<Monty Solomon <monty@roscom.com>>

Mon, 22 Dec 2003 00:26:43 -0500

Kevin Poulsen, SecurityFocus, 19 Dec 2003

A Cincinnati man who plead guilty Thursday to cracking and cloning giant

consumer databases was only caught because he helped out a friend in the hacker community. Daniel Baas, 25, plead guilty on 18 Dec 2003 to a single federal felony count of "exceeding authorized access" to a protected computer for using a cracked password to penetrate the systems of Arkansas-based Acxiom Corporation -- a company known among privacy advocates for its massive collection and sale of consumer data. The company also analyzes in-house consumer databases for a variety of companies.

From October 2000 until June 2003, Baas worked as the system administrator at the Market Intelligence Group, a Cincinnati data mining company that was performing work for Acxiom. As part of his job, he had legitimate access to an Acxiom FTP server. At some point, while poking around on that server, he found an unprotected file containing encrypted passwords.

Some of those passwords proved vulnerable to a run-of-the-mill password cracking program, and one of them, "packers," gave Baas access to all of the accounts used by Acxiom customers -- credit card companies, banks, phone companies, and other enterprises -- to access or manage consumer data stored by Acxiom. He began copying the databases in bulk, and burning them onto CDs. ...

<http://www.securityfocus.com/news/7697>

⚡ Moderation and Immoderation

<"Peter G. Neumann" <neumann@csl.sri.com>>
Mon, 22 Dec 2003 14:44:13 PST

Your RISKS moderator is absolutely mortified. After my silly OMITTED MINUS ONE gaffe in [RISKS-23.06](#) in the Mersenne prime item, I compounded it in [RISKS-23.07](#). (Thanks to all of you who responded.) I started out having typed $P \geq 1$ and did not like how it looked, and meant to change it to $P > 0$. Somehow I forgot to do so. In trying to keep many balls in the air at once, I unfortunately sometimes have to squeeze RISKS moderation in between handling the other balls. Having a ball sometimes becomes Halving a ball.

The "notsp" Subject line experiment has been a tremendous help in allowing me to separate the wheat from the chaff. Thanks to those of you who picked up on it. (I continue to get over 1000 spams a day that are caught by SpamAssassin, and many more that are not.) Nevertheless, I regret that I cannot put out more issues and include more of your would-be postings. On the other hand, if we had more RISKS issues, I would have to do with even more responses, and you all would have even more e-mail to read as well, so perhaps you should be happy I cannot devote more time to moderating. So moderation in moderating may be a good thing after all.

Incidentally, for those of you who have stumbled onto some of the annoying Majordomo glitches, I anticipate that RISKS will eventually be cutting over to Mailman -- which my lab is already using experimentally on other lists.

Let me take this opportunity to wish you all a risk-free holiday

season. PGN

✦ Re: Tragedy of the Commons (Norman, [RISKS-23.07](#))

<"Douglas W. Jones" <jones@cs.uiowa.edu>>

Thu, 18 Dec 2003 19:03:48 -0600

Science Magazine, 12 Dec. 2003, Vol 302, No 5652, has a set of articles on the Tragedy of the Commons, one of which is very relevant to us.

Tales from a Troubled Marriage:
Science and Law in Environmental Policy
by Oliver Houck, Pages 1926 to 1929

The section of this article that is most relevant to us is entitled: Four Cautionary Tales. There, he talks about how science has come to be used and abused in public policy debates surrounding environmental issues, but we're involved in a different public policy debate, and science is being used and abused here too. The 4 examples are:

"The lure of a return to scientific management" should be viewed with suspicion. There are attractive and rational arguments that favor iterative, impact based and localized management strategies instead of "unrealistic" one-size-fits-all policies. Several people spoke in these terms at the NIST meeting on voting systems Dec 10 and 11, urging incrementalism and arguing against top-down approaches that attempted to look at the big picture and overall system architecture.

"Good science" and "peer review" are sometimes invoked to set extremely high standards for the admissibility of scientific arguments that favor any change in current policy, but it is unusual to find such standards applied to the arguments favoring retention of the status quo. The head of the CS department at Kennesaw State cornered me recently using this argument against the Hopkins report on security flaws in Diebold's voting systems, despite the fact that the SAIC report had already come out confirming most of the flaws first reported in the Hopkins report; as far as he was concerned, the fact that the Hopkins report had not been subject to prepublication peer review was grounds for censure.

"The lure of money" has biased science. There are good studies of this in the health care field as well as the environmental field. Researchers with industrial funds are less likely to publish results that reflect negatively on their source of funds. Who is supporting the different scientists who have engaged in the voting systems debate? We ought to be very open about this. The conflict of interest stories that popped up after the release of the Hopkins report touch on this issue, illustrating the extent to which bogus conflicts can be as important here as real ones.

"The lure of the safe life" has led researchers to avoid drawing conclusions. We can do good science, confining ourselves to the technical and avoiding drawing conclusions that would engage us in public policy debate. Many of those on this list have elected to forgo this option, but

many of our colleagues may be more reluctant to participate. This is unfortunate and I think we need regular reminders. When outrageous claims are made for what computer science can do, or when utterly incompetent security audits are brought forward into the public debate, those who have technical qualifications should not stand by idly.

[Re: Proper Understanding of the Human Factor \(Norman, RISKS-23.07\)](#)

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Sat, 20 Dec 2003 09:37:34 +0100

In his argument for the view of Mike Smith ([RISKS-23.04](#)) and against that suggested by Dave Brunberg ([RISKS-23.06](#)) on Vicente's book *The Human Factor*, Don Norman invites us to consider two points of view on systems failure in which human operators are involved.

He suggests that 75% of accidents with such systems are blamed on operator error (in aviation, the generally-aired figure says accident reports attribute probable cause to pilot error in 70% of cases), and that the cause should be taken to lie rather in the system design which affords those kinds of errors. He points out that this view has been around for some half a century.

The other view is that of Brunberg, who gives hypothetical examples of the

"Bubba factor", according to which operators engage in typically human but, in terms of their professional skills and requirements, inappropriate behavior when operating a system.

Norman, prefers the first view. For example, it is a part of critical system design that hazards (defined as situations in which certain unwanted events, including accidents, are particularly afforded in some way or another) must be identified, and avoided or mitigated as far as possible.

The classic statement of the "Bubba factor" position is a comment made in 1949 by Edsel Murphy, an engineer on the USAF project MX191: Human Deceleration Tests, after observing some incorrect wiring that had led to failure of measuring equipment. If there was a way for one of the technicians to make a mistake, observed Murphy, that would be the way things would be done. Murphy's Law, as its successor has come to be known, is also half a century old [1].

So, Norman or Bubba?

I believe with Norman that more attention could be paid to the system affordances that encourage inappropriate operator actions or inactions. I also suspect that the operator's cognitive state is systematically underemphasised in most accident investigations, and consider proof of this claim to be a significant research project. Some progress has been made. Let me give four examples, based on a particular conception of human cognitive capabilities.

There are ways of defining an operator's "rational cognitive state" which do not depend on reconstructing his/her mental state, namely by looking at the information presented to the operator by the system and closing under simple inferences. This idea derives from (and may even be identical with) the "information theoretic" view proposed by Norman himself. One may consider such a state to be that of an ideal operator, and thereby somewhat unrealistic, but it suffices to highlight, in some significant cases, how a system afforded operator error.

Consider the "Oops" series of aircraft-simulator runs, in which researchers at NASA Ames Research Center set up scenarios for pilots of an MD-80-series flight simulator. The pilots were led to "bust" (fly through) their cleared altitude on climb. John Rushby has published what I consider to be a seminal paper, in which he used the Mur(phi) model checker to demonstrate that the pilot's "mental model" (what I called above the rational cognitive state) did not match the system state at a crucial point in the proceedings [1]. In other words, crucial information about the system was not presented to its operator. This is therefore a case in which the only prophylaxis is to design out the hazard situation. It amounts to a canonical example of Norman's contention.

Sidney Dekker gave the Tuesday Luncheon talk at the 21st International System Safety Conference in Ottawa in August 2003, in which he showed a series of still photographs of the views available to the pilots

of a Singapore Airlines B747-400, which attempted to take off from a closed runway in Taipei and collided with construction equipment. The accident was widely discussed in commercial aviation circles, particularly with respect to the ground guidance technology at the airport and the judicial treatment of the crew. Sidney's sequence of photographs gave me the impression that I would have made similar decisions in those circumstances to those which led to the accident (I am a pilot, though not a professional). This view had been promoted by some discussants since the accident, and I believe it is to be credited with keeping the crew out of jail.

A similar case of "seeing what the operator saw" is made by the series of photographs shown by Marcus Mandelartz of the signalling en route to the train derailment at Brühl in the Rhineland in Germany, in which a driver of an intercity train went through a switching points at something over three times the appropriate speed [3].

Finally, I have argued that the decision by the Russian pilot of one of the aircraft that collided over Lake Constance in July 2002 to descend in contravention of his ACAS "climb" advisory could well have been rational, given his "rational cognitive state" as defined above [4]. I also pointed out that all participants in that unfortunate affair, the two crews and the air traffic controller, had distinct "rational cognitive states", a situation engendered by a cognitive slip by ATC. I believe this situation

has been woefully incompletely analysed from the point of view of the ACAS system. To me, the situation represents a hazard that must be designed out or mitigated, as with any such system hazard. This view contrasts with that of, say, Eurocontrol, which advises that ACAS "resolution advisories" (RA) should be followed by pilots without exception, also a view propounded by many pilots. A more cautious view is expressed by the International Civil Aviation Organisation (ICAO), which advises that pilots should not manoeuvre against an RA, and an even more cautious view has been expressed by the UK Civil Air Authority, which advises that pilots should not manoeuvre against an RA without overwhelming reason. I believe the crew of the Russian aircraft had such reason, as shown by considering the "rational cognitive state" (I emphasise that the "rational cognitive state" is not to be identified with the actual mental state of the pilots, which we can no longer know). If so, only the UK CAA view is consistent with focusing on the system, and not the operator. This appears to me also to be a canonical example to which Norman's view applies.

All this argues for Norman's view. What is there to argue for Brunberg's?

Consider the following crude but general argument for the Bubba phenomenon.

Operators have responsibilities. They are intended to perceive certain partial system states and to devise actions which depend on those partial states. These actions are stipulated by procedures. In the case of some

systems, pilots flying airplanes for example, some of these actions and their consequences are unavoidably safety-critical. Human beings may freely choose their actions, and it is open to an operator of even the most carefully designed system, in such a situation, to choose an action which will lead to an unwanted event such as an accident.

One may contravene such an argument in commercial aviation only by advocating pilotless commercial aircraft, a prospect that fills not only some passengers but also some systems people like myself with dread.

To illustrate the situation which the argument highlights, consider an accident in November 2000 to a Luxair Fokker 50 turboprop on approach to Luxembourg Findel airport. The aircraft was on final approach using the ILS. The crew selected "ground fine-pitch" on the propellers while still airborne. This "low-speed fine-pitch regime [is] normally only usable on the ground" [5]. Control was lost, the aircraft crashed on approach, and most on board died.

An interlock prevents ground fine-pitch mode from being selected while the aircraft is airborne: power lever movement into this regime is inhibited. However, there was a known interlock failure mode in which the interlock does not function for some 16 seconds after the landing gear has locked down. A Notice to Operators concerning this phenomenon had been issued, and a system fix for this problem was available but had not been incorporated on the accident aircraft [5].

Activating ground fine-pitch while airborne is obviously a big no-no.

The big question is why this regime may have been selected. The report

has recently been issued [6]. It criticises the crew. "The captain put

the power levers into the beta range while trying to regain the glidepath

from above after beginning a go-around due to poor visibility, and then

reversing his decision - all without communicating with the first officer.

He had earlier begun what should have been a Category II [ILS] approach

without informing his colleague" [6]. The accident report says:

"All

applicable procedures as laid down in the operations manual were violated

at some stage of the approach" [6]. All this raises red flags to just about

everyone involved with flight.

The report "extensively questions the airline's hiring and training

practices" as well as noting that the "design [of the aircraft] did not

prevent the crew from selecting ground-idle while in flight - the final

error in a chain that led to the crash" [6].

The question. Norman or Bubba?, is ill-posed. Both Brunberg and Norman

overstate their cases. As Norman says, people are still too ready to fault

operators, even after 50 years. But operators must be allowed their free

will, otherwise one doesn't need an operator. It is open to operators

to freely choose wrongly, even catastrophically. And it happens.

PBL

References

[1] John Rushby, Using Model Checking to Help Discover Mode Confusions and Other Automation Surprises, in Reliability Engineering and System Safety

75(2):167-77, February 2002, also available from

<http://www.csl.sri.com/users/rushby/>

[2] Robert A.J. Matthews, The Science of Murphy's Law, in Peter Day, ed.,

Killers in the Brain, Oxford U.P. 1999.

[3] Marcus A. Mandelartz, Das Zugunglück in Brühl aus der Lokführerperspektive (The Train Accident in Brühl from the Perspective

of the Driver), in German, <http://www.online-club.de/~feba/br0.htm>

[4] Peter B. Ladkin, ACAS and the South German Midair, Technical Note

RVS-Occ-02-02, available from <http://www.rvs.uni-bielefeld.de>

[5] David Learmount, Propellers yield Lusair crash clue, Flight International, 26 November - 2 December 2002, p8.

[6] Kieran Daly, Luxair crew slammed in crash report, Flight International,

16-22 December 2003, p6.

Peter B. Ladkin University of Bielefeld, <http://www.rvs.uni-bielefeld.de>

✶ Poor writing is the problem, not PowerPoint (Re: [RISKS-23.07](#))

<"Simson L. Garfinkel" <slg@ex.com>>

Fri, 19 Dec 2003 11:47:02 -0500

Re: Over-reliance on PowerPoint leads to simplistic thinking

Having read about this in the report and some coverage in eWeek and

ComputerWorld, I need to argue that the real problem is not PowerPoint (as much as I dislike the program) --- the problem is that many engineers are simply poor verbal communicators.

> Because only about 40 words fit on each slide, a viewer can zip through a
> series of slides quickly, spending barely 8 seconds on each one.

This seems like poor rationalization. Here's what you can do with 40 words:

FALLING FOAM COULD DESTROY A SHUTTLE!

(hm; that's just six words.)

- * Falling foam has been clocked at faster than 500 mph
- * Impact with wing could destroy fragile ceramic tiles on launch
- * Repair not possible in space; shuttle would burn-up on re-entry

(that's another 30 words; total word count is 36)

I just finished a semester of paper grading in a class at MIT. Many of the students were really angry that I took off points for poor writing, improper citations, etc. "This is a class in computer security, not writing," one student told me (paraphrased).

I wrote a long e-mail back to that student that without the ability to write clearly, their security skills would be of little use.

✦ Why have electronic voting machines at all? ([RISKS-23.06,07](#))

<"Finn Poschmann" <finn@mail.org>>

Fri, 19 Dec 2003 15:42:20 -0500

Russell Cooper ([RISKS-23.07](#)) says that to raise voter turnout when people are broadly distributed, reducing the need for travel to a polling station is "highly desired" and a compelling reason for e-voting, and that this desired benefit is being neglected in common discussion.

In fact, in the e-government world, which is populated by hordes of promoters of e-democracy and e-everything else, there is much attention paid to the benefits of making voting easier. (Too much? I might note parenthetically that we should probably ask ourselves if we really want disinterested people to vote more often, but that would be a distraction.) In the endless rounds of worldwide conferences and discussion papers on e-governance and the "democracy deficit," what there is not enough of is attention to risks and costs.

We have difficulty in practice getting close to a verifiably accurate polling station implementation of e-voting, though as Rebecca Mercuri will tell you it is surely possible to do so. The risks and costs multiply when we contemplate e-voting from home.

Of course we can get *close enough* to an acceptably accurate and verifiable home-based system; after all, we use similar systems in financial

transactions representing many billions of dollars daily.
Encryption and
tunnelling protocols can be powerful tools.

Observations: 1) *Close enough* is nonetheless a long way off,
owing to
technical requirements and the concomitant need to raise voters'
comfort and
skill levels. 2) It will be expensive owing to equipment needs
on both ends,
where that equipment would not otherwise be necessary. 3) It
will be
intrusive. I should think we would want to know, while you hold
your eye to
the scanner and your finger on the pad sensor, that your true
voting wish is
being expressed. And what to do about the possibility that
someone is paying
you and watching your vote, or holding a gun to your head? I
don't know the
answer to that one, just as I don't know now why some US states
have so
enthusiastically adopted the mail-in ballot.

In any case, the costs of achieving a reasonably fair and
verifiable
e-vote-from-home are certainly large. What were the benefits
again?

[Remember, as other contributors have, that Internet voting
and other
remote voting schemes all suffer from the ability to sell your
vote --
along with all of the other problems of whom and what can you
trust. PGN]

[✶ Re: Why have electronic voting machines at all? \(Cooper, RISKS-23.06\)](#)

<Sander Tekelenburg <tekelenb@euronet.nl>>

Fri, 19 Dec 2003 08:41:53 +0100

[I may have missed a step in this thread, but the original subject seems to have been electronic voting machines vs paper voting. Somehow it moved to voting from the comfort of the home, which I think should be treated as a different subject.]

Wed, 10 Dec 2003 05:09:05 -0500, "Russ" <Russ.Cooper@rc.on.ca> wrote:

> Maybe I missed the comment, but it seems to me that one of the most
> compelling reasons for e-voting, getting more people out to vote, is being
> missed in these threads. Maybe voter turnout in the States is always >50%,
> it isn't here (Canada).

Technological security issues aside, it would mean giving up on secret voting. Not something to take lightly. Voting from the privacy of your home would make it even easier for people to force each other to vote for candidate x than the 'regular' abuse within the sacrecy of the home that's already happening on a grand scale. A public voting station, with secret voting, avoids that RISK.

While discussing the issues with electronic voting machines, and the suggestion that a paper trail would fix most of that, I ran into this. Some people seem to present that paper trail as a receipt: the voter gets to take it with her. That would mean people can force each other to prove they voted

for the candidate they were told to vote for. Dangerous. A paper trail is necessary (thus indeed: why electronic voting at all?), but it should not break secret voting.

[Almost all of the sensible proposals for voter-verified paper trails retain the paper within the system. Voters do not take them home.

However, David Chaum's proposal is somewhat different, allowing you to take a part of the audit trail with you from which you can verify your vote was correctly recorded.]

> I fail to see how anything else could be as likely to increase voter participation.

If voter's can't be bothered to go to a voting station, maybe it's healthier for society to leave it at that. You don't want utterly uninformed voters to vote, just for the sake of voting. You'll just get more votes for whoever happens to have the most likeable TV-face of the day... (No doubt some politicians see that too and are therefore in favour of e-voting...)

It would be nice to see more people participate. But I'm not sure what would be the way to make that happen. No doubt the causes and solutions will differ per country. In some countries better and more easily accessible education might help. But in countries that already have that you see many people still not voting. Sometimes as a (misguided) way of protest, sometimes because they think their one vote won't make a difference, sometimes because they feel

things are fine as they are.

> [...] in a country such as ours where people are broadly distributed,
> reducing the need for people to go to a polling station is highly desired.

Yes, different countries may need different solutions. In the (compared to Canada ;)) utterly overcrowded Netherlands a stroll to a voting station usually takes no more than 5 minutes. If that's too much work, then don't vote - and lose your right to complain about the government.

(In Dutch national elections turnout is around 70% on average I think. For EU elections it is something like 40% or even just 30%.)

Sander Tekelenburg, <<http://www.euronet.nl/~tekelenb/>>

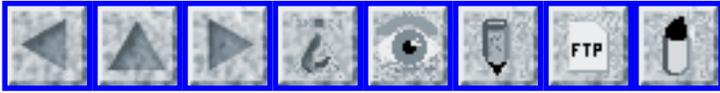
CFP: CyberCrime and Digital Law Enforcement Conference, Mar 2004

<"Michel E. Kabay" <mkabay@norwich.edu>>
Thu, 18 Dec 2003 14:57:15 -0500

Yale Law School's Information Society Project (ISP) invites you to the CyberCrime and Digital Law Enforcement conference, taking place on March 26-28, 2004 at Yale Law School.

Registration and further information are available at:
http://islandia.law.yale.edu/isp/digital_cops.htm

Nimrod Kozlovski, Fellow, Information Society Project, Yale Law School



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 9

Tuesday 23 December 2003

Contents

- [Rotorouted New Year's greeting?](#)
[PGN](#)
- [Loss of bus braking due to nearby illegally modified transceivers](#)
[Chiaki Ishikawa](#)
- ["Openness" in Government](#)
[Identity withheld by request](#)
- [GuineTel seeks ways of clamping down on scam fraud](#)
[Patrick O'Beirne](#)
- [AOL now filtering based on whether they like embedded URLs](#)
[Stever Robbins](#)
- [Guilt by technology](#)
[Dawn Cohen](#)
- [Murphy's Law](#)
[Mark Brader](#)
- [Important article on origins of Murphy's Law](#)
[Doug Mink](#)
- [Re: Railroad accident results from deactivated crossing gates](#)
[Geoff Kuenning](#)
- [Re: Proper understanding of "The Human Factor"](#)
[Merlyn Kline](#)

- [Poor writing is the problem, not PowerPoint](#)
[Paul A.S. Ward](#)
 - [Re: Diebold ATMs & Nachi worm; you ain't seen nuttin' yet!](#)
[Richard I Cook](#)
 - [Re: Diebold ATMs hit by Nachi worm](#)
[Tim Panton](#)
 - [Re: Voter information up for grabs](#)
[David E. Ross](#)
 - [Re: Online issue of civil claims](#)
[Robin Crorie](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Rotorouted New Year's greeting?

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

Tue, 23 Dec 2003 14:07:42 PST

Yesterday I decided to schedule in advance our annual home sewer cleanout derootification for 8 Jan 2004, to get the first call in the morning on the day that our yearly guarantee expires. The dispatcher assured me that would be fine and that they would call the day before to confirm. An hour later I received a call from the plumber saying that he would arrive in 10 minutes, and apologizing for taking so long!

You probably guessed what happened. The dispatcher put the order in for 8 Jan assuming that their scheduling system would infer 2004. But the system coerced the year to 2003, and it was treated as an urgent request (that had not been filled in 11.5 months).

Happy New Year!

⚡ Loss of bus braking due to nearby illegally modified transceivers

<Chiaki <ishikawa@yk.rim.or.jp>>

Sun, 21 Dec 2003 09:51:41 +0900

It has been reported widely in the Japanese press that electromagnetic interference caused by illegally modified transceivers on trucks is suspected of causing two accidents by disabling the braking system of commuter buses.

Mitsubishi Fuso Truck & Bus Corporation announced that two models of its buses are adversely affected by high-powered EMI from short distance and its braking system may not function properly under such conditions. Specifically, its breaking system that detects the wheel-locking condition falsely triggers due to the EMI and thus the brake doesn't work as intended.

Two accidents were reported last year where the bus drivers reported that the brake suddenly stopped working. However, after the police investigation, no visible malfunction was found.

The manufacturer continued investigation and found that high-powered radio signals emitted by a nearby transceiver (illegally modified and thus 1,000-10,000 as strong as permitted by law for such transceivers) can interfere with its braking control unit, resulting in false

information that the wheels locked due to braking. Upon this false information, it seems (my interpretation from what I read various reports) that the control unit decided to release the brakes, and thus caused unintended loss of braking.

It is not known whether such illegally modified transceivers were present nearby in two accident cases. But in other two instances where loss of braking was observed, the bus drivers saw suspicious trucks nearby.

The company could reproduce the condition in live experiments, and it will refit the 2200+ cars by replacing the control unit, sensors, pipes, circuit harness, etc. I think the company should be commended for its continued investigation after the accidents.

I have personally noticed voices of presumably truck drivers whose transceiver must have been modified to generate enormous amount of power from my audio equipment over the years. (Remember the CB radio craze of 1970's?) But this is the first time such strong emission is linked to real-world accidents. [I don't think so. We had CB interference knocking out cruise controls long ago. PGN]

The warning that I see and hear on airplanes during landing and take off is no longer a remote worry. I should be glad that most air runways seem to have enough distance from the nearby highway.

As we depend on computers and sensors for better control of *everything*

such as cars, home appliances, the malfunctions due to external EMI must be considered carefully, but I suspect that only the military agencies who have tried to harden the fighter planes and such against the EMI caused by nuclear blasts have the technical knowhow or mentality to cope with such problems caused by unusually and possibly illegally high-powered EMI.

(Yes, I know that the FCC regulations and similar usually protect the ordinary home appliances against the run-of-the-mill EMI from computers, etc. However, I doubt that electronic home appliance makers are ready to tackle the above the normal, high-powered emission caused by illegally modified transceivers. And they are a real threat along busy traffic route today. I hate to see various home appliances behave erratically every time a truck with such a transceiver passes by. Or for that matter, a whole field filled with tiny sensors blown by a strong zap of an illegally modified transmitter. Illegal or not, such dangers are going to be real and may have wide-spread consequences in the future.)

cf. The company web page:

<http://www.mitsubishi-fuso.com>

I found the reference to this topic in the Japanese web pages at above URL by following links, but am not sure if English pages have the reference.

The Japanese report appears dated 15 Dec 2003, so the translation may have to wait for a few more days.

✶ "Openness" in Government

<[Identity withheld by request]>

Tue, 23 Dec 2003 12:09:00 -0500

A while ago California, with the help of MCI, implemented an Internet based system, DROS, by which gun dealers verify that purchasers are eligible to own a gun.

While searching for information on this system, I happened across the following message

<http://caag.state.ca.us/firearms/mbw.htm>

which I found somewhat disturbing. However, looking further, I found the DROS users manual

<https://dros.vansis.wcom.com/wpsd/manual.pdf>

which tells the users to configure their Internet Explorer security settings as follows:

The ActiveX controls and plug-ins to Enable are
Download signed ActiveX controls
Download unsigned ActiveX controls
Initialize and script ActiveX controls not marked as safe
Run ActiveX controls and plug-ins

If these radio buttons are set to Prompt, you will be prompted each time you log into the application. Setting them to Enable is a time saving measure.

Although it is only the gun dealers' machines that are at risk, and the DoJ system is hopefully secure, I'm not sure that I like the idea that their

machines are so insecure.

✶ GuineTel seeks ways of clamping down on scam fraud

<"Patrick O'Beirne" <mail2@sysmod.com>>

Sun, 21 Dec 2003 19:37:31 +0000

By Brian King, Balancing Act's News Update 188 (21 Dec 2003)

<http://www.balancingact-africa.com>

Phantom Calls

In 2003, Terri Lockwood of Indianapolis, Indiana received a phone bill with hefty charges for calls to Guinea-Bissau, a West African country she had never heard of, and much less had reason to call. When she disputed the charges, the American operator AT&T told her that the calls were genuine, and that she or someone in her house must have called, or accessed an adult entertainment site on the Internet. The intruder was a program that had slipped unnoticed onto the family computer, and reconfigured the connection to dial a number in Guinea-Bissau (code 245).

The number, however, does not officially exist. The national operator, the regulatory body, and the International Telecommunications Union all agree that the number dialed from Terri Lockwood's computer is not programmed within the territory of Guinea-Bissau. Communications infrastructure of the country, furthermore, could not conceivably support the graphic-intensive

content production and broadcast of many adult entertainment sites. For the last few years the national operator Guine Telecom has been concerned with repairing basic telephony infrastructure damaged in a devastating civil war. At the beginning of this year Guine Telecom had no new cables to repair its network, no wires to install phones for clients, and approximately 50,000 people on waiting lists. This is not a company receiving revenue from a brisk adult entertainment business, legitimate or not, apparently conducted in its name.

The History

In 1989 the Government of Guinea-Bissau cemented a strategic partnership with Marconi (now part of the Portugal Telecom group) All international traffic to and from Guinea-Bissau would run through Marconi in Portugal. Marconi was also given the right to open and maintain bank accounts abroad in the name of Guine Telecom.

Critics of the company say that management of the company became increasingly chaotic and untransparent. Around 1996 Portugal Telecom managers set up a bank of computers at the earth station to receive pornographic calls from abroad. The calls were received at Guine Telecom and were immediately transmitted back without entering the national network. The practice reportedly generated significant new traffic to Guinea-Bissau, and the added revenue funded new investments in infrastructure.

On June 7, 1998 a failed coup d'etat tipped the country into civil war; key

infrastructure (such as the earth station) was destroyed and in the midst of it the bank of audiotext (read 'phone sex') computers.

After their departure in 1998 Portugal Telecom began withholding settlement payments for international calls terminating in Guinea-Bissau, and has continued to do so.

A journalist from the major Spanish newspaper El País confirmed a so-called 'epidemic' of calls to Guinea-Bissau from Spain, appearing on the bills of people who had no relationship with the country. In all these instances the Spanish operator Telefonica responded that the calls were genuine.

Around the same time, a dissatisfied Spanish pornography consumer actually called Guine Telecom to complain about the service. Technical Director Malam Fati was alerted, and so discovered for himself the existence of a number of web pages advertising live pornographic video. The pages appear to be designed to target particular countries; all are linked to a home page at www.sexhotel.com. The pages offer 'free' access to live pornographic video without requiring credit card information. Interested viewers need only to call a number on the screen (dialing instructions from each country are included), to receive a password. These access numbers bear the (245) international code, but the regional codes are not assigned within the territory of Guinea-Bissau.

For the rest of this story, go to:

<http://www.balancingact-africa.com>

Patrick O'Beirne, Systems Modelling Ltd., Gorey, Co. Wexford,
Ireland.
+353 55 22294

✶ AOL now filtering based on whether they like embedded URLs

<Stever Robbins <stever@private.verstek.com>>
Fri, 19 Dec 2003 12:02:41 -0500

I just got this bounce message. I was mailing a friend of mine
the URL of a
MOVEON.ORG Web site that's asking people to rate TV ads on
effectiveness,
etc., at conveying the downside of GW Bush's policies. AOL won't
even
deliver the message. Apparently, since the URL has generated
complaints
(presumably from Bush supporters or current Govt. employees),
I'm not even
allowed to tell AOL users about it.

RISKS: AOL can decide they don't like a particular URL, for
instance, of a
topic or candidate or public opinion poll that they disapprove
of, and voila
-- several million people now can't even be told about that
page! In this
particular case, it's hard to imagine who would complain about
it other than
people trying to get the page banned because it doesn't agree
with their
political views.

The offending URL (which I highly recommend) is double-u, double-
u,
double-u, bush in 30 seconds dot org.

> ----- The following addresses had permanent fatal errors

><.....@aol.com>

> (reason: 554 TRANSACTION FAILED: (HVU:B1) The URL
contained in your
> email to AOL members has generated a high volume of
complaints.?? Per our
> Unsolic)

✂ Guilt by technology

<"Dawn Cohen" <COHEND@wyeth.com>>

Tue, 23 Dec 2003 09:28:47 -0500

A friend was inspired by his sister, who just got an MP3 player installed in her car. He wanted to do the same.

He called the Mercedes dealer that he normally goes to, and asked if they could fit his car up with an MP3 player. He was politely informed that they could not. Undaunted, he asked whether an MP3 player could be installed if he was willing to put in a whole new stereo system. The gentleman on the line patiently explained that No, Mercedes does not make MP3 players available in any of their cars, new or old. As he put it, "MP3s are for people who download music. People who buy Mercedes cars can afford to buy their music."

✂ Murphy's Law (Re: ...the Human Factor, Ladkin, [RISKS-23.08](#))

<msb@vex.net (Mark Brader)>

Tue, 23 Dec 2003 00:51:11 -0000

> The classic statement of the "Bubba factor" position is a
comment made
> in 1949 by Edsel Murphy ...

Um, the Edsel was a *different* classic failure.

Edward Murphy's exact words have been forgotten, and credit for
the
term "Murphy's Law" is now disputed. For a full investigation,
or at
least as good a one as we're likely to see after so many years,
see:

[http://www.improb.com/airchives/paperair/volume9/v9i5/murphy/
murphy0.html](http://www.improb.com/airchives/paperair/volume9/v9i5/murphy/murphy0.html)

and the four pages linked from it (or substitute 1 through 4 for
the 0).

Mark Brader, Toronto, msb@vex.net

[↗ Important article on origins of Murphy's Law \(Re: Ladkin, R-23.08\)](#)

<Doug Mink <dmink@cfa.harvard.edu>>

Tue, 23 Dec 2003 14:22:49 -0500

> The classic statement of the "Bubba factor" position is a
> comment made in 1949 by Edsel Murphy, ...

I have seen numerous references to Edsel Murphy as the
originator of the
famous law, but this was the first reference with more details.
"Edsel"

seemed to me to be too uncommon to be associated with both a humorous failure of an automobile (and the scion of major manufacturing family) and a humorously successful law, so I looked into the matter on the Web. After several unsuccessful searches, I hit the jackpot with Nick Spark's article, "The Fastest Man on Earth", on the September/October Annals of Improbable Research, and available on their web site, HOT A.I.R.

<http://www.improb.com/airchives/paperair/volume9/v9i5/murphy/murphy0.html>

It gives a very good history of the relationship between Colonel John Paul Stapp (once the Fastest Man of the title), Project MX981, Captain *Edward* Murphy, and the famous Law, and is must reading for RISKS readers who daily do battle with the consequences of Murphy's Law.

Doug Mink, Smithsonian Astrophysical Observatory

✶ Re: Railroad accident results from deactivated crossing gates

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

Tue, 23 Dec 2003 00:15:36 -0800 (PST)

A friend once told me that in the Great Plains there are many accidents of this sort each year. Most crossings are completely unguarded, and at night a train on an unlit level crossing is almost completely invisible.

The friend pointed out that the cure is both trivial and cheap: all railroad

cars should be required to have reflectors (or reflective paint) on the sides. But it would cost a lot of money (in aggregate, though very little per \$100K car) and thus the railroads have steadfastly resisted the passage of any such regulation. Meanwhile, people continue to die.

The funny thing is, that reflective paint could be used for some very valuable advertising...

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

[Ah, another nice low-tech solution. PGN]

Re: Proper understanding of "The Human Factor" (Norman, [R-23.07](#))

<"Merlyn Kline" <merlyn@zyweb.com>>

Fri, 19 Dec 2003 10:28:27 -0000

> No wonder we continue to have problems. It is this attitude of developers

> that cause the very problems they complain about.

Isn't this a bit reversed? Yes, developers complain that they must devote more effort than they would like to ensuring that their software works in the face of operator-generated adversity. But in making that complaint they are recognising the requirement. And it *is* a requirement.

As if to underline all this, what is the very next story in the digest I am responding to?...

> A homeland officer who read the first prank e-mail but did not
note the
> April Fools reference, and did not read the second e-mail,
processed
> paperwork that authorized the detainee's release from a county
jail on 2
> Apr.

Could a system have been devised that would have prevented that?
Could such
a system have been embodied in the administrative software that
is
(presumably) used to run these processes?

✶ Poor writing is the problem, not PowerPoint (Garfinkel, Re: [R-23.08](#))

<pasward@tolstoy.uwaterloo.ca (Paul A.S. Ward)>
Tue, 23 Dec 2003 05:13:55 +0000 (UTC)

> the problem is that many engineers are simply poor verbal
communicators.

Without disagreeing with the above statement (Heaven knows, I've
read enough
poorly-worded documents by students to be firmly convinced of
this point), I
would argue that PowerPoint, and moreso WYSIWYG systems, are a
contributing
factor. Specifically, WYSIWYG systems lead to a focus by the
user on
appearance, not on structure or content.

✶ Re: Diebold ATMs & Nachi worm; you ain't seen nuttin' yet! ([R-](#)

23.04)

<Richard I Cook <ri-cook@uchicago.edu>>

Tue, 23 Dec 2003 06:04:56 -0600

Steve Summit wrote in [RISKS-23.04](#) about "several Diebold Automatic Teller machines...built atop Windows XP Embedded...infected by the "Nachi" worm last August and his concern about "critical functions [being] implemented using less-than-rugged components such as "consumer grade" operating systems."

It is interesting that, even at this rather advanced stage, we have so little 'feel' for the ways in which creating large, dependent socio-technical systems creates new -- and often startlingly large -- vulnerabilities. To describe an operating system as "consumer grade" implies that there are real alternatives available. But there are few such alternatives. New applications depend on the rich feature sets found in large operating systems and the problems with security and reliability of these are well known, albeit not well understood. A good deal of this seems to me to be related to version control and maintenance activities and the corrosive nature of the cost equation -- we have these systems, after all, because they are cheaper, not because they are more reliable!

ATMs are IMHO small potatoes. The U.S. Institute of Medicine has just released "Patient Safety: Achieving a New Standard for Care" (<http://www.iom.edu/report.asp?id=16663>) which continues the IOM's theme of

making safety through the creation of higher orders of computing systems -- basically an everything-is-connected-to-everything sort of model in which the entire process of healthcare delivery is mediated using computers in networks -- by outlining the needs for standards for data communications between systems. The rosy future is a world where your physician (or some robotic analog) 'writes' a prescription into a computer and there is nothing human in the way until the pill pops into your open mouth. Comparatively little attention has been paid to what the actual operating characteristics of a system composed of 106 Windows machines of 10^3 or 10^4 configurations running 10^8 to 10^9 lines of code might be.

I foresee an era when this trend is reversed and we deliberately uncouple systems into smaller, isolated subsystems; where software change is deliberately retarded in the hope of achieving stability; where end-to-end automated processes are broken apart and human intermediaries inserted in an effort to produce robust behavior of the larger entity; and where security and privacy issues drive large parts of the healthcare system completely 'off-line' so as to make them 'invisible'. Because healthcare reimbursement from Federal and insurance sources will be tied directly into on-line record keeping and so-called "quality measurement" computing, portions of healthcare delivery will be paid for out-of-pocket, essentially dividing the system into the "white" (visible, regulated, tabulated, on-line) system and the "black" (off-line, cash-and-carry, AMFYOYO) system. In

addition, you may find springing up a cottage industry of configurators, people capable of making your small, independent, unconnected, archaic, but quite useful computer nets working without connecting them to the larger world.

"Burning chrome" here we come!

🔥 Re: Diebold ATMs hit by Nachi worm (Dean, [RISKS-23.07](#))

<Tim Panton <tpanton@attglobal.net>>

Fri, 19 Dec 2003 9:00:00 0000

Drew Dean describes the tendency of 'security professionals' to focus on their specialty and not on the what might be called the "bigger picture".

It seems to me that there are two ways to fix this problem. The first is to spread the awareness of security in the programming community, de-specializing it and making it a core competence expected from designers. (we have made a small step here in this direction by making risks compulsory reading for all software engineers)

The second way is for managers to incorporate computer security into their analysis of business risks when developing or adopting a new product (again de-mystifying it).

As an aside, I don't quite buy Drew Dean's analysis of the ATM situation.

ATMs require frequent human intervention, to fill them with cash. This puts them in a different category from fully autonomous systems, like

weather

stations or unmanned space craft, where being able to force an upload of patches without onsite intervention is clearly "a good thing".

I think the thing that shocks me about the ATM story is the reliance on stock protocols with apparently no more security than I apply to my desktop systems. I mean, why not configure it to only accept signed updates, or only updates from a shortlist of ip addresses?

Yes, the world is a messy place, but I think I like the emerging computing monoculture even less.

✶ Re: Voter information up for grabs

<"David E. Ross" <david@rossde.com>>

Fri, 19 Dec 2003 07:52:32 -0800

Selling voter information to candidates is a very old situation. And it's not necessarily bad. (The lists are sold and not given away only because of the cost of printing them; the same is true of lists sold in electronic form.)

Early on, the lists were available to anyone. With the increased concern about privacy, they are now available only to legitimate candidates and campaign committees.

When I ran for local school board in the late 1970s and through the 1980s, I bought voter lists from the Registrar of Voters for 25c a page.

That
allowed me to focus my door-to-door campaign on homes where
actual voters
lived.

In a neighboring city, a city council candidate used her list to
challenge
illegally registered voters, individuals who registered from
their business
addresses (inside the city) instead of their residential
addresses (outside
the city, some in a different county) as required by California
election
law. Only persons who registered within the city were eligible
to vote in
the city council election. Some business owners perceived her as
anti-business and wanted to vote against her. (She won anyway,
served
several terms, and is now in the State Legislature.)

At each election, the lists are posted outside the polling
places for public
inspection. Anyone can review these lists and write down (or
photograph)
their contents.

I can drive to the county recorder's office. There, I can
review the lists
of property owners and the assessed values of their homes. I
can browse
through all the recordings of liens, quit-claims, and title
changes. Some of
those recordings also include wills and other declaratory
statements.

The point is: Some records of personal information are indeed
public. They
have been public in paper form for over a century. The fact
that they are
now public in electronic form is not necessarily bad. Bad uses
of these
data occurred before computers, and bad uses occur now. Laws
against those

bad uses may be older than the computer. While I am very concerned about privacy (and upset about the new federal law that invalidates the stronger California privacy law), I feel that privacy concerns should not eliminate the public availability of what have traditionally been public records.

David E. Ross <<http://www.rossde.com/>>

✶ Re: Online issue of civil claims ([RISKS-23.06](#))

<Robin.Crorie at cheshire.pnn.police.uk>

Fri, 19 Dec 2003 16:33:46 +0000

You are still referring to this service as new...??

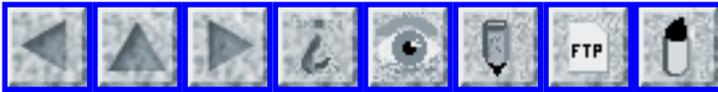
Actually, "Money Claim Online" is not at all a new service - I've used it twice in the last couple of years, first issuing a summons with it on 22 Feb 2002.

Whilst the potential risks are worthy of examination, those relating to potential use of the service whilst masquerading as a third party need to take into account the fact that there are *no identity checks whatsoever* when using the existing paper-based system. To my knowledge, there haven't been any related high-profile issues regarding this service yet, over this two-year period.

I won't even *dare* mention ID cards... oops I just did... :-)



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 10

Tuesday 30 December 2003

Contents

- [Cybercrime more than doubled in 2003](#)
[NewsScan](#)
- [Reliability of network vulnerability testing is decreasing](#)
[Charles Preston](#)
- [Biometrics: 'Not your father's fingerprints' win out](#)
[NewsScan](#)
- [Pointless "security"](#)
[Huge](#)
- [To Err is Human: Building a Safer Health System](#)
[Marc Auslander](#)
- [VoteHere reports computer break-in](#)
[Fredric L. Rice](#)
- [Re: Voter information up for grabs](#)
[Kelly Bert Manning](#)
- [Re: Why have electronic voting machines at all?](#)
[Peter Williams](#)
- [Electronic voting: social aspects](#)
[Andrew o' Baoill](#)
- [Re: Over-reliance on PowerPoint](#)
[Ron Bean](#)

- [Re: Poor writing is the problem, not PowerPoint](#)
[Julian Thomas](#)
 - [An economic argument against PowerPoint](#)
[Carson Harding](#)
 - [Re: Railroad accident](#)
[John Hines](#) [John A. Stewart](#) [Ed Ravin](#) [Chris Smith](#) [Matthew Delaney](#) [David Cantrell](#)
 - [Re: Loss of bus braking due to nearby illegally modified transceivers](#)
[Huge](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🔥 Cybercrime more than doubled in 2003

<"NewsScan" <newsscan@newsscan.com>>

Mon, 29 Dec 2003 10:23:57 -0700

This past year the Internet proved a lucrative haven for phishers, online auction scammers and Nigerians proffering cash-sharing partnerships, according to statistics from the Internet Fraud Complaint Center, which reports it received more than 120,000 online fraud complaints in 2003. That translates to an increase of 60% since 2002, when 75,000 complaints were processed. The Center provides cybercrime victims with a convenient process for filing complaints, which it then analyzes and routes to the appropriate FBI field office or local law enforcement agency for further action. [*The Register*, 29 Dec 2003; NewsScan Daily, 29 Dec 2003]
<http://www.theregister.co.uk/content/55/34667.html>

✦ Reliability of network vulnerability testing is decreasing

<Charles Preston <cpreston@gci.net>>

Tue, 23 Dec 2003 09:53:50 -0900

Both home computer users and corporations use outside testing services to do port scans and vulnerability scans. This testing is performed to verify that expected safeguards are in place, and that configuration changes haven't left the network more open than anticipated. Some are free port scans, like the <http://www.grc.com> service ShieldsUp, and some port/vulnerability scans cost tens to hundreds of dollars per IP address.

The testing is based on the assumptions that, subject to network congestion, packets sent to any port on a network perimeter device will arrive, and that open ports are equally visible from the Internet and from a computer in the building next door.

Both of these assumptions are incorrect for some ISPs.

What is increasingly occurring is that some ISPs are blocking certain ports from the Internet. Worse, when you inquire, they are incorrectly stating that they are not blocking any ports, and they are making changes without any notification to customers.

The same ports are not always blocked between two addresses on the same ISP network. This raises the possibility that a vulnerability test from the Internet will fail to disclose an actual vulnerability, which can be exploited from any address inside the ISP network. I had

exactly this
situation occur when testing a vulnerability scanning service.

Some ISPs have been blocking NetBIOS ports for home networks, such as on cable modems, but could quit blocking ports if asked, on an individual connection basis. This was to assist home users with Microsoft operating systems who had no other security.

I have been told by two ISPs that blocking is implemented in their routers or "core router" and cannot be changed for business connections.

A search on Google indicates that some ISPs are blocking a number of ports, not just NetBIOS, primarily in response to recent network worms.

In order to use a vulnerability scanning service, companies will be forced to check for ISP port blocking just at the outside of their firewalls, with the further problem that the results are subject to unannounced change at any time. This will lower the benefit of frequent periodic testing.

Charles Preston, Information Integrity

⚡ Biometrics: 'Not your father's fingerprints' win out

<"NewsScan" <newsscan@newsscan.com>>

Mon, 29 Dec 2003 10:23:57 -0700

The biometrics industry -- spurred on by heightened terrorist concerns -- has rolled out a variety of new ways to identify people, ranging

from retina and iris scans to mapping voice patterns or walking styles, but there's a clear winner among the competing technologies -- the old-fashioned fingerprint. "They are looking for proven technology that's stable and familiar," says Joseph J. Atick, CEO of biometric firm Identix. "It's not about technology. It's about lowering your deployment risk." But these aren't your father's fingerprints -- today's equipment does away with messy ink in favor of digital records, created by software when fingers are pressed against an electronic pad or sensitive photoplate. And often as not, the fingerprints are then combined with some other form of biometric ID, such as facial recognition. Meanwhile, growing use of passports, drivers' licenses and employment ID cards embedded with ID-data microchips is spawning a new business for data processing giants such as IBM, Unisys and Siemens. "The technology (to integrate ID data with public records) is advancing rapidly. The big growth will be in 2005 and 2006," says a Unisys official. [*The New York Times*, 29 Dec 2003; NewsScan Daily, 29 Dec 2003]

<http://partners.nytimes.com/2003/12/29/business/media/29face.html>

✶ Pointless "security"

<huge@huge.org.uk>

Wed, 24 Dec 2003 12:40:55 +0000 (GMT)

I live in the UK and my parents live in the USA. Every year, at Christmas, I send them a parcel containing food items that are hard or impossible to get in the USA, or are prohibitively expensive there. (Apologies if any of this takes on the attributes of a rant. I find it difficult to talk about this rationally.)

I find that as of 12th Dec 2004, any food items mailed to the US have to be pre-registered with the FDA. From the Web site <http://www.cfsan.fda.gov/~dms/fsbtact.html>:

"Nearly 20% of all imports into the U.S. are food and food products. In 2002 Congress passed the Bioterrorism Act as a part of its ongoing effort to combat terrorism - in this instance, by reducing the ability for international terrorists to carry out terrorist attacks in the U.S. by contaminating imported foods."

Now for the rant bit. I can appreciate that the US Government wants to protect the food supply against bio-terrorism, but what in the name of Ghod do they think this is going to achieve? Were I a bio-terrorist, about to ship a boxful of Ebola contaminated sausage to the USA, would I register it on the FDA site? Or would I write "Books" on the Customs form and send it anyway?

And that brings me to the registration process itself, in order that I might legally send Christmas Cake, Christmas Pudding and Marmite (*) to my poor deprived parents. At least I can do it online (see

<http://www.cfsan.fda.gov/~pn/pnoview.html>). But do I have to register at all? "Private residences of individuals" are excluded. Why? My box of Ebola could just as easily come from my kitchen as from the local sausage plant. And if I'm a terrorist (which I'm not), again I ask, why would I register at all? And if I do register (which I haven't), why threaten me with US law (which the site repeatedly does.) I know the US Government struggles with the concept of extra-territoriality

In short, what is the point of this? Other than make-work for Government employees. Still, at least the website works with Mozilla. I guess I should be thankful for small mercies.

"Something must be done. This is something. Therefore we will do it."

(* Yes, I know Americans regard Marmite as a bioweapon, but it isn't. Honestly.)

✶ To Err is Human: Building a Safer Health System

<Marc Auslander <marcslists@optonline.NOSPAM.net>>
Tue, 23 Dec 2003 20:36:31 -0500

In support of Don Norman's posting
Proper understanding of "The Human Factor",
I would recommend a 1999 Institute of Medicine report which makes pretty much the same argument about medical errors. It points out that one

consequence of taking an approach which blames the person, rather than the system, is that the information needed to fix the system is suppressed! To quote from the report:

"One of the report's main conclusions is that the majority of medical errors do not result from individual recklessness or the actions of a particular group--this is not a "bad apple" problem. More commonly, errors are caused by faulty systems, processes, and conditions that lead people to make mistakes or fail to prevent them. For example, stocking patient-care units in hospitals with certain full-strength drugs, even though they are toxic unless diluted, has resulted in deadly mistakes."

The report is at: <http://www.iom.edu/includes/DBFile.asp?id=4117>

VoteHere reports computer break-in

<"Fredric L. Rice" <fprice@skeptictank.org>>
Tue, 30 Dec 2003 10:21:33 -0800

E-voting firm reports computer break-in
Federal authorities investigating VoteHere intrusion
MSNBC.COM EXCLUSIVE
By Alan Boyle, Science editor
<http://www.msnbc.msn.com/id/3825143>

A company developing encryption-based software for secure electronic voting has itself become the victim of a computer break-in, the company's top executive told MSNBC.com. Federal authorities have confirmed

that the incident is under investigation. The intrusion into Bellevue-based VoteHere's corporate network occurred in October, said Jim Adler, VoteHere's founder, president and chief executive officer. No suspects have yet been named, but Adler said his company, in cooperation with investigators, had developed substantial information about the source of the intrusion over the past two months. "We feel that it may have been politically motivated," Adler said.

Adler's revelation came amid a deepening debate over e-voting and its vulnerability to election fraud -- and a controversy over surreptitious methods to get information about how e-voting software works.

[Another report indicates they know who the culprit is. PGN]

🔥 Re: Voter information up for grabs (Ross, [RISKS-23.09](#))

<bo774@freenet.carleton.ca (Kelly Bert Manning)>

Tue, 23 Dec 2003 22:56:28 -0500 (EST)

> .. I feel that privacy concerns should not eliminate the public
> availability of what have traditionally been public records.

Sounds very similar to the "shut up and get used to it" response I got from a Provincial Legislative Committee (chaired by Barry Jones) in my province.

Rather than giving it up as hopeless, I continued to lobby and to make

various interest groups (such as Doctor's professional associations, battered women's shelters, rape relief centers, police associations, etc.) aware of the issues and the evidence of voter list abuse.

During the election which got Mr. Jones into office, one campaign office reported that the only thing stolen during a break-in was the CD copy of the voter list. The computers and all the office equipment were left.

I also provided them with copies of documents I obtained after suing "Datex Services", a Vancouver-based junk-mailing-for hire outfit. Those invoices showed Datex purchasing a copy of the "geographic alpha sort" fiche copy of the voter list, 2 days before provincial legislation declaring such uses illegal was proclaimed.

While I had him in front of a Judge, Mr. Vandersteltdt of Datex stated that if he was denied access to voter lists for junk mailing purposes, he would simply create a fringe party to obtain a "free" copy.

That seemed to get some attention. Next thing I knew, both the provincial election act and the municipal act had been amended to allow voters to have their addresses suppressed, even from routine access by elections branch staff. The amended legislation authorizes seeding voter lists with fake names to allow abuse of the personal information to be detected.

My wife and I chose to opt out of the "motor voter" program which uses driver licence and vehicle registration changes of address to update the voter list. I got a bit of a hassle from a young poll clerk the

last time I showed up to vote, but an older clerk she consulted informed her that it is now quite common to be on a voter list without an address.

Election staff have wide discretion to suppress addresses. Shortly after the legislative change the Municipal Clerk for Squamish suppressed the address of every voter when a man with a history of violence ran, apparently seeking non-published addresses of people he was stalking. The severance was upheld by the Office of the Information and Privacy Commissioner.

<http://www.oipc.bc.ca/orders/Order69.html>

Re: Why have electronic voting machines at all? (Cooper, RISKS-23.06)

<Peter Williams <peterw@zip.com.au>>
Fri, 26 Dec 2003 22:55:25 +1100

I always find these discussions about voting systems fascinating, mainly because my experience is so utterly different to what gets discussed.

Here in Australia, elections are managed by the AEC, an independent federal statutory body with no links to any political party. (Their website at <http://www.aec.gov.au/> covers the whole process in great detail).

We don't use mechanical or electronic voting machines. The same standard applies in all electorates across the country. We vote by ranking

candidates in order of preference, by writing numbers in pencil in boxes on paper ballots, which are later counted by hand.

Voting in elections at all levels of government (local, state, federal) is mandatory for every citizen over the age of 18. If you don't vote, you get fined about \$20, unless you have a very good reason.

We have almost 13 million voters who vote in over 8000 polling places spread across a country roughly the size of the continental United States, and we still usually get most results reported within a few hours of the polls closing at 6pm on election Saturday.

As a computer engineer, I'm astounded at the idea that relying on a private company using proprietary software running on consumer-grade operating systems without a paper trail could even be considered as a reasonable way to run an election.

To my mind, if you're going to have a computerised voting system, it

- 1) must have specifications, source code, test procedures & results publicly available & open to rigorous scrutiny,

- 2) must use secured, tamper-resistant machines with stable operating systems in known & authorised configurations (I'm thinking some minimalist variety of BSD or Linux so that the underlying operating system source code can also be publicly available for inspection),

- 3) must give voters tangible evidence that their vote has been cast as they

intended (a printed human & machine readable "vote card" which gets checked by the voter then placed in a ballot box),

4) must link these "vote cards" back to the electronic vote (via an anonymous ID such as a serial number) so that they can be routinely cross-checked during counting to confirm that the electronic votes match the printed votes exactly, and

5) must provide extensive audit trails & logging to ensure that any necessary post-vote inspections & verifications can be confidently carried out.

Without at least that (and probably a whole lot more I haven't thought through yet), there's no way you can honestly be comfortable that your votes are reasonably safe from fraud, election rigging, or simply incompetence in counting.

✶ Electronic voting: social aspects

`<=?ISO-8859-1?Q?Andrew_=D3_Baoill?= <andrew@funferal.org>>`

Sun, 28 Dec 2003 12:09:47 +0000

I've recently posted an essay on electronic voting online, looking at some of the social and cultural aspects of the issue, and examining the implementation in Ireland. In short, the rush to prove how 'cutting edge' the Irish economy is has led to the unnecessary adoption of a system that

has serious flaws (no independent audit trail) and that may be of more harm than benefit to Irish democracy. It may be of interest to some readers.

<http://funferal.org/mt-archive/000455.html>

Andrew o' Baoill

PhD student, Institute of Communications Research, University of Illinois

andrew@funferal.org / +1-217-332-3263 / <http://funferal.org>

✶ Re: Over-reliance on PowerPoint (NewsScan, [RISKS-23.08](#))

<Ron Bean <rbean@shell.core.com>>

Fri, 26 Dec 2003 11:58:54 -0600

Ironically, the best antidote to PowerPoint may be a guide to technical writing that was published by NASA many years ago, and can still be downloaded from NASA's own servers:

<http://techreports.larc.nasa.gov/ltrs/1964-cit.html>

That page is a link to this file:

<http://techreports.larc.nasa.gov/ltrs/PDF/NASA-64-sp7010.pdf>

"Clarity in Technical Reporting" by S. Katzoff was written in 1955 and circulated informally at NASA's Langley Research Center. Popular demand led NASA to publish it officially in 1964. The PDF file on the web is a scan of a copy that was printed in 1973.

The first 16 pages are about written reports, the last 9 pages are about

verbal presentations. The author assumes that the slides will be charts and graphs, not bullet points.

Of course this doesn't solve the real problem at NASA, which is that people didn't want to talk about the bad news. Tufte's anti-PowerPoint document calls the NASA presentation "an exercise in misdirection", which implies that it was done that way on purpose.

[A response by Lauren Weinstein to this subject on Dave Farber's IP had this message, added here by PGN:

An interesting point is that the 1-inch recorder and the related sensor array was installed ONLY on Columbia. As the first operational shuttle, it had been outfitted with masses of sensors (and the tape system) that later shuttles didn't have. Luckily, they kept running the system instead of pulling it out or shutting it down, even 20+ years later... otherwise much of that data would have been unavailable.

It staggers the mind to think that that data tape (and the camcorder tape that apparently was loose from its case) survived at all.]

✶ Re: Poor writing is the problem, not PowerPoint (Garfinkel, [R-23.09](#))

<Julian Thomas <jt@jt-mj.net>>
Sun, 28 Dec 2003 21:22:11 -0500

>... Specifically, WYSIWYG systems lead to a focus by the user
on
>appearance, not on structure or content.

To say nothing of management who emphasize appearance, not
content.

✶ An economic argument against PowerPoint

<Carson Harding <harding at motd.ca>>

Mon, 29 Dec 2003 10:24:23 -0700

I worked for a time in an engineering department of a power
company. The
vice president in charge of engineering forbade the use of any
PowerPoint
presentation in any meeting he headed. His argument was
economic: he didn't
want his engineers wasting time and the company's money making
pretty
presentations when they should be engineering.

✶ Re: Railroad accident (Kuenning, [RISKS-23.09](#))

<John Hines <jbhines@newsguy.com>>

Tue, 23 Dec 2003 21:51:09 -0600

> all railroad cars should be required to have reflectors (or
reflective
> paint) on the sides.

They already do here in the US. All freight cars have reporting
marks,

which are read via optical readers. These are painted in highly visible reflective white on black for machine reading.

Taggers in the 'hood have figured out that if you don't paint over those marks, the RR doesn't have to repaint the car, and the artwork lasts till the next scheduled paint job.

Selling ad space on the sides of cars is of limited use, none to the rail car leasing companies, or the rail road, and you sure wouldn't want a railcar advertising your competition sitting on your rail spur.

[A sampling of other responses follows. PGN]

✶ **Re: Railroad accident (Kuenning, [RISKS-23.09](#))**

<"John A. Stewart" <alex.stewart@crc.ca>>

Wed, 24 Dec 2003 10:11:24 -0500

"A friend once told me that in the Great Plains there are many accidents of this sort each year. Most crossings are completely unguarded, and at night a train on an unlit level crossing is almost completely invisible."

Ah, statistics and word of mouth.

I work on a couple of preserved steam locomotives, so maybe I can give a slightly different perspective. I'll call this "John's Ten Steps to Enlightenment", and will let the reader determine whether the reasoning is

sound or not.

1) In Canada, and I presume in the USA, it is my understanding that at a crossing without gates, a car driver must stop, look, listen, then proceed.

2) Which, if my understanding is correct, leads me to wonder about the type of people who do not follow these rules; so:

3) A quick web search brings to light this *very* interesting web page:

<http://www.rrc.state.tx.us/divisions/rail/vtstats.html>

4) and looking at the "By Gender" column shows that, in this survey, by far, males are the ones that are getting killed driving through crossings. Which brings up:

5) a recent unprotected crossing accident in Southern Ontario where the police have indicated that impact was at 180km/h, and brakes were applied by the car driver when the car was doing 240 km/h. (references can be found again, I have not bothered, because this is an example reference, not a specific one)

6) maximum speed on roads in North America is, what, 65mph in some states?
100km/h in Canada?

7) young male drivers have very, very high insurance premiums, as inferred from talking to colleagues with male teens in their house.

8) all recent automobiles have computer controlled engines,

9) leading me to wonder if it is not the lack of paint on trains that is

killing males at grade crossings, but the speed that cars travel at;

10) bringing me to the conclusions that: 1) paint is not going to make much difference, at all; and 2) cars have the technology to restrict speed, it should be mandated so.

✶ Re: Railroad accident (Kuenning, [RISKS-23.09](#))

<Ed Ravin <eravin@panix.com>>
Wed, 24 Dec 2003 11:21:18 -0500

Don't they have signs that say "RR Crossing"? [...]

Railroad crossings are a good example of the "adverse operator" environment discussed earlier in RISKS postings. Even crossings with full gates have collisions from time to time, because of motorists deliberately "sneaking around" the gate when it is down.

Every intercity bus I've ever been on always stops before going through a grade-level railroad crossing. This is because the bus drivers have been properly trained and understand the consequences of making even the slightest mistake when crossing railroad tracks (especially if they're caught, they could lose both their bus driver's license and therefore their livelihood). I don't know how often buses collide with railroad trains, but I suspect it is very, very, infrequently.

✶ Re: Railroad accident (Kuenning, [RISKS-23.09](#))

<Chris Smith <smith@interlog.com>>

Sun, 28 Dec 2003 01:18:51 -0500 (Eastern Standard Time)

Then simply place the reflective markers on the far side of the crossing, facing across the tracks and *through* the train. Or place them at track level, beside or between the rails. In either case, the view of the reflectors will be regularly interrupted either by the body of the rail car or by the wheels. The overall effect will be that of a flashing light in the driver's view; this should be more likely to attract attention than the dark train.

This has a couple of other advantages. The solution is easily scalable, in that it can be deployed almost instantly at the most problematic crossovers. Furthermore, the rail owner of a crossing is not on the move across the country, and may be more amenable to local pressure to take action to make their crossings safer when presented with an easy and low-cost solution.

✶ Re: Railroad accident (Kuenning, [RISKS-23.09](#))

<David Cantrell <david@cantrell.org.uk>>

Mon, 29 Dec 2003 19:34:44 +0000

I would have thought that a better solution would be for drivers to look where they are going. Certainly when I am driving, I can see walls and hedges and trees when they leap out in front of me. I am quite sure that I would be able to see large moving metal objects in front of me.

Lord Protector David Cantrell | <http://www.cantrell.org.uk/david>

✦ Re: Railroad accident (Kuenning, [RISKS-23.09](#))

<"Matthew Delaney" <delaney@ucs.net>>
Thu, 25 Dec 2003 12:58:57 -0500

Regarding Geoff Kuenning's suggestion of attaching reflective markings to the sides of trains to prevent collisions... I wonder if the railroads who are against any such regulation have ever considered the cost of the damage from the vehicles that hit the trains.

Perhaps they did make sure that regulation was in place that completely absolved them of all liability in those types of accidents, so their cost is zero?

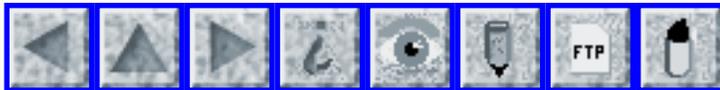
✦ Re: Loss of bus braking due to nearby illegally modified transceivers

<huge@huge.org.uk>

Wed, 24 Dec 2003 12:13:57 +0000 (GMT)

This is an old issue, and does not apply just to "illegally modified transceivers". I used to own a car whose engine management crashed when an entirely legal amateur radio 70cms handheld was operated inside the vehicle.

And with the pressure from governments to exploit bandwidth, the continuing rush to 'wireless everything' and the lack of analogue skills among todays electronic engineers, I can only see the problem getting worse.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 11

Tuesday 6 January 2004

Contents

- [Bank of England falls victim as e-mail scams rise by 400%](#)
[Keith A Rhodes](#)
- [Get ready for SPIM](#)
[NewsScan](#)
- [Israeli government suspends purchases of Microsoft software](#)
[NewsScan](#)
- [Input data error on tag transfer causes driver's arrest](#)
[Stanley A. Klein](#)
- [Forget your bank balance? It's available on the Internet](#)
[Monty Solomon](#)
- [Inadvertent use of wireless network](#)
[Ben Rosengart](#)
- [Car-monitoring service allows you to be your own Big Brother](#)
[Monty Solomon](#)
- [Secret ballots the Tel-Aviv University way...](#)
[Yaron Davidson](#)
- [Electronic voting: computer reliability aspects](#)
[Bob Axtell](#)
- [Re: Why have electronic voting machines at all?](#)
[Mark Newton](#)

- [Re: Loss of bus braking due to nearby illegally modified transceivers](#)
[Kenji Rikitake](#)
 - [REVIEW: "Disaster Recovery Planning", Jon William Toigo](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Bank of England falls victim as e-mail scams rise by 400%

<"Keith A Rhodes" <RhodesK@GAO.GOV>>

Mon, 05 Jan 2004 10:41:28 -0500

The Bank of England became the latest victim of e-mail fraudsters yesterday when many hundreds of thousands of people were sent hoax messages from admin@bankofengland.co.uk, a nonexistent bank address, urging them to open an attachment that would help prevent credit card fraud. This was reportedly the first time BoE was victimized by a "phishing" expedition that apparently fooled about 5% of their Visa customers into divulging their card and PIN numbers. The scam was detected when the Bank received over 100,000 automated replies mostly from corporate mailsites whose employees were on holiday! Halifax, NatWest, Barclays, Lloyds TSB, and Nationwide Building Society have also been previously subjected to similar attacks.

[Source:

James Moore and Robert Uhlig, *The Daily Telegraph*, 31 Dec 2003, PGN-ed]

<http://www.telegraph.co.uk/connected/main.jhtml?xml=/connected/2003/12/31/ecntbofe31.xml&sSheet=/connected/2003/12/31/ixconnrite.html>

✈ Get ready for SPIM

<"NewsScan" <newsscan@newsscan.com>>

Wed, 31 Dec 2003 08:48:41 -0700

Instant messenger spam, dubbed "spim," is increasingly clogging users' computers, popping up with the real-time regularity of instant messages and annoying users who complain they're now receiving several messages a day. Users can either accept or decline the spim, which often contains a link to -- what else? -- a pornography site. Ferris Research estimates about 500 million spim messages were sent in 2003, double the number sent in the previous year. And while instant-messenger spam "isn't nearly the industry that e-mail spam is, it's starting to increase," says the CEO of an antispam consulting firm. Experts warn that the recent crackdown on conventional spam may push illicit marketers to explore new avenues, including instant messaging. "The irony is that focusing like a laser on our No. 1 concern -- spam -- has painted e-mail spammers into a corner like never before and incited them to find other ways to try and reach our membership online," says an AOL spokesman. [*Wall Street Journal*, 31 Dec 2003; NewsScan Daily, 31 Dec 2003]

<http://online.wsj.com/article/0,,SB107228175621944800,00.html>
(sub req'd)

Israeli government suspends purchases of Microsoft software

<"NewsScan" <newsscan@newsscan.com>>

Wed, 31 Dec 2003 08:48:41 -0700

The Israeli government has become the latest national government to seek open-source alternatives to Microsoft's productivity software, citing cost as a major motivating factor. "The move with Microsoft was a purely economic decision," says a Finance Ministry spokeswoman. "The Israeli government will not be purchasing new products from Microsoft, but will implement its contract to secure existing systems. On a policy level, the government is committed to expanding computer use. We want open source technology to spread, so more people will be able to afford computers." The Finance Ministry has been working with Sun Microsystems and IBM to create a Hebrew language version of OpenOffice software, an open-source alternative to Microsoft Office. Some federal agencies in France, China and Germany, as well as the city government in Munich, have switched over to Linux-based servers and individual workstations. Other governments exploring open source alternatives include those in Britain, Brazil, Japan, South Korea, China and Russia. Governments account for about 10% of global information technology spending, according to IDC. [AP/*USA Today*, 31 Dec 2003; NewsScan Daily, 31 Dec 2003]

http://www.usatoday.com/tech/world/2003-12-30-israel-vs-microsoft_x.htm

✶ Input data error on tag transfer causes driver's arrest

<"Stanley A. Klein" <sklein@cpcug.org>>

Mon, 05 Jan 2004 13:29:21

I met Ms Reed at the Maryland Technology Showcase and heard this story. I'm cc'ing her so she can correct or update the story if necessary.

Ms Paula Reed traded in her minivan for an SUV over a year ago. The dealer told her that because the weight classes of the two cars were the same, she could transfer her tags, and that the dealer would take care of it.

Maryland has a two year cycle for tag renewal, and she didn't know the details of what to expect, so she went about her life.

She was driving down the street a few months ago when she was stopped by a police officer. The officer told her she was driving on expired tags. She replied that she usually sends in her tag renewals promptly and didn't remember receiving a renewal notice. The officer asked for her registration and all she had was the paperwork given her by the dealer when she bought the car. The officer checked her tag number with the Maryland Motor Vehicle Administration and found that there was no such tag in the system. The officer then accused Ms Reed of obtaining counterfeit tags, arrested her, and took her to the police station.

After she was released (with a court date), she checked on her tag

situation. It turned out that somewhere in the tag transfer process someone entered the wrong weight class for her new car. Somehow the system rejected the tag transfer but the error was not corrected. When her used minivan was resold by the dealer, her tags were deleted from the system. Either nobody knew that all this was happening, or whoever knew failed to take action to correct the error.

As of early December, she had been required to obtain new tags and was still awaiting her court date on the charges growing out of her arrest.

✶ Forget your bank balance? It's available on the Internet

<Monty Solomon <monty@roscom.com>>

Sun, 4 Jan 2004 01:33:52 -0500

Eric F. Bourassa, a privacy advocate at the Massachusetts Public Interest Research Group, knows how difficult it is to keep personal financial information personal. But even he was surprised at how easy it was for **The Boston Globe** to obtain his private bank account information. Trafficking in confidential financial information is commonplace on the Web, with a quick Google search turning up more than a dozen sites selling everything from Social Security numbers to bank balances. **The Globe** tested one of the sites in September, paying \$125 for Governor Mitt Romney's credit report and in the process discovering a major security weakness in the nation's

credit reporting network.

In November, with Bourassa's blessing, the Globe began to explore the shadowy world of asset search firms, which advertise that they can unlock the financial secrets of virtually anyone. The mystery is where these firms get their information. Does it come directly from financial institutions? Or does it come through more indirect, possibly illegal, methods?

The Globe agreed to pay Ohio-based I.C.U. Inc., whose Web address is Tracerservices.com, \$475 for Bourassa's bank account information and his stock and bond holdings. Not all of the information the Web site provided was accurate, but the bank account information, with the balance listed right down to the penny, was so close that it made Bourassa feel violated.

[Source: Bruce Mohl, *The Boston Globe*, 4 Jan 2004]

✶ Inadvertent use of wireless network

<Ben Rosengart <ben@narcissus.net>>

Tue, 30 Dec 2003 18:45:00 -0500

My brother D., home from college, called me today.

D.: I don't want to jinx anything, but it seems that my computer is connected to the Internet. I turned it on and saw that I had two new messages. And they're from *today*.

Me: I take it you're at Dad's [where nothing is set up for Internet

access]. Do you have a wireless card in there?

D.: Um, I don't know.

Me: Ok, go to System Preferences ... Network ... what do you see?

D.: [...] Connected via Airport.

Me: There you go.

D.: Are you saying there's a wireless network at Dad's?

Me: Wireless doesn't care about walls. [I know, that's not strictly

true, but it's what I said.]

D.: So I'm on some *neighbor's* wireless network?

Me: Yup.

D.: [Amazement and then laughter.]

I pointed out that all his network traffic is being broadcast on radio frequencies, and counseled him to configure his mail client to use encrypted protocols, and to watch out in general.

⚡ Car-monitoring service allows you to be your own Big Brother

<Monty Solomon <monty@roscom.com>>

Thu, 1 Jan 2004 03:04:56 -0500

Don't trust your teenagers or your spouse? Networkcar can tell you where they've been driving.

The way George Orwell imagined Big Brother was as a police state that imposed unrelenting surveillance on an unwilling public. Orwell never imagined that people would actually make nice with Big Brother as a matter of convenience, but that's one way to view the growing stream of data from automobiles that has attracted a lot of interest from the government and, so

far, not a lot of suspicion from the public. Some consumers actually are willing to pay for a service that lets the government know your car isn't breaking the law. For about a year, a La Jolla company has offered to provide remote sensing of a car's systems and to post that data to a private Web page, along with verifying to state agencies that the car is in compliance with the emission laws of California and a few other states. ...

[Source: Ralph Vartabedian, *Los Angeles Times*, 31 Dec 2003]
<http://www.latimes.com/classified/automotive/highway1/la-hy-wheels31dec31,1,1009805.story>

✶ Secret ballots the Tel-Aviv University way...

<Yaron Davidson <yarondav@post.tau.ac.il>>
Thu, 01 Jan 2004 14:33:29 +0200

The elections for faculty representatives in the Tel-Aviv University student union were held two days ago. (Now, this may be not as important as votes for government, but many of the representative run for actual political parties, and there are serious sums of money involved higher up, so these votes to have a meaning)

In the last couple of years , for all the usual reasons, the voting mechanism was changed to e-voting, namely a temporary PC with custom-made software connected over the university LAN to a server. No paper audit of course, have to match industry leading standards after all. The

voting
process itself is quite simple. You pass a bar-code reader over
the student
card to get an ID, select the faculty to vote in if you have
more than one,
get a list of all available candidates for the faculty, click on
small
"select" buttons next to those you want (with visual indications
being both
a check-box next to the names, and a second list containing
those you voted
for), and press a confirmation button.

No problems for me last year, but it seems many students had
difficulties
with either the bar-code reader or the program interface. So,
the delays
caused being apparently the most serious problem with the
system, this year
we had a wonderful solution. Oh, yes, before that, if I forgot
to mention,
votes of course must be secret, and they place a temporary
barrier around
the computer preventing anyone from looking in at you while you
vote.

I got to the computer, and a man with a badge claiming him a
"voting
supervisor" or some such takes my student's card, pass the bar-
code reader
in front of it, hands it back to me, motions toward the chair,
and tells me
to go ahead and vote. But he stays there, and looks at me and at
the
computer screen with a bored expression.

Me:"Eh... The votes are supposed to be secret..."

Him:"Yes, so ?"

Me:"So you can see who I'm voting for"

Him:"Oh, don't worry about that. I'm not related to any of this.
See ?"

and points to the nice badge.

Me:"What do you mean, not related. You're here, and you can see

who I

vote for. That's not secret!"

I get a "Why can't this idiot get it" and again

Him:"But it doesn't matter. I'm not even from this faculty. I don't care

who you vote for."

Me:"But surely I can't know that. I do have a right not to have people

seeing who I vote for". Heck, right, officially I'm not even supposed to

have a choice, nobody should come in a look even if I want them to.

Him:"Look, I'm not here to look at your vote. We had lots of people

having trouble understanding how to vote, and the reader couldn't handle

about two thirds of the cards, so I'm just here to help students vote

and save time. And you're holding up the line. Just vote already"

Me:"Fine, but not until you get outside this barrier and don't look in.

This won't solve the very serious general problem here, but it will

solve my immediate one and let me finish..."

So the dear fellow gets out with a bemused expression. I vote. I press the

confirmation button (15sec process so far, mostly spent locating my least

worse candidates in the rather long list). Then I have to wait around 20-30

seconds more because the confirmation screen insists on staying there with

my name and the candidates regardless of my clicking on it to make to go

away. All the while the "supervisor" muttering that it takes too long and

that's what he's there for. You want to speed up the process, put an OK

button on the confirm screen instead of time delaying it. That's 20 seconds

per student times several thousands of student, right there.

I go out, someone else gets in, and after he reads his cards and explains

what those "select" buttons are for to the poor soul, the "supervisor" turns

back to me still trying to figure out what the fuss is about.

Him: "You know, I really don't care about those votes. What I see doesn't

matter. I don't know who you are or who the candidates are."

I see one of our esteemed candidates standing there, points at her and

proceed.

Me: "And I'm supposed to trust your word for it? How can I know

you're not friends with her, or supports the same party that's behind

her? Maybe she bribed me to vote for her, and I could see I didn't?

Maybe you just nods to her to indicate who voted and who didn't? It

doesn't matter if none of these things are true. What matter it that it

can theoretically be. You want to say the votes are not secret, take

away this barrier, and let anyone see, fine. That's one way to do it.

But if you claim the votes are secret, and go through all this trouble,

then keep it secret and don't put someone in with me."

At this point several other students on the line starts to claim that

I'm right, and another one asked him to look outside. A former student

representative in the faculty gets there too and tries to mollify me by

saying that she'd watch over him. Right.

Anyway, than the guy comes up with another brilliant riposte.

Him: "Besides, if I wanted to see what you voted, I could just look it

up at the server later, I wouldn't have to sit here and watch you"

Ah. So he's saying that:

1. It doesn't matter what he does is wrong and forbidden, since he can

do the same thing in several different ways. Makes perfect

sense to me.

2. He can see at the server not only total vote counts, but WHAT I

PERSONALLY HAVE VOTED. WHAT?!

Me: "Are you trying to tell me your database doesn't hold an aggregate

count of vote and a separate list of who voted, but a list of what every

ID has voted ?!"

Him: "Ah... Well... See... Err..."

Me: "Because that's very bad practices. You should never keep this

information in the database in a way that's easily accessible. It would

make a mockery of calling these elections secret." Oh, wait, aren't we

doing that already? Hmmm...

Him: "No, no. Of course we only keep aggregative information. Sure.

Certainly. No individual votes. Nope. Not at all." Well, he denies it

three times, even more actually, so he must have been convincing. So why

didn't I buy it? Well, let's attack on a different front.

Me: "So in that case you can't go to the computer later and see what I

voted, then. You can only see the totals, but that will be published

anyway. If you want to see what I voted, you have to look here" Or put a

sniffer on a connected computer, or logging software on this computer,

or... Anyway, there went argument #1. I'd felt better to see #2 go but

I'd have a hard time buying that now.

Unfortunately, by that time the former representative got really insistent

about making me stop making a fuss, and the "supervisor" just had to help to

current voter, so I left the scene.

At least they solved the problem of students not understanding

the voting system. It is a biggie. Imagine someone solving that whole butterfly-ballot fiasco at the US by putting someone to help people punch the right hole, and not to worry since he's from a different state so he really doesn't care...

✶ Electronic voting: computer reliability aspects

<Bob Axtell <engineer@cotse.net>>

Thu, 01 Jan 2004 13:50:18 -0700

I perform electronics analysis on a consulting basis for clients.

A few years ago I was asked by a financial services client to verify a design concept which used, as its brain, a Windows-based computer system. Since the application was to maintain the credit-card numbers and transaction records of hundreds of people inside its memory and hard drive, an analysis was required. 50 hardware CPU's were used as engineering samples, using two Windows operating systems, and over a 3-month period, the results were clearly known, and the project dropped.

The results (still confidential), were eye-opening. In a nutshell:

1. Only ONE CPU ran without error for a continuous 96-hr period. In essence, it was determined that Windows O/Ss were too "buggy" to perform such a sensitive task.
2. Sensitive data could NOT be protected from an unknown trojan or virus

attack.

The other day, I learned, to my astonishment, that some new "voting machines" use Windows O/S as their core!

Why is it that my financial client saw fit to verify hardware security, yet States don't seem to see a need...

[Because they were protecting MONEY. Votes don't count.
(Joke) PGN]

Bob Axtell PIC Hardware & Firmware Dev <http://beam.to/baxtell> 1-520-219-2363

✶ Re: Why have electronic voting machines at all? (Williams, [R-23.06](#))

<Mark Newton <newton@internode.com.au>>
Wed, 31 Dec 2003 10:54:17 +1030

> If you don't vote, you get fined about \$20, unless you have a very good
> reason.

Before the Yanks get too upset about that, it's best to clarify.

Voting isn't compulsory. Registering to vote at least two weeks prior to the first election after your 18th birthday is compulsory. If you are a registered voter, it is compulsory to attend a polling place.

Once you have attended the polling place, it is not compulsory to vote (i.e., if you have some reason for not voting after you've gone to the

trouble of locating yourself 50 feet from a ballot box on election day, there's no reason why you can't just leave after having your name checked off).

Mark Newton, Network Engineer, Internode Systems Pty Ltd +61-8-82282999

⚡ Re: Loss of bus braking due to nearby illegally modified transceivers

<Kenji Rikitake <kenji.rikita@acm.org>>

Wed, 31 Dec 2003 09:04:02 +0900

RF Interference issues are getting much complicated these days. Many of them are caused by lack of understanding on using proper preventive methods, such as installing RF common-mode filters (or Ferrite cores) or decoupling the circuits with proper amount of capacitors on the power and input/output lines.

I once had to troubleshoot the interference to 100BASE-TX line from a legal 50W ERP (Effective Radiated Power) 1.9-to-28MHz amateur radio transceiver, simply because the antenna and the Ethernet link was too close, less than 2-meter distance. Two Ferrite cores at the each end of a long Ethernet cable solved the problem. I also observed a common-mode loop problem when you tried to connect a notebook PC to the transceiver.

Even a optocoupled device such as MIDI patchbays are prone to the RF interference because the optocoupling junction between the LED and phototransistor has certain amount of capacitance (a few picofarads), which a strong RF energy could pass through.

Truck drivers are unfortunately one of the major sources of illegal radio operators here in Japan, occupying most of V/UHF amateur radio frequencies and CB bands. They tend to raise the output of the transmitters to the maximum, typically in a few hundred watts, so many of car devices could be affected.

So you've got to be very careful. Your RFID card could be erratically activated.

Kenji Rikitake, JJ1BDX/3, JQ2KST and K1BDX

★ REVIEW: "Disaster Recovery Planning", Jon William Toigo

<Rob Slade <rslade@sprint.ca>>

Mon, 5 Jan 2004 12:47:56 -0800

BKDIREPL.RVW 20031105

"Disaster Recovery Planning", Jon William Toigo, 2003, 0-13-046282-9,

U\$54.99/C\$85.99

%A Jon William Toigo www.drplanning.org

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

%D 2003

%G 0-13-046282-9

%I Prentice Hall

%O U\$54.99/C\$85.99 +1-201-236-7139 fax: +1-201-236-7131

%O <http://www.amazon.com/exec/obidos/ASIN/0130462829/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0130462829/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0130462829/robsladesin03-20>

%P 482 p.

%T "Disaster Recovery Planning"

Toigo's first edition outshone almost all later DRP (Disaster Recovery Planning) and BCP (Business Continuity Planning) works. This edition vastly expands the resources and thinking on the topic. In the preface, Toigo examines the question of whether people will see this new edition as simply an exercise in opportunistic marketing, using the events of September 11, 2001 to promote a fresh work. He concludes that changes in technology do justify another edition. In addition, the new pieces giving post-9/11 perspectives from various parties (generally vendors) do provide some additional insights. The leading foreword, a first-hand account of the evacuation of one of the World Trade Center towers, offers interesting observations such as the fact that the tens of thousands of people using the exit stairwells created potential problems with respect to condensation on the stairs and walls of the structure.

Chapter one, an introduction to the topic, is no longer as incisive as it once was. However, there are still striking items, such as the mention of the Bank of New York information technology outage (lasting twenty seven hours) which led to a requirement to borrow twenty

two billion dollars, cascading into destabilization of the federal reserve fund and interest rate fluctuations. The advice is still practical, pointing out legislation that may indirectly support disaster recovery planning (although there is no mention of the widely used Americans with Disabilities Act), a detailed assessment of the uselessness of disaster recovery certifications and related groups, and suggestions for dealing with political realities. Various perspectives and disputes over risk are reviewed in chapter two, although the material becomes a bit disjointed when it ends with policy development. There is an excellent overview of fire protection and power problems, but the rest of the facility management material in chapter three is quite limited. A detailed examination of the options, products, and vendors related to data recovery (well beyond the usual discussion of full, incremental, and differential backups) is given in chapter four.

Chapter five deals with strategies for the recovery of centralized systems. This is the standard view of disaster recovery, but Toigo offers good, quality advice. Recovering decentralized systems is analysed in chapter six, although most of the solutions seem to rely on recentralising. End-user requirements, touching on remote computing, virtual private networks, and so forth, are discussed in chapter seven. Examination of network recovery, in chapter eight, is useful, although many solutions (such as wireless LANs) are not perused for problems (such as security), while, at the same time, they

are not pushed far enough (groups in many locations are now planning city-wide wireless networks which should be available in the event of the collapse of major telecommunications carriers). Emergency decision making, in chapter nine, concentrates on teams, functions, and flowcharts. References and resources for recovery management, mostly in the US, are in chapter ten. There is an odd inclusion of a story about vendor versus reseller infighting in the plan maintenance material in chapter eleven. The book concludes in chapter twelve.

While the later edition is sometimes too verbose, this work is definitely worthwhile for anyone in the security or disaster recovery planning field. Even if you have the first edition, continuity and recovery professionals will probably find that this latest work has fresh insights that justify its purchase.

copyright Robert M. Slade, 2003 BKDIREPL.RVW 20031105
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

Volume 23: Issue 12

Monday 12 January 2004

Contents

- [U.S. FAA warns of EFIS system fault](#)
[Peter B. Ladkin](#)
- [B747-400 Electronic flight displays rendered inoperative](#)
[Peter B. Ladkin](#)
- [Happy 2**30'th birthday, time_t! Now go patch Pro/ENGINEER](#)
[Paul Eggert](#)
- [Danish PM's private communications disclosed by MS Word](#)
[Theodor Norup](#)
- [Anti-spam law enacted -- so what's all this junk in my in-box?](#)
[NewsScan](#)
- [Want chips with that burger?](#)
[Jim Schindler](#)
- [Suing the customers](#)
[Joyce Scrivner](#)
- [Burger King wireless risk](#)
[Robert Franchi](#)
- [AP accidentally distributes celebrity phone numbers](#)
[Robert Franchi](#)
- ['Unfixable' Word password hole exposed](#)
[Brett McCarron](#)

- [VoteHere there and everywhere](#)
[Rebecca Mercuri](#)
 - [More voting snafus in Palm Beach and Broward Counties](#)
[Alan Fullilove](#)
 - [Correction re: Australian Voting](#)
[Eric Ulevik](#)
 - [Re: Electronic car doors trap man](#)
[Ian Mitchell](#)
 - [The dangers of PGN-ing](#)
[Simon Hogg](#)
 - [COMPSAC 2004 Call for Contributions](#)
[Yuen Tak Yu](#)
 - [EUSPRIG CFP July 2004 Klagenfurt](#)
[Patrick O'Beirne](#)
 - [REVIEW: "Ben Franklin's Web Site", Robert Ellis Smith](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ U.S. FAA warns of EFIS system fault

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

Wed, 07 Jan 2004 07:02:33 +0100

According to *Flight International*, 2-8 December 2003, p34, the U.S. FAA "has warned operators of Chelton Flight Systems FlightLogic [electronic flight information system] EFIS avionics that the equipment can provide misleading guidance under certain circumstances." The system is used on many aircraft in Alaska operating under Phase 2 of the FAA's general aviation Capstone program, which uses GPS to provide flight guidance and to track aircraft in flight. Apparently, the system indicates a uniform

rate of climb
of 300 ft/min for guidance in departure procedures, but some
departure
procedures require a higher climb rate for obstacle avoidance.

✈ **B747-400 Electronic flight displays rendered inoperative**

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

Wed, 07 Jan 2004 06:54:18 +0100

On 2 December, 2003, the U.S. National Transportation Safety Board issued Recommendations A-03-55 and A-03-56. The short document may be read at

www.nts.gov/Recs/letters/2003/A03_55_56.pdf

"On January 23, 2003, a Singapore Airlines (SIA) Boeing 747-400 experienced a complete loss of information on all six integrated display units (IDU) on the flight deck instrument panels while in cruise flight from Singapore to Sydney, Australia. The pilots flew the airplane for 45 minutes using standby flight instruments while they communicated with SIA maintenance personnel about the problem. SIA maintenance personnel advised the flight crew to pull out then push back in (or cycle) the circuit breakers for the EFIS/EICAS interface units (EIU), which returned the IDUs to normal operation. The flight continued to Sydney and landed without further incident."

"A similar event occurred on another SIA B747-400 on November 6, 2001 ..."
while on a Sydney to Singapore flight, during an emergency descent because

of an cabin pressure warning. Maintenance personnel recycled the EIU circuit breakers on the ground and restored the IDUs to normal operation.

"The six IDUs ... include the captain's Primary Flight Display (PFD) and Navigation Display (ND), the first officer's PFD and ND, and the main and auxiliary engine indicating and crew alerting system (EICAS) displays. The PFD and ND displays [sic] provide the pilots with attitude, altitude, airspeed, heading, and rate of climb and descent information. The EICAS displays provide the flight crew with the airplane's engine indicating information and annunciate advisories, cautions and warnings. Without these displays, the flight crew is required to use standby flight instruments, which consist of an altimeter, airspeed indicator, and artificial horizon/attitude indicator; the Boeing B747-400 does not have standby engine instruments. The loss of the IDUs would also eliminate the flight crew's access to data from the traffic alert and collision avoidance system, enhanced ground proximity warning system, and weather radar."

The EIUs are apparently responsible for data display on all six IDUs and preliminary investigation has indicated that all six IDUs blanked because all three EIUs stopped transmitting data. The EIUs are identical devices; the architecture is triple-redundant. The cause of this loss of data has not been determined, and no countermeasures have yet been identified that could inhibit the loss of all six IDUs again.

Boeing recommended cycling the EIU circuit breakers in such an event, and

the NTSB recommended that this procedure be included in the quick-reference handbook used by the flight crew to access procedures in an emergency.

The NTSB letter was also reported in **Flight International**, 9-15 December 2003, p13; and by Frances Fiorino on p31 of *Aviation Week and Space Technology*, December 15, 2003.

A similar loss of data to displays on an Airbus A340 in 1994 has been reported in *Risks* (Hatton, [RISKS-16.92](#); Ladkin, Rushby, [RISKS-16.96](#)), as also on a Boeing B767 in 1996 (Ladkin, [RISKS-18.19](#)). EFIS failure was also initially suspected in a turboprop accident in Zürich in 2000 (Ladkin, [RISKS-20.78](#)) but the final report fingers pilot error and not technical problems, according to the *Neue Zürcher Zeitung*, also 2 December 2003, www.nzz.ch/2003/12/02/english/page-synd4505738.html

There are lots of things one could say about such flight information display system architectures. All of them rely on the mechanical principles of the older mechanical systems, but add a layer of electronic display technology that was not present in the older systems, which drove the displays directly. This extra layer, most obviously, introduces categories of failure that were not present in the original systems, such as the failures exhibited in these incidents. I shall not address here the question of whether the benefits of such systems outweigh the risks.

The industry seems to be moving towards replacing the mechanical standby

flight instruments, built to designs that have functioned well for upwards of a century now, by electronic displays. Electronic standby instrument displays are available and are being advertised for many business jets.

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

🚨 Happy 2**30'th birthday, time_t! Now go patch Pro/ENGINEER.

<Paul Eggert <eggert@twinsun.com>>

Fri, 09 Jan 2004 17:10:24 -0800

About 13 hours ago, the POSIX `time_t` counter exceeded 2^{30} , thus reaching half its useful positive range (which counts seconds since 1970) on traditional hosts with 32-bit signed integer `time_t`. Unfortunately, some software produced by Parametric Technology Corp. was using that 2^{30} bit in time values, so today's milestone introduced timeout glitches into unpatched installations of PTC's Pro/ENGINEER, Pro/INTRALINK, and Windchill products. PTC has made patches available to all users, regardless of maintenance status; see <http://www.ptc.com/go/timeout/index.htm>.

I still do much of my computing on hosts with 32-bit `time_t`. I expect this to change in the next few years as 64-bit hosts take over, but I wonder: how many applications will break in January 2038 when `time_t` exceeds 2^{31} , even though the underlying hardware and OS works correctly? Mark

your calendars.

✶ Danish PM's private communications disclosed by MS Word

<"Theodor Norup" <thno@ita.cph.dk>>

Mon, 5 Jan 2004 23:10:34 +0100

The Danish newspaper Politiken cites a Ritzau (Danish telegram bureau)

telegram on Sun 4 Jan 2004

The Danish Prime Minister's Office has tightened IT Security with immediate effect following the disclosure of the origins of the document containing the New Year's speech of prime minister Anders Fogh Rasmussen. The speech had been written in a document originally authored by Christopher Arzrouni, head of the Trade and Industry Law section of the Association of Danish Industries ("Dansk Industri").

Till now, the ministry has distributed Anders Fogh Rasmussen's speeches to the press and others in word files but in two independent cases, just a few clicks on the computer did reveal the document's origin or which changes had been made. Therefore, the PM's office instituted a new procedure on Friday.

"We will in the future distribute speeches as PDF files so that such things will not happen" says ministry spokesman Michael Kristiansen.

At the same time, the ministry has begun checking its web site security. (my own translation)

Since the said Arzrouni chairs a well-known ultraliberalist (in the european sense) discussion society and since the PM does his best to convince voters that he himself has left former ultraliberalist convictions alone, the disclosure is very interesting at least.

One wonders what state secrets have been published by the government being blatantly ignorant to a very well-known MS word problem. And why an inappropriate word processor choice leads to a completely unrelated check of web site security.

The RISK: Wrongly believing that the higher echelons of governments and their technical support has more than a faint idea of IT security.

On the positive side: This may give some publicity to that infamous word problem.

✶ Anti-spam law enacted -- so what's all this junk in my in-box?

<"NewsScan" <newsscan@newsscan.com>>
Mon, 12 Jan 2004 10:15:53 -0700

The new federal anti-spam law went into effect Jan. 1, but consumers report their inboxes are more cluttered than ever -- what's going on? Critics say the new law doesn't actually ban spam but rather provides guidelines for sending junk e-mail legally. "Now we have a green light for what

would come to be called 'legal spam,'" says ePrivacy Group CEO Vincent Schiavone. John Levine, a board member of the Coalition Against Unsolicited Commercial E-Mail, concurs: "Basically, it's a bill of rights for companies that want to send junk e-mail." In addition, the federal law supercedes stricter laws recently passed in several states, such as California. "Everyone was planning for this California law, which was so draconian," says a California lawyer who defends accused spammers. "Once the federal government passed the federal law, everyone was kind of relieved." And while technology firms are eagerly pursuing new ways of blocking spam, skeptics say the ultimate solution won't be technological or legal, but will depend on developing more savvy users. Mary Youngblood, abuse team manager at EarthLink, suggests putting numbers in the middle of your e-mail address to make it more difficult to guess and using a separate address for online shopping and newsgroup postings. [AP, Jan 11 2004; NewsScan Daily, 12 Jan 2004]

<http://apnews.excite.com/article/20040111/D80003P00.html>

Want chips with that burger? (Simson Garfinkel)

<Jim Schindler <Jimschin@pacbell.net>>

Mon, 12 Jan 2004 10:10:40 -0800

Weblog: A Chip for Your Hamburger: Can radiofrequency I.D. devices

help stop the spread of beef tainted by mad cow disease?
[MIT Technology Review blog item]

Well, not quite, but this article in the RFID Journal indicates that both official[s] and the industry are now thinking of using RFID chips to enable greater tracking of meat through the food supply. This will help track things like infected beef (e.g., ground mad cows). What the article doesn't say is that this will also help protect against a terrorist attack --- or at least allow the tracking and faster recovery if terrorists go after the food supply. Simson Garfinkel

[Topic: Security and Defense]

<http://www.uptilt.com/c.html?rtr=on&s=5fo,4qkw,4rw,ij9s,j8tx,i328,m8yb>>

<http://www.technologyreview.com/blog/blog.asp?blogID=1227&trk=nl>

[Might this require edible RFID microchips that survive meat grinders and wind up in each hamburger patty? PGN]

⚡ Suing the customers

<Joyce Scrivner <kscriv@earthlink.net>>

Mon, 12 Jan 2004 13:10:23 -0600

Rockwell, is suing a law firm that is currently suing Rockwell's customers.

The law firm says that Rockwell has infringed on a patent. (I'm uncertain what relationship the law firm has to the patent holder.) The law firm

appears to assume that suing Rockwell's customers will get more money than suing Rockwell. Rockwell sees this as blackmail/threat because the law firm has not -- and cannot (without suing Rockwell) -- prove that the patent is or is not infringed. So Rockwell is now suing the law firm. Rather nasty.

In Rockwell Automation Inc. v. Schneider Automation Inc., 02-01195,

Rockwell says its technology is not covered by the Solaia patent, and

rather than battling that issue out in court, Niro Scavone and its clients

have sought to "'shakedown' manufacturers through threats of potential

business interruption or catastrophic damages."

<http://www.law.com/jsp/article.jsp?id=1039054478800>

✶ Burger King wireless risk

<"Franchi, Robert" <Robert.Franchi@fmr.com>>

Fri, 9 Jan 2004 16:53:35 -0500

Burger King Customer being told they are too fat to order a Whopper by hackers into the wireless speaker system at the drive through window!

http://www.ananova.com/news/story/sm_853744.html?menu=news.latestheadlines

✶ AP accidentally distributes celebrity phone numbers

<"Franchi, Robert" <Robert.Franchi@fmr.com>>

Fri, 9 Jan 2004 17:00:01 -0500

The Associated Press sent out a list of 250 celebrities' phone numbers by mistake. Many of the numbers are old and some of the celebrities are dead, but you can see the potential annoyance.

<http://www.sltrib.com/2004/Jan/01092004/utah/127432.asp>

✶'Unfixable' Word password hole exposed

<"Brett McCarron" <MCCARBWM@dfw.wa.gov>>

Fri, 09 Jan 2004 10:31:46 -0800

The password used to "protect" a Microsoft Word form can be revealed with a simple text editor, according to a recent BugTraq article. The RISK in this case goes beyond the ability to edit a protected document (you can bypass this anyway with Edit > Select All > Copy, open a new document and Paste). The real RISK is that the user's password is so easy to discover. Ideally, users would protect a form with a password that is different from their network authentication password(s). But in the real word ...

News Story

<http://news.zdnet.co.uk/software/windows/0,39020396,39118935,00.htm=20>

BugTraq Article

<http://www.securityfocus.com/archive/1/348692/2004-01-02/2004-01->

[08/0](#)

VoteHere there and everywhere

<Rebecca Mercuri <notable@mindspring.com>>

Tue, 06 Jan 2004 19:25:05 -0500

There's an interesting statement in the Volume 2, Number 1, January 4, VerifiedVoting.org newsletter regarding the VoteHere break-in.

VoteHere's website says that they sell a product called RemoteVote (c) "an e-voting election system that supports the convenience, ease-of-use, and mobility of online voting. It's unique in delivering best-of-breed security and information technology practices, easy to administer and easy to use - and has been praised for its effect on voter turnout and overall voter satisfaction."

But VerifiedVoting.org's news item says: "VoteHere, a Bellevue, Washington company developing security technology for electronic voting "suffered an embarrassing hacker break-in." The electronic intruder broke into the company's system last October and has now been identified, according to the company's CEO Jim Adler. This event got a lot of news coverage, but we're not sure of its significance, since VoteHere says they are going to release all their software."

Wait a second, we're not sure of its significance? VoteHere is

selling an Internet voting product but they apparently aren't capable of protecting their own network from attack and their sensitive files from theft. That certainly sounds significant to me, and this has absolutely nothing to do with whether their software is publicly accessible or not. The USA Today report quoted Adler as saying "the break-in did not affect the integrity of its voting technology." This certainly should reassure the "large and small corporations, professional associations, unions, cooperatives, universities, political organizations and government groups" that VoteHere is marketing RemoteVote that their product is not more vulnerable than the insecure platform it is running on top of. I know that I feel much better knowing that the hacker (and probably also his pals) has a copy of the source code.

🔥 More voting snafus in Palm Beach and Broward Counties

<Alan Fullilove <a.c.fullilove@ieee.org>>

Sat, 10 Jan 2004 14:30:55 -0500

Seems Palm Beach and Broward counties can't certify a recent election. The "winner" of the election won by 12 votes out of 10,844 cast. 137 votes were blank ballots.

From the PalmBeachPost newspaper:

"Florida law requires a manual or hand recount of all "under-votes"

and "over-votes" in an election decided by less than 0.25 percent.

But touch-screens leave behind nothing to count by hand. "

Oops !

http://www.palmbeachpost.com/politics/content/auto/epaper/editions/saturday/news_f3ff583cd1c3223d00af.html

✶ Correction re: Australian Voting (Williams, [RISKS-23.10](#))

<"Eric Ulevik" <eulevik@d2.net.au>>

Sat, 10 Jan 2004 20:34:50 +1100

I would like to correct some previous misinformation regarding the Australian electoral system.

In Australia, the law requires every person on the electoral roll to submit a valid vote. Simply getting your name checked off and leaving may result in the Electoral Commission staff recording a failure to vote. Note that the staff do not examine the votes before they are placed in the ballot box - meaning there is no enforcement of the validity requirement.

In the state of NSW, in my case, the penalty for not voting was a \$120 fine. I intended to refuse to pay the fine on principle as I do not believe in compulsory voting. However, the alternative penalty in the case was canceling my driving license.

Hence I voted 'donkey' - giving my preference by order on the ballot (which is determined randomly). Donkey votes are typically 5-10% of the Australian vote. The clear risk here is that attempting to enforce democratic principles increases the influence of random chance on the final results.

⚡ Re: Electronic car doors trap man (Healy, [RISKS-23.06](#))

<"Mitchell, Ian (MED, nVISIA)" <W.Ian.Mitchell@med.ge.com>>

Mon, 5 Jan 2004 14:03:54 -0600

I own a CRV 4WD. The way out in a situation such as this is probably through the rear window. Unlike the side windows, this is not electric. It is released by a button under the dash that connects to the window lock via a cable. Once released, the window can be pushed open from the inside. This completely mechanical system would presumably still function even when underwater, although if totally submerged it may be necessary for the water inside the vehicle to reach a certain level before the pressure can be overcome and the window opened.

⚡ The dangers of PGN-ing (Re: [RISKS-23.11](#))

<Simon Hogg <seth@hogg.org>>

07 January 2004 22:18

[PGN note: I messed up my PGN-ed version of the item with
Subject line

"Bank of England falls victim as e-mail scams rise by 400%"

It might more accurately have been titled

"Visa customers hit by phishing expedition seemingly from
Bank of England"

Oops! PGN]

As I'm sure many of the RISKS readers are aware, the Bank of
England is a
Central Bank and hence does not issue its own Visa (or any other
credit
cards) at least for consumers. Similarly, it doesn't operate
consumer bank
accounts. I suppose you could say that the Bank of England is
equivalent to
the Federal Reserve, *not* Bank of America. Therefore the BoE
is unlikely
to be a 'victim' in the ordinary sense of the word.

Therefore, I thought there was something a bit fishy with the
PGN version
saying that the "This was reportedly the first time BoE was
victimized by a
"phishing" expedition that apparently fooled about 5% of their
Visa
customers into divulging their card and PIN numbers."

Looking at the original news story the 'phishing' quote
apparently relates
to a different episode, "A campaign that targeted Visa credit
card holders
was said to have fooled one in 20 victims into divulging their
personal
details, including their card and pin numbers" *i.e. not the BoE
e-mail
itself*.

The point of the story is to say that lots of people were sent
an e-mail with
an executable attachment with the message "Please install our
special

software, that will remove all the keyloggers and backdoors from your computer." The implication (for the sender the hopeful implication) was that since the e-mail was apparently from the BoE, the software was in some way 'official'. Imagine the same e-mail in the US from someone@federal-reserve.gov.

I think the problem here is wider than a standard someone@aConsumerBank.com e-mail since it is apparently from a 'trusted' central bank (the one who controls the 'normal' banks) but it doesn't cause any direct 'damage' to the apparent sending agency.

So, three apparent risks;

1. Mis- / Dis-information (scaremongering?), accidental or otherwise, caused by incorrect summary of other news stories.
2. E-Mails apparently from a trusted source (common / usual RISKS here, but the 'trusted source' in this case is a 'super-trusted source').
3. For me the most worrying RISK is that the UK's "National High-Tech Crime Unit" came out with the very enlightening statement "We have opened the attachment, but we have so far not been able to find out what it does, if anything." How many programmers does it need to be able to analyse a piece of code to be able to work out what it does? Anti-virus labs are pretty good at this, so why not the Government-funded anti-crime 'specialists'? At least they are apparently being honest here(!).

COMPSAC 2004 Call for Contributions

<CS Asst Prof Dr Yuen Tak YU <ytyu@cs.cityu.edu.hk>>

Sun, 11 Jan 2004 19:38:55 +0800 (CST)

<http://www.cs.cityu.edu.hk/~ytyu>

COMPSAC 2004

The 28th IEEE Annual International Computer Software
and Applications Conference

September 27-30, 2004, HONG KONG

<http://rachel.utdallas.edu/compsac>

Major theme: DEVELOPING TRUSTWORTHY SOFTWARE SYSTEMS

15 Jan 2004: Deadline for WORKSHOP and PANEL PROPOSALS

15 Mar 2004: Deadline for REGULAR and WORKSHOP PAPERS

PROGRAM CO-CHAIRS:

W. Eric Wong, University of Texas at Dallas, USA, Email:
ewong@utdallas.edu

Karama Kanoun, LAAS-CNRS, France, Email: Karama.Kanoun@laas.fr

EUSPRIG CFP July 2004 Klagenfurt

<"Patrick O'Beirne" <mail2@sysmod.com>>

Wed, 07 Jan 2004 14:07:50 +0000

EuSpRIG 2004: Spreadsheet Risks, Development and Audit Methods

Theme: Risk Reduction in End-User Computing

Best practice for spreadsheet users in the new Europe

Thursday July 15th - Friday July 16th 2004

Klagenfurt University, Klagenfurt, AUSTRIA

For submission instructions, details of formatting, handling of
illustrations etc. download guidelines from www.eusprig.org

Patrick O'Beirne, European Spreadsheet Risks Interest Group

✶ REVIEW: "Ben Franklin's Web Site", Robert Ellis Smith

<Rob Slade <rslade@sprint.ca>>

Fri, 2 Jan 2004 07:56:31 -0800

BKBNFRWS.RVW 20031013

"Ben Franklin's Web Site", Robert Ellis Smith, 2000, 0-930072-14-6,

U\$24.50/C\$32.25

%A Robert Ellis Smith ellis84@rcn.com

%C P. O. Box 28577, Providence, RI 02908

%D 2000

%G 0-930072-14-6

%I Privacy Journal

%O U\$24.50/C\$32.25 401-274-7861 orders@privacyjournal.net

%O <http://www.amazon.com/exec/obidos/ASIN/0930072146/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0930072146/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0930072146/robsladesin03-20>

%P 407 p.

%T "Ben Franklin's Web Site"

In the introduction, Smith notes that Americans are both (and simultaneously) interested in protecting their privacy, and very curious about others. This work is a social history of American thought and feelings about privacy. The chapters are not numbered, but named. There is an attempt to assign date ranges to periods of events and opinion, but this effort is pretty much exhausted by the time the book ends.

"Watchfulness," from the late seventeenth to the early eighteenth century, notes an age of church based communities and close living.

Fear of the government registration is suggested to be primarily based

on anxiety about the fact that a low population (or other indicator of

lack of wealth) would reflect badly on the locale (or locals).

"Serenity" links geographic isolation with privacy, but mostly concentrates on early enumeration operations. The post office, more

about the census, and the beginnings of information technology with

Hollerith and Morse is in a chapter called "Mistrust." "Space" outlines the degradations of slavery, factories, and workhouses.

"Curiosity" looks at gossip and the popular press.

A chapter called "Brandeis" doesn't talk about him or his essay (with

Warren in the Harvard Law Review) as much as the intellectual environment and subsequent debate. Another reviews decisions and government actions in regard to different types of surveillance. It

is difficult to say what a chapter called "Sex" has to do with privacy, and it reuses a lot of material from "Serenity,"

"Curiosity,"

and "Brandeis." "Torts" examines various lawsuits related to invasion

of privacy. Politicking on the Supreme Court in cases possibly related to privacy populates a chapter called "Constitution."

"Numbers," unlike "Census," discusses the improper use of the Social

Security Number, as well as the concept of a national identity card.

Credit reporting agencies are examined in "Databanks."

"Cyberspace"

touches on a number of Internet related topics. "Ben Franklin's Web

Site" attempts to guess what Franklin's "Poor Richard's Almanac" would

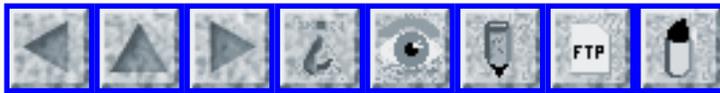
say about privacy, in pithy aphorisms: a kind of Poor Robert's list of

privacy protecting guidelines.

Smith's book is certainly an entertaining read, and does provide the occasional lost nugget of significant information on the development of thought in regard to privacy. It is, however, difficult to say how useful the work is for practical endeavours in pursuit of the protection of privacy, or development of current privacy policy.

copyright Robert M. Slade, 2003 BKBNFRWS.RVW 20031013
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

Volume 23: Issue 13

Friday 16 January 2004

Contents

- [Is the F-35 fighter jet is too reliant on foreign software](#)
[Lillie Coney](#)
- [Some rental cars keep tabs on drivers](#)
[Dewayne Hendricks via IP](#)
- [Israeli Post Office break-in](#)
[Gadi Evron](#)
- [Online poll rigging](#)
[Keith C. Ivey](#)
- [Students' data on Web, and NYU. on defensive](#)
[Monty Solomon](#)
- [Bruce Schneier on Orange Alert in Salon](#)
[Cory Doctorow via IP](#)
- [Some .mil and .gov subscribers of Risks Spammed](#)
[Dennis G Rears](#)
- [Errant weather alert](#)
[David Kennedy](#)
- [Moscow ML fails because of time overflow bug](#)
[Paul E. Black](#)
- [Re: Happy 2**30'th birthday, time_t!](#)
[Alistair McDonald](#) [Ed Ravin](#) [Massimo Dal Zotto](#)

- [Re: The dangers of PGN-ing](#)
[Peter Riocreux Huge](#)
 - [E-mail scam attacks AT*T Worldnet](#)
[John Reinke](#)
 - [PayPal spoofing](#)
[Jacob Palme](#)
 - [Announcement: Third Bieleschweig Workshop](#)
[Peter B. Ladkin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Is the F-35 fighter jet is too reliant on foreign software

<Lillie Coney <lillie.coney@acm.org>>

Fri, 09 Jan 2004 16:27:49 -0500

Defense: The House Government Reform Committee expects to hold hearings this year to determine whether the Lockheed Martin-made F-35 fighter jet is too reliant on foreign software, Defense Daily reported Thursday. The concern, according to a congressional source, is that the fighter, which has been hailed as a model for international cooperation, could require foreign software for integral parts of the aircraft's computer system. The <http://www.gao.gov/> General Accounting Office (GAO) is preparing a report on the issue and expects to brief committee members in about three to four weeks, the source added. The National Security, Emerging Threats and International Relations Subcommittee, chaired by Christopher Shays, R-Conn., frequently holds hearings on the status of such weapons-acquisition programs. The subcommittee's decision to look at the software

issue is part
of a broader concern about foreign software development and what
effect that
could have on the availability or security of the software.

✶ Some rental cars keep tabs on drivers (via Dave Farber's IP)

<Dewayne Hendricks <dewayne@warpspeed.com>>

Wed, 14 Jan 2004 00:33:21 -0800

Byungsoo Son (from Georgetown, Ontario) rented a car at a
Payless Car Rental
outlet in California for 12 days, with a contract rate of
\$259.51. When he
returned the car, he was charged \$3,405.05 and given a map
showing his
actual itinerary, tracked by GPS (including Las Vegas Nevada and
the Grand
Canyon in Arizona). He was charged \$1 for each mile driven
outside of
California -- in violation of his contract, whose stipulated the
car must
remain in California. [Source: Christopher Elliott, *The New
York Times*,
13 Jan 2004; PGN-ed] [http://www.nytimes.com/2004/01/13/
business/13gps.html](http://www.nytimes.com/2004/01/13/business/13gps.html)

[This is a classical cautionary RISKS case: READ THE FINE
PRINT! PGN]

Archives at: <<http://Wireless.Com/Dewayne-Net>>

IP Archives at: [http://www.interesting-people.org/archives/
interesting-people/](http://www.interesting-people.org/archives/interesting-people/)

✶ Israeli Post Office break-in

<Gadi Evron <ge@linuxbox.org>>

Sun, 11 Jan 2004 11:16:56 -0600 (CST)

My summary/article on what happened is at
www.math.org.il/post-office.rtf

[Thanks to Tom Van Vleck for alerting me to Gadi's article. A wireless gateway was surreptitiously installed in a computer rack in a Haifa branch of the Israeli Post Office (which also serves as a bank), perhaps allowing sniffing of passwords and other access. The perpetrators then remotely accessed the system to transfer money to newly opened accounts. The computer heist reportedly netted 56,000 shekels (USD\$13,000) in the few days it was in operation. Although withdrawals from the new accounts reportedly caused the perpetrators to be apprehended, Gadi speculates that with a little more care, the fraud could have gone undetected for much longer. PGN-ed]

✶ Online poll rigging

<"Keith C. Ivey" <kcivey@cpcug.org>>

Thu, 15 Jan 2004 07:58:42 -0500

The Senate Republican Conference has a Web poll on its front page about the capture of Saddam Hussein. Apparently the results weren't turning out the way they like (what a surprise for a Web poll!), so they changed

the form to switch the way two answers are recorded. Now if you choose the 1st choice, it's recorded as the 2nd, and vice versa. But there's no feedback to let you know it's happening. The change has been confirmed by checking Google's cache of the page. Here's the story:

http://atrios.blogspot.com/2004_01_11_atrios_archive.html#107414565730750569

If politicians are willing to tamper with something as insignificant as a Web poll, how much more tempting is it to tamper with the results of a real election?

Keith C. Ivey, Washington, DC <kcivey@cpcug.org>

[Added note: There was something very similar in November 2003 on Bill Frist's Senate site, too:

<http://reason.com/hitandrund/003421.shtml>

KCI]

Students' data on Web, and NYU. on defensive

<Monty Solomon <monty@roscom.com>>

Mon, 12 Jan 2004 00:41:53 -0500

Three years ago, when Brian Frank entered New York University, he signed up for intramural basketball, providing his name and his university identification number, which was also his Social Security number.

Yesterday morning, Mr. Frank, who is now a senior, learned from N.Y.U. that these details had been posted on the Internet. He was among about 1,800

N.Y.U. students who received the same e-mail notification from the university. In some cases, students' phone numbers were posted, too. ...

[Source: Karen W. Arenson, *The New York Times*, 10 Jan 2004]
<http://www.nytimes.com/2004/01/10/nyregion/10identity.html>

[An unidentified poster of the entire item in Dave Farber's IP list

added this pithy comment:

>Dave: Not mentioned in this article is that at the start of 2003,

>NYU laid off its senior system and network security manager, who

>had been with the university for nearly 18 years, in a budget-cutting

>round. At the time of the layoff, the manager was working on privacy

>issues, including HIPAA compliance.

PGN]

🔥 Bruce Schneier on Orange Alert in Salon (from Dave Farber's IP)

<Cory Doctorow <cory@eff.org>>

Fri, 09 Jan 2004 15:55:59 -0800

>Homeland insecurity

>The fact that U.S. intelligence agencies can't tell terrorists from children

>on passenger jets does little to inspire confidence.

>

>By Bruce Schneier

>

>9 Jan 2004 | Security can fail in two different ways. It can fail to

>work in the presence of an attack: a burglar alarm that a burglar

>successfully defeats. But security can also fail to work

correctly when

>there's no attack: a burglar alarm that goes off even if no one is there.

>

>Citing "very credible" intelligence regarding terrorism threats, U.S.

>intelligence canceled 15 international flights in the last couple of weeks,

>diverted at least one more flight to Canada, and had F-16s shadow others as

>they approached their final destinations.

>

>These seem to have been a bunch of false alarms. Sometimes it was a case of

>mistaken identity. For example, one of the "terrorists" on an Air France

>flight was a child whose name matched that of a terrorist leader; another

>was a Welsh insurance agent. Sometimes it was a case of assuming too much;

>British Airways Flight 223 was detained once and canceled twice, on three

>consecutive days, presumably because that flight number turned up on some

>communications intercept somewhere. In response to the public embarrassment

>from these false alarms, the government is slowly leaking information about

>a particular person who didn't show up for his flight, and two >non-Arab-looking men who may or may not have had bombs. But these seem more

>like efforts to save face than the very credible evidence that the

>government promised.

>

>Security involves a tradeoff: a balance of the costs and benefits. It's

>clear that canceling all flights, now and forever, would eliminate the

>threat from air travel. But no one would ever suggest that, because the

>tradeoff is just too onerous. Canceling a few flights here and there seems

>like a good tradeoff because the results of missing a real threat are so
>severe. But repeatedly sounding false alarms entails security problems, too.
>False alarms are expensive -- in money, time, and the privacy of the
>passengers affected -- and they demonstrate that the "credible threats"
>aren't credible at all. Like the boy who cried wolf, everyone from airport
>security officials to foreign governments will stop taking these warnings
>seriously. We're relying on our allies to secure international flights;
>demonstrating that we can't tell terrorists from children isn't the way to
>inspire confidence.
>
>Intelligence is a difficult problem. You start with a mass of raw data:
>people in flight schools, secret meetings in foreign countries, tips from
>foreign governments, immigration records, apartment rental agreements, phone
>logs and credit card statements. Understanding these data, drawing the right
>conclusions -- that's intelligence. It's easy in hindsight but very
>difficult before the fact, since most data is irrelevant and most leads are
>>false. The crucial bits of data are just random clues among thousands of
>other random clues, almost all of which turn out to be false or misleading
>or irrelevant.
>
>In the months and years after 9/11, the U.S. government has tried to address
>the problem by demanding (and largely receiving) more data. Over the New
>Year's weekend, for example, federal agents collected the names of 260,000
>people staying in Las Vegas hotels. This broad vacuuming of

data is

>expensive, and completely misses the point. The problem isn't obtaining

>data, it's deciding which data is worth analyzing and then interpreting it.

>So much data is collected that intelligence organizations can't possibly

>analyze it all. Deciding what to look at can be an impossible task, so

>substantial amounts of good intelligence go unread and unanalyzed. Data

>collection is easy; analysis is difficult.

>

>Many think the analysis problem can be solved by throwing more computers at

>it, but that's not the case. Computers are dumb. They can find obvious

>patterns, but they won't be able to find the next terrorist attack. Al-Qaida

>is smart, and excels in doing the unexpected. Osama bin Laden and his troops

>are going to make mistakes, but to a computer, their "suspicious" behavior

>isn't going to be any different than the suspicious behavior of millions of

>honest people. Finding the real plot among all the false leads requires

>human intelligence.

>

>More raw data can even be counterproductive. With more data, you have the

>same number of "needles" and a much larger "haystack" to find them in. In

>the 1980s and before, East German police collected an enormous amount of

>data on 4 million East Germans, roughly a quarter of their population. Yet

>even they did not foresee the peaceful overthrow of the Communist

>government; they invested too heavily in data collection while neglecting

>data interpretation.

>

>In early December, the European Union agreed to turn over
detailed passenger
>data to the U.S. In the few weeks that the U.S. has had this
data, we've
>seen 15 flight cancellations. We've seen investigative
resources chasing
>>false alarms generated by computer, instead of looking for real
connections
>that may uncover the next terrorist plot. We may have more
data, but we
>arguably have a worse security system.

>
>This isn't to say that intelligence is useless. It's probably
the best
>weapon we have in our attempts to thwart global terrorism, but
it's a weapon
>we need to learn to wield properly. The 9/11 terrorists left a
huge trail of
>clues as they planned their attack, and so, presumably, are the
terrorist
>plotters of today. Our failure to prevent 9/11 was a failure of
analysis, a
>human failure. And if we fail to prevent the next terrorist
attack, it will
>also be a human failure.

>
>Relying on computers to sift through enormous amounts of data,
and
>investigators to act on every alarm the computers sound, is a
bad security
>tradeoff. It's going to cause an endless stream of false
alarms, cost
>millions of dollars, unduly scare people, trample on individual
rights and
>inure people to the real threats. Good intelligence involves
finding meaning
>among enormous reams of irrelevant data, then organizing all
those disparate
>pieces of information into coherent predictions about what will
happen next.
>It requires smart people who can see connections, and access to
information
>from many different branches of government. It can't be seen by

the various
>individual pieces of bureaucracy; the whole picture is larger
than any of
>them.
>
>These airline disruptions highlight a serious problem with U.S.
>intelligence. There's too much bureaucracy and not enough
coordination.
>There's too much reliance on computers and automation. There's
plenty of raw
>material, but not enough thoughtfulness. These problems are not
new; they're
>historically what's been wrong with U.S. intelligence. These
airline
>disruptions make us look like a bunch of incompetents who cry
wolf at the
>slightest provocation. [...]

IP Archives at: <http://www.interesting-people.org/archives/interesting-people/>

[Also, See Bruce's Crypto-gram: <http://www.schneier.com/crypto-gram.html>

PGN]

✶ Some .mil and .gov subscribers of Risks Spammed

<"Rears, Dennis G [AMSTA-AR-FSP-S]" <d.rears@us.army.mil>>

Wed, 14 Jan 2004 18:11:39 -0500

It was just recently brought to my attention that over the last
week readers
of RISKS with e-mail addresses in the .mil and .gov domains have
been
getting spam that was sent to risks-mil@pica.army.mil. That
address was set
up years ago to help Peter manage the huge RISKS e-mail list.
As a favour
to Peter, I managed all .mil and .gov e-mail addresses for most

of the
1990s. As part of the Risks Distribution he would send mail to risks-mil@pica.army.mil, which then resent the mail to over 500 . mil/.gov subscribers. The risks-mil address was hidden so that people would not send to it. Last year I stopped the exploder list and all e-mail addresses from that list were forwarded to Peter to be included in his master list (with risks-mil@pica.army.mil being deleted from the master list). However I never got around to disabling the risks-mil@pica.army.mil address. Thus spammers were able to exploit this oversight via risks-mil@pica.army.mil. I have now taken steps to solve that problem by disabling the address. Yet another risk of not cleaning up things.

⚡ Errant weather alert

<David Kennedy CISSP <david.kennedy@acm.org>>

Tue, 13 Jan 2004 00:13:10 -0500

<http://www.washingtonpost.com/wp-dyn/articles/A63858-2004Jan7.html>

01/07/04: The National Weather Service's Office of Science and Technology in Silver Spring sent a test weather-alarm message on Wednesday afternoon. Intended for internal use only, it was instead sent via the Internet around the world. The alarm forecast a blizzard in the Washington DC area.

"We thought all of the systems that were capable of going live

out of this

other facility where they do development had been disconnected, so that

this could not happen again," Travers said. "Well, I guess they found out that something had not been disconnected."

[It gets better.]

Other weather-related services using the NWS feed contributed to the false alarm by re-sending it to their customers, some of whom use proprietary desktop weather clients like Weatherbug and Accuweather.

Jack Hayes, director of the Office of Science and Technology, said bogus

messages have snuck out before. His office wrestles with the challenge of

getting weather hazard information out as quickly as possible. Any human

who had looked out the window would have known this warning was a

mistake. But humans can gum up the works when trying to issue lifesaving

alerts. "Any time you have a human [in the process], you introduce a

delay in getting an important warning out to the public," Hayes said.

[NOTE a similar previous case: NOAA training session test message warns

of hotter weather as Earth nears the Sun ([RISKS-23.07](#)). PGN]

✶ Moscow ML fails because of time overflow bug

<"Paul E. Black" <paul.black@nist.gov>>

Fri, 16 Jan 2004 10:50:12 -0500

HOL, a system for proving theorems in Higher Order Logic,
<http://sourceforge.net/projects/hol/>
is implemented in Moscow ML, an implementation of Standard ML.
<http://www.dina.dk/~sestoft/mosml.html>
For soundness, HOL records the time along with new types or
theories
(collections of theorems, types, values, etc.) which are
created. When
time values overflowed on Saturday 10 January in a few libraries
of the
underlying Moscow ML 2.00, HOL was rendered unusable.

Moscow ML represents time as seconds since midnight 1 January
1970. After
10 January the number of seconds exceeded 2^{30} . Although this
was
anticipated and most code for time handled this, a few libraries
did not.

<http://www.dina.kvl.dk/~sestoft/mosml/y2004bug.html>

Maintainers issued a patch for HOL and fixes for Moscow ML
within days.

Paul E. Black, NIST, 100 Bureau Drive, Stop 8970, Gaithersburg,
MD 20899-8970
+1 301 975-4794 <http://hissa.nist.gov/~black/> paul.black@nist.
gov

✶ Re: Happy 2**30'th birthday, time_t! ([RISKS-23.12](#))

<"Alistair McDonald" <alistair@inrevo.com>>
Tue, 13 Jan 2004 00:00:59 -0000 (GMT)

Paul Eggert ends his piece with a thought that a lot of
applications will
break in 2038. I think that the problem will appear much sooner
than that,

as some software (reservation systems, timetabling, and so on) looks into the future.

I hope that the `time_t` wraparound will be a thing of the past by 2010, but I also hope that some legacy systems from "way back" will still be running. These systems, maybe embedded, might just fail once and carry on, or they might be useless as they interface with the real world and their dates will be 2^{32} seconds out.

Alistair McDonald InRevo Ltd. <http://www.inrevo.com> (+44)(0) 7017-467386

⚡ Re: Happy 231 birthday, `time_t`! ([RISKS-23.12](#))**

<Ed Ravin <eravin@panix.com>>
Tue, 13 Jan 2004 01:27:14 -0500

> About 13 hours ago, the POSIX `time_t` counter exceeded 2^{30} , thus reaching
> half its useful positive range (which counts seconds since 1970) on
> traditional hosts with 32-bit signed integer `time_t`.

My shop uses an old version of the Heimdal implementation of the Kerberos authentication system (supplied with NetBSD 1.5), and we found that after the Unix `time_t` "birthday", our Kerberos clients were issuing erroneous requests. The result was that many of our staffers coming in to work on Monday morning couldn't log in to their workstations.

It's moments like this that make me appreciate the necessity of

diverse software implementations - since we had other versions of Kerberos available (i.e. MIT Kerberos and a newer version of Heimdal with the bug fixed), all of which worked, we were able to quickly identify the buggy client program.

✉ **Re: Happy 2**30'th birthday, time_t! ([RISKS-23.12](#))**

<Massimo Dal Zotto <dz@cs.unitn.it>>
Tue, 13 Jan 2004 21:59:19 +0100 (CET)

We have another interesting precedent:

<http://catless.ncl.ac.uk/Risks/21.69.html#subj7>

Massimo Dal Zotto <dz@debian.org>

✉ **Re: The dangers of PGN-ing (Hogg, [RISKS-23.12](#))**

<Peter Riocreux <peter.riocreux@cakes.org.uk>>
12 Jan 2004 23:30:33 +0000

> As I'm sure many of the RISKs readers are aware, the Bank of England is a
> Central Bank and hence does not issue its own Visa (or any other credit
> cards) at least for consumers.

Except that it **does** have consumer accounts, it is just that eligibility is severely limited. Current (and possibly past) employees are

certainly able
to hold an account, but I know not what other persons may hold
one. As
such, it is perfectly possible that they could have been the
target of a
phishing expedition.

The RISK is assuming that the system is the same as in the US,
something
which, despite the UK government's best efforts, is still
commonly not the
case.

⚡ The dangers of PGN-ing (Hogg, [RISKS-23.12](#))

<huge@huge.org.uk (Huge)>
Fri, 16 Jan 2004 17:04:55 +0000 (GMT)

[PGN: Peter Riocreux's point above was also noted by Huge, who
added this:]

> How many programmers does it need to be able to analyse a
piece of code to
> be able to work out what it does?

In this case, none! The attachment was conveniently [and
correctly] named
as a keystroke logger.

⚡ E-mail scam attacks AT*T Worldnet

<"John Reinke" <reinke@att.net>>
Sat, 10 Jan 2004 10:44:00 -0500

-----Original Message-----

From: attwns-announcement-system

[mailto:CustomerNotifications@worldnet.att.net]

Sent: Saturday, January 10, 2004 1:04 AM

To: AT&T Worldnet Customers

Subject: ALERT: E-mail scam - [Billing Update Requested (URGENT)]

Dear AT&T Worldnet Service Member,

You may have received a fraudulent e-mail with the Subject line of "Billing Update Requested (URGENT) " from a sender's address that is either att.billing@worldnet.att.net or billing@worldnet.att.net. This counterfeit e-mail requests that you resubmit your credit card information for billing purposes.

[That] e-mail is not from AT&T Worldnet Service. Please do not respond to it -- instead disregard and delete it.

If you have already provided your credit card information in response to the fraudulent e-mail, we recommend you notify your credit card issuer immediately.

If at any time you receive an e-mail requesting billing information, please be aware that it is likely to be a scam. Authentic billing notifications sent by AT&T Worldnet Service will always direct you to visit the AT&T Worldnet Member Services secure site, where you will login with your userid and password to update your billing information.) Please forward any suspicious e-mail to AT&T Special Investigations at scam@abuse-att.net."

For more information on how to protect yourself against identity

theft,
please visit the US Federal Trade Commission's Identity Theft
web site, at
<http://www.consumer.gov/idtheft>

AT&T Worldnet Service

[But they overlook the fact that the message did direct the
reader to a
site that APPEARED to be an AT&T site. Sheesh, doesn't anyone
read over
there? John]

✶ PayPal spoofing

<Jacob Palme <jpalme@dsv.su.se>>
Sat, 10 Jan 2004 13:58:53 +0100

I received a message which is abbreviated below [and even more
by PGN]:

```
> Received: from unknown (HELO reva) (81.196.161.141)
>   by 0 with SMTP; 6 Jan 2004 01:55:14 -0000
> Reply-To: "service@paypal.com" <spooff@paypal.com>
> From: "service@paypal.com" <service@paypal.com>
> To: <jpalme@dsv.su.se>
> Subject: Account issue
> Date: Tue, 6 Jan 2004 03:51:33 +0200
>
> Due to concerns, for the safety and integrity of the PayPal
> community we have issued this warning message.
>
> It has come to our attention that your account information
needs
> to be renew due to inactive members and non-functioning
mailboxes.
> If you could please take 5-10 minutes out of your online
> experience and renew your records you will not run into
```

> any future problems with the online service.
>
> However, failure to update your records will result in account
> deletion [sic]. This notification expires on January 10,
2004.
>
> Once you have updated your account records your PayPal will
not be
> interrupted and will continue as normal.
>
> Please follow the link below and renew your account
information.
> <http://https-ebay.com> PayPal Service Department

When I clicked on the link, I got to a form which requested a
number of
personal data, including my credit card number, its security
code and its
PIN code! I have put up a copy of the form they asked me to fill
in at

<http://dsv.su.se/jpalme/temp/domain-name-spam-2c.pdf>

I got suspicious for several reasons:

(a) No company has ever before asked me for my credit card PIN
code.

(b) This information was requested by http, not https. But with
a domain
name, <http://https-ebay.com> which might make some people believe
it was
actually using https.

(c) Looking up in whois indicates that the owner of the domain
name
<https-ebay.com> is a private person, not a company.

To be on the safe side, I immediately blocked my credit card,
since I had
entered some information before I understood this was a spoof. I
also wrote
to PayPal, who confirmed that the mail was not from them!

I have learnt to be more careful and suspicious in the future!

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

[This is increasingly becoming a problem! We desperately need
some greater authentication and accountability. PGN]

✂ Announcement: Third BieleSchweig Workshop (abridged for RISKS)

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

Fri, 09 Jan 2004 08:45:13 +0100

The Third BieleSchweig Workshop on System Engineering.
Main themes: Risk Analysis and Root-Causal Analysis
An event of the German Chapter of the System Safety Society
12-13 February, 2004
Center for Interdisciplinary Research (ZiF), Bielefeld

Convened by
University of Bielefeld, Faculty of Technology, RVS Group
Siemens Transportation Systems, Rail Automation
Technical University of Braunschweig, Institute for Railway
Systems Engineering and Transport Safety

In the Third BieleSchweig Workshop, we shall have causal-analysis
presentations on the 1994 "Friendly Fire" shutdown of two
helicopters (WBA,
comparison with existing sociological and STAMP analyses), the
Herald of
Free Enterprise capsized (SOL, MES, ECF, comparison), the Brühl
derailment
(SOL) and the Royal Majesty grounding (SOL), and the development
of
CausalML, all of which work had been planned during the First
and Second
Workshops. On the new theme of risk analysis, we shall have

presentations on the PROFUND method, and on the Improved Risk Priority Number concept recently developed at Siemens. We shall hold moderated discussions on the causal analysis comparison criteria, as well as on one of the themes: visualisation, system safety tasks, investigative processes, and countermeasures.

We invite additional papers on themes in system engineering, especially concerned with risk analysis, from all applications areas. Please send proposals for talks (max. 2 pages) to

Peter Ladkin (ladkin@rvs.uni-bielefeld.de)
by Friday, January 23, 2004.

Further details, including travel information, may be found in the Third Bieleschweig Workshop announcement in the Bieleschweig pages available through www.rvs.uni-bielefeld.de .

Peter B. Ladkin, University of Bielefeld, 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

Volume 23: Issue 14

Tuesday 27 January 2004

Contents

- [Spirit Rover humbled by classic programming error](#)
[Robert Woodhead](#)
- [New virus infects PCs, whacks SCO](#)
[Monty Solomon](#)
- [Panel reports DoD SERVE System fatally flawed - bureaucrats in denial](#)
[Scott Miller](#)
- [Roadside camera claims car going 406 mph](#)
[greep](#)
- [The risks of naming](#)
[Ross Anderson](#)
- ["Outsourced and Out of Control"](#)
[Lauren Weinstein](#)
- [Pun-intended definitions](#)
[PGN](#)
- [UK data protection laws and the Law of Unintended Consequences](#)
[Richard Pennington](#)
- [Lie-detector glasses, 90% accurate?](#)
[Steve Holzworth](#)
- [DHS protects vendors of anti-terrorism technologies from liability](#)
[Jay Wylie](#)

- [Privacy & security threats in one](#)
[Jeremy Epstein](#)
 - [Rob Slade's review of Marcus Ranum's *The Myth of Homeland Security*](#)
[Marcus J. Ranum](#)
 - [Proceedings on ... Engineering Principles of System Security ...](#)
[Daniel P. Faigin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Spirit Rover humbled by classic programming error

<Robert Woodhead <trebor@animeigo.com>>

Tue, 27 Jan 2004 08:31:46 -0500

Is it just me, or is it truly ironic that the Spirit Rover (now, thankfully, on the road to recovery) was brought down by a variant of the classic "fixed length buffer" error?

See: <http://spaceflightnow.com/mars/mera/040126spirit.html>

Even on Mars, it seems, the RISKS are obvious. And clearly, the Spirit's designers had learned some lessons from previous space experience, and were not too proud of the technological terror they had created -- they had a way to boot into the monitor, so to speak.

Woodhead's Law: "The further you are from your server, the more likely it is to crash." (particularly appropriate in this case)

[There was an item on the radio news about the computer having tried to reboot something like 60 times. Next time we'll have to send gifted SysAdmins up with the rovers? PGN]

⚡ New virus infects PCs, whacks SCO

<Monty Solomon <monty@roscom.com>>

Mon, 26 Jan 2004 22:21:56 -0500

Robert Lemos, CNET News.com, 26 Jan 2004, 5:58 PM PST

A mass-mailing virus quickly spread through the Internet on Monday, compromising computers so that they attack the SCO Group's Web server with a flood of data on Feb. 1, according to antivirus companies. The virus--known as MyDoom, Novarg and as a variant of the Mmail virus by different antivirus companies--arrives in an in-box with one of several different random subject lines, such as "Mail Delivery System," "Test" or "Mail Transaction Failed." The body of the e-mail contains an executable file and a statement such as: "The message contains Unicode characters and has been sent as a binary attachment."

<http://news.com.com/2100-7349-5147605.html>

[Oodles of other URLs omitted. PGN, who has been wading through hundreds of extra messages today. GRRROAN.]

⚡ Panel reports DoD SERVE System fatally flawed - bureaucrats in denial

<Scott Miller <SMiller@unimin.com>>

Thu, 22 Jan 2004 14:17:58 -0500

A four member panel (out of a 10-member peer review group) has condemned the Pentagon's Secure Electronic Registration and Voting Experiment for inherent and irreparable security flaws in the public computing infrastructure.

"I think that a dedicated and experienced hacker could subvert the election rather easily..." - Dr. Aviel D. Rubin, technical director of Johns Hopkins' Information Security Institute.

"The only 100% way we can avoid some of the security issues [raised by the four panel members] is to not do this. And that is not something we will do..." - Glen Flood, a spokesman for the SERVE project.

Computerworld article -

<http://www.computerworld.com/securitytopics/security/story/0,10801,89290,00.html>

Panel report - <http://www.servesecurityreport.org/>

⚡ Roadside camera claims car going 406 mph

<greep <greep@mindspring.com>>

Wed, 21 Jan 2004 12:23:39 -0800

This is excerpted from the *Sun*

<http://www.thesun.co.uk/article/0,,2-2004031766,00.html>):

Driver Peter O'Flynn was stunned to receive a speeding notice claiming a roadside camera had zapped him -- at an astonishing 406MPH. The

sales

manager, who was driving a Peugeot 406 at the time, said: "I rarely speed and it's safe to say I'll contest this." Officials admitted it was a clerical bungle, but insisted he would still be prosecuted. (The Peugeot 406 Sport has a top speed of 129mph.)

🔥 The risks of naming

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

Fri, 23 Jan 2004 17:55:37 +0000

Regular RISKS readers know that many things can go wrong with naming, and affect systems that use ID cards, PKIs and suchlike. But this morning I came across a new and quite surprising failure mode.

I suddenly learned that I did not know how to spell my own name!

Recently, we had to manufacture a version of my name in Korean characters (Hangul) for a Chinese new year card. A local Korean scholar duly assisted and off went the card.

This morning, I was tipped off by one of the recipients that my name was

`wrong'. It turns out that people in Korea who work with information security have arrived at a consensus on the Hangulisation of my name, as

indeed they have for many other foreign computer science researchers. It

turns out that I'm not 'Los An-del-son', as my informant had suggested;

`everyone in Korea' knows me as 'Lo-ssue En-da-son'. So there we

have

it. You may be well-known by a name you never knew you had. I expect there was no way a Korean who was unaware of the consensus could have second-guessed the spelling.

So that's what it's like to be called Gaddafi / Ghazzafi / Qadhafi!

Meanwhile, on Wednesday, I went and got a visa for India, so now my passport has stuff in it in yet another script. And no doubt when I visited Japan there was at least one version of my name knocking about in at least one kind of kana.

This underlines the risks of the consensus emerging among governments post-9/11, which is that people acquire names only because a government issues a birth certificate; and so governments need to build huge infrastructures of databases, biometrics and ID cards to support this vital social function of knowing people's names. I rather fear that, in our multicultural world, the task of making everyone's names correct and consistent might lie beyond our technical and organisational capabilities.

✶ "Outsourced and Out of Control"

<Lauren Weinstein <lauren@vortex.com>>

Tue, 06 Jan 2004 09:03:47 -0800

Since the topic of outsourcing is of great concern currently, I've made

available a copy of my "Inside Risks" column that will appear in the upcoming February 2004 edition of "Communications of the ACM" (CACM).

It is titled "Outsourced and Out of Control" and is located at:

<http://www.pfir.org/outsourced-cacm>

As the column discusses, while the issue of job losses is serious enough, other factors, such as privacy and security risks, also need to be considered!

Lauren Weinstein, lauren@pfir.org 1-818-225-2800 <http://www.pfir.org/lauren>

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

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

⚡ Pun-intended definitions

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

Tue, 6 Jan 2004 14:05:15 PST

The Sunday *San Jose Mercury* (4 Jan 2004) had a wonderful article on the 50 best punny definitions of the year. Here is a sampling of a few with computer technology relevance.

off-shorn: vt. Getting cut because your job moved overseas.
[Rainer Richter, San Jose]

Microsofa: n. A piece of furniture that, while it looked fine in the showroom, gradually begins to dominate the living room, eventually forcing you to replace all the other furniture,

including the TV, to be "compatible". [Earl T. Cohen, Fremont]

motherbored: n. In many homes, a technology discussion at dinner between father and the kids. (Bruce Kerr)

Luddate: n. Someone you are going out with who does not understand the [Santa Clara] Valley's obsession with technology. (Lisa Lawrence, Palo Alto)

Crisco: n. A person who got fried by buying Cisco at \$80 a share. (Jim Schutz)

[Mercurial typo corrected in archive copy. PGN]

UK data protection laws and the Law of Unintended Consequences

<Richard Pennington <richardhelen.pennington@virgin.net>>
Sun, 18 Jan 2004 21:04:05 +0100

There are two cases causing a stir here in the UK where misinterpretation of the UK Data Protection Act has been blamed for serious unintended consequences, including loss of life.

Case 1: A school in Cambridgeshire (UK) advertised for a new caretaker (for US readers, read 'janitor'). Because of child protection legislation, a routine criminal record check was performed by local police on the successful applicant. Because the applicant had previously lived in another

area (Lincolnshire), the local police, as a matter of routine, contacted Lincolnshire police and received a 'clean' report; a similarly 'clean' report was then given to the school, who confirmed the appointment. The caretaker later murdered two of the schoolchildren (aged 9 and 10). The resulting inquiry revealed that the caretaker, while in Lincolnshire, had been the subject of multiple relevant allegations (indecent assault and worse), none of which had ever been brought to court. Lincolnshire police claimed that, under the (UK) Data Protection Act, they were obliged to destroy the records of the alleged offences when the investigations ended without a trial. As a result, the various investigations in Lincolnshire never heard about each other, and none of the information was forwarded to Cambridgeshire.

Case 2: Responding to an unpaid gas bill, British Gas disconnected the gas supply from an elderly couple in August 2003 (at which time the weather was extremely hot), and did not notify the local Social Services. The few months later, the couple were found in their apartment, dead from hypothermia (the weather now being much colder). British Gas claimed that (under the UK Data Protection Act) they were unable to contact local Social Services because they did not have the written permission of the couple to disclose their financial records.

In both cases, the UK Data Protection Registrar (the official in charge of information protection and privacy) has indicated that the official bodies

involved) misunderstood the meaning and intent of the legislation, despite existing guidance. The guidance is now in the process of being rewritten and clarified. But, in these two cases, four lives were lost.

[Note added in archive copy: A member of the Lincolnshire police has pointed out that the references to his police force are incorrect; this article should have referred to the Humberside Police. PGN]

✶ Lie-detector glasses, 90% accurate?

<Steve Holzworth <sch@unx.sas.com>>
Tue, 20 Jan 2004 17:33:11 -0500

Starkly excerpted:

<http://www.eetimes.com/story/OEG20040116S0050>

It may not be long before you hear airport security screeners ask, "Do you plan on hijacking this plane?" A U.S. company using technology developed in Israel is pitching a lie detector small enough to fit in the eyeglasses of law enforcement officers, and its inventors say it can tell whether a passenger is a terrorist by analyzing his answer to that simple question in real-time. ...

The company showed plain sunglasses outfitted with the technology at the 2004 International CES in Las Vegas earlier this month. The system used green, yellow and red color codes to indicate a "true," "maybe" or "false"

response. At its CES booth, V Entertainment analyzed the voices of celebrities like Michael Jackson to determine whether they were lying. ...

"It is very different from the common polygraph, which measures changes in the body, such as heart rate," said Richard Parton, V's chief executive officer. "We work off the frequency range of voice patterns instead of changes in the body." The company said that a state police agency in the Midwest found the lie detector 89 percent accurate, compared with 83 percent for a traditional polygraph.

[SCH - oh, excellent! I only have a 1 in 10 chance of being falsely accused.]

Steve Holzworth, Senior Systems Developer, SAS Institute - Open Systems R&D
VMS/MAC/UNIX Cary, N.C. sch@unx.sas.com

⚡ DHS protects vendors of anti-terrorism technologies from liability

<Jay Wylie <jwylie@ece.cmu.edu>>
Sun, 18 Jan 2004 14:11:53 -0500 (EST)

[This note considers an] article "Guarding Against Terrorism-- And Liability" by Roland L. Trope in the January 2004 issue of *IEEE Spectrum*.

The article gives some details about the SAFETY (Support Anti-terrorism by Fostering Effective Technologies) Act of 2002. The act protects vendors of

anti-terrorism products that have been vetted by the Department of Homeland Security and designated as QATT (Qualified Anti-Terrorism Technology) from liabilities that arise from any failings of the anti-terrorism technology. Specifically, the DHS determines a level of insurance that must be carried, and this level caps the liability of the vendor.

Seeing the quality of software that is produced in an environment in which software vendors are free of liability, I am concerned about the quality of products generated under such protection as offered by SAFETY. As well, the color-coded threat levels of the DHS does not give me much confidence in their ability to evaluate technologies that offer protection from terrorism (security is complicated, colors are not). Most disappointing though, is that a publication of a professional society of engineers is more concerned about vendors being aware of the protection from liability than questioning whether such protection is appropriate.

P.S., More info on SAFETY can be found at www.safetyact.gov, but the secure web site certificate is not configured properly...

✶ Privacy & security threats in one

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Wed, 21 Jan 2004 12:33:59 -0500

I've recently joined LinkedIn, which is one of the crop of electronic meeting places for making business contacts based on six degrees

of separation. I'm pretty suspicious of the privacy issues, and therefore won't tell them anyone I know about, unless I see that they're already members. That obviously limits the size of my circle, but gives me (and my contacts) more privacy.

To boost the number of members, they recently sent out a message encouraging people to use a new feature: it will compare everyone in your Outlook contact list to the list of members, and tell you who you know about who's already a member. The tool is an ActiveX control (since I don't run IE, I don't know if it's signed or unsigned). There's no warnings on their site about the dangers of running code of this sort... but there is a note "When you start importing, you will see a security warning similar to this one:
[image of an ActiveX control approval box] Simply press the "Yes" button to agree to the upload."

So they're encouraging you to risk both your privacy **and** your security in one easy step.

Thanks but no thanks.

⚡ Rob Slade's review of Marcus Ranum's **The Myth of Homeland Security**

<"Marcus J. Ranum" <mjr@ranum.com>>
Mon, 26 Jan 2004 20:20:28 -0500

[First of all, an explanatory note. In deciding to run Rob Slade's review of Marcus Ranum's book, *The Myth of Homeland Security*, Wiley, 2004, I thought that -- because of the nature of the topic -- it would be appropriate to give Marcus an opportunity to respond. Because he has completely encapsulated the content of Rob's review in his commentary, I decided to avoid duplication and just run the response with the review interstiated (and prefaced by "> "). I hope that is a reasonable strategy for RISKS readers. PGN]

First off, let me thank Rob for being so kind as to review my book in this forum. If there's "no such thing as bad publicity" I suppose I must be grateful. :) I'd like to take the liberty to comment on a few aspects of the review.

> Chapter one asserts that Homeland Security is (along with a number of other similar terms) a convenient invention. Information warfare is derided as such a device, and although I could agree in terms of books such as Erbschloe's (cf. BKINFWFR.RVW), I don't think Ranum gives enough thought to the work by Dorothy Denning (cf. BKINWRSC.RVW).

My book was aimed at a popular audience - the intended victims of the Homeland Security scam - rather than at computer security professionals who are familiar with Dr. Denning's books. My object in the book is not to engage in a debate of scholarship as much as to point out some

of the
obvious bogusness that is being put about in the popular media.
As I express
in my book, even the "serious" Information Warfare proponents
are guilty of
using it as a FUD-vehicle to sell their services and products,
and
completely ignore many serious flaws in the concept - such as
the problem of
logistics as applied to "cyberweapons." Simply saying that my
book doesn't
pay adequate attention to Denning should not justify dismissing
it.

> He is also seemingly inconsistent in his positions, arguing
> generally against biometrics and profiling, but then apparently
> endorsing them.

You must have skimmed that section. :) I pointed out that
biometrics
actually wouldn't have prevented any recent terrorist incidents,
though
widescale deployment of biometrics would have been vastly
beneficial to the
vendors of said systems. ;) If you consider that an
"endorsement" it's an
endorsement of faint praises. :) I was rather dismayed to see
that, in
another gesture of homeland security grandstanding, the
biometrics passport
hype has managed to gain some momentum. Nobody in the homeland
security
arena seems to be able to address the problem: so what if you
know WHO the
person is, how do you know what kind of person they are?

> The arguments are not reasoned: he is for a national identity
system, but
> admits elsewhere that the 9/11 terrorists had valid
identification.

I am NOT in favor of a national identity system. I DO think it
is ridiculous

to have 50 states issuing ID based on 50 different trust criteria, using 50 different types of alteration-resistance technology, and with no way of checking to see if they're actually real without calling that state's Department of Motor Vehicles. The issue I was trying to point out is that, in such an environment, it's silly to be requiring ID before letting someone on a plane. Does that make me in favor of a national identity system? My point is that if we're going to go down this route we may as well get it right and stop trying to slap half-arsed measure atop half-arsed measure.

> Chapter seven says that the army is good, the border patrol is looking for
> the wrong things (although this is confusingly amended to a position that
> they have the technology but aren't using it), and the FBI and CIA have an
> ongoing turf fight.

I understand the need to make your review more entertaining by being flippant - I did NOT say "the army is good" and you know it, if you actually read the book. Chapter seven focuses on the fundamental reasons why military approaches to security, law enforcement approaches to security, and intelligence approaches to security will all be different and are, in fact, highly incompatible. That's a much different discussion from "the army is good" and you know it. :) As someone who reviews books for publishers myself, I know the importance of not allowing my personal feelings about a book to influence how I present its contents. I would have no problem with

your review if you kept it fair (e.g.: "Ranum tries to make a case that the FBI and CIA will be unable to ever converge on a cooperative approach to counterterrorism and fails because blah blah blah" but jocularly summarizing aspects of a writer's thinking as you do above is more appropriate for a music review in a punk rock magazine than a review in a technical mailing list.

> Cyberattacks are an unreal myth, says chapter nine, but our
> information infrastructure is mostly undefended. The lack of
> standardization in government systems is seen as making
government
> systems harder to defend (even though homogeneity means that a
single
> attack can penetrate everything).

Note: the parenthetical above is the reviewer's opinion, not a position I take in my book. My focus on the feebleness of government security is from a viewpoint of manageability, technical competence, and lack of standardization, not from a "monoculture" hype perspective.

> While this material starts off very well, possibly due to
Ranum's greater
> familiarity with strictly technical issues, he makes numerous
errors in
> regard to viruses and malware. His lack of experience in this
specific
> area reappears in chapter ten, where he says that even
outdated antivirus
> scanners should have caught Code Red because the exploit was a
known one.

I am really annoyed by this part of your review. Never mind that you're obviously the malware guru, but in this forum you're pretending to be a book reviewer. As such, it's not proper to mis-characterize a book to

suit your

ends. I said NOTHING like what you attribute to me, above. My comments on

CodeRed in specific and malware in general were broad and read:

"When CodeRed broke out, my company's system administrator knew about it

within an hour, had verified that our systems weren't vulnerable to it, and

had gone on to doing something else. We weren't vulnerable to CodeRed

because CodeRed relied on a vulnerability that the security community had

known about for the past three months, and that had been fixed by most

diligent system administrators."

Does that say something about even outdated virus scanners? I also touched

on malware briefly when I wrote, about CodeRed and Slapper (malware in

general) "What the public at large may not realize is that these attacks

usually only disrupt organizations that have failed to take even basic

precautions to protect themselves." This is not "out of date antivirus

scanners" I am referring to here, but the combination of reasonable A/V

policy, boundary attachment scanners, firewalls, etc. These techniques DO

work and they work well. Organizations that get reamed by malware and worms

are frequently trying to "have their cake and eat it too" from a security

perspective and prefer to blame others rather than their own inability to

follow simple best practices.

I am disturbed that you'd so seriously mis-characterize a book you're

reviewing in a public forum like this. Did you actually read my book before

you wrote your review? If I send you a copy will you read it, please?

> However, scanners would not have caught Code Red since it did not
> write itself out to a file, and also because scanners search for
> strings or patterns, not exploits. (If anything should have caught
> Code Red it was more likely to have been the firewalls that Ranum has
> made his name in designing.)

I'm just amazed that you're taking off on this point. The only reference to CodeRed in Chapter nine are both on page 141 and nowhere do I say anything about A/V scanners. Did you actually read Chapter nine, or are you perhaps confusing my book with another? [Actually, the specific mitigation we had in place at NFR that made CodeRed a non-event was our proxy firewall, as you guessed.]

> Those of us who work in the security field can certainly sympathize
> with the tone of Ranum's work. Yes, governments (and businesses) are
> foolish. Yes, the general public sees a complex problem in simplistic
> terms. Yes, you can find instances of stupidity in any large
> enterprise. But does any of this have a real bearing on how security
> can be improved, or how we should look at it?

When the general public sees a complex problem in simplistic terms and is being sold trumped-up stupid solutions for nosebleed prices it is QUITE useful to point it out to them. That was the purpose of my book. Improving security and how we should look at it was not the purpose of the

book. My entire career has been spent on the latter issues, working with my peers to do what I can from a technical standpoint. The purpose of this book was not to teach Joe Sixpack how to design a trust model; it was to help Joe Sixpack understand why he's being asked to spend \$30 billion and would have probably gotten more use out of the money if he'd had a good bonfire with it.

> (Particularly to a non-American audience, this book must read like a long string of sometimes whiny complaints.) Yes, Ranum starts off by saying that he is not actually offering solutions, but that bald statement hardly absolves him of not offering anything, including insights.

I can only hope my book offers some insights. I could swear I thought I put a few of them in there when I wrote it but I can't seem to find them, now...

> Presumably, however, we are not the target audience, and the book is aimed at demonstrating to the general public that Homeland Security is, as the cover graphically puts it, a house of cards.

Finally! Thank you! It's good that you put one thing in the review that I can wholeheartedly agree with! Yes, that's what this book was all about!!!!!!

<sarcasm>

Thanks for writing such a careful, perceptive, and fair review.
</sarcasm>

Proceedings on ... Engineering Principles of System Security ...

<"Daniel P. Faigin" <faigin@solarium.aero.org>>

Fri, 23 Jan 2004 09:02:38 -0800 (PST)

ACSA has announced the availability of the electronic proceedings for the ACSA-sponsored Workshop on the Application of Engineering Principles to System Security Design (WAEPSDD) at <http://www.acsac.org/waepsdd>

The goal of the workshop was to examine engineering fundamentals, the principles and practice of designing and building secure systems.

The engineering principles identified by the workshop as most beneficial to apply to security systems are presented in the two group reports.

The proceedings also contain the workshop position papers, notes from the chair and editor, and list of contributors and organizers.

Daniel Faigin, ACSA Secretary, Chair: ACSAC 20 (see www.acsac.org)



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 15

Monday 2 February 2004

Contents

- [E-mail activity: VaVaVoom MyDoom!](#)
[PGN](#)
- [Risks of virus scanners](#)
[Steve Bellovin](#)
- [AP blames virus transmission on users](#)
[Kevin Dalley](#)
- [US-CERT warns of worm, forgets to mention operating system](#)
[Kevin Dalley](#)
- [More controversy over SERVE Internet voting project](#)
[Dan Keating via Lillie Coney](#)
- [Finally! The Nigerian e-mail scammers caught](#)
[NewsScan](#)
- [Re: Spirit Rover humbled](#)
[Paul Czyzewski](#) [Mark Brader](#) [Dan Riley](#)
- [Re: UK data protection laws and ... Unintended Consequences](#)
[Richard Pennington](#) [Dave Harris](#) [Mark Brader](#)
- [Google targeted by pranksters](#)
[Monty Solomon](#)
- [On paypal and eBay scams](#)
[John Sinteur](#)

- [Postbank spoofing](#)
[Talmon](#)
 - [Disciplinary action for teaching someone to use the address bar?](#)
[Neil Youngman](#)
 - [REVIEW: "The Hanged Man's Song", John Sandford/John Camp](#)
[Rob Slade](#)
 - [REVIEW: "Defense and Detection Strategies Against Internet Worms", Nazario](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✉ E-mail activity: VaVaVoom MyDoom!

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

Mon, 2 Feb 2004 9:41:36 PST

SpamAssassin is now trapping over 1100 e-mail spam messages to me and RISKS each day. IN ADDITION to that, the recent malware activity (MyDoom, etc.) is awesome. After putting out [RISKS-23.14](#) on 27 Jan, I did not get a chance to look at the RISKS mailbox until this morning, and there were 2528 NEW messages, of which only about 40 were legitimate postings. Note that I run absolutely **no** MS software, so don't bother to blame me for any of the bogus e-mail that seems to come from RISKS.

Subject	Messages
-----	-----
test	407
hi	296
hello	240
status	197
mail deliv..	188
mail trans..	185
returned ma.	161

error ... 89
server report 85
undeliver... 77
failure not. 67
... virus .. 44

and many many more with gibberish that I deleted on the basis of their subject lines alone.

Many thanks to those of you who remember to use the helpful tag string [noted in the last message in each issue, and which will change as soon as the spammers start using it]. That tag really encourages me to look at your e-mail first -- or even at all. It also enables me to scan through the thousands of items that SpamAssassin traps, and I think I have found only one legitimate message that got caught in its web. (My sincere regrets if I accidentally deleted any of your legitimate messages.)

Incidentally, RISKS is hugely backlogged at the moment, with material for about three issues waiting for catching up -- without even thinking about everything that this issue will generate.

Side note: MyDoom hit SCO yesterday at midnight, as predicted, infecting PCs beginning in New Zealand. SCO was reportedly completely paralyzed by the denial of service attacks, which are expected to continue through 12 Feb.

⚡ Risks of virus scanners

<Steve Bellovin <smb@research.att.com>>

Wed, 28 Jan 2004 21:56:26 -0500

For fairly obvious reasons, I just upgraded a family member's anti-virus software. She asked me to check a suspicious message; when I saw that the body said "The message contains Unicode characters and has been sent as a binary attachment," I knew what I was dealing with.

Of course, the AV software did detect it, and dealt with it in an appropriately permanent fashion. But how did it notify the user of what it found? It created a .txt file -- as an attachment in the e-mail message...

How long, I wonder, till a virus uses that exact filename and syntax to hide behind? Recall that MyDoom is already calling itself things like "document.txt .scr" and the like, to try to hide the real extension. Why are the good guys trying to teach people to click on attachments?

AP blames virus transmission on users

<Kevin Dalley <kevin@kelphead.org>>

Wed, 28 Jan 2004 19:32:13 -0800

Anick Jesdanun, an AP Internet Writer, wrote an article stating:

The continued spread of a cleverly engineered computer virus exposes a key flaw in the global embrace of technology: Its users are human.

The article is available at:

<http://story.news.yahoo.com/news>

?tmpl=story&cid=528&e=4&u=/ap/20040128/ap_on_hi_te/e_mail_worm

The e-mail contacts an attachment marked
application/octet-stream; text.zip
or
application/octet-stream; data.zip

Unzipping the file gives you an executable, perhaps data.scr or text.pif, again with a misleading name. Unfortunately, the mail reader knows how to unzip and execute the file without any warning to the user.

Anick blames the user's trust for the damage. If the user were warned before the file were executed, the problem would not be as serious.

comp.risks has covered this topic in 20:44, in June, 1999, where Steven M. Bellovin says:

The underlying problem is that there are two different mechanisms used to determine file type, and hence how it should be "opened". One is what is displayed to the user; the other is what is actually used. That way lies danger.

⚡ US-CERT warns of worm, forgets to mention operating system

<Kevin Dalley <kevin@kelphead.org>>

Wed, 28 Jan 2004 23:26:31 -0800

In one of its first actions, US-CERT issued a warning about the MyDoom.B worm. Unfortunately, US-CERT forgot to mention the operating

systems which are susceptible to attack from the worm. The technical warning is available at:

<http://www.us-cert.gov/cas/techalerts/TA04-028A.html>

The warning contains hints that the OS is some form of Windows, mentioning the Windows System directory, but doesn't come out and identify any operating systems.

On the other hand, CERT's (without "US") warning of Novarg.A worm:

http://www.cert.org/incident_notes/IN-2004-01.html

has a link titled "Steps for Recovering from a UNIX or NT System Compromise". CERT doesn't mention the susceptible operating systems, either, but one could assume that UNIX is at risk.

Chew on these CERTs and you will be lucky to see a spark of light.

More controversy over SERVE Internet voting project ([RISKS-23.14](#))

<Lillie Coney <lillie.coney@acm.org>>

Fri, 30 Jan 2004 12:35:12 -0500

In a joint letter being sent to several congressional committees, Republican and Democratic party organizations for citizens living abroad are opposing the Pentagon's SERVE system for Internet voting in the forthcoming presidential election. About 100,000 ballots are currently expected to be cast using this system, in 50 counties. [Source: Bipartisan

Request Seeks

Halt to Internet Voting: Groups Fear Citizens Abroad Will Be Compromised,

Dan Keating, *The Washington Post*, 30 Jan 2004, Page A19; PGN-ed]

✶ Finally! The Nigerian e-mail scammers caught

<"NewsScan" <newsscan@newsscan.com>>

Mon, 02 Feb 2004 08:52:18 -0700

Police in the Netherlands have arrested 52 people suspected of using the so-called "Nigerian e-mail scam" to defraud Internet users by sending them spam e-mails asking for their help in transferring a large sum of money out of Nigeria or some other troubled country in exchange for a generous percentage-fee. A task force of 80 officers raided 23 apartments, seizing computers, fake passports and 50,000 euros (\$62,000) in cash. Most of those arrested were believed to be Nigerian. [Wired.com, 2 Feb 2004, NewsScan Daily, 2 Feb 2004]

http://www.wired.com/news/ebiz/0,1272,62124,00.html?tw=wn_tophead_5

[Observing how scam e-mail has increased, I suspect that this is still just the tip of the viceberg. PGN]

✶ Re: Spirit Rover humbled ([RISKS-23.14](#))

<Paul Czyzewski <paulcz@speakeasy.net>>

Wed, 28 Jan 2004 00:57:15 +0000

The article mentioned,

<http://spaceflightnow.com/mars/mera/040126spirit.html>

contains this statement:

"Spirit bogged down because it didn't have enough random access memory, or

RAM, to handle the current amount of files in the flash -- including data

recorded during its cruise from Earth to Mars and the 18 days of

operations on the red planet's surface"

Does anyone reading RISKS know how they test mission software, and how

rigorously? It's nearly unbelievable that "what happens when Spirit

accumulates lots of files?" apparently wasn't tested.

✶ Re: Spirit Rover humbled ([RISKS-23.14](#))

<msb@vex.net (Mark Brader)>

Wed, 28 Jan 2004 02:17:08 -0000

> ... variant of the classic "fixed length buffer" error?

Wouldn't this actually be a variant of the classic "failure to detect and

recover sensibly from a full disk" error? Not at all the same thing.

✶ Re: Spirit Rover humbled ([RISKS-23.14](#))

<Dan Riley <dsr@mail.lns.cornell.edu>>

29 Jan 2004 19:07:34 -0500

I would have thought the reason it rebooted so many times is precisely because there isn't a sysadmin handy. Nothing terrible will happen if the rover reboots--it doesn't fall flaming from the skies or fall over a cliff, it doesn't threaten the lives of astronauts, it simply sits immobile on the (apparently lifeless and inactive) surface of mars for a minute or two while it reboots. However, if the rover software gets locked into a state it can't recover from, it is lost--there is no one there to push the reset button (except, hopefully, a deadman timer). Given those conditions, it seems like sensible RISKS engineering practice to make the best try at restoring a known system state--by rebooting--at the slightest sign of an inconsistency in the system state. It obviously also needs some sort of "safe mode" that depends on as little hardware as possible and allows mission control to intervene--and apparently that exists.

✶ Re: UK data protection laws and ... Unintended Consequences

<Richard Pennington <richardhelen.pennington@virgin.net>>

Wed, 28 Jan 2004 23:26:03 +0100

(Correction, [RISKS 23.14](#))

I am afraid that I have to make a correction to my posting in [RISKS-23.14](#).

My posting covered two particular cases, and the correction refers to case

1.

1. It has been brought to my attention that although the perpetrator's earlier home town is in North-East Lincolnshire, the local police is not in fact Lincolnshire Police but Humberside Police, and therefore Lincolnshire Police were in no way responsible for the events described. I therefore offer my apologies to all concerned at Lincolnshire Police.

2. It has also been brought to my attention that the Data Protection Registrar has been re-titled the Information Commissioner.

I am also indebted to Graham Smith for pointing me at the following relevant news item from the BBC news website (which explains both cases far better than I ever could):

<http://news.bbc.co.uk/1/hi/uk/3395071.stm>

There is certainly room for debate on the conflict between (a) the presumption of an individual's innocence until proven guilty, and (b) the requirement to protect society at large (and children and the vulnerable in particular), in the case where an individual repeatedly attracts the attention of the police without ever being brought to court.

✦ Re: UK data protection laws and ... Unintended Consequences (R-23.14)

<brangdon@cix.compulink.co.uk (Dave Harris)>

Thu, 29 Jan 2004 19:55 +0000 (GMT)

> The caretaker later murdered two of the schoolchildren (aged 9 and 10).

This implies the children went to the school where the caretaker worked.

Not so. They went to a different school, and the murderer came into contact

with them through his girlfriend (who did work at their school). It is

likely that the murders would have happened even if the caretaker was denied

his job.

You can discover more details of the case by searching on the caretaker's

name, "Ian Huntley". There is a summary at:

http://en.wikipedia.org/wiki/Ian_Huntley

The previous accusations against Huntley were unproven. The risk to the

children has to be balanced against the risk of unfounded allegations being

allowed to destroy the career of an innocent man.

✶ Re: UK data protection laws and ... Unintended Consequences (R-23.14)

<msb@vex.net (Mark Brader)>

Wed, 28 Jan 2004 02:40:28 -0000

> The resulting inquiry revealed that the caretaker, while in Lincolnshire,

> had been the subject of multiple relevant allegations

(indecent assault
> and worse), none of which had ever been brought to court. ...

So "Innocent until proven guilty" is now an Unintended
Consequence? Remind
me never to have anyone make false allegations of serious
offenses against
me next time I'm in England. Oh, wait, how do I do that?

Not to say that what is described is not a tragedy, but if there
is fault to
be found with the police, it's **not** for not telling the school
about the
earlier cases. It's for failing to get the criminal tried and
convicted
back then. And even this is only true if the earlier alleged
offenses were
genuine. (One can imagine an unlikeable person being the
subject of false
allegations and later turning to actual crime.)

> As a result, the various investigations in Lincolnshire never
heard
> about each other ...

And that'd be their fault too. For police, it **is** reasonable
to consider
that someone previously suspected should be suspected again:
this is all
right precisely because a police suspect is not, ipso facto, a
criminal.

Google targeted by pranksters

<"Monty Solomon" <monty@roscom.com>>
Mon, 26 Jan 2004 17:38:49 -0500

Google targeted by pranksters: Web site operators, bloggers skew
results

Verne Kopytoff, *San Francisco Chronicle*, 26 Jan 2004

Who among the many candidates running for president is unelectable? George W. Bush -- if the search results on Google can be believed.

His biography is the first result to appear on Google for the Web query "unelectable." It's just one in a long list of similarly bizarre results on the search engine over the years that are the result of manipulation, not their relevance.

Called Google bombs, these are pranks engineered by Web site operators and creators of Web logs. They take advantage of the way Google ranks search results to get certain Web sites listed higher for specific queries than they otherwise would be.

That's why President Bush's biography also appears as the top result for the search query "miserable failure." ...

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/01/26/BUG3M4GVDS1.DTL>

✶ On paypal and eBay scams (Re: [RISKS-23.13](#))

<John Sinteur <john@sinteur.com>>
Sat, 17 Jan 2004 11:16:05 +0100

> [This is increasingly becoming a problem! We desperately need
> some greater authentication and accountability. PGN]

It will get worse very soon. I've received several e-mails,

apparently from paypal, about a UK branch they are setting up, announcing the move of just about all european customers to that branch instead of the US one. None of the messages so far have asked me to take any action, so I haven't bothered to check if paypal is indeed moving to the UK or not. Personally I will check every move very carefully, DNS registry, https certificates, etc... This is in itself already a Risk, since paypal must now assume on every administrative mail they send that people will simply not believe them, but the bigger risk is that I'm probably almost alone in these checks. Anybody want to bet scammers will attempt to abuse potential confusion round the move to paypal.co.uk (if it is real) for their own phishing expeditions?

✶ Postbank spoofing

<Talmon@MI.unimaas.nl>

Tue, 20 Jan 2004 08:54:36 +0100

Not only PayPal users are being tricked into providing sensitive information. In The Netherlands an e-mail has circulated that asked Postbank clients who use electronic banking to provide user identification and password information. They used a similar approach as in the PayPal case. The e-mail contained what looked like a proper webaddress, but when looking at the source (it was an HTML message) another web address was

hidden there. By clicking on the link, you got to a non-Postbank website, with ordinary http: rather than https:.

I was warned by the fact that the e-mail was delivered to my work e-mail address rather than my private e-mail address. In addition, the language of the mail was more Flamisch (the Belgian variant of Dutch) than proper Dutch.

The Postbank had a warning about this e-mail on the home page of their website on the same day as I received the e-mail.

⚡ Disciplinary action for teaching someone to use the address bar?

<Neil Youngman <n.youngman@ntlworld.com>>
Sat, 17 Jan 2004 09:43:20 +0000

On the Hertfordshire Linux User Group mailing list there is a bizarre story of a teacher disciplined for teaching a student to use the address bar

(<http://mailman.lug.org.uk/pipermail/herts/2004-January/000198.html>)

"Early last year (during her previous stint at my school) I was accused of "hacking the server" (FYI, there are at least 3 servers).

Investigation, letters and phone calls by concerned parents showed that the actual concern was that I had informed a student in Year 9 how to use "about:some_HTML_here" in the address bar, to test HTML on the fly

in IE.

He then used it to do "about:server1".
For the un-HTML-enlightened among us, this would create a blank page with a link to \\server1, which would show a normal Explorer Window with all the shared folders on server1. What else that student did I was never told."

I can't see that this offers anything you couldn't get via network neighbourhood, but then I'm no Windows expert. FWIW, I tried this on IE6/W2K and got no more than an error message.

RISKS here are more of technophobia than direct RISKS of technology.

⚡ REVIEW: "The Hanged Man's Song", John Sandford (John Camp)

<Rob Slade <rslade@sprint.ca>>
Mon, 26 Jan 2004 08:32:27 -0800

For a bit of lighter relief:

BKHGMNSG.RVW 20031112

"The Hanged Man's Song", John Sandford (John Camp), 2003,
0-399-15139-7, U\$25.95/C\$39.00

%A John Sandford (John Camp) js@johnsandford.org
%C 375 Hudson Street, New York, NY 10014
%D 2003
%G 0-399-15139-7
%I Berkley
%O U\$25.95/C\$39.00 <http://www.berkley.com/berkley>

online@penguin.com

%O [http://www.amazon.com/exec/obidos/ASIN/0399151397/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0399151397/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0399151397/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0399151397/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0399151397/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0399151397/robsladesin03-20)

%P 321 p.

%T "The Hanged Man's Song"

It is always a delight to find a new John Sandford/John Camp novel, a pleasure that is unalloyed by any regrets and annoyances in regard to technical goofs. As was the quality of the technical material in "The Fool's Run" (cf BKFLSRUN.RVW) and "The Devil's Code" (cf. BKDVLSCD.RVW), so it is with "The Hanged Man's Song."

The technology is firmly grounded in reality. The communities, both blackhat and law enforcement, do not have the jarring quality found in all too many works where the author becomes fascinated with "hackers." (Having lugged around a number of "development" laptops in order to demonstrate company products, I was wryly glad to find that someone else knows that not *all* such machines are featherweights :-)

There is an intriguing idea for distributed backup of secure-but-secret data, although I suspect that even very young computer wizards would very quickly act to close loopholes and find anomalies.

I'm a bit surprised that a careful and paranoid group, such as is described in the novel, did not take more care with authentication, perhaps through a "web of trust" model, but I suppose that would have gotten in the way of the plot. Onion routing would also have

been
handy for these people, but, again, would not be as exciting.
(I also
want to get my hands on that quad track DVD-R: the best I can
find for
my own systems is the basic single track that only lays down 5-6
gigs.)

The main complaint I would have with this particular work is
that the
technology seemed somehow divorced from the primary thread of the
plot. This seems an odd statement to make, given the three-
cornered
race by technically savvy people, turning primarily on computer
forensics and data recovery, but I was left feeling that this
was more
akin to an old-fashioned chase thriller. Albeit an interesting
one.

copyright Robert M. Slade, 2003 BKHGMNSG.RVW 20031112
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)

★ REVIEW: "Defense and Detection Strategies Against Internet Worms",

<Rob Slade <rslade@sprint.ca>>
Wed, 21 Jan 2004 07:35:36 -0800

Jose Nazario

BKDDSAIW.RVW 20031128

"Defense and Detection Strategies Against Internet Worms", Jose
Nazario, 2004, 1-58053-537-2, U\$85.00/C\$131.95
%A Jose Nazario jose@crimelabs.net
%C 685 Canton St., Norwood, MA 02062

%D 2004
%G 1-58053-537-2
%I Artech House/Horizon
%O U\$85.00/C\$131.95 800-225-9977 artech@artech-house.com
%O [http://www.amazon.com/exec/obidos/ASIN/1580535372/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1580535372/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/1580535372/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1580535372/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/1580535372/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1580535372/robsladesin03-20)
%P 287 p.
%T "Defense and Detection Strategies Against Internet Worms"

The preface states that the book is intended for security professionals, security researchers, and academics in the field of computer science. It is obvious that the author has attempted to write the material in a scholastic tone, but the necessary rigour and structure of thought is missing.

Chapter one, an introduction of sorts, provides random information of questionable utility, such as the table listing the discovery of vulnerabilities compared against the time that elapsed before those loopholes were first released in active worms: no particular pattern seems to be indicated.

Part one is supposed to be a background and taxonomy. Chapter two provides us with a definition. Nazario has obviously taken the Cohenesque definition of viruses (as attaching to files) and then assumed that a worm is any self-replicating program that does **not** so bind. The definition therefore appears to include almost all current viruses, and yet the author also attempts to ascribe certain characteristics to worms, such as control and construction of a network, and communication with other worm nodes. His later examples

of worms, however, include a number that do not contain any of these aspects. He lists a number of components of worms, and yet the communications, command, and intelligence elements are not inherently part of much of modern malware, usually existing simply as specialized payloads. A simplistic growth pattern (and the fact that worms can generate network traffic) is presented in chapter three, but the actual traffic patterns examined do not fully correspond to the projected graph. The history and taxonomy given in chapter four has numerous errors: even the fictional representative, the tapeworm from Brunner's "The Shockwave Rider," is introduced erroneously, since it didn't shut down the network in the book, but rather opened it. Workstations affected by the infamous Xerox PARC worm could be restarted, and a vaccine was not needed or produced. The Morris Worm was an enormous nuisance, but it hardly "crashed the Internet." (And Loveletter did the rounds in 2000, not 2001.) There is a quick precis of a number of lesser known worms, and this may be helpful as a reference, but the analysis is very limited. The construction of a worm is described in chapter five, but the outline is often at odds with that given in chapter two.

Part two reviews worm trends. Chapter six reworks some of the material from five in a facile listing of infection patterns (and presents an artificial "Shockwave Rider" pattern that does not seem to have any correspondence to reality). "Targets of attack," in chapter seven, simply enumerates network connected devices. Nazario does attempt to bring in abstract concepts related to network topologies, but these have little practical bearing on worms in reality. The possible futures for worms, as expressed in chapter eight, deals

mostly with existing and already used technologies. There is some effort made to model effects, but these are not fully analyzed.

Part three turns to detection. Chapter nine looks at traffic analysis, but only in terms of network based intrusion detection with rudimentary appraisal. Honeypots and "dark networks" (ranges of unused IP addresses) are said to be ways to detect and trap worms, but the explanation and dissection of the topic in chapter ten is very narrow. Signature based detection, in chapter eleven, revisits network based intrusion detection, and adds a brief mention of file scanning.

Part four looks at defences. Chapter twelve's review of host based defence deals primarily with system hardening, antivirus scanners, and the concept of throttling. Nazario seems very loath, in his discussion of firewalls in chapter thirteen, to admit that this is simply another type of signature. The use of scanning within application level proxies is examined in chapter fourteen, although there seems to be some confusion with circuit level proxies at points. Chapter fifteen, entitled "Attacking the Worm Network," outlines a number of active measures: except for the idea of "sticky" tarpits (after the LaBrea program model) all of them require extensive specific knowledge of individual worms. A concluding chapter is provided in sixteen.

Nazario's work does address the often neglected topic of worms, and he does break away from the mass of virus books that are locked into the traditional "file and boot infectors" model. His examples are drawn

from more recent events, and he does attempt to analyze network effects and complications, rather than simply looking at systems in isolation. While he is to be commended for all this, his definition is too broad to provide for serious new modelling of the problem, and his analysis fails to provide a basis for future work. Still, for those who need a more complete picture of the malware threat, this work should be considered. It does provide new information, and does attempt to address the difference between worms, viruses, and other forms of malware. In this regard, it is a significant improvement over such lackluster spacefillers as Skoudis "Malware" (cf. BKMLWFMC.RVW), the "E-mail Virus Protection Handbook" (cf. KEMLVRS.RVW), Dunham's "Bigelow's Virus Troubleshooting Pocket Reference" (cf. BKBVRTPR.RVW), Schmauder's "Virus Proof" (cf. BKVRSPRF.RVW), and even Grimes' somewhat better "Malicious Mobile Code" (cf. BKMLMBCD.RVW).

copyright Robert M. Slade, 2003 BKDDSAIW.RVW 20031128
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

Volume 23: Issue 16

Tuesday 3 February 2004

Contents

- [Security holes at DMVs nationwide lead to ID theft and safety concerns](#)
[Monty Solomon](#)
- [Defeating phishing scams](#)
[Andrew Rose](#)
- [A nasty Phishing attempt](#)
[Avishai Wool](#)
- [Another wireless risk](#)
[Chris Meadows](#)
- [Hotel reservation system easily confused](#)
[Richard S. Russell](#)
- [Browsers, online forms, rendering and opt-in marketing](#)
[Alistair McDonald](#)
- [Drunk unlocks police car with own key](#)
[Max](#)
- [Re: Happy 2**30'th birthday, time_t!](#)
[Steve Summit](#)
- [Re: Suing the customers](#)
[Paul Robinson](#)
- [Re: Lie-detector glasses, 90% accurate?](#)
[Ron Bean](#) [Peter B. Ladkin](#)

● [REVIEW: "Biometrics", Woodward/Orlans/Higgins](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Security holes at DMVs nationwide lead to ID theft and safety concerns

<Monty Solomon <monty@roscom.com>>

Mon, 2 Feb 2004 09:50:52 -0500

<http://www.cdt.org/>

Security Holes at DMVs Nationwide Lead to ID Theft and Safety Concerns

CDT has issued a report entitled "Unlicensed Fraud" documenting rampant internal fraud and lax security at state motor vehicle administration offices across the country placing the reliability of all driver's license at risk. While heavy public attention has been placed on new national standards and new technologies for driver's licenses, studying local news reports from throughout 2003 CDT finds that basic management processes to stop bribery and theft are lacking. In the report, CDT offers policy recommendations to address this dire issue. 2 Feb 2004

Unlicensed Fraud: How bribery and lax security at state motor vehicle offices nationwide lead to identity theft and illegal driver's licenses:

[pdf]

<http://www.cdt.org/privacy/20040200dmv.pdf>

✦ Defeating phishing scams

<Andrew Rose <andrew.rose@dataconnection.com>>

Mon, 19 Jan 2004 10:11:35 -0000

PGN commented on another 2 phishing scams highlighted in [RISKS-23.13](#),

> [This is increasingly becoming a problem! We desperately need
> some greater authentication and accountability. PGN]

Work on a technical (part-)solution named SPF ("senders permitted from") is underway at <http://spf.pobox.com/>. This simple technique has domains publish so-called SPF records in the DNS. The SFP records detail those machines that may validly send email for the domain in question. This allows receiving MTAs to reject or flag email that claims to come from e.g. paypal.com but isn't sent by a machine that is authorised to send on behalf of paypal (e.g. a phisher).

The technical work on SPF is now complete and adoption has started. Several thousand domains have published SPF records including some very large domains such as aol.com. Plugins exist for most of the popular MTAs - the only notable exception being MS Exchange.

For a more detailed overview see <http://spf.pobox.com/for-mit-spam-conference.gif>. Those who are still interested should then read <http://spf.pobox.com/> and join the mailing list.

⚡ A nasty Phishing attempt

<Avishai Wool <avishai_w@yahoo.com>>

Sat, 24 Jan 2004 09:12:42 -0800 (PST)

Perhaps this is ho-hum for RISKS readers, but I thought I'd pass this along anyway.

I got a nasty spam today which I excerpt below.

It purports to be from the FDIC, and asks the reader to go to the FDIC web site and "verify" bank account details. It uses the

`http://reasonable.site.name @criminal.site.ip.address/index.html`

trick, where the "reasonable" site name is treated as a username. The criminal site probably attempts to harvest these details (I tried it but the site was unresponsive).

This is a clever piece of social engineering, which is especially effective against non-US residents that have (or had) a US bank account.

Avishai

> Subject: Important News About Your Bank Account

> Date: Sat, 24 Jan 2004 09:32:39 -0400 (EST)

>

> [snip]

> As a result Department Of Homeland Security Director Tom Ridge has advised

> the Federal Deposit Insurance Corporation to suspend all deposit insurance on

> your account until such time as we can verify your identity and your account

> information.

> Please verify through our IDVerify below. This information will be checked

> against a federal government database for identity
verification. This only
> takes up to a minute and when we have verified your identity
you will be
> notified of said verification and all suspensions of insurance
on your
> account will be lifted.

> <http://www.fdic.gov/idverify/cgi-bin/index.htm>
(the link behind the text was <http://www.fdic.gov/SOH@202.63.206.88/index.htm>)

> Failure to use IDVerify below will cause all insurance for
your account
> to be terminated and all records of your account history will
be sent to the
> Federal Bureau of Investigation in Washington D.C. for
analysis and
> verification.

Avishai Wool, Ph.D. <http://www.algosec.com> <http://www.eng.tau.ac.il/~yash>
yash@acm.org +972-3-640-6316

Another wireless risk

<Chris Meadows aka Robotech_Master <robotech@eyrie.org>>
Mon, 26 Jan 2004 16:13:37 -0600

The other day I was in the position of needing to print out my
credit card
site's invoice display. Since I don't have a fully functional
printer at
home, and I needed to make a photocopy anyway, I decided to take
my Mac
Powerbook down to Kinko's and print it off there.

The problem was, when I plugged the Powerbook into their

Ethernet link

(called a "Macintosh link" for some reason by their onsite documentation...never mind that any computer with an Ethernet port could use

it), I couldn't reach the Internet. (Nor could I see any printers in my

application...and the printer driver disk the Kinko's clerk helpfully

offered didn't help, because it only had drivers for OS 9, not OS X.)

However, the fellow who'd just vacated the laptop station had been using

wireless, and he said that should work. And I did a quick scan, found an

open wireless router labelled "linksys," (the way they didn't even bother to

change the default name should have warned me, I suppose...but given the

general lack of computer adroitness I had observed in the staff, that

carelessness seemed to fit right in) with a Lexmark printer on it, and

Internet access...so I called up the invoice and hit print, then asked the

Kinko's clerk where that particular printer was.

Longtime RISKS readers should be able to guess what came next.

"But we

don't have a wireless network...and we don't have any Lexmark printers

either." Further research indicated that the wireless router was hooked

into a Bellsouth DSL connection, presumably someone's nearby home or

business. So I had just printed my credit card invoice to some total

stranger's printer...and had no way even to find out where it was so I could

get it back. Fortunately, the invoice didn't contain any *truly* sensitive

information, such as my SSN or account number (beyond "ends with").

And I was closing that account anyway.

The risk here is kind of the inverse of the "usual" risk associated with a wireless system...instead of "you never know who might be using your network," it's "you never know whose network you might be using." The combination of an open wireless network and a location where you would expect there to be one can easily enough confuse you into conflating the two.

✶ Hotel reservation system easily confused

<"Richard S. Russell" <RichardSRussell@tds.net>>
Fri, 23 Jan 2004 23:33:08 -0600

Our science-fiction group in Madison, Wisconsin, runs the world's only feminist-oriented SF convention, WisCon. Every year we hold it in the same hotel. Our publicity is required to say "Mention WisCon 2004 when making reservations to get the group rate.". I asked why the "2004" part was necessary and was told that, because of the hotel's automated reservation system, the rates for WisCons 2002, 2003, 2005, 2006, etc. are also in the computer, and the reservation-takers apparently can't figure out from the dates of the reservation (2004 May 28-31, if you're interested) which one you're signing up for. Therefore, instead of building in a single central error-checking process, they rely on a distributed network of hundreds of naive human beings to each individually get it right -- assuming that the

convention committee has done ITS part and diligently included the year every time it mentions the name of the convention.

Richard S. Russell, 2642 Kendall Av., Madison WI 53705-3736 1-608-233-5640

🔥 Browsers, online forms, rendering and opt-in marketing

<"Alistair McDonald" <alistair@inrevo.com>>

Wed, 21 Jan 2004 08:32:18 -0000 (GMT)

I completed a `_long_` online form for the UK's DTI on information security breaches (<http://www.infosec.co.uk/page.cfm/Action=Form/ID=13/t=m>) if you want to complete it. This took me over 10 minutes. At the end, there were the usual options to untick the boxes and not have your information shared, and so on. There was, however, a strange twist.

My browser (Opera 7.23 for Linux) failed to display the end of the page. It simply stopped halfway through one of the personal information lines.

I didn't want to fill in the form again using another browser, so I had to view the source code and use the keyboard to navigate through the various tick boxes.

Then, I had another thought: the form had questions like "If you do not wish to receive information ... please untick here." The boxes were unchecked by default - should I check them or leave them unchecked? The

message indicated
that I should take an action - i.e. toggle the boxes, but
perhaps they
should have been on by default, but my browser failed to do
this, perhaps
due to non-standard HTML or script. By leaving them unticked,
I'd be OK -
but no, I had to take an action.

However, it occurred to me that both of these errors could be
used in a
deliberate way to confuse users and collect more personal
information for
opt-in marketing.

By the way, the form was way too long. It was 266K, had nearly
7000 source
lines, and 224 input controls (including any hidden ones). It
should have
been broken up into about a dozen smaller pages with Next and
Prev buttons
to navigate between them. Of course, that would be more
difficult to code.:-)

🔥 Drunk unlocks police car with own key

<Max <max7531@earthlink.net>>
Tue, 13 Jan 2004 20:57:58 -0800

Shinichi Kiyono, 32, was arrested on suspicion of car theft
after he
reportedly mistakenly unlocked a police investigation vehicle
with his own
car key while drunk, then drove to an empty lot and fell asleep
in the
vehicle. He turned himself in when he woke up in a Nissan that
was not his,
although it was the same make and color. Nissan says it makes
more than

20,000 types of keys.

A spokesman for Nissan Motor Co., the maker of the vehicles, said the firm produced more than 20,000 types of keys for its vehicles, and that it was almost impossible for separate keys to be used in different cars, even if they were the same model, but that it was not impossible for keys to very occasionally fit other cars. Prosecutors subsequently decided not to indict him.

[Source: PGN-ed from the Japanese daily *Mainichi Shimbun*, 18 Dec 2003:

<http://mdn.mainichi.co.jp/news/archive/200312/18/20031218p2a00m0dm005000c.html>

See also: "Drunk who unlocked police car with own key escapes prosecution":

<http://www12.mainichi.co.jp/news/mdn/search-news/896474/drun20who20unlocked20police20car20escapes20prosecution-0-1.html>]

[I would be interested to see how many other police cars this guy's key can open. Max]

[Count the number of Nissans on the road, and divide by 20,000, to get a very rough estimate. PGN]

🚀 Re: Happy 230'th birthday, time_t! ([RISKS-23.12](#))**

<Steve Summit <scs@eskimo.com>>

Thu, 22 Jan 2004 18:40:14 -0500

Paul Eggert wondered how many time-related problems there might be in 2038

even though most machines by then will presumably be capable of using 64 bits. I'm afraid the answer is: quite a lot. Even if every CPU and OS is using 64-bit `time_t`'s by then, I expect there will still be countless instances of 32-bit time representations lying around on disk, baked into binary data file formats which still reflect the original 32-bit size. Upgrading CPU's and recompiling programs will not, of course, automatically update all of the terabytes worth of data files written and maintained by prior versions of the programs. (In other words, it's all too likely that 2038 will be to Unix as Y2K was to COBOL.)

For those who use binary data files, a nice exercise is to write a pair of functions for reading and writing between in-memory `time_t` values (however big they happen to be today), and 6- or 8-byte on-disk values, making sure that the functions are implemented such that they work without change when compiled on a system with 32-bit `time_t`'s, or recompiled for a machine with 64-bit `time_t`'s. (Of course, decoupling data file representations from implementation-defined in-memory representations is almost always a good idea; this is merely a timely example.)

⚡ Re: Suing the customers (Scrivner, [RISKS-23.12](#))

<Paul Robinson <postmaster@paul.washington.dc.us>>
Sat, 24 Jan 2004 19:43:32 GMT

> Rockwell, is suing a law firm that is currently suing
Rockwell's customers.

> [...]

I think Rockwell doesn't have a leg to stand on. A patent gives the holder of it the right to prevent others from making, using or selling a patented device. Anyone in the chain of persons not having a license from the patent holder can be sued. If you purchase an ACME refrigerator from Pat's Appliance Store, and it turns out that the ACME refrigerator has a patent-violating component in the in-door ice maker, the owner of that patent can sue ACME, they can sue Pat's Appliance store, and they can sue you. All three of you are jointly and severally violating the patent holder's rights under the law and they can sue any or all of you. Usually the manufacturer is the only one who is sued but in theory anyone who doesn't have a license, either directly or indirectly, is an infringer and can be sued.

There was an incident a few years ago, when the manufacturer for the electronic fare collection system implemented in the Washington Metrorail system used some components that violated a patent (because the manufacturer didn't have a license.) The patent holder chose to sue the Washington Metropolitan Area Transit Authority (WMATA) instead of suing the manufacturer. WMATA simply chose to settle by purchasing a license from the patent holder. I don't know if the transit authority ever got the extra cost back from its supplier.

This is the exact same situation the RIAA is dealing with in the case of people who are allegedly swapping songs over peer-to-peer networks. (The RIAA's real agenda is obviously control, not money, but suing people to scare others is a fairly effective way to influence behavior. If the RIAA were interested in money, they would have taken up the offer of a billion dollars in payments from licensing fees through sale of use of the service, and Napster - the original one - would still be operating.)

The point is, even if the patent holder is wrong about their product being infringed, legally they may choose to target the manufacturer's customers. Some of them could conceivably counter sue if the company is intentionally misusing the legal process but that's an iffy proposition, as some people who tried to sue DirectTV over it's efforts to squeeze money out of anyone who purchased a smartcard programmer from certain sites that sold devices that allegedly could allow someone to obtain DirectTV's service, whether or not the person actually did or could have used the programmer to unlawfully obtain their signals, discovered. A court found the attempts by DirectTV to demand (enormous amounts of) money for alleged signal theft (whether or not any actually happened) in place of filing suit was a legitimate action by DirectTV, and ordered them to pay its costs to defend the case.

N.B. To prevent *me* from being sued in case I have named someone who really exists, the name "ACME" and "Pat's Appliance Store" are fictional examples

not intended to represent any real-life company or organization. :) But I'm not worried anyway because I don't have any money and am unlikely to be sued. :(

> In Rockwell Automation Inc. v. Schneider Automation Inc., 02-01195,
> Rockwell says its technology is not covered by the Solaia patent, and
> rather than battling that issue out in court, Niro Scavone and its clients
> have sought to "'shakedown' manufacturers through threats of potential
> business interruption or catastrophic damages."
> <http://www.law.com/jsp/article.jsp?id=1039054478800>

It's not a 'shakedown' if you use the courts. If I threaten you if you don't pay me for something, that's extortion and a crime. If I threaten to sue you if you don't settle, that's legal. If I just sue you anyway, whether I have a case or not, that's also legal. As many people are relatively upset over in the case of SCO and it's claims it has some rights over Linux due to alleged infringement. It may be relatively slimy but it's by the book legal, unfortunately.

["If the lessons of history teach us anything it is that nobody learns the lessons that history teaches us."]

★ Re: Lie-detector glasses, 90% accurate? (Holzworth, [RISKS-23.14](#))

<Ron Bean <rbean@shell.core.com>>

Tue, 27 Jan 2004 22:01:04 -0600

> It may not be long before you hear airport security screeners
ask, "Do you
> plan on hijacking this plane?"

I'd be highly tempted to reply "No, do you plan to stop beating
your wife?"

Reading the rest of the article, it sounds like it's detecting
people's
emotional "hot buttons", rather than lies per se. They talk
about using it
as a "love detector" also... (there should be a joke about
lonely airport
screeners in there somewhere, but I won't attempt it).

The article also says:

"The technology delivers not only a true/false reading, but a
range of
high-level parameters, such as "thinking level," which
measures how much
as subject has thought about an answer they give, and "SOS
level," which
assesses how badly a person doesn't want to talk about a
subject."

I bet a good actor could reverse-engineer this, given enough
time with the machine.

> The company said that a state police agency in the Midwest
found the lie
> detector 89 percent accurate, compared with 83 percent for a
traditional
> polygraph.

What's the rate for false positives vs false negatives?
[See the next item! PGN]

✶ Re: Lie-detector glasses, 90% accurate? (Holzworth, [RISKS-23.14](#))

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

Wed, 28 Jan 2004 11:31:14 +0100

Steve Holzworth reported that the manufacturer said that "a state police agency in the Midwest" had found "lie detector glasses" to be "89% accurate".

That figure doesn't tell us anything about the usefulness of the glasses. To obtain useful information, one needs to categorise errors as false positives (that you are identified as lying when you are in fact telling the truth. I shall call these Type 1 errors) and false negatives (that you are identified as truth-telling when you are in fact lying. I shall call these Type 2 errors), and one needs to know the background rate of truth-telling/lying. The company spokesman did not offer the classification into types, and I doubt that he or the "state police agency" had any reliable information about the background rate of lying.

To illustrate, let us interpret the "89% accuracy" statement as meaning that the instrument is in error in 1 out of 10 uses. I consider three cases with a 1 in 10 error rate.

Case 1: The background rate is also 1 in 10, all errors are Type 2, and the instrument identifies no one as lying. Then Steve has zero chance of being falsely accused.

Case 2: All errors are Type 1, and the background rate of lying is zero.

Then Steve has a 1 in 10 chance of being falsely accused.

Case 3: Errors are evenly split between Type 1 and Type 2, and the

background rate of lying is 1 in 2. Then Steve has a 1 in 20 chance of being

falsely accused. More worryingly, if he were to be intent on hijacking a

commercial aircraft, he also stands a 1 in 20 chance of passing the test

(Type 2 errors are 1 in 20)!

Now, consider what it would take to establish the background rate of

lying. Cut to the chase: it is difficult to impossible in serious use.

More specifically: This rate is likely dependent on the community, as well

as the selection procedure for testing, and it is also dependent on the

social importance of the proposition against which truth-telling/lying is

assessed. If everyone thinks lying is socially inappropriate, and you ask

them if they had exceeded the speed limit sometime in the last year, and all

know you have no possibility of enforcing sanctions given a positive answer,

then you are likely to obtain a very high rate of truth-telling, maybe even

perfect. On the other hand, if you sample a community in which more

importance is attached to getting off the hook than it is to whether one

tells the truth, but in which ceteris paribus truth-telling is preferred to

lying, and you ask people whether they have committed specific unsolved

murders, and sanctions are rigorously enforced, then everyone

may well
answer "no" to each question. In this case, the background error
rate is
identical to the unsolved-murder rate.

If you are Hercule Poirot, and you know the murderer acted
alone, then you
know this rate (for, in his mysteries, there is a closed
society, and
everyone professes innocence at first). Otherwise, one would
have to perform
controlled experiment. Performing a controlled experiment is
ipso facto
selecting one very specific value of community parameter, and is
not
obviously a guide to communities which differ from that one.

In short, in case it wasn't obvious anyway, the company
spokesman is BSing,
as are most people who claim to have measured the accuracy of
lie-"detector"
apparatus.

Peter B. Ladkin, University of Bielefeld, <http://www.rvs.uni-bielefeld.de>

REVIEW: "Biometrics", Woodward/Orlans/Higgins

<Rob Slade <rslade@sprint.ca>>
Fri, 30 Jan 2004 08:16:43 -0800

BKBIOMTC.RVW 20031204

"Biometrics", John D. Woodward/Nicholas M. Orlans/Peter T.
Higgins,
2003, 0-07-222227-1, U\$49.99/C\$74.95
%A John D. Woodward
%A Nicholas M. Orlans

%A Peter T. Higgins
%C 300 Water Street, Whitby, Ontario L1N 9B6
%D 2003
%G 0-07-222227-1
%I McGraw-Hill Ryerson/Osborne
%O U\$49.99/C\$74.95 905-430-5000 +1-800-565-5758 fax: 905-430-5020
%O <http://www.amazon.com/exec/obidos/ASIN/0072222271/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0072222271/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/0072222271/robsladesin03-20>
%P 432 p.
%T "Biometrics"

The book is intended for both students and professionals, covering all of the aspects and uses of biometrics. The chapters are written by a number of contributing authors. For example, Richard E. Smith, author of "Authentication" (cf. BKAUTHNT.RVW) wrote the introduction found in chapter one. It is an excellent precis of the uses of, and requirements for, authentication, paying particular attention to the use, strengths, and weaknesses of biometrics. The functional aspects of biometric assessment; feature extraction, storage, error rates, and so forth; are covered well in chapter two. (There is a rather odd confusion of genetic and phenotypic sources of biometrics: aside from behavioural measures and DNA testing itself, almost all biometrics are expressed characteristics, and therefore phenotypic.)

Part two deals with types of biometrics. Chapter four provides fascinating details on the history, technology, storage, indexing, and

searching of fingerprint records, and a brief mention of hand geometry. After the wealth of technicalities about fingerprints, the very basic explanations of enrollment of face and voice recognition are disappointing. The material on iris and retina scanning, in chapter five, is slightly better, but signature and keystroke dynamics again get minimal coverage in chapter six. Eleven of the more esoteric biometrics are briefly described in chapter seven, ranging from standards such as DNA testing to odd entries like sweat pore distribution or body odour.

Part three looks at various aspects or factors to consider in implementing biometrics. Chapter eight looks at the question of "liveness" testing. (This is the biometrics topic beloved of students the world over: "What if you cut off the guy's finger and used that?" Students tend to be rather gruesome creatures.) Most of chapter nine is devoted to a guide for contracting out, or questions to ask contractors or vendors. Various standards bodies are described in chapter ten. Chapter eleven talks about issues involved in testing of biometric systems.

Part four deals with privacy, policies, and legal issues. Chapter twelve examines both the threats and the benefits that biometrics holds for privacy. There is a detailed and interesting look at (mostly US) law and decisions relating to privacy, and the implications for biometric applications, in chapter thirteen. Chapter fourteen does have brief case studies of the use of biometrics at the Super Bowl and in Virginia Beach, but concentrates on the legal issues. Chapter fifteen deals with the American digital signature law, and the potential relation to the inclusion of biometrics in the

process. Some material is repeated from earlier chapters.

Part five reviews selected biometrics programs. Chapter sixteen covers government and military programs, most related to law enforcement. Searching the FBI files of civil (or non-criminal) fingerprint files, in chapter seventeen, reiterates a fair amount of content from chapter four. Private sector programs, in chapter eighteen, are primarily concerned with face recognition in casinos or a variety of systems for banks, but others are mentioned. Chapter nineteen presents a very detailed and thoughtful analysis of the possibilities for a national identity card.

Because this book is essentially a collection of standalone essays by a variety of authors, there is a great deal of overlap and duplication of material, and at times this repetition becomes annoying. This is, however, the most useful and informative work on biometrics that I have reviewed to date, and the analysis, in particular, is comprehensive and even-handed. I would recommend this as both a serviceable introduction to anyone who must work with biometrics, and as a guide to the controversies surrounding them.

copyright Robert M. Slade, 2003 BKBIOMTC.RVW 20031204
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

Volume 23: Issue 17

Tuesday 2 February 2004

Contents

- [How to Hack an Election](#)
[Hendrik](#)
- [UK: Vital e-crime evidence often destroyed](#)
[Iain Thomson via Keith A Rhodes](#)
- [Security Holes at DMVs Nationwide Lead to ID Theft and Safety Concerns](#)
[Monty Solomon](#)
- [Porn viewers work for hackers](#)
[Robin Burke](#)
- [January clearance sale](#)
[Scott Nicol](#)
- [Re: Spirit Rover humbled](#)
[Jim Griffith](#)
- [A scary thing](#)
[Erann Gat](#)
- [Phishing and a new IE security patch](#)
[Sidney Markowitz](#)
- [MyDoom and SCO](#)
[Steve Wildstrom](#)
- [RISKS actually gets *relatively little* MyDoom Traffic](#)
[Chris Smith](#)

- [Re: Risks of virus scanners](#)
[Paul Tomblin](#) [Alan J Rosenthal](#)
 - [Re: The risks of naming](#)
[Robert de Bath](#)
 - [Re: Drunk unlocks police car with own key](#)
[D. Joseph Creighton](#) [David Hollman](#)
 - ["Loss of Identity" theft](#)
[Terry A. Ward](#)
 - [REVIEW: "Kerberos: The Definitive Guide", Jason Garman](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **How to Hack an Election (*NYT* editorial)**

<Hendrik <hiz--rsk@islandnet.com>>

Sun, 1 Feb 2004 11:57:48 +0900

The New York Times had the following editorial on line on 31 Jan 2004, at <http://www.nytimes.com/2004/01/31/opinion/31SAT1.html> - they conclude with the remark "Given the growing body of evidence, it is clear that electronic voting machines cannot be trusted until more safeguards are in place." I wonder what safeguards they envision that would allow us to trust electronic voting.

How to Hack an Election

Concerned citizens have been warning that new electronic voting technology

being rolled out nationwide can be used to steal elections. Now there is

proof. When the State of Maryland hired a computer security firm to test

its new machines, these paid hackers had little trouble casting multiple votes and taking over the machines' vote-recording mechanisms. The Maryland study shows convincingly that more security is needed for electronic voting, starting with voter-verified paper trails. [...]

They were disturbingly successful. It was an "easy matter," they reported, to reprogram the access cards used by voters and vote multiple times. They were able to attach a keyboard to a voting terminal and change its vote count. And by exploiting a software flaw and using a modem, they were able to change votes from a remote location. [...]

UK: Vital e-crime evidence often destroyed

<"Keith A Rhodes" <RhodesK@GAO.GOV>>
Fri, 30 Jan 2004 11:41:24 -0500

[I wonder if these are the same forensic experts who couldn't figure out how the Bank of England scam software worked?]

Vital e-crime evidence often destroyed; National High Tech Crime Unit warns firms to leave computer forensics to the experts
By Iain Thomson, vnunet, 29 Jan 2004, <http://www.vnunet.com/News/1152379>

Companies that fall victim to computer crime may be inadvertently destroying evidence in their efforts to find the perpetrators. Detective Chief

Superintendent Len Hynds, of the National High Tech Crime Unit (NHTCU), said that its Confidentiality Charter, launched in December 2002, was encouraging more businesses than ever to report computer crime. But there are sometimes problems with gathering evidence if preliminary investigations have been carried out before the police are called in.

Speaking at the Homeland and Corporate Security Summit in London DCS Hynds said: "There are examples of companies which wrestle with problems for months without calling us and that can lead to problems in the evidential trail. The private sector is going to be key to being even more effective in solving crimes. However, we need to develop common standards in terms of dealing with high-tech crime between the private and public sectors."

Cyber-criminals are becoming ever more sophisticated in their activities. Tactics include hiding files that are disguised as bad sectors on a hard drive, and using other PCs as mail servers to shield illegal activities.

Michael Colao, senior consultant at Dresdner Kleinwort Wassertein, said: "What we see is well-meaning IT professionals going in and doing what you see on every bad crime film: they muddy the waters. You only have one opportunity to collect the evidence you need to prove your case. Human resources send in well-meaning IT help desk staff who don't know what they are doing and ruin the evidence. You need a professional computer forensic team in there as soon as possible."

✦ Security Holes at DMVs Nationwide Lead to ID Theft and Safety Concerns

<Monty Solomon <monty@roscom.com>>

Mon, 2 Feb 2004 09:50:52 -0500

CDT (<http://www.cdt.org/>) has issued a report entitled "Unlicensed Fraud" (<http://www.cdt.org/privacy/20040200dmv.pdf>) documenting rampant internal fraud and lax security at state motor vehicle administration offices across the country placing the reliability of all driver's license at risk. While heavy public attention has been placed on new national standards and new technologies for driver's licenses, studying local news reports from throughout 2003 CDT finds that basic management processes to stop bribery and theft are lacking. In the report, CDT offers policy recommendations to address this dire issue. February 2, 2004

✦ Porn viewers work for hackers

<"Robin Burke" <rburke@cti.depaul.edu>>

Wed, 28 Jan 2004 13:48:42 -0600

The following article describes an attack against the web images (so-called "CAPTCHAS") that are used to prevent robots from using certain

web applications such as the creation of free e-mail accounts. The images are a form of "Turing Test", easy for a human user of normal ability to process, but difficult for a piece of software. The attack involves routing the CAPTCHA image to a page that advertises free porn. Users have to decode the CAPTCHA to get the advertised images and in doing so, unwittingly assist spammers in creating bogus e-mail addresses.

"But at least one potential spammer managed to crack the CAPTCHA test. Someone designed a software robot that would fill out a registration form and, when confronted with a CAPTCHA test, would post it on a free porn site. Visitors to the porn site would be asked to complete the test before they could view more pornography, and the software robot would use their answer to complete the e-mail registration."

<http://www.post-gazette.com/pg/03278/228349.stm> (Relevant section is near the end)

One poster to a related thread in Slashdot (<http://slashdot.org/article.pl?sid=04/01/28/1344207>) reported that his site shut down its (CAPTCHA-protected) free e-mail service recently due to a sharp increase in spammer-generated accounts.

Robin Burke, Associate Professor, School of Computer Science, Telecommunications, and Information Systems, DePaul University
<http://josquin.cti.depaul.edu/~rburke/>

January clearance sale

<Scott Nicol <snicol@apk.net>>

Sat, 31 Jan 2004 11:42:04 -0500

Buy something, get whatever you can stuff into your parka free!

That's right, go into a <name of big home-improvement store deleted to protect the guilty> when the outside temperature is a little cold (say, 10 degrees F). Pick up a \$2 screwdriver and a \$100 multimeter. Pay for the \$2 screwdriver, but stuff the \$100 multimeter in your jacket. When the fancy schmancy EAS (Electronic Article Surveillance) system goes off as you are walking out the door, don't worry, the clerks will ignore it and yell to you "you're fine - that thing always goes off when its cold".

I saw this happen about a dozen times while waiting in line at <big home improvement store>. I have no idea if the customer had a \$100 multimeter in their jacket, but then again, neither did the employees of the store!

I couldn't find technical details on Checkpoint EAS systems <<http://www.checkpointsystems.com/content/eas/default.aspx>>, but Sensormatic <<http://www.sensormatic.com/EAS/default.asp>> provided details such as <[http://www.sensormatic.com/EAS/EASGetDocument.asp?FileName=Digital Pro-Max DS NUS.pdf](http://www.sensormatic.com/EAS/EASGetDocument.asp?FileName=Digital%20Pro-Max%20DS%20NUS.pdf)>, which states "Ambient Temperature: 0 C to 50 C (32 F to 122 F)"

This particular problem would likely only affect stores with sensors near very large outside doors, such as home improvement and warehouse

stores.

✶ Re: Spirit Rover humbled ([RISKS-23.15](#))

<griffith@dweb.org (Jim Griffith)>

Tue, 03 Feb 2004 17:56:25 -0500

I'm so disappointed that PGN didn't go with the obvious pun -- that Spirit was willing, but its flash was weak...

[Thanks, but I didn't think Rover's park was worse than its plight. PGN]

✶ A scary thing

<Erann Gat <gat@jpl.nasa.gov>>

Wed, 28 Jan 2004 17:44:28 -0800

I just had a scary thing happen to me. I got the following e-mail:

```
Return-path: <remind@newman.newman-grt.oscar.aol.com>
Date: Wed, 28 Jan 2004 20:12:08 -0500 (EST)
From: Netscape Registration <remind@newman.newman-grt.oscar.aol.com>
Subject: Information you requested
To: gat@jpl.nasa.gov
Original-recipient: rfc822;gat@jpl.nasa.gov
```

Dear User,

The information that you requested from Netscape is below:

Thank you,

Netscape Registration

<http://home.netscape.com/>

except that where the ***** is there was a password that I often use for low security applications.

Trick is, I have never to my recollection signed up with Netscape. To say nothing of the fact that the e-mail didn't come from Netscape (none of the received headers were from netscape).

⚡ Phishing and a new IE security patch

<Sidney Markowitz <sidney@sidney.com>>

Wed, 04 Feb 2004 10:16:16 +1300

[RISKS 23.16](#) mentioned phishing with URLs of the form [@criminal.site.ip.address/index.html](http://reasonable.site.name) which use the username:password@hostname format of URL for social engineering.

Microsoft has just released a security update for Internet Explorer which deals with vulnerabilities caused by some special characters preventing the entire URL from being displayed in the browser's address bar and status line. That vulnerability has been used with phishing URLs like the above to suppress display the portion of the URL starting from the '@'.

They went one step further, however, and eliminated all support

for the
username:password@hostname syntax in http URLs in the Internet Explorer browser, with optional registry entries to allow or remove the support from programs that embed IE as an object.

The Microsoft Knowledge Base article about the security update is at
<http://support.microsoft.com/default.aspx?kbid=834489>

It refers to information about the URL syntax at
"INFO: URL Syntax for Authentication Without Dialog Prompt"
<http://support.microsoft.com/default.aspx?kbid=200351>

I have seen some objections to Microsoft unilaterally dropping support for a URI syntax allowed in RFC 2396, thereby breaking websites that use this form of URL for user logins. I think in this case Microsoft did the Right Thing for security. RFC 2396 applies to the generalized URI, which includes, for example http:// and ftp:// URLs. The specifics for the http: case (RFC 1738, 2616, etc.) do not use that syntax, while ftp: does. Username password syntax in an http URL was always a nonstandard extension that introduced various security vulnerabilities.

MyDoom and SCO

<"Steve Wildstrom" <steve_wildstrom@businessweek.com>>
Mon, 2 Feb 2004 16:34:32 -0500

Writing on Feb. 2, it's very hard to assess what the real impact of the

MyDoom-generate denial of service was on SCO. We do know that, notwithstanding the hype and heavy breathing from anti-virus companies, that it had little or no impact on the performance of the Internet as a whole.

It's very hard to assess what is going on at SCO, because www.sco.com <<http://www.sco.com/>> was mostly inaccessible from Wednesday, Jan. 28 on (I'm indebted to Netcraft <<http://www.netcraft.com/>> for their site-performance reporting.). Darting on Wednesday, my efforts to reach the SCO site variously generated forbidden access (403) errors, time outs, or sporadic availability. At some point on Sunday, DNS entries for ww.sco.com were removed; later traffic to the site was directed to a Google search page. On Monday, SCO transferred the site to www.thescogroup.com <<http://www.thescogroup.com/>> . According to Netcraft, that server lies within the same IP address space as www.sco.com <<http://www.sco.com/>> , so it would appear that whatever is happening to the server, SCO's network is holding up fine.

Netcraft also reported on the afternoon of Feb. 2 that in anticipation of the MyDoom.B phase of the attack, Microsoft has shortened the TTL for www.microsoft.com <<http://www.microsoft.com/>> to 60. MyDoom.B appears to have gotten significantly less distribution than the A variant.

I think the real untold story of MyDoom is that network administrators, especially at the big ISPs, have gotten much better at containing the damage from these attacks. MyDoom may have been the fastest spreading virus ever, but it seemed much less disruptive than SoBig.F last

summer.

After the first few hours, the main virus-related traffic I saw was the continuing stream of spurious bounce messages and the phony "you have sent a virus" alerts. It wouldn't be hard to eliminate those messages completely--turn off the virus alert feature, which has been rendered worthless by return address spoofing, and don't send bounce messages in reply to messages bearing known signatures, like the MyDoom generated ones.

Steve Wildstrom, BusinessWeek Technology & You columnist
1200 G St NW Suite 1100, Washington, DC 20005

⚡ RISKS actually gets *relatively little* MyDoom Traffic

<Chris Smith <smith@interlog.com>>

Tue, 3 Feb 2004 02:12:49 -0500 (Eastern Standard Time)

I note that you had 2528 new e-mails between Jan 27 and Feb 2, under a week.

Over the week beginning 26 Jan at 3PM, I *personally* received over 30,000 e-mails involving MyDoom. That's just me -- I'm not an ISP or anything. I haven't kept really close tabs, but I estimate this is between 700 and 1000 megabytes.

There are two reasons for this. The first is subtle. As finally detailed at the bottom of Symantec's info page on MyDoom at <http://securityresponse.symantec.com/avcenter/venc/data/w32>.

novarg.a@mm.html

one of the lesser known behaviours of MyDoom is the key. After finding an e-mail address by searching locally on the infected machine, MyDoom then also uses a combination of the domain and a list of common usernames. Almost all of the names are common given names - except mine: smith

I maintain an address at a popular freemail/webmail site, using this username. Thus whenever an instance of MyDoom finds any e-mail from this site, there is a chance it has found me as well. This isn't even one of the REALLY BIG webmail sites. Although I've got lots, I expect anyone at hotmail or aol with a name on the MyDoom list has even more.

The second reason everyone knows - bounces back to spoofed From: addresses. I estimate that between 1/3 and 1/2 of my e-mails are of this variety.

The volume of bounces and directs together makes clear that MyDoom uses these made-up addresses both for From: and To: addresses.

It is worth noting that the vast majority of MyDoom traffic contains spoofed From: and From_ (sender) information. Implementation of something like Sender Permitted From (SPF) could have stopped most of these in their tracks. MyDoom has effectively converted me into an SPF evangelist - because if the history of worms has shown us anything, it's that once a technique is shown to be useful to worms, it isn't RISK that it will show up again - it is pretty much certain.

Anyone who argues that there are too many RISKS with something

like SPF will
have to provide me with a good alternative.

Even after all this, I refuse to accept that my name is a RISK.

⚡ Re: Risks of virus scanners (Bellovin, [RISKS-23.14](#))

<ptomblin+netnews@xcski.com (Paul Tomblin)>

Mon, 2 Feb 2004 21:29:16 +0000 (UTC)

> Why are the good guys trying to teach people to click on
attachments?

I would think antivirus software companies would seem to have a
very large
incentive to keep users doing the stupid things that get them
infected. If
people stopped clicking on attachments, the AV companies would
be out of
business overnight.

Paul Tomblin <ptomblin@xcski.com> <http://xcski.com/blogs/pt/>

⚡ Re: Risks of virus scanners (Bellovin, [RISKS-23.15](#))

<flaps@dgp.toronto.edu (Alan J Rosenthal)>

Tue, 3 Feb 2004 11:25:52 -0500 (EST)

> Why are the good guys trying to teach people to click on
attachments?

But opening "attachments" is a fact of ms-win life. The
commonest text-like

file format is the Microsoft Word (.doc) format. When people turn ms-word files into e-mail messages, they generally do so by "attaching" them. So ms-win users are used to opening attachments, routinely.

I don't think it's useful to tell people not to open attachments, because this is simply infeasible. They are going to open attachments. In fact, the message to all telling them not to open attachments is likely to be a .doc file attachment (unless it's powerpoint, or a flash animation).

I think that what ms-win needs is a clearer separation between data and program. There need to be file formats which are not programmable, which can be viewed safely. Assuming that plain text is (for no real reason) not an option, Microsoft could lead the way by releasing a version of its office suite which does not implement "macros". Very few users will miss them, and everyone else will be impressed by Microsoft's technical mastery in producing word processors which are incapable of transmitting viruses.

✉ Re: The risks of naming (Anderson, [RISKS-23.14](#))

<Robert de Bath <robert\$@mayday.cix.co.uk>>

Wed, 28 Jan 2004 07:48:21 +0000 (GMT)

R. de Bath
R. Debath
R. Bath

R. De'ath

And thats in ONE language! (The 'proper' surname is "de Bath")

Rob (Robert de Bath <robert\$ @ debath.co.uk>) <<http://www.cix.co.uk/~mayday>>

[In addition, Arabic names seem to have many variants. PGN]

🔥 Re: Drunk unlocks police car with own key ([RISKS-23.16](#))

<"D. Joseph Creighton" <djc@cc.UManitoba.CA>>

Tue, 3 Feb 2004 14:39:51 -0600 (CST)

I own a 1999 Sonoma and a 2000 Chevy Venture, both built by General Motors.

The combination ignition/pass key is interchangeable to open either vehicle's door but will not start the other vehicle, presumably due to the chipped key required by the newer model (the Sonoma does not have it). One hopes that, even though the mechanical door locks are being shared, the chips would have a 1:1 mapping of keys to ignitions.

Incidentally, my dealer didn't think of it as a RISK when I first brought it to their attention. They felt I should consider it a feature since so many others pay to have this done.

D. Joseph Creighton [ESTP] | Systems Analyst, Database Technologies, IST
Joe_Creighton@UManitoba.CA | University of Manitoba Winnipeg, MB, Canada, eh?

Re: Drunk unlocks police car with own key

<"Dave Brunberg" <DBrunber@FBLEOPOLD.com>>

Tue, 3 Feb 2004 15:39:28 -0500

Forget keys, one time I was on a business trip to St. John's, Newfoundland.

I rented a maroon Oldsmobile Alero from the National Car Rental at the airport. The car was equipped with a keyless entry system on the key-ring.

I rent so many cars that most of the time I forget what kind of car I'm

driving on any given trip. One day, I went into a local supermarket,

leaving my rental parked in a spot near the entrance after locking it

remotely. Upon exiting the store, I walked over to my Alero, pressed the

unlock button on the keychain, and hopped in. I inserted the key and

started the engine. At this point I noticed that my briefcase was not on

the passenger seat where I had left it. After a moment of panic, it took

about three seconds to realize that I was in somebody else's car. I turned

it off, got out, and pressed the lock button on the remote. The car locked

itself and I went looking for my rental, which was in a spot two rows over

behind a big pickup truck.

What are the odds of having not only a matching door/ignition key, but also the keyless entry remote?

David W. Brunberg

✂ **Re: Drunk unlocks police car with own key ([RISKS-23.16](#))**

<David Hollman <dhollm@yahoo.com>>

Tue, 3 Feb 2004 14:14:23 -0800 (PST)

This story SOUNDS quite apocryphal [, like urban legends noted in]

<http://www.snopes.com/autos/law/copcar.asp>. In fact, things might be much worse than this story indicates, and I have a personal example to demonstrate.

Last year I took a train out to my parent's from the city; in the parking lot they left me a car complete with a magnetic hide-a-key box for the car key which I did not have. Upon opening the box, I found there was a house key instead!

After fruitlessly searching for another key I decided to try the house key on a lark, and to my great surprise it actually OPENED the driver's-side door of the car (which was a 1991 Jeep Cherokee).

Sadly for me this key did not actually start the car. However, since I was in an extremely out-of-the-box frame of mind, I jammed a paperclip in the ignition, heard the distinctive buzzing, turned the "key" and STARTED THE CAR!

(See photo - <http://daiv.ods.org/sockimages/display/1526.jpg>).

The blade on a friend's pocketknife later accomplished the same trick.

NB0: This was actually my dad's system of security through obscurity. Since putting the car key in a hide-a-key box is very insecure he would leave a house key which he knew would open the door, and then would hide the ignition key inside the car. The flaw? Not telling me this in advance!

NB1: Getting into the car was never the primary concern anyway, since on a Cherokee you can grip the rubber of the rear window and easily pull the window out of the door, then climb into the trunk. Useful if you lock your keys in.

NB2: On a Grand Cherokee (at least models from the late 90s) you can *always* open the rear window using the button on the door. This will set off the alarm if locked, but it opens regardless!

✶ "Loss of Identity" theft

<"Terry A. Ward" <terrywa@elp.rr.com>>
Mon, 26 Jan 2004 21:55:32 -0700

I was recently the executor of a relative's estate and was shocked to discover that I was able to cancel his private health insurance, his veteran's health benefits, one dozen credit cards, and all of his retirement direct deposit payments with simple phone calls. At no time did anyone ask me to prove that I was who I said I was or whether I had executor power over his estate. I simply presented a plausible sounding story, knew

his social security number and his account numbers and was able to close his accounts over the phone. To make it even more interesting our last names are not even the same!

The possibility for mischief should be obvious with such an insecure system.

Not exactly computer-related but very scary indeed.

REVIEW: "Kerberos: The Definitive Guide", Jason Garman

<Rob Slade <rslade@sprint.ca>>

Wed, 28 Jan 2004 08:33:21 -0800

BKKRBSDG.RVW 20031018

"Kerberos: The Definitive Guide", Jason Garman, 2003, 0-596-00403-6,

U\$34.95/C\$54.95

%A Jason Garman

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 2003

%G 0-596-00403-6

%I O'Reilly & Associates, Inc.

%O U\$34.95/C\$54.95 800-998-9938 fax: 707-829-0104 nuts@ora.com

%O <http://www.amazon.com/exec/obidos/ASIN/0596004036/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0596004036/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0596004036/>

[robsladesin03-20](#)

%P 253 p.

%T "Kerberos: The Definitive Guide"

Kerberos is not flashy, but it is a venerable and mature technology. Yes,

it has limited scalability, but most of the "successful" PKI (Public Key Infrastructure) projects are small enough that they could easily have been accomplished with Kerberos technology: an eminently elegant solution to the problem of communicating and authenticating over any channel that is, or must be, assumed to be insecure.

Chapter one provides a history, base concepts, and variants of Kerberos. Terms and components are given in chapter two. The Needham-Schroeder work, and the idea of ticket-granting, is in chapter three. Implementation, in chapter four, reviews design, UNIX and Windows servers, and special considerations for a mixed environment. The troubleshooting chapter, five, for once comes early enough in a book to be of use. Security aspects external to Kerberos, and specific settings for different implementations, are covered in chapter six. Chapter seven looks at some generic support for applications, as well as some specific programs that already have Kerberos support built in. Cross realm trust is one of the advanced topics, but most of chapter eight concentrates on special requirements for Windows. Chapter nine is a kind of review of the book, involving the various topics that have been discussed in a sample Kerberos installation. Chapter ten looks at the future of Kerberos, with possible public key additions, Web applications, and smartcards. An appendix contains an administrative command list.

While Kerberos may not be as highly regarded as the more mathematically

complex asymmetric cryptographic systems, it still have many uses, and this book provides the outline, background, and details to help you take full advantage of them.

copyright Robert M. Slade, 2003 BKKRBSDG.RVW 20031018
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu
<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 18

Thursday 12 February 2004

Contents

- [Software bug contributed to blackout](#)
[Kevin L. Poulsen](#)
- [*WashPost* registration expired, newsroom hampered](#)
[Bill Hopkins](#)
- [GM will recall some Chevrolet Corvettes](#)
[Monty Solomon](#)
- [Police face sack in ongoing privacy incidents](#)
[NewsScan](#)
- [Three degrees of outsourcing leads to data disclosure](#)
[Ed Ravin](#)
- [Privatization vs privacy](#)
[Friedrich Knauss](#)
- [TiVo watchers uneasy after post-Super Bowl reports](#)
[Monty Solomon](#)
- [Cable modem hackers conquer the co-ax](#)
[Kevin Poulsen via Monty Solomon](#)
- [Electronic copyrights](#)
[Jim Griffith](#)
- [Opposition to SPF](#)
[Ian Jackson](#)

- [Actually, SPF makes things worse](#)
[Markus Fleck-Graffe](#)
 - [Re: Drunk unlocks police car with own key](#)
[Crispin Cowan](#)
 - [Microsoft warns of widespread Windows flaw](#)
[Robert Lemos via Monty Solomon](#)
 - ['Mydoom' Creators Start Up 'Doomjuice'](#)
[Matti Huuhtanen via Monty Solomon](#)
 - [Re: MyDoom and SCO](#)
[Scott Miller](#)
 - [Don't rely on Social Security Numbers -- AGAIN!](#)
[Robert Ellis Smith](#)
 - [Re: UK data protection laws ... Unintended Consequences](#)
[R M Crorie](#)
 - [An interesting spam-filter risk](#)
[Geoff Kuenning](#)
 - [NSF: Science of Design](#)
[Sol J. Greenspan via Gene Spafford](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Software bug contributed to blackout

<"Kevin L. Poulsen" <klp@securityfocus.com>>

Wed, 11 Feb 2004 19:38:06 -0800

A previously-unknown software flaw in a widely-deployed General Electric energy management system contributed to the devastating scope of the 14 Aug 2003 northeastern U.S. blackout.

The bug in GE Energy's XA/21 system was discovered in an intensive code audit conducted by GE and a contractor in the weeks following the blackout, according to FirstEnergy Corp., the Ohio utility where

investigators say the blackout began. "It had never evidenced itself until that day," said spokesman Ralph DiNicola. "This fault was so deeply embedded, it took them weeks of pouring through millions of lines of code and data to find it."

On Tuesday, the North American Electric Reliability Council (NERC), the industry group responsible for preventing blackouts in the U.S. and Canada, approved a raft of directives to utility companies aimed at preventing a recurrence of the outage. One of them gives FirstEnergy a June 30th deadline to install any known patches for its XA/21 system, though the company says it's already installed the fix. A NERC spokesperson said all electric companies using GE's XA/21 system would likely be instructed to install the patch in a final report due next month.

<http://www.securityfocus.com/news/8016>

[Also reported to RISKS by Chuck Weinstock. PGN]

***W**WashPost* registration expired, newsroom hampered**

<"Bill Hopkins" <whopkins@wmi.com>>

Mon, 9 Feb 2004 15:31:49 -0500

The New York Times, 6 Feb 2004, reported (and not **too** smugly) that newsgathering at its rival **The Washington Post** was disrupted when registration lapsed for washpost.com, which the newsroom uses for e-mail.

The renewal notice from Network Solutions was delivered unnoticed to a "dropbox" (whether e-mail or the old-fashioned kind was not clear). However, the registration was renewed soon after the disruption started, before any squatters could jump on it. (Don't dwell on that image.)

GM will recall some Chevrolet Corvettes

<Monty Solomon <monty@roscom.com>>

Tue, 10 Feb 2004 17:11:00 -0500

General Motors will recall certain Chevrolet Corvettes to correct a condition in which the vehicle can operate when the electronic steering column lock fails to unlock. The vehicles included in this recall are 1997-2000 Corvettes with automatic transmissions in the United States, Canada, and Mexico; 1997-2004 Corvettes with automatic transmissions in Europe and export countries; 1997-2004 Corvettes with manual transmissions in North American, European, and export countries. GM is still working to determine the recall population and the breakdowns by countries; however, the estimate is a total of about 127,000. For manual transmissions, the dealers will reprogram the Powertrain Control Module software, at no cost. GM has not confirmed any occurrences of this condition in the field. There are no confirmed crashes, injuries, or fatalities related to the condition.

[Source: 10 Feb 2004, PR Newswire; PGN-ed]

<http://finance.lycos.com/home/news/story.asp?story=40508961>

Police face sack in ongoing privacy incidents

<"NewsScan" <newsscan@newsscan.com>>

Thu, 12 Feb 2004 10:01:29 -0700

Australian Police in Victoria are facing an embarrassing new privacy scandal after an internal audit found fresh evidence of improper access to confidential computer files. The audit has found up to 35 police have used the police Law Enforcement Assistance Program (LEAP) computer to check information on a security guard charged with manslaughter over the death of former Test cricketer David Hookes. All police who have accessed the files, other than homicide squad police investigating the death, are expected to be asked by ethical standards department police to justify their actions. Police who cannot give legitimate reasons face the sack. This incident comes in the wake of an investigation in 2003 into allegations that the files of 32 current and former Victorian Members of Parliament have been accessed without legitimate reason. [*TheAge*, 11 Feb 2004; NewsScan Daily, 12 Feb 2004]

<http://www.theage.com.au/articles/2004/02/11/1076388435627.html>

Three degrees of outsourcing leads to data disclosure

<Ed Ravin <eravin@panix.com>>

Mon, 9 Feb 2004 21:15:51 -0500

According to Bob Sullivan, MSNBC, 8 Feb 2004

<http://www.msnbc.msn.com/id/4186130/>

A programmer hired by a community college to manage a database for a child care center posted the entire database onto an Internet site in order to obtain help doing the database work. The database contained sensitive information like names, addresses, children's schedules, etc. At one point the fellow was warned that he shouldn't be posting confidential information, but apparently he had a bit of trouble with the concept:

On Jan. 26, another programmer -- who requested anonymity -- sent a message to Dennis, warning him of the possible privacy problems. He replied: "Thank you for the note. That was my mistake and I will be more careful in the future," according to the programmer. The next day, Dennis posted the same database in a different question.

The person who ended up doing the work (recruited via rentacoder.com) is three outsourcing steps away from the county agency that maintained the data in question. It's fairly common for social service agencies to outsource most of their work to non-profits, but it appears that neither the first outsourcing level (the community college) nor the second (the alleged "programmer", Dennis, who posted the databases) had the ability to actually do the work. At least no one seems to have sent this job to

India...

✦ Privatization vs privacy (Re: Three degrees of outsourcing ...)

<friedrich.knauss <fknauss@cultureshark.net>>

Mon, 9 Feb 2004 16:21:49 -0800

[The previous item] exemplifies some of the risks of allowing private corporations to manage sensitive data without adequate government oversight.

The current administration's efforts at increasing data collection against its own citizens, along with its promotion of privatization, bodes for similar future events on a national scale.

✦ TiVo watchers uneasy after post-Super Bowl reports

<Monty Solomon <monty@roscom.com>>

Tue, 10 Feb 2004 22:21:05 -0500

Ben Charny, CNET News.com, 5 Feb 2004

Janet Jackson's Super Bowl flash dance was shocking in more ways than one:

Some TiVo users say the event brought home the realization that their

beloved digital video recorders are watching them, too. [On 9 Feb 2004,]

TiVo said the exposure of Jackson's breast during her halftime performance

was the most-watched moment to date on its device, which, when combined with

the TiVo subscription service, lets viewers pause and "rewind" live television broadcasts, among other features. TiVo said users had watched the skin-baring incident nearly three times more than any other moment during the Super Bowl broadcast, sparking headlines that dramatically publicized the power of the company's longstanding data-gathering practices.

<http://news.com.com/2100-1041-5154219.html>

[Evidently, it pays to keep abreast of TiVo's capabilities. PGN]

✶ Cable modem hackers conquer the co-ax (Kevin Poulsen)

<Monty Solomon <monty@roscom.com>>

Wed, 11 Feb 2004 20:21:07 -0500

Kevin Poulsen, SecurityFocus, 5 Feb 2004

A small and diverse band of hobbyists steeped in the obscure languages of embedded systems has released its own custom firmware for a popular brand of cable modem, along with a technique for loading it -- a development that's already made life easier for uncappers and service squatters, and threatens to topple long-held assumptions about the privacy of cable modem communications. The program, called Sigma, was released in its final version last month, and has reportedly been downloaded 350 to 400 times a day ever since. It's designed to be flashed into the non-volatile memory of certain models of Motorola's Surfboard line, where it runs in

parallel with the device's normal functionality. It gives users almost complete control of their cable modem -- a privilege previously reserved for the service provider.

The project is the work of a gang of coders called TCNiSO. With about ten active members worldwide, the group is supported by contributions from the uncapping community -- speed-hungry Internet users who rely on TCNiSO's research and free hackware to surmount the bandwidth caps imposed by service providers, usually in violation of their service agreement, if not the law. To them, Sigma is a delight, because it makes it simple to change the modem's configuration file -- the key to uncapping, and, on some systems, to getting free anonymous service using "unregistered" modems. "I've known TCNiSO for two years now and I've done a lot of things with their techniques," wrote a Canadian uncapper in an e-mail interview. "Sigma is the greatest one I've seen." ... [<http://www.securityfocus.com/news/7977>]

✶ Electronic copyrights

<griffith@dweeb.org (Jim Griffith)>
Thu, 05 Feb 2004 18:46:54 -0500

In 1997, I wrote a piece for rec.humor.funny based on an idea by Steve Lancaster, in which the Mars Pathfinder landing was reported from the

Martian point of view, a la Roswell.

<http://groups.google.com/groups?selm=Sb43.21d1%40clarinet.com>

<http://www.netfunny.com/rhf/jokes/97/Jul/marspress.html>

It was well-received, and I'm rather proud of that piece. In early January, some anonymous nitwit took my original piece, changed about four words to make it fit Spirit instead of Pathfinder, tacked on a couple of brand new paragraphs, and sent it circulating again, anonymously. This modified version has now shown up in various monthly astronomy publications, always without attribution.

As moderator of RHF, I understand the difficulties of identifying the original source of a piece, and the ease with which people remove attributions. I'm disturbed by the casual way so many publications blindly printed the piece without doing a serious attempt to identify the source or the original version. Granted, that source isn't immediately obvious, but a reasonable Google search or a date-sorted Google Groups search would have definitively identified both the author and the original wording. In effect, Google Groups is now my primary hope for preserving my original copyright (although I did have the foresight to encode in the piece an in-joke that only I know -- and the plagiarized versions preserve that in-joke). Had I originally distributed the piece via e-mail, I'd now have no hope of ever claiming credit or preserving the original version.

I'm mainly disturbed by the ease with which the original piece was

corrupted, and that that corruption was blindly accepted and propagated. It is now the case that corrupted version is more prevalent than the original.

This is disappointing, given that an advantage of electronic communications is supposed to be the way it preserves information. I wonder if we'll find that in a hundred years, the most popular Internet version of "Romeo and Juliet" is one with a new, happier ending?

✶ Opposition to SPF (Re: Rose, [RISKS-23.16](#))

<Ian Jackson <ijackson@chiark.greenend.org.uk>>

Wed, 4 Feb 2004 14:25:33 +0000

Andrew Rose <andrew.rose@dataconnection.com> writes:

> The technical work on SPF is now complete and adoption has started.

I strongly disagree that technical work on SPF is complete:

* The current specification is absolutely terrible, when one looks at the details. (As an experienced developer of networking software including a DNS resolver and an SMTP mail rejection agent, and participant in standards processes, I should know.)

* SPF proponents haven't taken the proper route through the IETF for their

`standard' -- where the details of the spec might have been fixed.

Instead, they're going for a publicity campaign to `bounce' people into adoption.

* Many people I respect (myself not included) think that the principle of operation of SPF is broken for technical reasons. I'm sure those people can explain that themselves.

For a personal perspective from a member of the IESG, see <http://www.interesting-people.org/archives/interesting-people/200401/msg00037.html>

✶ Actually, SPF makes things worse (Re: Rose, [RISKS-23.16](#))

<Markus Fleck-Graffe <fleck@isoc.de>>

Wed, 04 Feb 2004 03:28:47 +0100

Re: Defeating phishing scams, Andrew Rose, [RISKS 23.16](#)
> The technical work on SPF is now complete and adoption has started.
> Several thousand domains have published SPF records including some very
> large domains such as aol.com.

The SPF scheme requires all e-mail forwarders to rewrite the sender's e-mail envelope and return-path addresses. For example, each posting to a mailing must be rewritten to a local domain of the list host before redistribution.

To enable (administrative) e-mail bounce notifications, each forwarding host is also more or less required to generate specially encoded one-time "sender" addresses for each forwarded e-mail, and keep a corresponding database of "reverse mappings" for an unspecified period of time. [<http://spf.pobox.com/srs.html>]

The SPF website calls this an "unfortunate" problem -- extremely unfortunate because every pre-existing mail transport agent in the world is incompatible with the SPF scheme and will lead to silent discarding of lots of legitimate (forwarded) e-mail (which would be considered forged by SPF-agnostic receiver sites).

Worst of all, SPF will not stop spammers and viruses/worms from spreading - spammers will just start to set up their own SPF infrastructures (with throw-away domain names), and worms will just use legitimate e-mail addresses of compromised host PCs. (In fact, spammers nowadays are increasingly using compromised third-party PCs for their mass mailings as well, preferably badly secured ones with high-bandwidth connectivity to the Internet such as through cable modems OR xDSL lines.) In addition, the backwards-mapping database of SPF-aware mail forwarders must itself be secured against abuse of the e-mail bouncing mechanism by spammers and worms - by introducing even more stateful data keeping to their forwarding databases. The SPF site even proposes adding time-limited cookies to secure against this "open (back-)relay" problem -- what an awful hack!
[1]

The RISKS? Several e-mail providers are adopting a half-baked non-solution with obvious deficiencies and a potential for silently sinking lots of legitimate e-mail into a black hole. And a proprietary three-letter ISP is trying to force their (centralized!) single-server world-view of

communication protocols onto the Internet.

✶ Re: Drunk unlocks police car with own key (Brunberg, [RISKS-23.17](#))

<Crispin Cowan <crispin@immunix.com>>

Thu, 05 Feb 2004 02:06:13 -0800

> What are the odds of having not only a matching door/ignition key, but
> also the keyless entry remote?

Apparently pretty good odds :)

I heard 2nd- or 3rd-hand of an inventive software security person (name omitted because I want them to still talk to me :) who wanted to investigate precisely this problem when keyless entry first came out. Apparently the initial key space for keyless entry was only 16 bits, and so my friend built a device to brute-force the keyspace with a fairly powerful radio broadcaster attached. Friend then took the device to a large parking lot, turned it on, and watched with amusement as dozens of cars around the parking lot started honking and unlocking.

I *think* the keyspace has improved since then, but I would bet it has not improved enough.

Crispin Cowan <http://immunix.com/~crispin/> CTO, Immunix

<http://immunix.com>

Immunix 7.3 <http://www.immunix.com/shop/>

[Things have improved enormously since the early garage-door

openers, many

of which opened and closed each time the orbiting Russian Sputnik went

overhead. I have not noted that marvelous case here since [RISKS-8.38](#),

which appropriately was issued on the Ides of March 1989, so it is worth

recalling for newer readers. Don't forget, all the RISKS archives are

searchable at Lindsay Marshall's Web site (www.risks.org).
PGN]

Microsoft warns of widespread Windows flaw

<Monty Solomon <monty@roscom.com>>

Tue, 10 Feb 2004 17:43:55 -0500

Microsoft has a message for Windows users: Patch your computers quickly.

Robert Lemos, CNET News.com, 10 Feb

On Tuesday, the software giant released a fix for a networking flaw that affects every computer running Windows NT, Windows 2000, Windows XP or

Windows Server 2003. If left unpatched, the security hole could allow a worm

to spread quickly throughout the Internet, causing an incident similar to

the MSBlast attack last summer. ...

[<http://news.com.com/2100-7355-5156647.html>]

What You Should Know About the Windows Security Updates for February 2004

http://www.microsoft.com/security/security_bulletins/20040210_windows.asp

Microsoft Security Bulletin MS04-007

ASN.1 Vulnerability Could Allow Code Execution (828028)

<http://www.microsoft.com/technet/security/bulletin/MS04-007.asp>

Microsoft Security Bulletin MS04-006

Vulnerability in the Windows Internet Naming Service (WINS) Could Allow Code Execution (830352)

<http://www.microsoft.com/technet/security/bulletin/MS04-006.asp>

Microsoft Security Bulletin MS04-004

Cumulative Security Update for Internet Explorer (832894)

<http://www.microsoft.com/technet/security/bulletin/MS04-004.asp>

'Mydoom' Creators Start Up 'Doomjuice'

<Monty Solomon <rebates@roscom.com>>

Tue, 10 Feb 2004 15:22:31 -0500

Finnish computer security experts warned Tuesday of a new worm, known as

"Doomjuice," that is expected to attack computers infected by "Mydoom,"

despite the fact it's programmed to stop spreading later this week. The

virus, first detected by F-Secure on Monday night, has so far infected at

least 30,000 computers worldwide since it was activated Sunday, said the

company's director of antivirus research, Mikko Hypponen.

Like Mydoom.A and Mydoom.B, the new worm is designed to strike Microsoft

Corp.'s Windows operating systems and is programmed to launch a worldwide

attack on the web site of SCO, one of the largest UNIX vendors in the world.

[Source: Matti HUUHTANEN, Associated Press, 10 Feb 2004, AP Online]

<http://finance.lycos.com/home/news/story.asp?story=40507941>

✶ Re: MyDoom and SCO (Wildstrom, [RISKS-23.17](#))

<Scott Miller <SMiller@unimin.com>>

Wed, 4 Feb 2004 18:58:46 -0500

> Writing on Feb. 2, it's very hard to assess what the real
impact of the
> MyDoom-generate denial of service was on SCO.

I find it curious that with about a week's notice of the actions
of the
MyDoom.A payload, SCO found it impossible to prepare an
effective strategy
in advance of the attack. I also find it somewhat curious (but
anecdotal)
that all of the MyDoom infected e-mail messages received on my
personal POP
account ~appeared~ to be sourced from the allwest.com domain,
with admin
contacts listed as physically located in Utah. As a result of
the nature of
the MyDoom.A payload and of the consequent reward offered by
SCO, Darl
McBride and his misbegotten (IMO) anti-Linux campaign have
received a great
deal of publicity and a reprieve from what appeared to be an
imminent slip
from the public consciousness. A cynical person (not I, heaven
forfend)
might be tempted to speculate whether SCO could have been
involved in the
release of the worm, or at best, played willing victim.

✶ **Don't rely on Social Security Numbers -- AGAIN!**

<"Robert Ellis Smith" <ellis84@rcn.com>>

Mon, 9 Feb 2004 09:42:50 -0500

Terry Ward in [RISKS-23.17](#) reports that to cancel another person's insurance, credit, etc., "I simply presented a plausible sounding story, knew his social security number ***"

And yet lots of professionals and private citizens still think that the key to preventing identity theft is MORE reliance on Social Security numbers.

The reality is that SSNs are no longer private bits of information, if they ever were, and no longer serve to authenticate an individual's identity. So each of us has to cease going along with this deceit.
Robert Ellis Smith, Privacy Journal

✶ Re: UK data protection laws ... Unintended Consequences (R-23.14,15)

<R M Crorie <risks@crorie.com>>

Tue, 03 Feb 2004 21:58:35 -0000

Mark Brader states ([RISKS-23.15](#)):

> It's for failing to get the criminal tried and convicted back then. And
> even this is only true if the earlier alleged offenses were genuine.

Errrrmm... and even if "genuine" (=true?), how would they achieve that, precisely? If there was insufficient evidence to pass the first

(evidential) test by which Branch Crown Prosecutors decide whether or not to prosecute, presumably the recommendation here is to manufacture more...? :-)

> For police, it **is** reasonable to consider that someone previously suspected should be suspected again: this is all right precisely because a police suspect is not, ipso facto, a criminal.

But that is at the heart of the argument: to know about the previous suspicion, the data about the (unsubstantiated) allegation would need to be retained for that purpose, which is precisely what is not **explicitly** provided for in the Act. My understanding is that the Information Commissioner was already pressing two other forces to delete data for that very reason, i.e. some non-conviction information was being retained by them for "longer than necessary", but there is nothing to explain what "necessary" actually means -- in fact, the only explicit guidance is that it was, and is, for forces themselves to make that decision!

In any event, any evidence supporting the allegation(s) not proceeded with is completely inadmissible in proceedings for any new allegation. That's the way society has made the rules, that's the way they are followed.

Damned if you do, and damned if you don't...

✶ An interesting spam-filter risk

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

Mon, 9 Feb 2004 12:09:12 -0800 (PST)

I'm a member of a mailing list in which one of the members has chosen to sign up for one of those "identity verification" services for preventing spam. Every time anybody sends to the list, we get an autoresponse from "roberto@riskfreemail.com", who asks us to go out of our way to prove that we're humans.

The RISKS of this approach are well known, and most list maintainers (PGN included) refuse to allow subscribers to use these services.

The problem in the current case is that nobody can figure out which of our 950+ subscribers is the culprit! That has led one member to propose that a group of volunteers divide up the subscriber list and send test e-mails to people until we discover one that produces the annoying bounce.

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

NSF: Science of Design

<Gene Spafford <spaf@cerias.purdue.edu>>

Wed, 11 Feb 2004 11:18:48 -0500

This message is to inform you that a new NSF funding opportunity called SCIENCE OF DESIGN [Solicitation NSF 04-552] has been posted by the CISE Directorate. The CISE web page (<http://www.cise.nsf.gov>) has a

link to the
program page under "CISE FY04 Emphases" and there is additional
information
under "Hot Topics" on the CISE web page. [See the Program URL:
http://www.cise.nsf.gov/funding/pgm_display.cfm?pub_id=13078]

The goal of this solicitation is to stimulate research and
education
projects that build the Science of Design. This solicitation
focuses on the
scientific study of the design of software-intensive systems
that perform
computing, communications and information processing. Complex
interdependencies strain our ability to create, maintain,
comprehend and
control these systems. The Science of Design seeks to rectify
this situation
by building a foundation for the systematic creation of software-
intensive
systems. This foundation will consist of a body of theoretical
and empirical
knowledge on design, computational methods and tools for design,
and new
design curriculum for the next generation of designers.

Sol J. Greenspan, Ph.D., Chair, Science of Design Coordinating
Group
Directorate for Computer and Information Science and
Engineering [PGN-ed]

[If you have learned anything from reading RISKS, it might be
quite
relevant here! PGN]



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 19

Weds 18 February 2004

Contents

- [Mississippi voids November 2003 e-vote election for errors](#)
[Steve Corrick](#)
- [Canadian medical tests give reversed results](#)
[Danny Burstein](#)
- [911 mistake: Wisconsin rescuers go to wrong town; victim dies](#)
[David LaRue](#)
- [Interesting device to steal ATM accounts](#)
[Mabry Tyson](#)
- [Officials Say Mob Stole \\$200 Million Using Phone Bills](#)
[William K Rashbaum via Monty Solomon](#)
- [Amazon reviewers identified -- as the authors!](#)
[NewsScan](#)
- [Alleged Trojan horse in Israeli anti-ballistic missile system](#)
[Gadi Evron](#)
- [GAO Report Warns of Airline Security Shortcomings](#)
[Lillie Coney](#)
- [GE says blackout bug patched](#)
[Kevin L. Poulsen](#)
- [Strategic planning for VeriSign restart of "Site Finder"](#)
[Lauren Weinstein](#)

- [FTC warning about private no-spam registry](#)
[NewsScan](#)
 - [TiVo's privacy policy](#)
[Terence Eden](#)
 - [Re: Privatization vs privacy](#)
[Aaron](#)
 - [Challenge/Response spam blocking](#)
[Thomas Harrington](#)
 - [Social Security number as identity: not secure](#)
[Carl Fink](#)
 - [Re: Spirit Rover humbled](#)
[Timothy Prodin](#)
 - [Sputnik & garage door openers](#)
[Kyle York](#)
 - [Re: SPF and its critics](#)
[Lawrence Kestenbaum](#)
 - [Exploiting software](#)
[Gary McGraw](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **Mississippi voids November 2003 e-vote election for errors**

<GardenEarth@aol.com>

Sun, 15 Feb 2004 08:52:44 EST

[via Rebecca Mercuri <notable@mindspring.com> PGN]

So the election machine companies say no one has every proved vote fraud on the voting machines. However, the same cannot be said of massive machine error. Here's a real clincher to the line about voting machines being the safest, most secure form of voting ever devised.

Mississippi Senate Declares Last November's Election Invalid

In the November 2003 election, Hinds County, Mississippi used the WINnVote touchscreen machine (the same as the one used in Fairfax County, Virginia disastrous election). Poll workers had trouble starting the machines, some of the machines overheated and had to be taken out of service, poll workers were scrambling to find enough paper ballots, and many voters left with polls without voting because of the long delays.

<<http://www.clarionledger.com/news/0311/04/mvproblems.html>>

The problems were investigated by a Mississippi Senate committee, and on January 19, it recommended invalidating the outcome of the race for the District 91 Senate seat and holding the election over. Two days later, the Senate approved the recommendation. The new election is set for February 10. The last we heard the Democratic candidate, Dewayne Thomas, was considering pulling out of the race and conceding to his opponent, Richard White. We hope Thomas doesn't allow faulty machines to determine an outcome that should be decided by the voters.

<<http://www.clarionledger.com/news/0401/21/ma04.html>>

Oh, and just for good measure...

Venezuela had to cancel its 2000 national election because of voting machine problems

<http://news.bbc.co.uk/1/low/world/americas/764372.stm>

Let all our votes be counted,

Steve Corrick <OperationEnduringVote.org>

Canadian medical tests give reversed results

<danny burstein <dannyb@panix.com>>

Fri, 7 Nov 2003 23:50:38 -0500 (EST)

[Apologies to Danny for this item taking so long to surface.
PGN]

About 3,000 people got opposite results when they were tested for gonorrhea and chlamydia over an 18-month period. Because of a faulty diagnostic machine in Cranbrook (southeastern British Columbia), positive and negative test results for the two sexually transmitted diseases were reversed.

About 3,000 people were tested. The 83 that were positive were incorrectly told they were clean. The 2,900 or so that were negative were told they were positive and were given the standard treatments. From a health standpoint the 83 sick folks come out the worst, because their treatment was delayed for months or years. But even the folk who were well went through the drug protocols and other exams and treatments -- which have their own secondary effects, plus, of course, the social/inter-personal problems which being (mis)diagnosed with an STD will cause, especially with regard to patient partner tracking.

One Would Have Thought that someone in the medical office or the lab or the insurance or the pharmacy or somewhere..., looking at 3,000 test results, would have quickly noticed that instead of finding a positive

rate of 3%
these tests were coming back at 97%. One would Also Have Thought
that enough
of these people would have gotten a second set of tests so as to
raise
eyebrows a lot earlier.

[Thousands Given Wrong STD Results (Associated Press, 30 Oct
2003; PGN-ed
from Danny's initial abstracting]

[http://www.newsday.com/news/health/wire/
sns-ap-std-tests-reversed,0,3203781,print.story?coll=sns-ap-
health-headlines](http://www.newsday.com/news/health/wire/sns-ap-std-tests-reversed,0,3203781,print.story?coll=sns-ap-health-headlines)

[Also, see US Gov't FDA recall notice \(which suggests there were
similar
incidents in other places\) :](#)

<http://www.fda.gov/cdrh/recalls/recall-072103.html>

Canadian local coverage:

<http://cnews.canoe.ca/CNEWS/Canada/2003/10/29/240955-cp.html>

✶ 911 mistake: Wisconsin rescuers go to wrong town; victim dies

<"David LaRue" <Huey.DLL@GTE.Net>>

Thu, 12 Feb 2004 23:26:15 -0500 (EST)

Rescue personnel from the Neenah-Menasha Fire Rescue service
responded to a
911 emergency call for a possible heart attack victim within two
minutes.

However, it was the right address in the wrong town. (Both
towns had the
identical address.) [Source: An AP article (from the *Star
Tribune*,
datelined Neenah, Wisconsin) PGN-ed.]

Whereas there are procedures and database checks to prevent incorrect locations in the 911 databases, it is still possible for neighboring cities to have identical addresses. The risks here are that the data may look correct and even validate, but still be wrong.

[We have reported at least one similar case previously. PGN]

🔥 Interesting device to steal ATM accounts

<Mabry Tyson <Tyson@AI.SRI.COM>>

Fri, 13 Feb 2004 16:40:46 -0800

Bank ATMs Converted to Steal Bank Customer IDs

<http://www.utexas.edu/admin/utpd/atm.html>

A team of organized criminals is installing equipment on legitimate bank ATMs in at least 2 regions to steal both the ATM card number and the PIN. The team sits nearby in a car receiving the information transmitted wirelessly over weekends and evenings from equipment they install on the front of the ATM (see photos). If you see an attachment like this, do not use the ATM and report it immediately to the bank using the 800 number or phone on the front of the ATM.

The equipment used to capture your ATM card number and PIN is cleverly disguised to look like normal ATM equipment. A "skimmer" is mounted to the front of the normal ATM card slot that reads the ATM card number and

transmits it to the criminals sitting in a nearby car.

At the same time, a wireless camera is disguised to look like a leaflet holder and is mounted in a position to view ATM PIN entries.

The thieves copy the cards and use the PIN numbers to withdraw thousands from many accounts in a very short time directly from the bank ATM.

✶ Officials Say Mob Stole \$200 Million Using Phone Bills (Rashbaum)

<Monty Solomon <monty@roscom.com>>

Thu, 12 Feb 2004 03:11:31 -0500

New York organized crime figures reportedly bilked millions of unsuspecting consumers out of more than \$200 million over five years by piggybacking bogus charges on their telephone bills ("cramming"). [Source: William

K. Rashbaum, *The New York Times*, 11 Feb 2004; PGN-ed]

<http://www.nytimes.com/2004/02/11/nyregion/11MOB.html>

✶ Amazon reviewers identified -- as the authors! (NewsScan)

<"NewsScan" <newsscan@newsscan.com>>

Tue, 17 Feb 2004 07:59:24 -0700

Authors in the news -- unintentionally

A software glitch exposed the real identities of book reviewers

at Amazon's Canadian Web site -- thereby revealing that some authors are in the practice of posting anonymous glowing reviews of their own work. [Surprise.] One defender of the practice is author John Rechy, who wrote a favorable review of his latest book, posting the review anonymously as "A Reader From Chicago." Rechy says: "That anybody is allowed to come in and anonymously trash a book to me is absurd. How to strike back? Just go in and rebut every single one of them." The glitch has since been unglitched. [AP/*San Jose Mercury News*, 14 Feb 2004; NewsScan Daily, 17 Feb 2004] <http://www.siliconvalley.com/mld/siliconvalley/7955264.htm>

⚡ Alleged Trojan horse in Israeli anti-ballistic missile system

<Gadi Evron <ge@linuxbox.org>>
Wed, 18 Feb 2004 18:36:02 +0200

On 15 Feb 2004, an article appeared in one of Israel's leading newspapers, *Maariv*, claiming a Trojan horse might have been installed by Egypt in the Israeli Arrow anti-ballistic missile system. You can find an article I wrote on the subject, specifying the known facts at: <http://www.math.org.il/arrow-trojan.html>

Also solarday@hotmail.com +972-50-428610 (Cell)
http://vapid.reprehensible.net/~ge/Gadi_Evron_Emails.asc

GAO Report Warns of Airline Security Shortcomings (*LATimes*)

<Lillie Coney <lillie.coney@acm.org>>

Thu, 12 Feb 2004 10:23:30 -0500

In its report (released on 13 Feb 2004), a General Accounting Office study notes that CAPPS II (intended to pick out potential terrorists from among millions of air passengers) has run into "significant challenges" posing "major risks" to its deployment and public acceptance. Problems include overall system reliability and false positives, and resolving the rights of those falsely identified. Passenger-provided information would be outsourced to government contractors for analysis, the government would check supposedly validated identities against a watch list, and the result would be a green, yellow, or red risk rating for each would-be passenger. Allegedly only about 4% would be rated yellow, and "an average of only one or two people a day" would be rated red. [Remember that even a 1% false positive rate would mistakenly identify tens of thousands of travelers.]

"But the GAO report found that the agency has not adequately addressed seven of eight concerns raised by Congress. These include preventing abuses, protecting privacy, creating an appeals process, assuring the accuracy of passenger data, testing the system, preventing unauthorized access by hackers and setting out clear policies for the system." GAO investigators

concluded that, though the agency was making advances in all these areas, progress was incomplete. [Source: Ricardo Alonso-Zaldivar, *Los Angeles

Times*, 12 Feb 2004; PGN-ed]

[www.latimes.com/technology/la-na-profiling12feb12,1,3293045.story
?coll=la-headlines-technology](http://www.latimes.com/technology/la-na-profiling12feb12,1,3293045.story?coll=la-headlines-technology)

⚡ **GE says blackout bug patched (Re: [RISKS-23.18](#))**

<"Kevin L. Poulsen" <klp@securityfocus.com>>

Thu, 12 Feb 2004 16:08:13 -0800

GE Energy has now acknowledged the bug reported by SecurityFocus earlier

this week ("Software bug contributed to blackout," [RISKS-23.18](#)).

The AP reports that the company says it distributed an advisory and a

fix to more than 100 utility customers last fall.

<http://www.securityfocus.com/news/8032>

⚡ **Strategic planning for VeriSign restart of "Site Finder"**

<Lauren Weinstein <lauren@vortex.com>>

Tue, 10 Feb 2004 17:17:27 PST

Given that VeriSign is strongly hinting that they'd like to soon restart

their notorious and disruptive Site Finder domain diversion scheme

(see: <http://www.washingtonpost.com/wp-dyn/articles/A25819->

[2004Feb9.html](#)),

I believe it would be prudent for the Internet community to begin planning now for appropriate legal, business, and technical actions and reactions for that or related possible eventualities.

The PFIR Forum on "E-Mail Issues, Problems, and Solutions":

<http://forums.pfir.org>

is available immediately for this purpose as a starting point (even though Site Finder issues transcend e-mail). I can spin off a separate forum for this discussion later if traffic and circumstances warrant it. We need to be discussing these issues now so that if and when VeriSign starts the clock on a Site Finder reactivation we won't be blindsided again.

Also, any e-mail on this topic that is not suitable for the public

discussion forum is invited at:

vs@pfir.org

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

lauren@privacyforum.org

Tel: +1 (818) 225-2800 <http://www.pfir.org/lauren> <http://www.factsquad.org>

[factsquad.org](http://www.factsquad.org)

>>> "The VeriSign Song": <http://www.pfir.org/vs-song> <<<

FTC warning about private no-spam registry

<"NewsScan" <newsscan@newsscan.com>>

Tue, 17 Feb 2004 07:59:24 -0700

The Federal Trade Commission has cautioned computer users not to fall victim a Web site claiming to offer an e-mail version of the federal do-not-call

registry. Despite the official-looking appearance of the site's URL, the

"Do Not E-mail Registry" has no affiliation with the U.S. government, and is

apparently a scam for collecting e-mail addresses on behalf of spammers.

However, the site's operators say their registry serves

"legitimate direct

marketers" who want to make sure their mailings don't go to spam opponents.

The e-mail addresses collected by the registry are made available to bulk

mailers in an encrypted form allowing them to check for any overlap with

their own mailing lists without seeing the actual addresses.

[*The

Washington Post*, 15 Feb 2004; NewsScan Daily, 17 Feb 2004]

<http://www.washingtonpost.com/wp-dyn/articles/A41490-2004Feb14.html>

TiVo's privacy policy

<Terence Eden>

Fri, 13 Feb 2004

TiVo has always been very open about its data retention policy.

It has the

ability to review every IR command sent to the box and can track what people

watch and how they watch certain programmes. When signing up to the TiVo

service, people are explicitly asked if they want to opt-

IN to the

monitoring scheme. Anecdotally, most people are happy to be monitored in

the hope of improving the quality of TV programming.

The RISK? Assuming that all data retention is unasked for,

unwarranted and
unhelpful!

✦ **Re: Privatization vs privacy (Knauss, [RISKS-23.18](#))**

<Aaron <aaron@justaaron.com>>

Fri, 13 Feb 2004 17:27:07 -0700

> [The previous item] exemplifies some of the risks of allowing
private
> corporations to manage sensitive data without adequate
government oversight.

The item has nothing to do with government/private interaction,
except
for the fact that it was a government/private interaction.

The risks apply to **any** sensitive database, public or private.
Should we
be asking for "adequate government oversight" of **private**
databases?

Trying to get sensitive work done on the cheap, without
oversight, without
verifying qualifications, is asking for trouble no matter who
owns the
database, no matter what's in the database. If the agency
couldn't afford
proper maintenance, the solution should have been to not have
the database
at all.

The current administration does not have a monopoly on
stupidity; it's quite
abundant in the universe and easy to stumble over. Politicizing
the risk
only obscures the issue.

Challenge/Response spam blocking

<Thomas Harrington <tph@acm.org>>

Thu, 12 Feb 2004 18:30:18 -0700

Many of you have probably noticed that people who use Earthlink can now opt for a challenge/response spam-protection system. As Earthlink implements this, the first time you send an e-mail to someone using this feature, you get an autoresponse directing you to a web page where you're supposed to prove yourself to be human, providing your name and optionally a short message. Do so and the message goes through.

To defeat auto-completion of this web page by scripts they include an image showing five random letters, which is distorted in the hope of defeating OCR software. You're supposed to type in the five letters in a box in the web form.

Only those images aren't all that random.

Because of some business requirements I won't go into just now, I end up confronting this page quite frequently. And my web browser auto-completes forms-- which is nice, since I'm inevitably filling in the same information. What's surprising is that when doing this, my web browser often fills in the "random" image text correctly. It's not always right at first, but if I type the first letter (or sometimes the first two), it completes the rest of the letters correctly.

Some experimenting indicates that in dozens of visits to this challenge page, I've only seen about a dozen distinct "random" text images. I hardly ever type more than the first one or two letters showing anymore. Getting one of 12 right on a random guess is a low success rate by most measures. But consider that the spammers who are supposed to be blocked by this are already operating a business model where one success in several million is reputedly enough to be profitable.

Addendum 15 Feb 2004: Challenge/Response spam blocking

I just wanted to add some additional information that's come to light in the past few days.

1. Earthlink's challenge-response system seems to be buggy. Today, despite numerous attempts, it keeps telling me I've misread the letters image, for multiple e-mails I'm trying to send. I have a couple of customers at Earthlink who are probably going to think I'm ignoring them, but Earthlink is just not letting me send them messages. After doing this a few times I decided to try their help link for visually-impaired people (I'm not visually impaired, but saw no other option). This directed me to an online web-based chat from which I was repeatedly disconnected until I gave up. Hopefully this customer won't be too upset at what would look to him like I'm not listening to him... Right now Earthlink's spam-blocker is so effective that it's preventing even legitimate e-mail from getting through.

2. As a side-effect of this I've discovered what happens if you enter the image text incorrectly (or at least the server thinks you've entered it incorrectly): You get to try again, apparently as many times as you like. Given my previously-discovered non-randomness of the challenge images, it'd be short work for a spammer to load up a script with a collection of correct answers to the challenge, and just have it keep trying until it gets the right one. As I've described previously, the set of correct answers is very small, so this would be nowhere near as challenging as a typical dictionary-style attack.

✶ Social Security number as identity: not secure

<Carl Fink <carl@fink.to>>

Thu, 12 Feb 2004 22:01:35 -0500

I needed to use my corporate travel web site today, after not using it since I first signed up. As you might expect, I had forgotten my password.

To have a password mailed to me, I enter my user ID and request it. No problem, except the user ID is my Social Security number, and the password is mailed back unencrypted.

In other words, anyone who knows my SSID and has access to the corporate mail system can hijack my account. My employer's travel web site is a service of getthere.com.

Carl Fink <carl@fink.to> <http://www.jabootu.com>

[We've been over this topic many times here, but the message still
needs to be reinforced. PGN]

✦ Re: Spirit Rover humbled ([RISKS-23.15](#))

<"Prodin, Timothy (T.R.)" <tprodin@ford.com>>

Tue, 03 Feb 2004 22:24:51 -0500

What the Rovers do not have is a simple precaution that would prevent the continuous reset loop that Spirit went through. A simple counter that tracked the number of resets per Sol, the mission timekeeping unit, would have allowed the Rover to degrade gracefully to an "Operator Intervention Required" state. The current strategy came close to putting Spirit into an unrecoverable condition; cut into useful life of the mission; and, most importantly, obscured valuable diagnostic information.

The RISK? Using a reset to clear from unrecoverable errors can get you in trouble if the reset does not clear the root cause of the error state.

✦ Sputnik & garage door openers (Re: [RISKS-23.18](#))

<Kyle York <kyork@cisco.com>>

Tue, 17 Feb 2004 09:24:02 -0800

> Things have improved enormously since the early garage-door
> openers, many
> of which opened and closed each time the orbiting Russian
> Sputnik went
> overhead. I have not noted that marvelous case here since
[RISKS-8.38](#), PGN]

This piqued my curiosity so I thought I'd look around. I've not
found the
Sputnik/garage door opening to be more than an urban legend and
was
wondering if you've references to the contrary. Most of what
I've found
seems to derive from the same source. It seems sunspots are a
more logical
conclusion.

From alt.folklore.urban:

The full link if you're interested:

<<http://www.google.com/groups?threadm=3BDFE8A4.3BE6D2FF%40midway.uchicago.edu>>

The 20MHz frequency of Sputnik was not used for things like
garage door
openers, which probably used the 27MHz frequency band (the
same one used
by CB in later years). That band was allocated by the FCC for
low-power
devices (under 100 milliwatt), including remote controls, and
cheap toy
walkie-talkies. It continued to be used for walkie talkies
after CB became
big, but other remote-controlled devices were moved off this
band up into
the VHF frequencies after the CB craze hit.

[Can anyone provide evidence that this is NOT an urban
legend? PGN]

✉ **Re: SPF and its critics ([RISKS-23.18](#))**

<Lawrence Kestenbaum <polygon@potifos.com>>

Fri, 13 Feb 2004 01:49:33 -0500 (EST)

Ian Jackson and Markus Fleck-Graffe (in [RISKS 23.18](#)) offer some technical criticisms of the SPF proposal. I am not competent to judge the networking pros and cons, but the e-mail system as it exists is most assuredly broken.

My e-mail address has been public for years, and appears on my web site, which gets hundreds of thousands of visitors per month. I get a steady stream of unsolicited (yet valuable) personal mail from web site users. And I do get at least a couple hundred spam and virus/worm e-mails per day. I cope.

But the junk has suddenly reached a new level.

Starting in early January, some spamhaus started using my e-mail address in the From: and Reply-to: lines of a large quantity of bulk messages advertising a product claimed to change the size of a body part. As a result, I received thousands of bounce and rejection notices from all over the world. The flow diminished for a couple of days, then resumed in full force, as the spammer sent out new waves of bulk mail, now advertising a get-rich-quick scheme. It's February 13 now, and the bounces are still pouring in.

Of course the actual miscreant is hidden because the spams themselves are originated from what are probably DSL or cable modem connected Windows machines under remote control by the spammers. For a while, I read headers and sent complaints about obviously compromised machines to abuse@ the applicable ISP, but some of those bounced, and most of the rest ignored me. Of course a lot of the spam-bounce messages didn't send enough of the headers back to even figure out who I could complain to.

Especially annoying are nastygrams from spam detection services, which should know that spam headers are forged. I have also received rejection notices which announce that the e-mail was refused because it originated at or forwarded through a spammer-compromised server -- so why are they sending ME a rejection notice?

On top of this came the MyDoom outbreak. Almost every Windows-based virus or worm scans browser caches for e-mail addresses, where (mostly) webmaster addresses are to be found. Therefore, when an outbreak occurs, anyone with a popular web site suddenly gets thousands of copies of the latest plague.

I can cope with that. But the malware ALSO uses the same list of found addresses to forge From: lines. Hence, thousands of virus/worm e-mails generated in other places have my address in the header. And when the recipient isn't deliverable, thousands of bounce messages come to me, and are obviously harder to filter out than the actual virus.

Worse yet are virus protection programs which generate autoreplies to the forged address, to inform me that my server (a Unix box) is infected with MyDoom. Um, if your software is smart enough to recognize MyDoom (or any other virus of recent years), why is it too dumb to know that the From: line has nothing to do with the origin of the item?

The critics of SPF suggest that spammers would simply find or invent other addresses to use. Frankly, I don't care about that, so long as they stopped plastering my personal address on hundreds of thousands of fraudulent and disreputable spam messages and viruses, and clogging my server's net connection with vast piles of misdirected bounces.

Lawrence Kestenbaum, P.O. Box 2563, Ann Arbor MI 48106,
polygon@potifos.com
The Political Graveyard, <http://politicalgraveyard.com>

✶ Exploiting software

<"Gary McGraw" <gem@cigital.com>>
Wed, 18 Feb 2004 14:32:49 -0500

What are the RISKS of publishing a book on how to break software? What are the RISKS of pretending software exploits are really dumb and building lame technology to "stop" them? How do these RISKS trade off? Judge for yourself by reading **Exploiting Software** by Greg Hoglund and Gary McGraw

(Addison-Wesley 2004).

Early review:

http://www.ieee-security.org/Cipher/BookReviews/2004/Hoglund_by_bruen.html

Gary McGraw CTO, Cigital <http://www.cigital.com>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 20

Weds 25 February 2004

Contents

- [King/Drew patient monitors shut off following 2 deaths](#)
[Sheri Alpert](#)
- [Bug in Windows-operated toilet system](#)
[Wendy M. Grossman](#)
- [Physical security of electronic voting terminals](#)
[Tobin Fricke](#)
- [Chipmakers race to plug the buffer overflow problem](#)
[NewsScan](#)
- [Buffer overflows and Multics?](#)
[Tom Van Vleck](#)
- [An old filtering problem, but worth repeating](#)
[Drew Dean](#)
- [Anti-captcha technique](#)
[Lindsay Marshall](#)
- [Further misdirected on-line trip planning](#)
[Mark Brader](#)
- [Conspiracy Theory: mortgage scams](#)
[NewsScan](#)
- [Osama Bin Laden is not on the no-fly list?](#)
[Peter Wayner](#)

- [MS Java Virtual Machine issue](#)
[Ferdinand John Reinke](#)
 - [Garage-door openings by aircraft](#)
[John Slimick](#) [Kevin G. Rhoads](#)
 - [Re: Garage-door openers](#)
[Peter B. Ladkin](#)
 - [Re: Garage-door openers by Sputnik](#)
[Steve Bellovin](#)
 - [Re: Drunk unlocks police car with own key](#)
[Adam Laurie](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ King/Drew patient monitors shut off following 2 deaths

<Sheri Alpert <salpert@nd.edu>>
Thu, 11 Sep 2003 21:39:00 -0500 (EST)

On 10 Sep 2003, Tracy Weber and Charles Ornstein reported in the *Los Angeles Times* that the Martin Luther King Jr./Drew Medical Center was disconnecting a new \$411,000 patient-monitoring system, after the deaths of two patients for whom alarms failed to alert nurses that urgent attention was needed in the summer of 2003. [PGN-ed]
<http://www.latimes.com/news/local/la-me-kingdrew10sep10,1,3521718.story>

⚡ Bug in Windows-operated toilet system

<"Wendy M. Grossman" <wendyg@pelicancrossing.net>>
Sat, 21 Feb 2004 11:01:12 +0000

I was at a press conference on Thursday with PalmSource at One Aldwych, which is one of those hyper-modern London hotels. One of its features is a airplane-style vacuum-operated toilet system. One of the Palm execs told me that while they were staying at the hotel this system failed, and any time they wanted to use the bathroom or take a shower they had to call the reception desk and get escorted to the corporate headquarters in the building next door to use the facilities there. For a couple of *days*.

It transpires that the entire plumbing system is run by a Windows-based computer system and whatever went wrong with it was so obscure that they had to get a technician from the company that supplied it on a plane down from Scotland to fix it and reboot.

The Blue Screen of Sewage?

[There's a "Sucker" Borne Every Evacuation! PGN]

✶ Physical security of electronic voting terminals

<Tobin Fricke <tobin@csua.berkeley.edu>>

Wed, 25 Feb 2004 14:32:17 -0800

A cart of Diebold electronic voting machines was delivered today to the common room of this Berkeley, CA boarding house, which will be a polling place on Tuesday's primary election. The machines are on a cart which is

wrapped in plastic wrap (the same as the stuff we use in the kitchen). A few cable locks (bicycle locks, it seems) provide the appearance of physical security, but they aren't threaded through each machine. Moreover, someone fiddling with the cable locks, I am told, announced after less than a minute of fiddling that he had found the three-digit combination to be the same small integer repeated three times.

One wonders whether paper ballots would be handled differently, how the terminals are stored between elections, what checks are done for tampering before the use of the terminals, and what physical security features are built into them.

✶ Chipmakers race to plug the buffer overflow problem

<"NewsScan" <newsscan@newsscan.com>>

Mon, 23 Feb 2004 08:56:20 -0700

The next generation of microprocessors will plug the gaps that have resulted in "buffer overflow" vulnerabilities, causing Microsoft to issue repeated "critical security alerts." The buffer section of computer memory stores a finite amount of data. To exploit the flaw, hackers cause more data to be sent to the buffer than it can hold, forcing it to overflow into the next chunk of buffer memory, where they then deposit their malicious code. This leaves the computer open to attack, as demonstrated by the

devastating

Slammer and Blaster worm invasions in 2003. "Buffer overflows are the largest class of software vulnerabilities that lead to security flaws," says the head of one security company. The new chips will be designed to block this avenue of attack, although security experts predict that determined hackers will find other ways to insert computer viruses -- for example, by making a program jump to a subsection of its own code at the wrong time, perhaps to open a data port to a hacker. [*New Scientist*, 22 Feb 2004;

NewsScan Daily, 23 Feb 2004]

<http://www.newscientist.com/news/news.jsp?id=ns99994696>

[Historical reminder: In 1965, the Multics hardware (GE then Honeywell

645) provided segmented, paged, ring-structured hardware enabled the

software to achieved measures of security that are not common today. The

combination of hardware, the PL/I language subset, the language runtime

environment, the stack discipline (non-executable, which cut way down on

overflows; also, the stack grew to higher addresses, making the overflow

of a buffer unlikely to clobber the return address in the stack frame),

and good software engineering discipline helped prevent most buffer

overflows in Multics. See Tom Van Vleck's subsequent message, as well as

his Web site, multicians.org. PGN]

✶ Buffer overflows and Multics?

<Tom Van Vleck <thvv@multicians.org>>

Mon, 23 Feb 2004 16:23:45 -0500

To make a big deal out of providing the 40-year-old feature of marking a region of memory non executable is kind of sad. Multicians look at each other and make the rubbing-sticks-together gesture.

It seems to me that the marketing guys and the popular press writers don't understand the feature, the need for the feature, or what the feature will and won't accomplish.

It's not magic. It fixes some common problems, leaving other problems untouched. It's not a substitute for defensive coding and proper management of storage; all it means is that if there is a mistake, it is more work for an attacker to exploit it.

As Paul Karger points out, when attackers are frustrated by one measure, they don't abandon their attacks. They keep looking for other holes. A fix like this, applied by itself, will lead to a new equilibrium between attackers and defenders, maybe favoring one or the other, but the game will remain the same.

Closing one open barn door is good, but it needs to be complemented by a systematic approach to enumeration of openings, and a method of closing the openings by architectural design that applies to all openings. So I was taught by my leaders on the Multics project, including Corby, Bob Morris, Jerry Saltzer, Ted Glaser, PGN, and many more.

✂ An old filtering problem, but worth repeating

<Drew Dean <ddean@csl.sri.com>>

Tue, 24 Feb 2004 12:13:49 -0800 (PST)

Mike Cassidy has a column in the *San Jose Mercury News* on 24 Feb 2004 entitled "Sending e-mail can be a struggle if your name has a 4-letter word." A Scottish gentleman named Craig C*ckburn (generally pronounced Coburn) had all too difficult a time receiving his e-mail. It turns out that Mr. C*ckburn's job title is "senior IT application speci*list", which also has problems due to the word "speci*list" containing the substring "ci*lis" (when used as a proper noun, a Vi*gra competitor).

Not new, but increasingly painful for many people.

<http://www.mercurynews.com/mld/mercurynews/business/8026783.htm>

Drew Dean, SRI International

PS: How many spam filters will barf on this message? Or will PGN edit it?

[Indeed. I took mercy on Drew's message and have tried to avoid the expected filters. Note other words such as "multiraci*alism", "soci*lism", "commerci*lism", and even "commerci*lise" (British), also get trashed, not to mention words in other languages. (The asterisks above are easily interpreted as the letter "o" or "a".)]

*@#\$\$%! <expletive deleted> PGN]

✂ Anti-captcha technique

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

Fri, 20 Feb 2004 13:26:37 -0000

I don't remember seeing a posting about the suggested anti-captcha technique that was discussed recently on slashdot. A "captcha" is the (horrible) name used to describe the distorted graphics referred to by Thomas Harrington in [RISKS-23.29](#). The (completely brilliant) idea is that every time spammers have to deal with such an image they bring it up on the screen of someone who is looking for free porn and pretend that they are doing a check. The user will respond and the answer gets forwarded back up the line. The /. discussion is at <http://yro.slashdot.org/article.pl?sid=04/01/28/1344207&mode=flat>, the original Boing-Boing posting is at http://boingboing.net/2004_01_01_archive.html#107525288693964966

Very hard to beat human ingenuity.

✂ Further misdirected on-line trip planning

<msb@vex.net (Mark Brader)>

Mon, 23 Feb 2004 13:49:09 -0500 (EST)

[Adapted from alt.fan.cecil-adams (by PGN, who adds that Mark contributed two similar items to [RISKS-20.62](#), with a follow-up by Chris Smith in [RISKS-20.63](#))]

Phil Jern" <pjern1@comcast.net>:

Somewhere around here I have driving directions that I printed out a few

years ago that showed 4,900-odd miles for a trip from New Jersey to Atlanta

that included 2 borders crossings in and out of Canada.

Bill Kinkaid <billkinkaid@telus.net>

The transit system here has a trip planner feature on their Web site

(translink.bc.ca). You key in where you want to start, where you want

to wind up and when, and it tells you which buses to take and when to

get them. A few times in off-hour periods (say Sunday morning) it's

given me some very bizarre routings where I can look at the map and

say "I get on this bus here and get off it there, just tell me when".

Telling me to go from Marpole to Coquitlam via South Delta and Surrey

Centre, f'rinstance.

Mike Brandt <MyLastName@syr.edu>

In the early days of Amtrak's online trip planner, I asked it about trains

from Portland (Oregon) to Seattle. There are several trains each day that

make this 3.5 hour trip. The first choice on the route planner's list was

Portland -> Chicago -> LA -> Seattle, taking about a week, and passing

through Portland again 3.5 hours before arriving in Seattle.

✶ Conspiracy Theory: mortgage scams

<"NewsScan" <newsscan@newsscan.com>>

Thu, 19 Feb 2004 09:19:51 -0700

Lawsuits filed yesterday by AOL and Earthlink accuse individuals and companies of running spam networks. The AOL suit alleges a conspiracy between three Floridians and two Americans living in Thailand to route mortgage-scam solicitations to AOL customers and to defeat AOL's spam filters through a company called Connor-Miller Software Inc. Earthlink is accusing 16 individuals and companies in Florida, California, Tennessee and Michigan of operating a multi-state spam operation that has sent more than a quarter of a billion e-mail messages promoting herbal supplements, Vi*gra and adult dating services and of using stolen identity documents to open Earthlink Internet accounts that were used to transmit the spam. The attorney who represents the Florida defendants in the AOL lawsuit argues that his clients are innocent of spamming: "They set up a network, just like AOL is a network." [*The Washington Post*, 18 Feb 2004; NewsScan Daily, 19 Feb 2004]
<http://www.washingtonpost.com/wp-dyn/articles/A52951-2004Feb18.html>

✶ Osama Bin Laden is not on the no-fly list?

<Peter Wayner <pcw@flyzone.com>>

Fri, 20 Feb 2004 07:44:05 -0500

"According to airline-security documents obtained by this magazine, the name Osama bin Laden was punched into the computer by an airline official and, remarkably, that name was cleared at the security checkpoint all passengers must pass through before being issued a boarding pass. "

http://www.wnd.com/news/article.asp?ARTICLE_ID=37167

Seems like a very general RISK. Some Turing machines just don't halt if they don't find the right name.

✶ MS Java Virtual Machine issue

<"Reinke @ A" <Reinke@att.net>>

Mon, 23 Feb 2004 11:21:22 -0500

Are you familiar with the MS Java Virtual Machine (MSJVM) issue? After September 30th 2004, Microsoft will no longer be able to support this technology. As a result, customers who have the MSJVM installed after this date will be vulnerable to potential attacks that will attempt to exploit this technology. This problem is compounded by the fact that Microsoft will no longer be able to provide software updates or patches to the MSJVM. This issue is not just a concern for organizations that use Java, but will also impact anyone who has the MSJVM installed. More alarming, many organizations

aren't even aware that they have MSJVM installed. [...]

Ferdinand John Reinke, Consultant, 3 Tyne Court, Kendall Park,
NJ 08824

✶ Garage-door openings by aircraft (Re: [RISKS-23.19](#))

<John.Slimick<slimick@pitt.edu>>

Wed, 18 Feb 2004 22:14:26 -0500 (EST)

Sometime in the late Sixties when my wife and I were living on Arbor Road in Menlo Park (not far from SRI), I was standing outside close to my landlord's garage when a lumbering four-engine jet liner passed overhead, possibly a little lower than usual. As it passed overhead, the garage door began to open (it had one of the earlier remote openers). After the plane passed, I went over and closed the door.

When I asked about it to other, more knowledgeable people, I was told that the aircraft transponder was the culprit, and the phenomenon was not unknown in the Bay area.

✶ Garage-door openings by aircraft (Re: [RISKS-23.19](#))

<"Kevin G. Rhoads"<Kevin.Rhoads@Dartmouth.EDU>>

Mon, 23 Feb 2004 11:04:18 -0500

We had a house with a 1970-ish vintage garage door opener. Many of these used frequencies that were "shared" with certain aviation uses.

Whenever our house was in the approach path to Boston/Logan the door would get triggered easily two to three times a day. When the jets were not being approach-routed over us, it rarely happened -- only once that I remember. I simply disabled the remote receiver.

Using a single frequency with no keying as a trigger is like using a one-pin lock, or a 1 character password.

I don't think that needs any further explanation in the RISKS forum.

Re: Garage-door openers ([RISKS-23.19](#))

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Thu, 19 Feb 2004 08:41:01 +0100

Cases of garage doors opening uncommanded through radio-frequency interference are not urban legends, although I don't know specifically about Sputnik.

In 1981, I briefly owned a house on Arlington Avenue in Kensington, CA, with an automatic door. I slept often in the room over the garage. When there was a storm in the Bay Area, SFO sometimes used Rwy 19 for landings, instead of the usual 27L/R. The initial approach was radar vectors, and many aircraft used to fly over the Berkeley Hills. I recall that a number of

times when aircraft flew over in the early morning, I heard the garage door open. (It piqued both my curiosity and my sense of security, so I remember going to some effort to figure out possible correlations. The aircraft were the only one that I recall. Police radios could have been another - the police station was just up the road and cars used Arlington Avenue all the time. But I recall ruling that out.) That was the only time of which I am aware at which the door opened uncommanded. I don't know when the garage door was installed. The house was some 20-30 years old then, as I recall.

I didn't know much about avionics at the time, so I didn't confirm it through technical details.

I seem to recall mentioning something about this in Risks at some point.

An urban legend with which I am directly familiar concerns mobile phones on gas station forecourts igniting fuel fires. I wrote about it in "An Example of Everyday Technical Risk Analysis". I analysed the principles on which at least one authority seemed to base its regulatory stance, and pointed out that they were very different from a technical risk analysis. For example, the UK regulators based their official position on the fact that mobile phones are RF devices, and there were regulations governing use of RF devices in the presence of flammable substance, although a correspondent at HSE suggested that the possibility of external short circuits, caused say

when someone drops a phone while using it, would be a natural concern (I pointed out that this was precluded by the physical design of phones that I had looked at).

There is a postscript. My sister reported to me in 2002 that local gas stations put up notices saying that due to then-recent incidents of phone use setting off fires, mobile phone use was "not permitted". She asked the station attendant, and got no precise information. I inquired at the UK Health and Safety Executive, and Simon Brown told me that the more recent reports had been investigated and HSE had concluded that there was no substance to them.

Then, end of 2003, there were reports of "exploding" mobile phones. The New Scientist was interested (although I do not know what if anything they published). Nokia had issued a statement about it, in which they said that some third-party replacement batteries had been shown to be defective. I saw a German public television program about it. It interviewed a man to whom it had happened (as his car was passing under the mail Amsterdam-Köln train line at Dinslaken), showed pictures of his phone, showed his hospital admittance record (his arm/hand was mildly burnt), interviewed labs who had investigated such incidents, and showed lab technicians provoking such an explosion. Pretty substantial stuff, no legend. It can happen.

Apparently, some third-party replacement battery providers do not have adequate quality control and the short circuit protection

mechanisms

on the batteries they sell may be as ineffective as the batteries are defective. A battery which internally short-circuits can explode in exactly this way. The program explicitly recommended not using inexpensive batteries from manufacturers/suppliers that were not well-known (I recall it stopped short of advising people only to use original equipment, although some interviewees recommended that.)

Of course, this may happen irrespective of whether the phone is in use, or even of whether it is switched on, although I imagine both situations raise the chances that a defective battery will internally short-circuit. So it may well be that there are now good grounds for the adage "don't use your phone on gas station forecourts", but based on the possibility of internal shorts, rather than on their status as RF devices, or on the possibility of external shorts. And better to keep it away from the fumes altogether; not in your pocket or handbag, but in the car with the windows shut. If you have a non-original battery, that is.

A colleague pointed out that car batteries are in principle susceptible to the same process, and there are plenty of inexpensive car batteries around, but no one is recommending or requiring that drivers remove or disconnect their car batteries before driving on to a forecourt. Of course, if they did, they couldn't.....

Peter B. Ladkin, Professor of Computer Networks and Distributed Systems,
Faculty of Technology, University of Bielefeld, 33594 Bielefeld,

Germany

✶ Re: Garage-door openers by Sputnik ([RISKS-23.19](#))

<Steve Bellovin <smb@research.att.com>>

Thu, 19 Feb 2004 10:06:24 -0500

I flat-out don't believe the sputnik connection -- the signal strength from orbit would have been extremely low.

I haven't been able to find hard numbers, but here are some back of the (SMTP?) envelope calculations.

Sputnik's perigee was 215 km (sources given below). Assume that a garage door opener's range is 21.5 m; if the satellite has comparable transmission efficiency and power and an (assumed) inverse square signal drop-off, we're dealing with a 10^{-8} difference in power.

Of course, Sputnik's transmitter was more powerful. I haven't been able to find any data on that, but we can bound it. Sputnik massed 83 kg. Assume that its entire mass was batteries -- clearly, that's an overestimate -- and assume that a vintage 1957 garage door transmitter had 83 grams of battery (probably too low). That gives a 10^3 improvement in maximum transmitter power. We can be very generous and assume a 10^2 factor for better batteries, better transmitters, etc., but we're still left with a signal strength deficit of 10^3 . Sure, Sputnik had better antennas

than the garage door opener, but the receiving antennas are constant. I don't see how this adds up.

I should add that battery weight and power capacity was a major concern for the designers; furthermore, the antennas were omnidirectional.

I may be off-base here, and I'll let people with more knowledge of radio calculate further -- but to me, this just doesn't add up.

Sources:

<http://www.hq.nasa.gov/office/pao/History/sputnik/14.html>

<http://www.hq.nasa.gov/office/pao/History/sputnik/russ3.html>

<http://nssdc.gsfc.nasa.gov/database/MasterCatalog?sc=1957-001B>

<http://nssdc.gsfc.nasa.gov/nmc/tmp/1957-001B-trajectory.html>

Steve Bellovin, <http://www.research.att.com/~smb>

Re: Drunk unlocks police car with own key

<Adam Laurie <adam@algroup.co.uk>>

Fri, 06 Feb 2004 14:41:23 +0000

I have had a couple of experiences with radio car remotes and have also recently been doing some research with older style IR remotes...

Firstly, the radio remotes... on a recent business trip i got a call from my wife in which she described a situation when she got locked out of her car as the radio remote had stopped working. she could unlock the door with the physical key, but the remote had also disabled the ignition

system so she
could not start the car. she was at a shopping centre, it was
early evening,
getting dark, and she had 4 children (not all mine, i should
point out! :)
she had just picked up from school and was desperate to get
home... when she
called the garage they said it would take two hours to get out to
her. clearly this was unacceptable in the circumstances, so they
came up
with another solution... the solution was to tell her the
procedure for
resetting the key. having reset the key, she then followed
another procedure
to resynchronise the car. she did this and it all worked fine.
when she
described the procedure to me, it was clear that the process was
completely
insecure as it did not require physical access to the car (i.e.
no ignition
key or door key sequence was required). as it happened, a few
days later, a
friend was giving me a lift to the railway station and on the
way he had to
drop off a rental car. as we left it on the forecourt (it was
late and the
place was closed), i noticed he was using an identical remote to
the one for
my wife's car. i had mine with me so we decided to experiment...
and yes,
you are probably way ahead of me here... after performing the
sequence, a
dozen or so cars on the forecourt happily chunked their locks
open and
flashed their indicators to show that they had been reset! it
would appear
that sending a 'base' code from a freshly reset key caused the
receivers on
the cars to also reset and synchronise to my key. i didn't try
starting any
of them, as ThatWouldBeBad(tm), but being able to open the doors
is risky
enough.

This caused me to wonder just how simple those codes were, and how hard they would be to brute force. not being an electronics/radio whizz, i was slightly stumped on how to intercept and analyse the signals, so i decided to first have a go at something simpler, for which such tools already existed, and which i suspect uses similar underlying protocols - i.e. infra red. the tool i used was LIRC (<http://www.lirc.org/>), which includes a nice graphical utility to show you the 'shape' of the signal. zapping it with my garage door opener showed that they were using an 8 bit code (plus stop bits etc.), and the particular code for my garage door was 0xE3. lirc also has a learn facility, which produces config files in human readable form. the config for my learned remote looked like this:

```
begin codes
```

```
    E3      0x0000000000000000e3
```

it was then a simple task to write a script which spat out the other 255 possible codes:

```
    00      0x000000000000000000
    01      0x000000000000000001
    02      0x000000000000000002
    etc.
```

and another simple script to send every possible code. running the script successfully popped the garage door not only when it hit the expected 'e3' code, but also on another one (apparently the garage operators had installed a second parallel system as they could no longer get spare

remotes for the
old one). total time to try every code was under a minute.

i have since used the same technique to discover 'hidden' menus
on TVs
(particularly useful in hotels with pay per view :), and suspect
that there
are lots of other similar applications out there waiting to be
discovered...

the risk here is that because the code is 'invisible' there is a
tendency to
make it simple. i have seen the same mistake in network
connected security
devices such as proximity card readers for door controls - the
card itself
is secure, but the command that ultimately gets sent over the
wire to the
locking mechanism is a simple ascii string, such as "0" for open.

btw, if anyone has any ideas how i could convert the radio remote
signals to something i could analyse/replicate, please get in
touch... i
have scanners/transceivers etc., but am completely clueless when
it
comes to non digital stuff... :P

Adam Laurie, A.L. Digital Ltd., The Stores, 2 Bath Road, London
W4 1LT UK
+44 (20) 8742 0755 <http://www.thebunker.net> <http://www.aldigital.co.uk>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 21

Thursday 26 February 2004

Contents

- [Bar codes for your health](#)
[NewsScan](#)
- [*Computer Weekly*'s campaign against government incompetence](#)
[Pete Mellor](#)
- [Malicious IT design in support of the cold war](#)
[Sam Garst](#)
- [Flaws threaten VoIP networks](#)
[Lillie Coney](#)
- [Fixed-length fields strike again](#)
[Robert Israel](#)
- [Toll Collect doesn't](#)
[Peter B. Ladkin](#)
- [SPF and SRS](#)
[Ben Rosengart](#)
- [Re: Risks of SPF](#)
[Peter da Silva](#)
- [Re: SPF and its critics](#)
[Dimitri Maziuk](#)
- [Theft of Client Information at Israeli Bank's "Information Fortress"](#)
[Gadi Evron](#)
- [Re: Interesting device to steal ATM accounts](#)
[Gadi Evron](#)
- [Info on RISKS \(comp.risks\)](#)

✶ **Bar codes for your health**

<"NewsScan" <newsscan@newsscan.com>>

Thu, 26 Feb 2004 08:07:18 -0700

Federal officials say that the use of bar codes to identify prescriptions has the potential to cut in half the 7,000 hospital deaths [!] attributed to medication error every year. The Department of Health and Human Services has announced a regulation requiring that drugmakers and blood suppliers add the codes to most of their products within the next two years. HHS Secretary Tommy G. Thompson says, "The pharmaceutical industry wants it, hospitals want it, doctors want it -- all we needed was the catalyst to put all it together." [*The Washington Post*, 26 Feb 2004; NewsScan Daily, 26 Feb 2004]
<http://www.washingtonpost.com/wp-dyn/articles/A6995-2004Feb25.html>

⚡ *Computer Weekly*'s campaign against government incompetence

<Pete Mellor <pm@csr.city.ac.uk>>

Sat, 21 Feb 2004 19:14:48 +0000 (GMT)

You might be interested to read about *Computer Weekly*'s campaign about the recent disastrous attempts by various UK Government. departments to procure large IT systems. CW have submitted evidence to the National Audit Office (UK equivalent of the GAO). See:

<http://www.computerweekly.com/articles/article.asp?liArticleID=128417&liArticleTypeID=1&liCategoryID=2&liChannelID=28&liFlavourID=1&sSearch=&nPage=1>

<http://www.computerweekly.com/articles/article.asp?liArticleID=128417&liArticleTypeID=1&liCategoryID=2&liChannelID=28&liFlavourID=1&sSearch=&nPage=1>

The URL is for Tony Collins' front-page article on 17 Feb 2004. For the related articles, just follow the links.

Peter Mellor, Centre for Software Reliability, City University,
Northampton Square, London EC1V 0HB +44 (0)20 7040 8422

⚡ Malicious IT design in support of the cold war

<Sam Garst <samgarst@netaxs.com>>

Thu, 19 Feb 2004 11:26:22 -0500

On 2 Feb 2004, *The New York Times* printed an editorial by William Safire entitled "The Farewell Dossier" describing a CIA campaign in the early 1980s that supplied Russia with deliberately flawed technology; this lead directly to the massive explosion of a Siberian gas pipeline. The CIA became aware that the KGB was purchasing technology on the black market, and endeavored to supply the KGB with technology that would pass inspection, and later fail catastrophically.

Two risks leap out at me (trying hard to separate out several moral issues):

- I may test for poor design, or poor manufacturing, but these products were designed to pass testing, and then fail. Should I start testing for malicious design (perhaps, if you're building sensitive infrastructure, this is common practice)?
- These intentional flaws could 'leak' into the legitimate product lines. Hopefully, these companies had (and still have) good software build processes and code repositories.

The article is no longer available at New York Times, but is available:

<http://seclists.org/lists/isn/2004/Feb/0011.html>

Safire indicates the story is from a soon-to-be published book: Thomas C. Reed's "At the Abyss".

✶ Flaws threaten VoIP networks

<Lillie Coney <lillie.coney@acm.org>>

Wed, 14 Jan 2004 11:45:24 -0500

[Source: Robert Lemos, Flaws threaten VoIP networks, CNET News.com, 13 Jan 2004; PGN-abstracted]

http://news.com.com/2100-1002_3-5140284.html?tag=nefd_lede

A technical review conducted by the British government has found several security flaws in products that use VoIP and text messaging, including those from Microsoft and Cisco Systems. The flaws affect software and hardware that support the real-time multimedia communications and processing standard, known as the International Telecommunications Union (ITU) H.323 standard.

The security problems can cause a product that supports H.323 to crash. For example, in Cisco telecommunications products running its IOS operating system, the vulnerability could be used to cause the devices to freeze or reboot. However, on Microsoft's Internet Security and Acceleration Server 2000, which is included with Small Business Server 2000 and 2003 editions, the vulnerability could allow an attacker to take control of the system.

✶ Fixed-length fields strike again

<Robert Israel <israel@math.ubc.ca>>
Sun, 8 Feb 2004 18:54:42 -0800 (PST)

According to a recent report in the Israeli paper Haaretz
<<http://www.haaretzdaily.com/hasen/spages/392009.html>>
the Israel Defense Forces will have to pay tens of millions of shekels to fix a two-year-old automated system for calling up reservists: the system allocates 9 digits for a reservist's cell-phone number, but in a few months all Israeli cell phones will have 10 digits. According to the article, "The army will also look into expanding the fields for personal and other telephone numbers to prevent future problems."

Robert Israel, Department of Mathematics, University of British Columbia
Vancouver, BC, Canada V6T 1Z2 <http://www.math.ubc.ca/~israel>

✶ Toll Collect doesn't

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Wed, 25 Feb 2004 20:22:41 +0100

Headline news last week in Germany, as well as in papers with an eye on Europe [1,2,3], has been the failure of the Toll Collect consortium to deliver a toll-collection system for heavy goods vehicles that use the German Autobahn network. (Autobahns are the German equivalent of U.S. freeways.)

The system is based on GPS tracking of heavy goods vehicles, using boxes ("On Board Units", OBU) carried in the vehicles. The OBUs contain GPS receivers, and forward their data to a central data installation using European standard GSM mobile telephony.

The consortium consists of Deutsche Telekom, Germany's quasi-privatised ex-public telephone operator, DaimlerChrysler, which own 45% each, and France's autoroute toll system operator Cofiroute (a concern of Vinci SA), which has 10%. The consortium has some 24 major subcontractors, amongst whom are such well-known names as HP, Siemens/VDO, Sun, Vodaphone, T-Mobile, Oracle, Peoplesoft, and SAP [4].

In-service date was supposed to be 31 August 2003. There are estimated to

be 1.4 million trucks which should pay a toll, of which 400,000 are from other lands. It was planned to deliver 450,000 OBUs by the in-service date; other users were to use static machines at entry points. There were problems with the OBUs, and even five weeks after in-service date only 210,000 had been installed. There were also problems with the bookkeeping software at the data center, which turned out not to have appropriate interoperability with other systems used by truck operators [4].

The contractual arrangements for developing the system were, to someone like me, cause for concern. Although details of the call had been known in essence since August 2001, a call for proposals was issued in April 2002 after a law putting the government's "Anti-Traffic-Jam Program" into force had been passed. The contract was awarded to the consortium on 8th July 2002. The government apparently wanted a twelve-month development schedule. One of the two final bidders said this was "unrealisable"; the winner (Toll Collect, or Electronic Toll Collect as it was then known) proposed an eleven-month development schedule, with a four-month trial period during which the usual contractual penalties for non-performance would be waived. Legal challenges held off starting work in earnest until September 2002. The contract was slated to employ about 350 programmers and 80 SW testers. The development costs are said to lie somewhat over EUR 600M (which is the value of the low-price offer from a Swiss toll-system company, that couldn't provide the necessary insurance and was eliminated early) [4,5].

Talks have taken place between the government and the consortium to establish the rate of compensation for default and how things shall move forward. The talks broke down on 17th February, with the government declaring it would cancel the contract and declaring damages of around EUR 6.5 billion (\$8.2 billion) [8,9].

The consortium is already paying EUR 250K/day in fines since December 1, 2003, increasing to EUR 500K/day in March 2004. The government rejected the consortium's offer of EUR 600M per year in compensation [2]. At least one German journal is reporting a week after talks supposedly "broke down" that the fine payment has increased to EUR 1M/day [6], but that represents only some 60% of the rejected compensation offer, so it is hard to tell what is happening.

The consortium says it has "solved software problems causing the delay" [2]. DaimlerChrysler chairman Jürgen Schrempp, one of the most well-known figures in German industry (and maybe in U.S. industry also) says "there is a chance, even with this long delay, to make the system work" [1]. The consortium has offered to deliver a system with reduced functionality by 31 December, 2004, with full functionality implemented a year later [2].

There are lots of figures floating around concerning revenue lost, and costs, and such like. Numbers are seemingly hard-edged things, that bring with them the aura of independence from politics and suchlike. I like to perform arithmetic on such figures to see how they add up. When they don't - and they often don't in this case - one can suspect that they

represent negotiating positions rather better than they represent a true accounting. Here are a few, which I recommend treating with caution.

The project worth was said to be EUR 7.73 billion, with a service lifetime of 12 years [5]. This figure amounts to ~EUR 54M/month. The government estimates foregone revenue at EUR 156M per month [2] (derived from EUR 6M per day over a 26-day truck-driving month). Lost revenue from the former "vignette" (sticker) system, which was taken out of service by 31 August 2003, amounts to EUR 30-38M/month. All new road projects and related public-works projects have been put on hold because of the "revenue shortfall" [3]. Some estimate that up to a quarter of transport ministry projects may be cancelled in 2004, putting 70,000 jobs on the line [3].

One major problem appears to be that the government wrote this EUR 156M/month anticipated revenue into its budget already. That is why those road-building projects are on hold and those 70,000 jobs are "endangered". Yes, that's right. Someone let a contract for a complex, highly-distributed system, of a sort which did not exist anywhere before, with a non-trusted, indeed partially non-trustworthy, user group numbering in the millions, that would cost of the order of a billion euros and ~450 technical-person-years to develop, which was to be in full revenue service inside a calendar year from development start date. And then apparently allowed the whole road-construction industry to become dependent on that anticipated revenue, as well as part of the railways.

Another major problem appears to be that a consortium containing two giants of German industry signed up to that astonishing contractual schedule.

As Andreas Hagen wrote, concerning this so-called Public-Private Partnership (also in German), the contractual politics "didn't do citizens any favors. [It was] badly negotiated, and besides that, the bear's hide was shared out before the bear was shot" [6, my translation].

The contract, by the way, has remained secret, although there is nominally a requirement that it be public. Even the German parliament has not seen it [5]. So few, if any, independent people with the capacity to evaluate them know what the system requirements were or how well they were met. Or, for those interested in the future rather than the past, how close the technology is to meeting them.

The contract is so remarkable that few tech-savvies believe that the consortium can have negotiated it in good faith. Some even have a hard time believing that the government negotiated it in good faith, although more are inclined to believe it just didn't know what it was doing.

The stories of the negotiations over default bring to mind the game of chicken, in which two drivers drive their cars head-on towards each other at full speed, and the first to swerve loses (everyone cites [7], but I have just failed to find the example). One sees evidence of the strategy of removing one's steering wheel and visibly throwing it out the car

window. But the current case is not a two-player game, nor even a zero-sum game. It is a game of partial coordination, in the terminology of [7]. There is a dealer who owns both cars, employs one of the drivers, and keeps the other in business. He is very concerned about the outcome, and prefers not to lose either of his cars, but is likely to care much less about the drivers. His name is Joe Public. Both sides have an obligation to Joe to fix what is wrong, whether it be technical, contractual or political. It is unlikely to impress Joe over the long term if one of the drivers throws his steering wheel out of the window and then claims the other driver loosened it.

It is clear that the risks of the contract were poorly calculated by both sides. The government appears to have believed there was no risk to itself, even though it can hardly seriously have expected DaimlerChrysler and Deutsche Telekom to finance the entire German road construction industry in the event of a default. It stands convicted of bad planning. The consortium members appear to have underestimated the damage to their reputations and consequences for future business that a significant default would entail. There is even a suspicion that they negotiated the original contract knowing, but not adequately conveying, the odds that it could not be fulfilled. At the least, it exhibited either hubris or bad faith, even though we do not know which.

As Chairman Schrempp said, "mistakes were made by all sides" [1].

Many technology-savvies have no problem in believing that such a system could be delivered in good working order in three or four years. But for many people including some of my colleagues there now appears to be difficulty in believing anything Toll Collect says on the matter, not necessarily for technical reasons.

Oh, yes, a word or two on the technical issues. Putting the blame on "software problems" tells us little. It could have been that the software development process did not measure up to best practice; it could also have been that difficult engineering issues that could not be solved in the hardware were pushed into the software and the software development team didn't know how to solve them either. It could also have been that there were design or specification problems which first manifested themselves, or needed to be solved, in SW. Most likely, it was all three.

The Economist says that "important features were left out of the software, such as the ability to work with the payment cards and accounting systems used by most trucking firms. Worse, gremlins charged trucks for being near motorways, rather than on them, or drained batteries while engines were switched off" [3]. German sources give a more specific, longer list of particular problems [4].

It also probably didn't help that the European Union issued a requirement during system development that the design enable the data to be made available to a variety of processing companies, presumably to enable competition in the data-processing phase. In the original design the data

would be shared with just one processing company, DaimlerChrysler Services Mobility Management [4].

It seems to me to be premature to sum up. I'll just leave it here, with thanks to Heiko Holtkamp and Jan Hennig, who helped me in finding sources.

PBL

References

[1] German engineering loses luster, Mark Landler, International Herald Tribune, Friday, February 20th, 2004, <http://www.iht.com/articles/130404.html>

[2] Berlin kills contract to build satellite-based toll system, International Herald Tribune, Wednesday February 18th, 2004, <http://www.iht.com/articles/130098.html>

[3] Road rage: European road tolls; Germany's truck tolls crash, The Economist, January 24th-30th, 2004, available for a fee through www.economist.com

[4] Detlef Borchers, Verursachbedingt verspätet, c't No. 22, 2003 (in German), available for a fee through www.heise.de

[5] Joachim Budeck, Dr. Egbert Meyer, Ausgebremste Automatik, c't No. 21, 2002 (in German), available through www.heise.de

[6] Andreas Hagen, Zwischenspiel oder letzter Akt mit Toll Collect? (in German), Telepolis magazine, 25th February 2004, <http://www.heise.de/tp/deutsch/special/eco/16827/1.html>

[7] Thomas C. Schelling, The Strategy of Conflict, 1960 & 1980, Harvard University Press.

[8] Stolpes Brief an Toll Collect [German Transport Minister Manfred Stolpe's letter to Toll Collect] (in German), 17 February 2004, published by N-TV news channel and CNN Germany, available at <http://www.n-tv.de/5215294.html>

[9] Der Kündigungsbrief von Manfred Stolpe an Toll Collect [also a copy of Stolpe's letter] (in German), 17 February 2004, published by the Süddeutsche Zeitung, available at <http://www.sueddeutsche.de/wirtschaft/artikel/880/26854/>

Peter B. Ladkin, University of Bielefeld, <http://www.rvs.uni-bielefeld.de>

SPF and SRS

<Ben Rosengart <risks@narcissus.net>>

Wed, 18 Feb 2004 18:47:17 -0500

Much of the controversy around SPF <<http://spf.pobox.com/>> focuses on the "Sender Rewriting Scheme" <<http://spf.pobox.com/srs.html>>. I don't like SRS either, but I think SPF can be used without it. Maybe I'm wrong, but here's my argument, let's see if anyone can shoot it down.

Rationale for SRS: mail that is forwarded with the envelope sender unchanged may appear to violate SPF policy. If we rewrite the envelope sender address at forwarding time, we can change it to something that will conform to SPF policy.

Anti-rationale for SRS: since we know where our forwarded mail will come from, we can tell SPF to accept mail from those sites "uncritically". Every forwarder -- be it a forwarding address or a mailing list -- has an e-mail address associated with it. We can look up the SPF data for that address and extend extra trust to the authorized clients, by letting them send us mail with any envelope sender.

What's wrong with this picture? One possible criticism: a forwarding site has a permissive policy, perhaps its SPF record ends with ?all. Solutions:

1. Instead of using SPF to determine your forwarded-mail policy, write your own SPF-style policy and apply that to mail which fails ordinary SPF.
2. Pressure the forwarding site to adopt a more restrictive policy.

Another criticism: this gives a lot of trust to the forwarding site(s). The trust could be abused. I have no answer for this except that it's worth it to dump SRS.

[MORE From Ben on Wed, 18 Feb 2004 21:22:46 -0500]

I realized after I sent you the previous note that there are some points I neglected to address; specifically, more problems with my proposal.

- o It requires SPF to be configurable on a per-user basis. This will annoy people who want to simply slap SPF into their Internet-facing MTA and forget about it.
- o It requires explicit end-user configuration, while SRS is theoretically transparent.

I still think it's worth considering -- SRS is really ugly.

✉ Re: Risks of SPF ([RISKS-23.18-19](#))

<Peter da Silva <peter@abbnm.com>>
Wed, 18 Feb 2004 18:53:45 -0600 (CST)

Implementing SPF would do nothing for the people receiving thousands of bounces (myself included). It would simply add another filter that bounced messages back to us because "we" weren't using the right server.

What, that wouldn't happen? You'd think not, but then you'd think that the antivirus companies sending us "bounces" would have caught on some time in the past three or so years that the majority of viruses have been forging sender addresses too...

The only anti-spam scheme that I have found that works even remotely well is requiring some kind of personally chosen token for every incoming message, along with an accept list (whitelist, greenlight list) for special cases like mailing lists. Anything else, including a standardised challenge-response based system, can be bypassed often enough for spammers to keep trying.

The token can be anything, something on the subject line, something added to an e-mail address, an extra header line... just so long as it can't be automated in bulk it's fine. Eventually spammers will catch on and we'll have to come up with a cryptographically secure message signature... but that's for the future.

The "notsp" token RISKS uses is a simple example of this scheme. I set up something barely more elaborate for my family months ago and their spam load has almost vanished. As I recall there's been one or two hopeful "419" spammers who read the bounce and actually bothered to negotiate the 'firewall'... over a period of months, down from hundreds of spams (including of course several 419-ers) every day.

✉ Re: SPF and its critics (Kestenbaum, [RISKS-23.19](#))

<dmaziuk@bmrw.wisc.edu (Dimitri Maziuk)>
Fri, 20 Feb 2004 11:40:46 -0600

E-mail was not designed with spammers in mind, just like the rest of TCP/IP was not designed with 1337 h4x0rz and script-kiddies in mind.

We know that slapping a band-aid onto implementation to fix deficiencies in

design doesn't work and creates more problems, we've seen it over and over again. Every time I see a proposal like SPF I can't help wondering where its authors have been in the last couple of decades so that they managed to miss this important piece of knowledge.

On the other hand, there's no reason to believe anyone will rush to implement new and improved SMTP when/if ever that comes along -- nobody's in a hurry to switch to IPv6, are they?

> The critics of SPF suggest that spammers would simply find or invent other
> addresses to use. Frankly, I don't care about that, so long as they stopped
> plastering my personal address on hundreds of thousands of fraudulent and
> disreputable spam messages and viruses, and clogging my server's net
> connection with vast piles of misdirected bounces.

We can do it without breaking anything. We already have directory servers, we already have digital signatures. All we need is a way to query Domain Name Service for directory server of a domain, and a standard directory query-response for an e-mail address and associated public crypto key.

Get your domain administrator to publish domain's e-mail addresses and associated public keys on a directory server (BTW, contrary to the popular belief, X.509 was intended for this sort of thing, and not for storing login passwords).

Digitally sign your messages. Recipient's mail server then queries directory server to find out if From address is valid, and verifies digital signature to make sure message is signed with key associated with that address. This is as much as SPF will really do, but without breaking SMTP headers, forcing users to send mail via their domain's mail forwarder, etc. -- i.e. without any of SPF's obvious problems. Message integrity check using strong crypto is just an added bonus.

Apart from technical problems with implementing (large scale, in case of e.g. aol.com domain) PKI (see e.g.

<http://www.mit-kmi.com/articles.cfm?DocID=385>),

expect a lot of political resistance to this scheme. It is putting weapons of mass destruction^W^W^W^W crypto software in the hands of Joe A. User -- law-enforcement agencies ain't gonna like that. Commercial certificate authorities won't like it because it effectively makes every sysadmin their own CA. And then there is a whole lot of crypto standards to choose from: ssh, ssl, pgp...

And then, here's the real clincher: legislature _wants_ to legalize e-mail spam. Fax spam is illegal because it puts the costs on the recipient: you have to pay for toner and paper. But so does e-mail spam: you have pay your ISP for bandwidth. So if they wanted to ban spam, they'd simply apply existing law to it. Ergo, they don't want to ban spam, and all "anti-spam" legislations are really there to legalize it. Ergo, all you're going to achieve by implementing SPF, blocklists, blacklists, whatever, is to open yourself to lawsuits from "legal" spammers.

To get back where I started: we know that technical solutions for non-technical problems don't work. We are clearly dealing with non-technical problem here.

Do not expect another Perl wrapper around good old sendmail to fix anything.

✶ Theft of Client Information at Israeli Bank's "Information Fortress"

<Gadi Evron <ge@linuxbox.org>>
Thu, 19 Feb 2004 12:39:08 +0200

According to reports, a break-in occurred at the Israeli Bank Leumi's "Information Fortress". The perpetrators accessed the perimeter physically and proceeded to steal and delete critical client information from the "main server", using a laptop computer they allegedly hooked into the network.

You can find an article I put together, with known facts on the story:
<http://www.math.org.il/leumi-breakin.html>.

Phone: +972-50-428610 (Cell).
http://vapid.reprehensible.net/~ge/Gadi_Evron_Emails.asc

✶ Re: Interesting device to steal ATM accounts ([RISKS-23.19](#))

<Gadi Evron <ge@linuxbox.org>>
Thu, 19 Feb 2004 13:05:01 +0200

- > Bank ATMs Converted to Steal Bank Customer IDs
- > <http://www.utexas.edu/admin/utpd/atm.html>

Israeli news site Ynet has a story on an ATM theft that has an uncanny resemblance to what's described in the article I am replying to.
(In Hebrew: <http://www.ynet.co.il/articles/0,7340,L-2877093,00.html>)

Apparently such a system was installed at a branch of the Israeli Bank HaPo`alim in the city of Ramat Gan, resulting in the theft of 200,000 INS (approximately 44,500 USD).

The bank mentioned in its press release that suspicious activity was detected in three other branches of the bank, but no signs of such an ATM theft system was found. Furthermore, since any bank customer can draw money

from any bank's ATM, a portion of the customers belonged to other Israeli banks.

The Ynet article also mentions that the crime was apparently committed by a Romanian gang.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 22

Monday 1 March 2004

Contents

- [Stolen heart monitor](#)
[Nigel Metheringham](#)
- [Keeping online games honest](#)
[NewsScan](#)
- [4.6-million DSL subscribers' data leaked in Japan?](#)
[via Dave Farber](#)
- [E-mail robbery, the easy way](#)
[Ralf Ertzinger](#)
- [Solving e-mail problems economically](#)
[Peter B. Ladkin](#)
- [Laptop security](#)
[Gadi Evron](#)
- ["Where did it print?" 1990 version](#)
[Daniel P. B. Smith](#)
- [Buffer overflows and Burroughs/Unisys](#)
[Keith Gobeski](#) [Michael LeVine](#)
- [MS Java Virtual machine](#)
[Curtis Karnow](#)
- [Garage-Door openers; Rapid disassembly of PCS phones](#)
[Charles Jackson](#)

- [Re: Garage-door openers](#)
[Michael Kent](#)
 - [Re: Garage-door openings by aircraft](#)
[Scott Peterson](#)
 - [Further misdirected on-line trip planning](#)
[Bob Heuman](#)
 - [Amtrak Website routing](#)
[Richard S. Russell](#)
 - [REVIEW: "Developing Secure Distributed Systems with CORBA", Lang/Schreiner](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Stolen heart monitor

<Nigel Metherringham <Nigel.Metherringham@dev.InTechnology.co.uk>>

Fri, 27 Feb 2004 11:57:09 +0000

Seen at <http://news.bbc.co.uk/1/hi/wales/3492778.stm>

A mother is urgently appealing for help after her eight-year-old son's

heart monitor scanner was stolen from her car outside the family home.

Daniel Hunter from Bridgend in south Wales, is fitted with a pacemaker

which is monitored by the scanner -- the size of a mobile phone -- without

which his health is at risk. It is the only one he can use, and if it is

not found he will have to undergo potentially dangerous operation to be

fitted with a new pacemaker -- a device which sends electrical impulses to

the heart to keep it beating regularly.

The idea of an implantable medical device apparently requiring physical

reconfiguration (at least) to talk to an external monitor implies a level of trust in the reliability of the external device which is seriously scary.
The RISKS hardly need pointing out here...

✶ Keeping online games honest

<"NewsScan" <newsscan@newsscan.com>>

Mon, 01 Mar 2004 08:14:17 -0700

IT GlobalSecure sells software that prevents network vandals and dishonest players from manipulating online gambling. The company's chief executive says: "If you look online, there are whole Web sites either complaining about cheating or sharing ways to cheat. We've had people who are even just playing gin rummy online saying, 'We think we're being cheated, but we don't know what to do.'" The firm's software is based on encryption technology that can be applied to any network gaming system to validate the randomness of events in games of chance, verify player identities and create audits of each game. [*The Washington Post*, 1 Mar 2004; NewsScan Daily, 1 Mar 2004]

<http://www.washingtonpost.com/wp-dyn/articles/A17983-2004Feb29.html>

[What about keeping the gambling software "honest"? PGN]

✶ 4.6-million DSL subscribers' data leaked in Japan? (From IP)

<[Identity unknown]>

Thu, 26 Feb 2004 18:09:55 -0500

[From Dave Farber's IP list, where the identity of the contributor was withheld. PGN]

The Tokyo Metropolitan Police arrested three men on suspicion of trying to extort up to 3 billion yen (U.S. \$28 million) from Softbank. The suspects claimed that they obtained DVD and CD disks filled with 4.6 million Yahoo BB customer information. The two of the suspects run Yahoo BB agencies which sells DSL and IP Telephone services.

Last month, Softbank was contacted by the suspects who demanded investment to their venture in exchange for the disks. Although the company confirmed that a part of the customer data shown by the blackmailers was that of real Yahoo BB customers, the company so far has not admitted their whole customer data was stolen. The police and Softbank will examine the data on the seized disks. It will take several days before we know the exact scale of the leak. According to Softbank, the stolen data includes name, address, telephone number, and e-mail. No billing or credit card information was leaked.

Also, it has been reported that the police in Nagoya arrested another man who attempted to extort 10 million yen (U.S. \$ 90,000) from Softbank. The man sent the company e-mail messages including the one with 104 customer

data and claimed to have over 1 million customer information on floppies. He worked as a temporary customer support personnel for Yahoo BB in the past and it was likely that he stole the customer data while he worked for the DSL provider. The police considers the Nagoya attempt is not related to the Tokyo case and the sources of the data leak are different.

At this point, there is only speculation on how the customer data was stolen. The data was not accessible from the public networks and Softbank denied any intrusions to their computer networks from the outside. It was likely to be an inside job. There might have been an accomplice (s) in the company or its subsidiaries/affiliates. An Softbank executive stated that there were over 100 people who could log-on to the PCs connected to the customer database. The company is in the process of cheking the log to find any suspicious access to the data. (Although Softbank is a victim of hideous crime, I expect that there will be a lot of scrutiny on the company's policy and practice regarding data security and privacy protection.)

Although the both extortion attempts were foiled, the backgrounds of the Tokyo suspects are disturbing. One of the Tokyo suspect is the leader of a right-wing political organization. In Japan, the shady right-wing groups are often a part of the organized crime(Yakuza gangsters) or have a close tie with Yakuza. It is unthinkable that the 4.6 million personal data fell into the hands of the underworld. The bogus Internet bills from the use of dating and porn sites have become social problem in Japan.(Even they

have no idea
of using those services, some people send money when they
receive a letter
or e-mail from the collection agencies sounding like Yakuza-
related. I am
hoping the suspects are just bluffing.)

The other two are the followers of a powerful religious group
affiliated
with a major political party. According to some tabloids, one of
them was a
former ranking member and was participated in the wiretapping of
the home of
the communist party leader in some 30 years ago (The communist
party and the
religious party were strongly criticising each other then.).
Although he was
acquitted in criminal courts, a civil trial acknowledged his
involvement
(like O.J.?).

The opposition parties are demanding the government to
investigate the
unprecedented scope of the personal data theft and a committee
in the House
of Representatives is considering to call Masayoshi Son, the
Softbank
president to testify.

IP Archives at: [http://www.interesting-people.org/archives/
interesting-people/](http://www.interesting-people.org/archives/interesting-people/)

✶ E-mail robbery, the easy way

<Ralf Ertzinger <ralf@camperquake.de>>

Mon, 1 Mar 2004 23:23:45 +0100

The German online news magazine Spiegel Online [1] recently

reported on an interesting combination of risks [2]: using T-Online as your Internet provider, and having a WLAN access point.

T-Online is Germany's largest Internet provider, and while this in itself is not a risk, T-Online has always used a unique approach towards POP3 mail delivery. When being connected via T-Online, one does not have to provide a username or password to connect to the T-Online POP3 server in order to fetch mail, since the user is identified by his IP address.

Combine this with the growing number of (unsecured) WLAN access points and DSL routers and you get to read other people's mail just by driving along the streets. T-Online is aware of the problem, and provides information to secure WLAN access points on their web site, but changing the POP3 identification system (which was introduced long before anyone thought of broadband Internet, connection sharing and wireless LAN) seems to be almost impossible, having millions of customers.

[1] <http://www.spiegel.de>

[2] <http://www.spiegel.de/netzwelt/technologie/0,1518,288033,00.html>

[PGN showed this a colleague, who commented thusly:

"Just how long have we been telling people that it's a bad idea to do authentication based on IP address? The Berkeley r-commands, after all, where supposed to be an interim solution, IIRC. That was 1982.

Anyways, I'm quite sure that this was known to be a Bad Idea (tm) before T-Online went into business."

And when a very well-known bank first put up its Internet banking on the

Web, it authenticated on IP addresses. Bad ideas are often popular.

PGN]

✉ Solving e-mail problems economically (Re: Kestenbaum, [RISKS-23.19](#))

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

Thu, 19 Feb 2004 10:47:37 +0100

Lawrence Kestenbaum substantiates in his [RISKS-23.19](#) note the considerable problem generated by inappropriate e-mail server responses to virus/worm/spam e-mail, which I noted with regard to Sobig (Some observations on e-mail phenomenology, [RISKS-22.88](#)). However, his last paragraph misplaces blame.

The spammers and worm/virus writers are no more responsible for the amounts of junk generated by misconfigured e-mail servers than I am responsible for the damage caused by an automobile whose driver does not observe my bicycle until the last second and manoeuvres suddenly.

I agree with Kestenbaum that the e-mail system is more or less broken.

The Economist has addressed the issue in its edition of 14 Feb 2004

(Business Section. The article is available on its WWW site for a fee to

non-subscribers). In an article entitled "Make 'em pay" (supertitled "The

fight against spam", subtitled "The dismal science takes on

spam"), the journal suggests that techies have had a go at the problem, then politicians, and now economists are "taking over". Risks readers may recall that Bill Gates said in an interview at the recent World Economic Forum at Davos that certain measures Microsoft favors will get rid of spam in two years. One of those proposals was a per-mail fee, like postage. The article says that "Sceptics noted that Microsoft could also help by fixing security flaws in its products -- the latest confessed to this week -- that can be exploited by spammers".

The article discusses various schemes, namely those by Goodmail Systems, IronPort Systems, and Balachander Krishnamurthy at AT&T Labs.

I hope that the techies and politicians are not yet finished. The payment proposals distinguish between two classes of user: bulk mailers and others. (The post office does also: bulk mail there is cheaper than ordinary mail.) Bulk mailers should, somehow, pay. But not all bulk mailers are spammers. I suggest that a much more fundamental distinction lies between fraudulent e-mail (e.g., that with intentionally false header information) and non-fraudulent e-mail. In my opinion, this issue must be addressed come what may. Fraud in electronic communication covers much broader issues, even for business, than spam and its responses: for example, one needs reliable processes for establishing, validating and enforcing contracts electronically. E-mail authentication would be a great help.

Since the e-mail server market is dominated by very few pieces of SW, one

imagines a coordinated effort to alter e-mail protocols to introduce some degree of authentication, say along the lines of Tripoli, lies at least as well within reach as schemes to introduce payment for e-mail. We may presume that producers of such SW are well aware of such proposals, and we may conclude that they are not favored because they do not fit someone's business model.

I find some confirmation for this conclusion in that schemes to introduce individual payment for free e-mail service are being touted at the very time when just the reverse is happening with telephony: schemes for Internet telephony are apparently arousing interest in major telecommunications companies over the traditional individual payment model.

I imagine that if one is a commercial SW producer it is easier to make money by responding incrementally to Internet users' issue du jour rather than by introducing a procedure that would handle a large class of such problems all at once.

One argument in favor of the business model could be that the economy which has sprung up to deal with spam and Internet security issues is now large enough to lobby successfully against any proposal that would reduce its potential clientele at a stroke. If this is so, then incremental modification would seem to be the only socially viable possibility. What a depressing thought.

Peter B. Ladkin, University of Bielefeld, <http://www.rvs.uni-bielefeld.de>

⚡ Laptop security

<Gadi Evron <ge@linuxbox.org>>

Sat, 28 Feb 2004 10:23:24 +0200

I always say, whenever laptops are mentioned: "Forget everything else, I have nightmares already!".

The loss of information due to laptop thefts is extremely high, here is an innovation that may possibly be as useless as car theft alarms (unless you are nearby and didn't leave the laptop in the car), but it's a good start. This may actually be useful.

What I'd like to see is a GPS device with wireless communication to my cell phone. It can be a quiet indicator, or perhaps ring when it is being moved.. or even when I move too far away from it.

You can find the article at:

<http://www.canada.com/vancouver/story.html?id=511952d3-89a0-4a03-a092-be29eaeb346f>

⚡ "Where did it print?" 1990 version (Re: Meadows, [RISKS-23.16](#))

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

Thu, 5 Feb 2004 18:58:49 -0500

Chris Meadows account of printing sensitive information using a wireless

network at Kinko's, only to discover that it had not printed on any printer

at Kinko's, reminded me of a vaguely similar occurrence circa 1990. I

worked in R&D at a Fortune 500 minicomputer company, which at that time had

one "corporate" fax number which connected to _one_ fax machine whose phone

line was, understandably, usually busy. Someone at another company needed to

send me an urgent fax. He happened to have a copy of my company's phone

book. After listening to his fax machine redial continuously for five hours,

he checked the phone book and noticed that it listed about fifteen fax other

numbers. He selected the "R&D Documentation" number, and called me to let me

know he had just gotten his confirmation that it had been received at "R&D

Documentation." I went to R&D Documentation.

They had no fax machine. They did not know of any "R&D Documentation" fax

machine. Indeed, they did not know of any fax machine in R&D. The phone

book had no information beyond the machine names and numbers.

I worked my personal connections as best I could, asking every knowledgeable

old-timer I knew to regale me with lore and legends relating the locations

of _any_ fax machines other than corporate. I slowly discovered the location

of several fax machines. The fifth one--located in Purchasing--happened to

be the one that identified itself as "R&D Documentation." They'd inherited

the machine and the phone line, and nobody knew how to change the message,

so they'd left it set that way.

Daniel P. B. Smith, dpbsmith@world.std.com alternate:

dpbsmith@alum.mit.edu

✶ Buffer overflows and Burroughs/Unisys

<Keith Gobeski <gobeskik@acm.org>>

Thu, 26 Feb 2004 08:27:26 -0500

Burroughs (now Unisys) large (now Clearpath/Libra) systems have had hardware detection of buffer overflows since at least the late sixties. Only memory areas marked as code are executable and only certain processes can mark the memory as such. Consequently, data cannot be executed. Furthermore, although data can be overwritten by the user, hardware bounds checking in conjunction with memory bounds markers prevents writing outside the bounds of data owned by the user. Usually this is a fatal error terminating the process. The fatal error can be suppressed so that the process continues, but the process still cannot write into data areas not owned by itself or into code areas. To a certain extent, these mechanisms also serve to protect the user from himself.

Of course, the MCP (OS) can overcome these limitations through the use of special constructs in the language (NEWP) in which the OS is written, as can other processes written in NEWP and granted privileged abilities.

It is also worth noting that only high-level languages are used for programming: there is no assembler or machine code programming (not even for

the MCP, although some NEWP constructs are very close to machine code).

⚡ Re: Buffer overflows and Multics

<Michael LeVine <mlevine@redshift.com>>

Thu, 26 Feb 2004 09:01:59 -0800

IIRC the late VAX/VMS systems also had built in buffer overflow prevention features, probably a lesson learned from Multics. The hardware had protections that could be set on memory segments to be: Execute/No execute and read only/write only/read-write, and the OS system calls requiring buffers also had to have the length of the buffers specified.

⚡ MS Java Virtual machine

<"Karnow, Curtis E A." <ckarnow@sonnenschein.com>>

Thu, 26 Feb 2004 08:24:14 -0800

Issues associated with the MSJVM have been the subject of legal proceedings between Sun and Microsoft. Further information on the transition can be reached at

http://today.java.net/pub/n/SUN_Upgrade_Site

Garage-Door openers; Rapid disassembly of PCS phones" ([R23 20](#))

<"Charles Jackson" <chuck@jacksons.net>>

Thu, 26 Feb 2004 08:36:00 -0500

* Regarding garage-door openers:

Early garage door openers were quite simple. IIRC, some of them were no more than a sequence of Antenna, Bandpass filter, Energy detector.

They operated at low powers in bands shared with other operations. Thus, false triggering of the garage door opener would not be uncommon. Steve Bellovin's calculations are correct. No way Sputnik could be exacted to trigger a garage door opener. In contrast, a 707 flying 1,000 feet above such a garage door opener could easily trigger it.

Modern garage door openers use modulated sequences-i.e. a string of 1s and 0s-to carry commands. False triggering by other systems, such as land mobile or aircraft transmitters, is thus highly unlikely.

* Regarding exploding batteries in cellular phones:

This is not an urban legend. It has been widely reported. I recently received a letter, dated 9 Feb 2004, from legal counsel for the manufacturer of the wireless phone that I use. Some quotes from that letter:

"an allotment of batteries ... Might contain a risk hazard."

"the root cause was a quality-control issue at the battery manufacturer"

"Of the 50,731 units shipped in the United States ... four(4)

confirmed

reports of rapid disassembly. Of these four (4) reports, one involved

personal injury in the form of a second-degree burn . . "

Continued use of the phone ... could result in injury due to ... rapid

disassembly (which may appear as an explosion) ... "

The risks of this lawyer weasel wording are obvious. While engineers may

immediately recognize the hazards associated with "rapid disassembly" the

everyday user may not. Only later in the letter does the more familiar term

"explosion" appear.

✉ **Re: Garage-door openers (Ladkin, [RISKS-23.20](#))**

<"Michael Kent" <michael.k@ntlworld.com>>

Thu, 26 Feb 2004 20:03:44 -0000

I had a similar experience recently and reading this prompted me to check something I thought I remembered reading.

In late 2002 the Shell company was under fire for having hidden mobile phone masts in the forecourt signs of 210 of its 1,100 UK petrol stations.

<http://news.bbc.co.uk/1/hi/uk/2309645.stm>

The criticism was directed at the perceived health risks associated with

these masts -- a much discussed subject in it's own right. I have been

involved in the approval process for locating a transmitter close to gas

storage tank, and most risks are calculated objectively.

Substance stored,
loading and dispensing methods, transmitter power, distances etc
are all
taken in to account.

I am somewhat bemused that the urban myth of the dangers of
using mobile
phones in petrol stations is still being spread by the companies
who own
them.

✶ Re: Garage-door openings by aircraft (Re: [RISKS-23.19](#))

<Scott Peterson <scott4@mindspring.com>>

Thu, 26 Feb 2004 09:12:17 -0800

A true story that can be found in the *LA Times* archives
discusses problems
back in the 1980's when Reagan was president. When he was
staying at his
ranch in California, Air Force One would be parked at a local
Air Force base
near Riverside California. Whenever that plane was there,
everyone for
several miles around would know because their garage door
openers would stop
working.

As soon as the plane left, they'd be working again. The Secret
Service
would not comment.

[This was noted in my ACM SIGSOFT Software Engineering Notes
vol 11 no 2,

April 1985, issue, four months before the first issue of
RISKS. Most of

the relevant pre-RISKS cases are indexed in my Illustrative
Risks doc:

<http://www.csl.sri.com/neumann/illustrative.html>

(with .pdf and .ps for printing rather than browsing). PGN]

✶ Further misdirected on-line trip planning ([RISKS-23.20](#))

<"R.S. (Bob) Heuman, Toronto, ON, Canada" <rsh@idirect.com>>

Thu, 26 Feb 2004 12:47:54 -0500

Try to plan a trip from Calais, Maine to Sault Ste Marie, Michigan, using the DeLorme mapping product, or a trip from Niagara Falls, New York to Detroit, Michigan. Look at the results and be prepared to spend extra time or days on the road. The same thing happens if you are trying to travel to anywhere where traveling through Canada is substantially shorter than traveling through the US.

The reason? Delorme leaves Canada out of their product totally! To go from upper Michigan to upper Maine you go south of the Great Lakes if using their product but north of the Great Lakes if trying for a rational trip.

If you ask Delorme, who are located in Maine, they shrug their shoulders and say that those who really care about that minor problem know to use other sources of information... [I.E. They don't seem to care.]

For what it worth, the risks are not only online...

Amtrak Website routing

<"Richard S. Russell" <RichardSRussell@tds.net>>

Thu, 26 Feb 2004 09:42:27 -0600

In [Risks 23.20](#), Mike Brandt <MyLastName@syr.edu> was quoted as writing: "In the early days of Amtrak's online trip planner, I asked it about trains from Portland (Oregon) to Seattle. There are several trains each day that make this 3.5 hour trip. The first choice on the route planner's list was Portland -> Chicago -> LA -> Seattle taking about a week, and passing through Portland again 3.5 hours before arriving in Seattle."

Has the problem been fixed? You be the judge. I live in Madison, Wisconsin, about 1/3 of the way across the North American continent. My sister lives in Denver, Colorado, about 2/3 of the way across. Amtrak's recommended route for getting from here to there had me going via Minneapolis to Seattle (apparently a magnet for Amtrak customers), then to San Francisco, then backtracking to Denver -- about 4 times as long a trip as necessary once you add the extraneous north-south travel to the extraneous east-west travel. My solution was to take a bus to Chicago and catch the direct train to Denver from there. I was bemused to notice, however, that the westbound train to Denver was scheduled to leave Chicago half an hour BEFORE the eastbound one arrived from Minneapolis and Madison, so Amtrak was apparently trying to spare me a 23.5-hour layover in the Windy City. Good theory; bad implementation.

Solution: More frequent passenger trains. I continue to be frustrated that Congress insists that Amtrak must be 100% self-supporting while it lavishes billions of dollars in subsidies on its competitors -- highway builders; air-traffic control, National Weather Service, and airline bail-outs; and even the Army Corps of Engineers to keep the nation's locks, dams, and coastal waterways open to barge and riverboat traffic. The game is rigged, and once again the victims are being blamed for the system's failures.

Richard S. Russell, a Bright (the-brights.net), 2642 Kendall Ave
Madison WI 53705-3736 608+233-5640 RichardSRussell@uwalumni.com

✶ REVIEW: "Developing Secure Distributed Systems with CORBA",

<Rob Slade <rslade@sprint.ca>>
Thu, 26 Feb 2004 08:32:07 -0800

Ulrich Lang/Rudolf Schreiner

BKSDSCO.RVW 20031201

"Developing Secure Distributed Systems with CORBA", Ulrich Lang/
Rudolf

Schreiner, 2002, 1-58053-295-0, U\$69.00/C\$106.95

%A Ulrich Lang

%A Rudolf Schreiner

%C 685 Canton St., Norwood, MA 02062

%D 2002

%G 1-58053-295-0

%I Artech House/Horizon

%O U\$69.00/C\$106.95 617-769-9750 800-225-9977 fax: +1-617-769-6334

%O [http://www.amazon.com/exec/obidos/ASIN/1580532950/
robladesinterne](http://www.amazon.com/exec/obidos/ASIN/1580532950/robladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/1580532950/
robladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1580532950/robladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1580532950/
robladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1580532950/robladesin03-20)

%P 308 p.

%T "Developing Secure Distributed Systems with CORBA"

Chapter one is an introduction, but it very quickly gets into CORBA

(Common Object Request Broker Architecture) jargon, and C++ API calls.

The explanations could be written with more clarity for outsiders.

Security is first defined, in chapter two, in terms of restricting

access, but the authors are not clear about whether they are primarily

concerned with integrity or confidentiality. The material then goes

on to a good overview of security management basics and a very brief

outline of some security concerns in the CORBA environment. The lead-

in to the CORBA security architecture, in chapter three, is a lengthy

discussion of the benefits of flexibility, abstraction, and simplicity: the authors then note that the CORBA architecture is not

simple. MICO, an open source CORBA compliant object request broker,

has a security component (MICOsec), and chapter four is dedicated mostly to installation instructions. Chapter five looks at programming CORBA level one security, using MICOsec and C++, while

chapter six takes a longer look at the more complex level two requirements. CORBA security does have support for applications that

do not contain any security provisions (a rather interesting concept),

and these are reviewed in chapter seven.

CORBA security is not widely understood, and this work can assist both those needing a conceptual idea of the system and those needing to program with it.

copyright Robert M. Slade, 2003 BKDSDSCO.RVW 20031201
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu
<http://victoria.tc.ca/techrev~rslade> or <http://sun.soci.niu.edu/~rslade>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 23

Tuesday 2 March 2004

Contents

- [July 2002 air collision revisited](#)
[Paul Cox](#)
 - [FBI employee snoops through confidential police databases](#)
[Declan McCullagh](#)
 - [Data Protection and an increasingly paranoid world](#)
[Matthew Byng-Maddick](#)
 - [When entries aren't screened](#)
[Gillian M Brent](#)
 - [Re: Malicious IT design in support of the cold war](#)
[Henry Baker](#) [Diomidis Spinellis](#)
 - [MS self-inflicted DDoS](#)
[Doug Sojourner](#)
 - [Re: MS Java Virtual Machine issue](#)
[Jonathan de Boyne Pollard](#)
 - [Re: SPF and its critics](#)
[Greg Bacon](#)
 - [SPF is harmful. Adopt it.](#)
[Jonathan de Boyne Pollard](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ July 2002 air collision revisited

<"Paul Cox" <pcox@eskimo.com>>

Sun, 29 Feb 2004 02:23:39 -0800

<http://www.avweb.com/eletter/archives/avflash/203-full.html#186793>

An air-traffic controller was stabbed to death at his home near Zurich. The controller was working the sector when two airplanes had a mid-air collision in July, 2002, a crash which killed 71 people on the two planes (one was a cargo carrier, which limited the death toll) over Lake Constance, Switzerland.

This submission isn't about the RISKS of being an air-traffic controller, but rather serves to remind those of us in the business of RISKS we have not yet rooted out from the ATC system.

The investigation into the crash has not yet been finalized, but they have released some interesting points.

1) Only one controller was on duty at the time. While he might not have been busy and could handle the traffic, the fact is that two sets of eyes is generally accepted as being better than one set.

2) A collision-alert system in the control center was down for maintenance.

3) A phone warning from the previous controllers in Germany was not received by the Swiss controller.

4) The biggest problem was that the Russian pilots followed the instructions of the controllers (to descend) instead of the on-board "TCAS" collision avoidance system (which said to climb); the pilots in the DHL aircraft (the other plane) were following the TCAS system and were also descending.

To be frank, having a single controller staffing the position is a RISK but one which is taken quite frequently in ATC. Usually it is not a problem, but there is significant emphasis right now in the US ATC system to reduce staffing and "do more with less" in terms of #s of controllers.

Nearly all aviation crashes these days are a result of a "chain" of events, and frequently changing a single factor would quite possibly break the chain.

In this case, we can see a few things that need changing. Europe's ATC system is a mess compared to the neat, orderly system in the United States, because in Europe each nation has their own ATC system.

This is inefficient, to say the least, because the countries are so (relatively) small and airspace sector (and control center) design has to be built around the boundaries of the particular nations, rather than around the airports and natural flows of the aircraft.

As we have seen, it's not only inefficient, but also possibly unsafe. The good news is that Europe has been working on modernizing the ATC system design and improving it, allowing ATC to be a truly European system instead

of a hodgepodge of systems (French, German, Swiss, Spanish, Belgian, Dutch, etc).

The conflict alert system being down for maintenance is a classic risk -- nearly all ATC providers do not have completely functional redundant systems for backup while the primary one is off-line. In the USA, the primary system (NAS-HOST) has a conflict alert function; the backup system (DARC) does not. The main factor driving this decision is cost; it would be much more expensive for ATC providers to have two full-capability systems.

While NAS-HOST functions are down for maintenance, controllers do not have the computerized conflict alert. In yet another classic good/bad kind of tradeoff, the maintenance is usually performed on the "mid" shift (graveyard overnight shift). This is good because air traffic is much lower; it's bad because the controllers are probably less alert and able to adapt due to plain old circadian rhythms. (Controllers' schedules are horrible for this, but that's another RISKS post.)

Finally, we turn our attention to the TCAS. Potential problems with the TCAS system have been in RISKS before, and this exact scenario was also predicted by many in the ATC and aviation industry.

The specific scenario that was predicted, and which apparently happened in the Switzerland crash, was this: Two aircraft are in conflict. Their TCAS systems activate and proscribe a course of action for each aircraft which,

if followed, should separate them.

(It should be noted that each plane has a TCAS system on board, and while they are capable of operating independently they typically operate in conjunction, so the resolution suggested works well for both aircraft.)

At the same time, the controller sees the situation developing and issues instructions to one or both aircraft; these instructions might be what the TCAS is saying to do, or might not.

The pilots on the aircraft then have to figure out what to do.

In the worst-case scenario, the TCAS tells one plane to climb and another to descend; ATC tells the first plane to descend and the pilots follow THAT instruction, which only makes matters worse as both planes are now trying to descend below the other. Planes smack, everyone in the air dies.

The problem is that the controller, whose job is to sit and issue these sorts of instructions at all times, has NO WAY of knowing that the TCAS unit is suggesting a course of action, and can therefore be giving a perfectly good instruction to one aircraft while the TCAS unit is giving a horrible instruction to the other aircraft.

(Or vice-versa; the point isn't that the commands themselves are good/bad, but that TCAS and ATC are trying to resolve the situation with conflicting instructions that only make things worse.)

Now, in theory this problem has been "solved". Controllers are told and

pilots are trained that when a TCAS conflict resolution happens, the pilots are to follow the TCAS instructions- even if they are in conflict with instructions from ATC.

Unfortunately, the possibility for confusion still exists. In this case, it was probably exacerbated by the fact that the Russian plane's pilots came out of an aviation system which heavily emphasized ground control and discouraged pilots making "their own call" in the air; the Russian pilots were (apparently) predisposed to follow the ATC instructions instead of the TCAS instructions.

Perhaps their training was not sufficient; perhaps the TCAS unit wasn't operating properly. However, the biggest problem is that different people will sometimes make different choices no matter how much training you give them; one aircrew follows the TCAS, one follows ATC.

In any case, this crash perfectly illustrated the TCAS RISK which has existed for over a decade, and which is still not solved in any manner -- namely, that ATC has no way of knowing if/when TCAS resolutions are being broadcast in the cockpits unless the pilots inform ATC, and usually in this last-minute situation there isn't time to do so.

What I found interesting in skimming back through the RISKS archives is that this RISK, which has been borne out, was tossed back and forth like a political football- and decidedly non-scientific means were used to dismiss the RISK.

The US ATC union, NATCA, pointed out repeatedly that this RISK existed, but was frequently dismissed as merely hyping the issue because "they don't like giving up control" to the pilots in the cockpit.

*** From [RISKS-13.78](#), by Nancy Leveson, September 1992:

"In the report (which was surprisingly good) they also mentioned that the controllers hate TCAS because they lose control and that the pilots love it because they gain control."

"If you read about TCAS, you need to be aware that it is in the midst of a big political struggle. The pilots love it (there was a representative from ALPA on the CNN report). The controllers hate it....So watch who is speaking when you hear about TCAS and its problems or advantages."

"In case there is anyone who doesn't know, my Ph.D. students (Mats Heimdahl, Holly Hildreth, Jon Reese, Ruben Ortega, and Clark Turner) and I are working on a formal system requirements specification of TCAS II. This will serve as the official FAA specification of TCAS and also as a testbed application for their dissertations on safety analysis and risk assessment."

The irony here is profound. The controllers' union was raising the issue and providing data, anecdotal evidence, and proposing scenarios which were both entirely possible and possibly occurring; the scientist dismissed those concerns by labeling them as politically motivated... but failed

to give any evidence of where the union had gone wrong.

In March 1993, [RISKS-14.44](#), John Dill, an ATC in Cleveland, Ohio, laid out nearly exactly the same scenario that I did above- ATC giving one set of instructions, TCAS giving another.

In [RISKS-15.51](#) and [15.66](#), an incident in Portland, Oregon, again illustrated the issue with TCAS.

[RISKS-16.25](#) had a submission that was highly critical of an NBC "Dateline" report on TCAS. Andres Zellweger claimed "The fact is that TCAS substantially reduces the risk of midair collisions." The report had presented the controllers' view fairly positively, but many in the aviation world made claims like Mr Zellweger's.

However, this begged the simple question- how many midair collisions were occurring PRIOR to TCAS's implementation? Real answer: nearly zero. How many happened AFTER the implementation: Still nearly zero. This is not evidence of improvement, of course.

In [RISKS-17.18](#), [18.83](#), [19.55](#), and [20.11](#), we have more reports of incidents that mirror the warnings of controllers.

In [RISKS-20.12](#), we had a report of a "good" TCAS move and a "bad" TCAS move, and the submitter, David Wittenberg, asked the \$64,000 question at the end of his submission: "So the controllers got one pair of planes into a bad situation, and TCAS bailed them out; and TCAS got another set of planes into a bad situation and the controllers bailed them out. How are

the pilots to know which one to trust when they must make decisions quickly?"

[RISKS-20.60](#) and [20.62](#) had more reports of TCAS-induced mishaps and near-collisions.

In [RISKS-10.16](#), dated back 18 July 1990, I found this question from Henry Spencer: "This brings to mind an interesting thought: who gets the blame if (when) a TCAS warning *causes* a collision, through either electronic or human confusion?"

Well, unfortunately for the controller in Switzerland, it appears that at least one angry family member held ATC responsible for a RISK that controllers had been pointing out for years.

The (ongoing) history of the TCAS system is nearly a perfect example of how implementing technology can be good, bad, or somewhere in the middle. It'll be a great subject for dissertations in the future, I believe.

Aviation is still not perfected. We might like to think that it is, but it's not; errors still do occur.

What this whole story points out, to me, is that we must continue to ensure that the humans are given enough training and support to be in a position to succeed; that the automation we implement must be shown to IMPROVE safety, and through hard evidence and not mere assertions that it does; and that we should not dismiss the naysayers simply because we think they have an axe to grind.

Sometimes there really are people out to get the paranoid guy.

Paul Cox, ZSE

✶ FBI employee snoops through confidential police databases

<Declan McCullagh <declan@well.com>>

Thu, 26 Feb 2004 22:54:28 -0600

Assistant Attorney General Christopher A. Wray of the Department of Justice Criminal Division and U.S. Attorney Roscoe C. Howard of the District of Columbia announced that Narissa Smalls, a legal technician in FBI Headquarters, was sentenced to 12 months in prison on charges stemming from her unlawful access of the FBI's Automated Case Support (ACS) computer system. [Source: FBI legal technician pleads guilty to unlawfully accessing the FBI's computer system, WWW.USDOJ.GOV, 26 Feb 2004; PGN-ed from Declan McCullagh's Politech mailing list, archived at <http://www.politechbot.com/>

✶ Data Protection and an increasingly paranoid world

<Matthew Byng-Maddick <mbm@colondot.net>>

Fri, 27 Feb 2004 11:52:45 +0000

As most here will know, the UK has had Data Protection legislation for some time, requiring companies to register their data processes where personally

identifiable data is involved. *The Metro*, London's free newspaper (seen all over the Underground) printed by the right-wing *Daily Mail* group, has been printing lots recently about the Soham murders and Data Protection. The essence is that several police records were binned for this convicted murderer, that might have helped police find him earlier.

Of course, they don't say what has been mentioned here and in other places, that the school where he was caretaker was not the one where the murdered children were, and that even if he'd been a plumber or a builder, he'd probably still have been in a position to murder the two girls. The Data Protection Act is being blamed for the fact that people with no understanding of the Act's requirements binned the records.

So, here we have the newspaper hinting that they think Data Protection Act is rubbish and should be scrapped.

The contrast came to me this morning; the London Underground Oystercards have been mentioned here previously. I have one of these devices. Apparently, I shouldn't be putting it in my back jeans pocket and sitting on it, because it's now started to work <50% of the time. According to the man behind the counter at the ticket office at 11:45 last night, this is not the "massive design flaw" that I seem to think it is in such a system, that they do not cope with moderately rough handling, and paper (well, printed) tickets are "obsolete", being, as they are, based on an old technology. (So where have we heard that one before, then?).

So, having asked for a replacement card, I was instead handed a form to fill in (London Underground adore bureaucracy), and told to bring this form back with a proof of address/identity. Now, when I got the oystercard, I had to fill in a form with address details on it (no proof needed). The number printed on the Oystercard is enough of a key to be able to get all of the information that they request on the form (including name, address, photocard number, what tickets are loaded), and I pointed out that it seemed crazy to be getting this information again. Typically, for London Underground, the staff member looked at me as if I was mad. As well as this, the form asked for my signature on the following text:

(TfL - Transport for London, government body overseeing all transport issues

within London,

LUL - London Underground Limited, private company who own and operate the

Underground system)

| I declare that the information I have provided on this form is true to

| the best of my knowledge. I consent to TfL and/or LUL checking the

| information I have given. I accept that if the information I have given

| is inaccurate one or more of the following may happen: my use of the

| replacement card may be stopped; I will be liable for any balance due to

| TfL/LUL (and I will pay it); legal action may be taken against me.

This is just one example of where the Data Protection Act is not effective enough, not that it would help here, either.

RISKS:

- + Spurious sensationalistic reporting dulling the senses of those who are most in need of the awareness
- + Private company, in virtual monopoly position, imposing ever more onerous data requirements on its customers
- + People being required to sign unpleasant and open-ended liability in order to be able to buy season tickets to use a busy city's transport system
- + People taking it as read that they have no right to privacy any longer, in this world of terrorism
- + And of course, the obvious and standard: replacing "obsolete" technologies that work well with technologies that haven't been properly tested for real world conditions (though he claimed that they had to reprint paper tickets reasonably often, I never had (user-fixable) problems where they failed to go through the machine)
- + And, lastly a relatively good risk to the Oyster itself, having an expensive ticket which only stores the data in electronic form, with no (tied) user/staff-verifiable print of what the data contained should be (ie. if the readers don't work, they have to take your word for it)

Matthew Byng-Maddick <mbm@colondot.net> <http://colondot.net/>

✶ When entries aren't screened

<Gillian M Brent <Gillian.M.Brent@optus.com.au>>

Sun, 29 Feb 2004 02:58:08 +1100

Apparently Channel 14 in News 14, Raleigh, NC, have a Web interface for people to submit school and business closing announcements during the bad weather. All well and good, except that it seems no-one was checking the entries.

A number of the more dubious entries are included on the discussion board at <http://mb3.theinsiders.com/fcarolinacanesfrm1.showMessageRange?topicID=3254.topic&start=1&stop=20> (complete with screenshots), but I have to concur with Mr Steele whose Live Journal included the screenshot for "Tutone Inc, Closed Thursday and Friday, Call Jenny at 867-5309". <http://www.livejournal.com/users/mdsteele47/28884.html>

The risk - leave a public-broadcast message service un-moderated and it won't be long before the humourous, the annoying, and the simply obscene get through.

✶ Re: Malicious IT design in support of the cold war (Garst, [R 23](#) [21](#))

<Henry Baker <hbaker1@pipeline.com>>
Thu, 26 Feb 2004 19:52:11 -0800

It seems to me that Microsoft "Windows" is payback for these CIA misdeeds.

It passes the tests, then fails catastrophically... Or perhaps the CIA assumed that the USSR would slavishly copy Windows the way they had copied

OS/360, and never imagined that the US DoD would itself have to use Windows.

Maybe the CIA is now being hoist with its own petard??

✶ Re: Malicious IT design in support of the cold war (Garst, [R 23 21](#))

<Diomidis Spinellis <dds@aueb.gr>>

Mon, 01 Mar 2004 23:42:22 +0200

Although the issue of maliciously designed components is interesting, I find the specific story regarding the malicious IT design of the gas pipeline control software difficult to believe. According to the article [1]:

"When we turned down their overt purchase order, the K.G.B. sent a covert

agent into a Canadian company to steal the software; tipped off by

Farewell, we added what geeks call a "Trojan Horse" to the pirated

product. [...] The pipeline software that was to run the pumps, turbines

and valves was programmed to go haywire," writes Reed, "to reset pump

speeds and valve settings to produce pressures far beyond those acceptable

to the pipeline joints and welds. The result was the most monumental

non-nuclear explosion and fire ever seen from space."

The above excerpts make the pipeline software appear to be an off-the-shelf application. However, software of this complexity is not sold shrink-wrapped on CDs with a glossy manual that a covert KGB agent can

steal. Even if we are not talking about a bespoke application, the software would have to be adapted, tuned, and configured by its developers for the specific environment. A typical ERP system has to be expensively configured for the needs each company by trained specialist consultants; I can not imagine the pipeline control software to have a "Tools - Options - Joints - Weld quality" setting implied by the article.

[1] <http://seclists.org/lists/isn/2004/Feb/0011.html>

Diomidis Spinellis - <http://www.dmst.aueb.gr/dds>

MS self-inflicted DDoS

<Doug Sojourner <dsojourner@matrixsemi.com>>

Fri, 27 Feb 2004 09:19:03 -0800

The other day my children called me to the computer ... they had a prompt to download software, and (thanks to careful training) were suspicious.

It turned out to be Microsofts Critical Patch warning -- they wanted us to download a patch right away. Given their concern that most or all attacks come from black-hats reverse engineering the patches <<http://news.bbc.co.uk/1/hi/technology/3485972.stm>>, it is understandable that they would want us to patch quickly. However, if you ask every windows user on the net to upgrade NOW, you probably haven't got bandwidth for the response. Microsoft didn't.

We ended up patching later.

✶ Re: MS Java Virtual Machine issue (Reinke, [RISKS-23.20](#))

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

Sat, 28 Feb 2004 18:22:53 +0000

In [RISKS-23.20](#), Ferdinand John Reinke states that Microsoft will no longer "be able" to support its own JVM from 2004-10-01 onwards, and, as a result,

```
FJR> customers who have the MSJVM installed after this
FJR> date will be vulnerable to potential attacks that
FJR> will attempt to exploit this technology.
```

I have to ask how he thinks that the risks of potential vulnerability are any different to those in the situation `_before_ 2004-10-01`. They aren't, of course. The software is not, after all, magically changing somehow on that date to become more vulnerable. (Is he aware of some Microsoft-implemented time bomb in its JVM that he hasn't told us about?) If it's vulnerable to attacks, it is vulnerable `_now_`. Conversely, if it isn't vulnerable to attacks, it won't suddenly become vulnerable. The date on which support stops is irrelevant to concerns about its vulnerability.

Additionally, he says

```
FJR> More alarming, many organizations aren't even aware
FJR> that they have MSJVM installed.
```

Again, I have to ask how he thinks that Microsoft's JVM is any different in this respect from the numerous other bits and bobs that many organisations, who just take whatever comes on the discs and in the software updates, will be unaware that they have installed on their machines. The risk of not knowing what softwares one's machine has on it applies to all softwares, isn't specific to Microsoft's JVM, and isn't related to whether those softwares are supported by their manufacturers.

✶ Re: SPF and its critics (Maziuk, [RISKS-23.21](#))

<Greg Bacon <gbacon@hiwaay.net>>

Fri, 27 Feb 2004 15:43:36 -0600

Dimitri Maziuk was right on when he wrote

> To get back where I started: we know that technical solutions for
> non-technical problems don't work. We are clearly dealing with
> non-technical problem here.

Spam is an instance of the well-known problem from economics known as the tragedy of the commons. The fix is ditching the bad framework, but we refuse to learn from history and instead allow our hubris to goad us into codifying more expectations for people to ignore.

✶ SPF is harmful. Adopt it. (Re: Kestenbaum, [RISKS 23.18](#))

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

Sat, 28 Feb 2004 20:57:05 +0000

Lawrence Kestenbaum says, with respect to his mail, that

LK> the junk has suddenly reached a new level.

My response to that is the same one that I gave to Jon Seymour in response to his submission to [RISKS 22.95](#) last year:

Welcome to the club. You're late.

You can find a condensed history of my experience at
<URL:<http://homepages.tesco.net/~J.deBoynePollard/deluge-of-microsoft-worms.html>>.

People now have more success contacting me via Fidonet than they do contacting me via Internet, a situation that I find amusingly ironic.

Lawrence Kestenbaum also says

LK> The critics of SPF suggest that spammers would

LK> simply find or invent other addresses to use.

But this is missing the point. The fact that, as with many other anti-UBM measures for SMTP-based Internet mail, SPF creates yet another arms race is but one of the many things wrong with it. There has been a lot of discussion of the glaring faults of SPF in several discussion fora (which I encourage RISKS readers to read, by the way). When the turn came for the "gmail" mailing list to have the discussion, I listed 12 of the problem areas to consider for SPF in <URL:news://news.gmane.org./402321C2.7825F3FA@Tesco.NET>, but that is by no means an exhaustive list.

Lawrence Kestenbaum then says that he doesn't care about the arms race that SPF initiates (a lamentably short-term and short-sighted attitude, especially in light of the history and consequences of the "Bayesian filters" arms race)

LK> so long as [spammers stop] plastering my personal
LK> address on hundreds of thousands of fraudulent and
LK> disreputable spam messages and viruses, [...]

But, of course, SPF won't actually stop that at all. The tool for proving that one did or didn't write something, signed message bodies, has long since been invented anyway.

On the gripping hand, perhaps the fact that widespread adoption of SPF will do serious damage to the SMTP mail architecture is a good thing. In the battle against unsolicited bulk mail, we've concentrated upon the wrong problem time after time, with mechanisms that address the wrong thing and that don't address the actual "unsolicited" and "bulk" qualities of undesirable mail. SMTP has become less usable, more patchy, and more balkanised with each new bodge, yet continues to bend and not quite break completely. Perhaps the adoption of SPF will turn out to be the straw that finally breaks the camel's back, and that thus finally forcibly weans us off this bad habit of addressing the wrong problem.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 24

Wednesday 3 March 2004

Contents

- [Risks of Leap Years and Dumb Digital Watches, quadrennial posting](#)
[Mark Brader](#)
- [GAO's latest evaluation of DOD software development practice](#)
[James Paul](#)
- [Trouble with Mars rover Spirit](#)
[Erling Kristiansen](#)
- [RFID tags in new US notes explode when you try to microwave them](#)
[Michael Borek](#)
- [State looks at false bills from AT&T](#)
[Peter Howe via Monty Solomon](#)
- [California e-voting: did programmers even try it?](#)
[Joel Garry](#)
- [Anti-Spam Solutions and Security, Neal Krawetz](#)
[Monty Solomon](#)
- [Legal Mercedes driver jailed for 18 months](#)
[Stefan Lesser](#)
- [Re: Stolen heart monitor](#)
[Dave Brunberg](#)
- [Re: Buffer overflows and VMS](#)
[Stanley F. Quayle](#)

- [Re: Buffer overflows and Burroughs/Unisys](#)
[Bill Hopkins](#)
 - [Re: A320 Incident](#)
[Peter B. Ladkin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Risks of Leap Years and Dumb Digital Watches, quadrennial posting

<msb@vex.net (Mark Brader)>
Tue, 2 Mar 2004 19:33:50 -0500 (EST)

All right now, how many people reading this...

-> saw a previous version of this message in [RISKS-6.34](#), [13.21](#),
[17.81](#),
and/or [20.83](#);

-> have watches that need to be set back a day because, unlike the
smarter kind of digital watch, they went directly from
February 28
to March 1;

-> and *hadn't realized it yet*?

[Please answer to yourself, but not to RISKS. We don't really
need a
hand count. PGN]

✶ GAO's latest evaluation of DOD software development practice

<"Paul, James" <James.Paul@mail.house.gov>>
Tue, 2 Mar 2004 14:17:46 -0500

The General Accounting Office (GAO) today released the following report:

Defense Acquisitions: Stronger Management Practices Are Needed to Improve

DOD's Software-Intensive Weapon Acquisitions. GAO-04-393, 1 Mar 2004

<http://www.gao.gov/cgi-bin/getrpt?GAO-04-393>

Quoting from Highlights of GAO-04-393:

"Software developers and acquirers at firms that GAO visited use three fundamental management strategies to ensure the delivery of high-quality products on time and within budget: working in an evolutionary environment, following disciplined development processes, and collecting and analyzing meaningful metrics to measure progress. When these strategies are used together, leading firms are better equipped to improve their software development processes on a continuous basis. An evolutionary approach sets up a more manageable environment - one in which expectations are realistic and developers are permitted to make incremental improvements. The customer benefits because the initial product is available sooner and at a lower, more predictable cost. This avoids the pressure to incorporate all the desired capabilities into a single product right away. Within an evolutionary environment, there are four phases that are common to software development: setting requirements, establishing a stable design, writing code, and testing. At the end of each of these phases, developers must demonstrate that they have acquired the right knowledge before proceeding to

the next development phase. To provide evidence that the right knowledge was captured, leading developers emphasize the use of meaningful metrics, which helps developers, managers, and acquirers to measure progress. These metrics focus on cost, schedule, the size of a project, performance requirements, testing, defects, and quality. "In a review of five DOD programs, GAO found that outcomes were mixed for software-intensive acquisitions. The F/A-18 C/D, a fighter and attack aircraft, and the Tactical Tomahawk missile had fewer additional cost and schedule delays. For these programs, developers used an evolutionary approach, disciplined processes, and meaningful metrics. In contrast, the following programs, which did not follow these management strategies, experienced schedule delays and cost growth: F/A-22, an air dominance aircraft; Space-Based Infrared System, a missile-detection satellite system; and Comanche, a multimission helicopter...."

Why GAO Did This Study

"The Department of Defense (DOD) has been relying increasingly on computer software to introduce or enhance performance capabilities of major weapon systems. To ensure successful outcomes, software acquisition requires disciplined processes and practices. Without such discipline, weapon programs encounter difficulty in meeting cost and schedule targets. For example, in fiscal year 2003, DOD might have spent as much as \$8 billion to rework software because of

quality-related issues.

"GAO was asked to identify the practices used by leading companies to acquire software and to analyze the causes of poor outcomes of selected DOD programs. GAO also was asked to evaluate DOD's efforts to develop programs for improving software acquisition processes and to assess how those efforts compare with leading companies' practices."

What GAO Recommends

"GAO recommends that the Secretary of Defense direct the military services and agencies to adopt specific controls to improve software acquisition outcomes. These practices should be incorporated into DOD policy, software process improvement plans, and development contracts. DOD concurred with two revised recommendations and partially concurred with two others."

✶ Trouble with Mars rover Spirit

<Erling.Kristiansen@esa.int>

Tue, 2 Mar 2004 13:55:38 +0100

A good explanation of what happened to Spirit is at <http://www.eetimes.com/sys/news/OEG20040220S0046>

In brief:

- A software upload took place in order to correct some problem
- A utility to delete files belonging to the old software was uploaded, but the upload failed
- This failure was apparently forgotten or ignored, resulting in

less file

space being available for experiment data than anticipated

- When the file system overflowed, a reboot occurred. This, apparently, was

the intended behaviour

- The reboot could not complete due to insufficient available file space

- An infinite loop of reboots was entered

RISKS, as I perceive them:

- Relying on mission planners, working on assumed rather than actual file

space, to not overflow file system

- A file system that does not fail gracefully when overflowed

- A boot sequence that requires resources that may become unavailable

RFID tags in new US notes explode when you try to microwave them

<mikkeles@netscape.net (Michael Borek)>

Tue, 02 Mar 2004 09:54:25 -0500

"Prison Planet" (<http://www.prisonplanet.com/022904rfidtagsexplode.html>) is

carrying a story of an experiment on microwaving the new US \$20.00 bills

which contain RFIDs. (The site includes pictures of the results.)

Apparently, the new bills were setting off every RFID monitor they passed

through! Wrapping the bills in aluminium foil stopped this behaviour, but

they decided to try microwaving the bills. This led to the RFIDs exploding

and burning the face of Andrew Jackson's picture.

This could become quite common a problem as word passes that microwaving can destroy RFIDs without the proviso that this may (will) damage the goods.

(A discussion is also being carried on Slashdot:
<http://slashdot.org/article.pl?sid=04/03/02/0535225&mode=nested>)

✶ State looks at false bills from AT&T

<Monty Solomon <monty@roscom.com>>
Tue, 2 Mar 2004 12:24:52 -0500

Company denies telemarket scheme, Peter J. Howe, *The Boston Globe* 2 Mar 2004

Massachusetts utility regulators said yesterday that they are investigating a pattern of AT&T Corp. allegedly sending bogus bills to people who are not customers of the company, then trying to sell them AT&T phone service when they call to complain.

After similar concerns emerged in upstate New York last week, the Massachusetts Department of Telecommunications and Energy said yesterday it has received more than 30 complaints since January from Bay State residents who said they got bills from AT&T although they have never had AT&T service or canceled it months or years earlier. ...

http://www.boston.com/business/globe/articles/2004/03/02/state_looks_at_false_bills_from_att/

California e-voting: did programmers even try it?

<"Joel Garry" <JoelG@AnabolicInc.com>>

Tue, 2 Mar 2004 10:36:32 -0800

I think I electronically voted at a polling place in the California Primary today. California has an odd primary rule where, if you register non-partisan, you are allowed to put bad data into the party of your choice, if they have chosen to let non-partisans do so. So I decided on a particular party, inserted the card, chose "large print," and was presented with page 1 of 8, a blank screen. It seems the program dynamically assigns the various items to the pages, which evaluates to 4 pages with normal type, and 7 for large type. So for large type it doubles the number of regular type pages and presents the blank page first. Poll workers did not seem to understand this, and the help line for them to call was continually busy.

[This RISK intentionally left blank. JG]

Anti-Spam Solutions and Security, Neal Krawetz

<Monty Solomon <monty@roscom.com>>

Tue, 2 Mar 2004 00:47:23 -0500

Dr. Neal Krawetz, Anti-Spam Solutions and Security
SecurityFocus, last updated 26 Feb 2004,
<http://www.securityfocus.com/infocus/1763>

In a recent survey, 93% of respondents reported dissatisfaction with the large volume of unsolicited e-mail (spam) they receive. The problem has grown to the point where nearly 50% of the world's e-mail is spam, yet only a few hundred groups are responsible. Many anti-spam solutions have been proposed and a few have been implemented. Unfortunately, these solutions do not prevent spam as much as they interfere with every-day e-mail communications.

The problems posed by spam have grown from simple annoyances to significant security issues. The deluge of spam costs up to an estimated \$20 billion each year in lost productivity -- according to the same document, spam within a company can cost between \$600 and \$1,000 per year for every user.

✶ Legal Mercedes driver jailed for 18 months

<Stefan Lesser <stefan.less@burdadigital.de>>

Tue, 2 Mar 2004 12:40:57 +0100 (W. Europe Standard Time)

Re: Solving e-mail problems economically ([RISKS-23.22](#))

> The [...] virus writers are no more responsible for the amounts of junk
> [...] than I am responsible for the damage caused by an automobile whose
> driver does not observe my bicycle until the last second and manoeuvres
> suddenly.

In recent German jurisdiction, exactly that happened.

The driver of a Mercedes Coupe was jailed for 18 months after the death of a woman and her 2-year-old daughter. Apparently the mother, who was driving on the leftmost lane of a 3-lane Autobahn, was frightened by the fast approach of the Coupe and swerved right across all three lanes into a tree. The cars didn't even touch each other. Although at the time of the accident the Mercedes was going at nearly 155mph, there was nothing illegal about that as there are no "global" speed limits on the German Autobahnen.

Apart from the somewhat irritating court decision, which is open for retrial, there now seems to be the actual RISK of being prosecuted for the mis-reactions of others... [Also, death threats against the judge! PGN]

English URL: <http://www.timesonline.co.uk/article/0,,588-1006376,00.html>

German URL: <http://www.stuttgarter-nachrichten.de/stn/page/detail.php/600908>

Stefan Lesser, Support Center Muenchen, Burda Digital Systems GmbH,
Am Kestendamm 2, 77652 Offenburg <http://www.burdadigital.de>
+49/89/9250-3433

[Interesting case. Check out the details. PGN]

✶ Re: Stolen heart monitor

<"Dave Brunberg" <DBrunber@FBLEOPOLD.com>>
Tue, 2 Mar 2004 08:56:50 -0500

>>The idea of an implantable medical device apparently requiring physical
>>reconfiguration (at least) to talk to an external monitor implies a level of
>>trust in the reliability of the external device which is seriously scary.
>>The RISKS hardly need pointing out here...

I think the RISKS of allowing unauthenticated remote reprogrammability of an implanted medical device may be just as scary. One way of reducing that RISK may be to have some sort of an "emergency broadcast" safe mode in which a new external monitor could identify itself to the implant and authorize through a highly secure key which would require knowledge of a passphrase to transmit. Of course, you'd really have to remember to change the default password....

David W. Brunberg, Engineering Supervisor, The F.B. Leopold Company, Inc.

✶ Re: Buffer overflows and VMS (Levine, [RISKS-23.22](#))

<"Stanley F. Quayle" <stan@stanq.com>>
Tue, 02 Mar 2004 09:55:28 -0500

> IIRC the late VAX/VMS systems also had built in buffer overflow prevention
> features, probably a lesson learned from Multics.

In fact, all systems running OpenVMS (formerly known as VAX/VMS) do. Memory protection was built into the design of both the VAX and Alpha

processors.

The Itanium version of OpenVMS uses the processor's built-in in memory protection, as well.

Pages can be set to be most any combination of read, write, or execute, with different protections depending on operating mode: user, supervisor, executive, or kernel.

C programmers moving to OpenVMS quickly discover what the ACCVIO error message means.

Stanley F. Quayle, P.E. N8SQ +1 614-868-1363 Fax: +1 614 868-1671
8572 North Spring Ct. NW, Pickerington, OH 43147

✶ Re: Buffer overflows and Burroughs/Unisys (Gobeski, [RISKS-23.22](#))

<"Bill Hopkins" <whopkins@wmi.com>>

Tue, 2 Mar 2004 12:02:47 -0500

Keith Gobeski's note on the Burroughs stack architecture's improvements over many of its successors (compliment stolen from Wirth, IIRC) reminds me of the discussions in the late '70s of whether and how it could support the hot, new C language. Eventually it could, mostly, but it was ugly.

The key to a language-oriented architecture is preserving the language's abstractions (in this case the data array abstraction) in the run-time

environment. The Algol abstraction is clean: an array and an index combine properly if the index is within the declared range; otherwise it is illegal. An array row descriptor identified the memory segment and the limit, so an out-of-range access caused an exception. There was no other way for a program to get at the memory, so it was inherently safe.

Since C's memory abstraction is basically the hardware address, and addresses can be manipulated arbitrarily, any reasonably complete C implementation had to abandon tagged segments as array rows, instead putting all arrays in a single segment, keeping an allocation map in a locally-managed stack, etc. in order to generate an index for a memory access. All the (parallel, fast) hardware assist for arrays was lost, replaced by (sequential, slower) software. Some of the pathological C constructions were still impossible, of course; you couldn't force it to execute data. As Unix (itself a reaction to Multics OS complexity) became trendy, who knew this was a Good Thing?

The rise of the processor chip (and byte-oriented memory, and college courses in C) put an end to the experiments outside Burroughs/Unisys, as chip areas forced simple architectures (some actually *called* RISCs) without support for elegant and useful abstractions. Heck, software can always make up for hardware deficiencies, right?

(A 1982 ACM Computer Architecture News paper, "The Architecture of the Burroughs B5000 --20 Years Later and Still Ahead of the Times?" by Alastair

J. W. Mayer, is still relevant another 20 years later. It's on his web site at <http://www.ajwm.net/amayer/papers/B5000.html>)

✶ Re: A320 Incident (Ladkin, [RISKS-21.48](#), June 2001)

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

Tue, 02 Mar 2004 11:41:42 +0100

In [RISKS-21.48](#), 21 June 2001, I reported on an incident to a Lufthansa A320. The A320 is a "fly-by-wire" aircraft, in that primary control is effected through computers and electrics rather than mechanical means.

The captain's (CAP) sidestick controller was miswired during maintenance so that a "bank right" command initiated a "bank left" control signal and vice versa. This was discovered on take-off, when the captain corrected a left wing dip due to turbulent air flow with right sidestick movement ("bank right") and the aircraft's left wing dipped further, reportedly coming within two meters of touching the ground. The copilot took priority control (a feature of the electronic control architecture) and recovered the aircraft. The crew flew up a few thousand feet altitude, familiarised themselves with the problem as best they could, and returned to land the aircraft.

It turned out that two wires connecting the CAP's sidestick to one Elevator

and Aileron Computer (ELAC), of which there are two, had been reverse-connected during maintenance, and the fault had been discovered neither by post-maintenance check, nor by post-maintenance cross-check, nor by the flight crew's pre-take-off control system check.

I had suggested in my [Risks 21.48](#) note that I was puzzled by the partial reports of the incident then available. The final report was published as report 5X004-0/01 in April 2003 by the German Federal Bureau of Aircraft Accidents Investigation (german acronym BFU) and is available in English at http://www.bfu-web.de/berichte/01_5x004efr.pdf Thanks to John Sampson for bringing it to my attention.

Salient facts are as follows. During previous flights, one of the two ELACs failed. Maintenance found a defect in the X-TALK-BUS between ELAC Nos 1 and 2, found to be "caused by a bent connection pin (Pin 6K) in the plug segment AE of the socket for the ELAC no. 1." The attempt to replace just the pin failed and it was decided to replace the plug segment AE. There was no suitable spare plug AE for this series of airplane in stock, and the AE segments they had were not compatible with the remaining installed segments, so it was decided to replace all four plug segments AA, AB, AD, AE with a compatible set. This meant that "in a confined space approx. 420 assigned connector pins had to be reconnected."

The method chosen was "ONE TO ONE", whereby "the wires were disconnected one after the other from the old plug and immediately connected to the new one."

The mechanics used the wrong wiring diagram.

How could this be? Well, an airplane and its equipment are identified by serial number (SN). The manufacturer knows what equipment was installed at build. Subsequently, the manufacturer issues Service Bulletins (SB) for modifications to installed equipment, and these SBs have different grades of urgency. Some are only "recommended", for example. So the installed equipment is identified by SN, and further by the log of which SBs have been accomplished. The applicable wiring diagram on p2 of the Airplane Wiring Manual (AWM) contained a designation that said it was applicable to airplanes with an "effectivity range" of 013-018 and those with effectivity 001-012 on which SB 27-1030 had been accomplished. P4 of the AWM was applicable to those airplanes with effectivity range 001 to 034 on which SB27-1030 and SB27-1084 had been accomplished. SB27-1084 had been accomplished, but not SB27-1030, and the aircraft had effectivity 017. Hence p2 was applicable, but the mechanics thought p4 was applicable as SB27-1084 had been accomplished.

Each numbered wire consists of a twisted red-blue pair. In segment AE, the "Monitor Channel" is connected by pair 0603. The Control Channel is connected by pair 0597. P2 specifies that these wires must be cross-connected (blue to red, red to blue) between the sidestick and ELAC plug. P4 specifies that these wires must be connected straight through (red to red, blue to blue).

Furthermore, in the Aircraft Wiring List (AWL), the twisted

pairs are always assigned in the order red, then blue, in the alphanumeric sequence of plug segment coordinates, except for these two wires. Wire 0603 is assigned blue then red to the pins 3C/3D, and wire 0597 blue then red to 15J/15K. Why? The manufacturer wanted to effect a uniform wiring for all its FBW airplanes, and from a certain type series on, the A320 wiring was planned to be identical to that of the A330 and A340. An interchange of colors was accepted for a certain transition period, and this aircraft belonged to the transition series.

The BFU report points out that, had only the AE segment been exchanged, only the Monitor Channel would have been falsely connected, and with high probability an error message would have appeared on the cockpit aircraft monitoring display (ECAM). It doesn't say at which point this message would have appeared - at check, at cross-check (both performed only with the right sidestick), or at pre-take-off check (about which I speculate that maybe only the right side stick operation checked again - see last paragraph).

The process of reconnecting 400-odd wires was a "major action on the control system", and the manufacturer Airbus requires in AMM 20-52-10 that a continuity check be performed on each individual wire, followed by an operational or functional test of the related function. This action was orally cancelled by maintenance supervisors upon inquiry by the mechanics, the reason being that the functional test to be performed after

maintenance
would reveal wiring errors. Well, it didn't.

It was also required to perform a functional check and a control system check independently of each other. Well, they were performed simultaneously, and the check person "had not been informed sufficiently about the previous work flow", in particular that the reconnected wires had not been measured as required.

Further, the control system test and functional test were performed only from the right sidestick, not from both, and a visual comparison check of the control surfaces was not performed. The report points out that the manufacturer's instruction in AMM-27-93-00-710-050 is ambiguous. It talks about how to perform the test with "the side stick". There are two. The mechanics told the investigators that it did not matter which sidestick was used to perform the tests, since "as both ELACs were connected to each other[,] possible faults of the one or the other ELAC would surely be indicated. This statement indicates lacking system knowledge of the mechanics."

The cross-check staff member also used the same system documents to conduct his cross-check that were used by the staff member who conducted the first check. Regulations require a second set of documents to be used, to assure independence, which was thereby lost.

The BFU points out that reconnecting all 400* wires of the ELAC plug "was

connected to a high risk of errors." It also says that "a complicated and complex documentation system which thus is difficult to handle increases the risk of mistakes. The 173 procedural instructions valid for the area concerned contain many cross references making handling considerably more difficult. It was very time-consuming to find out which procedural instructions were relevant to the tasks to be performed."

The BFU also points out that quality assurance and monitoring, including checks of the maintenance organisation by the LBA (the German regulator) were inadequate.

After starting the engines, the AFTER START CHECKLIST for flight crew apparently only contained the instruction that the lateral flight controls were to be checked for full deflection, but not for the correct direction of deflection.

The report illustrates the "causal chain" through the "Swiss Cheese Model" of James Reason. The "holes" that "line up" and allow the accident to happen are:

1. "Quality assurance: insufficient support of the work flow, misinterpretation of regulations";
2. "Documentation: complex, difficult-to-handle working documents; accomplished works was [sic] misdocumented";
3. "Mistakes: inverted connection of 2 pairs of wires on ELAC plugs";
4. "Test procedures: use of incorrect documentation wrongly accomplished tests; severity of action was not kept in mind";
5. "Flight Operation: Checklist are [sic] insufficient; aileron deflection

were [sic] not checked for correct deflection" leading to "Occurrence: "Serious Incident" Aircraft reacts inverted to the input of the left sidestick at the time of the take off".

These factors correspond roughly to the statement of causes and contributing factors.

In my [RISKS-21.48](#) note, I recounted my puzzlement engendered by the partial accounts then available, on the basis (a) that the plugs were standardised, and that (b) a mistaken wire-up on ELAC 1 would have caused command signals in the reverse sense to those detected by ELAC 2 and the three Spoiler Elevator Computers (SEC), and I felt this should have been detected by the aircraft monitoring systems.

Concerning (a), the report makes clear that the plug wiring was by no means standardised. The airplane belonged to a "transitional series" in which two wiring pairs were to be cross-connected, and the mechanics thought they should be connected straight-through, thanks to confusion over the appropriate wiring diagram.

Concerning (b), the control signal discrepancy - ELAC 1 sensing a "bank left" command and ELAC 2 and the three SECs sensing "bank right" - was not detected by the aircraft monitoring systems and displayed on the ECAM during test because the left sidestick was not tested. However, had CAP checked sidestick deflection during pre-take-off check, this discrepancy would surely have been triggered. Had only the first officer checked the

lateral controls, the discrepancy would not have shown. The report says that "according to statements of the crew, this check was accomplished pursuant to the valid procedures." I wonder whether the "valid procedures" require both pilots to perform pre-take-off flight control checks?

So the report leaves me still puzzled. If the CAP's sidestick had been moved in the direction of lateral control at any time before takeoff, then the two ELACs would have received contradictory sensor information, and ELAC No. 1 would have received sensor information contradicting that received by the three SECs. I also suppose that both pilots should to perform pre-take-off control checks, since sidestick operation is independent. So we are either to suppose that a standard comparison across multiple channels is not performed by the control system architecture, or else that CAP did not perform a control check before departure and therefore either the pre-take-off checklist procedures omit an important requirement not noted by the BFU, or that the crew lied about performing the check according to procedures. It would have been more satisfactory had the report sorted these possibilities out.

Peter B. Ladkin, University of Bielefeld, <http://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

Volume 23: Issue 25

Thursday 4 March 2004

Contents

- [Leap Year Strikes Again](#)
[Chuck Weinstock](#)
- [Pssst, wanna buy a spambotnet?](#)
[Rob Slade](#)
- [July 2002 air collision revisited](#)
[Michael Bacon](#)
- [Damaging consequences of response to password-protected viruses](#)
[Vassilis Prevelakis](#)
- [Spring '04 Sun Outage Notification](#)
[starband via Mich Kabay](#)
- [SPAM Countermeasures](#)
[Scott MacQuarrie](#)
- [Re: RFID tags in new US notes explode when you try to microwave them](#)
[Michael Borek responding to Paul Schleck](#)
- [And Another E-Voting Problem](#)
[David Bolduc via Dave Farber's IP](#)
- [Moseley Braun paper](#)
[Peter Zelchenko](#)
- [Avi Rubin on e-voting after yesterday's primary](#)
[Dave Brunberg](#)

- [Denial of service in criminal justice](#)
[Dick Mills](#)
 - [REVIEW: "Hiding in Plain Sight", Eric Cole](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Leap Year Strikes Again

<Chuck Weinstock <weinstock@sei.cmu.edu>>

Tue, 2 Mar 2004 18:36:45 -0500

I do not know the attribution for this:

"America's Railroads! Ya gotta love 'em!"

"I have learned from two separate sources that the original software

update-related outage scheduled for Sunday was indeed to be 1 1/2 hours.

Normal, anticipated work done by the computer was finished ahead of time

so the outage would have a minimal effect. In tests, the software was

found to function properly. They started the update, deleting the old

software and installed the new, and then...

It was Leap Year, and the date was 29 Feb 2004. Whoever wrote the new

software didn't take that into account, so nothing was working. Realtime

dispatching on the railroad, using a separate system, was not affected; but

the disabled system was down for more than four hours longer than originally

planned.

Perhaps related, perhaps not: BNSF, like Amtrak, has outsourced its IT

operation to a company which has in turn off-shored the work to

the other
side of the International Date Line; perhaps it should now be
caused India
Business Machines."

[Our local Y2K patch for Columbia-MM failed on 1 Jan 2004,
adding one
day to the date of each message in the summary listing. It
had already
been re-patched for 2001. PGN]

⚡ Pssst, wanna buy a spambotnet?

<Rob Slade <rslade@sprint.ca>>
Thu, 4 Mar 2004 13:39:18 -0800

You probably will have heard of the bickering going on between
the authors
of the Bagle, Netsky, and MyDoom virus families. (This type of
thing goes
on all the time. Frequently the insults are directed at virus
researchers
and antivirus companies. I haven't yet been libeled in a virus:
the vxers
prefer to use Amazon to put up "reviews" of my books :-)

The fight made the front page of our local paper, *The Vancouver
Sun*, this
morning, albeit below the fold.

[http://www.canada.com/vancouver/vancouver_sun/news/story.html?
id=41657381-
15b6-449b-bbfa-9f2de1ff80ec](http://www.canada.com/vancouver/vancouver_sun/news/story.html?id=41657381-15b6-449b-bbfa-9f2de1ff80ec)

The article is a bit over the top in places, referring to "the
first cyber
struggle for world domination of the Internet."

The assertion that most concerns me is:

"At stake are vast armies of Internet-connected computers that virus makers are trying to control. Once under their control, they sell access to the computers to spammers, who use them to send out a constant barrage of junk mail."

We know that a large number of recent viruses and worms install limited backdoors into the machines that they infect. We also know that a very large proportion (most, according to some studies) of spam is coming from individual machines, and therefore probably distributed nets. The article later goes on to point out that the recent trend towards having "expiry dates" in a number of viruses can be interpreted as an attempt to ensure that the networks of infected machines can only be used for a limited time, thus creating a renewable market.

All of this does suggest that virus writers are creating such networks, and the recent discoveries out of Germany do confirm that attempts are being made to market spamming nets.

I doubt that the trend will continue for long.

vxers will undoubtedly continue to create networks of backdoored machines.

For one thing, it provides a terrific means for "seeding" your creation out into the world. (MyDoom, Bagle, and Netsky have all enjoyed "instant" success out of any proportion to their design.)

But virus writers have never been able to get along with anyone,

including
each other. (I think I can safely make this assertion in view
of the
current fight going on.) This characteristic is somewhat
detrimental to
getting a business organized.

At this point, I think the "selling to spammers" business is
working, but
not very structured. Soon the vxers will start to realize that
you have to
advertise in order to get work, and contact your customers in
order to get
paid.

In the meantime, I suppose that law enforcement types could
round up more
than a few vxers with sting operations ...

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)

✈ July 2002 air collision revisited (Cox, [RISKS-23.23](#))

<"Michael \ (Streaky\) Bacon" <himself@streaky-bacon.co.uk>>
Wed, 3 Mar 2004 07:35:55 -0000

In [RISKS 23.23](#), Paul Cox wrote: "The specific scenario that was
predicted, and which apparently happened in the Switzerland
crash, was
this: Two aircraft are in conflict. Their TCAS systems activate
and
proscribe a course of action for each aircraft which, if
followed,
should separate them."

Surely the course of action is prEscribed, not prOscribed?

"In the worst-case scenario, the TCAS tells one plane to climb and another

to descend; ATC tells the first plane to descend and the pilots follow

THAT instruction, which only makes matters worse as both planes are now

trying to descend below the other. Planes smack, everyone in the air dies."

I must be missing something. Surely this is the "pass to starboard"

scenario designed to avoid collisions at sea? If one plane is commanded to

climb and the other to descend, they will not (assuming immediacy of commit) collide.

"Unfortunately, the possibility for confusion still exists. In this case,

it was probably exacerbated by the fact that the Russian plane's pilots

came out of an aviation system which heavily emphasized ground control and

discouraged pilots making "their own call" in the air; the Russian pilots

were (apparently) predisposed to follow the ATC instructions instead of

the TCAS instructions."

It was reported at the time that Russian pilots are trained (rather than

"discouraged") to ignore the TACS - which accords with the old Soviet air discipline in general.

It has also been my experience, and that of many pilots flying internationally, that many Russian pilots have an apparently poor command of

English. As those who speak more than one language can relate to, this can

be easily exacerbated by stress. I was in the jump-seat of a British Airways 757 bound for Rome when the crew became aware that there were severe misunderstandings between an Aeroflot captain and an Italian ATC controller (with a thick accent). Our captain begged permission to assist and during a 40 minute period acted as liaison and interpreted the ATC instructions to the Aeroflot captain. The aircraft landed safely and our captain entered a report on the incident. Later that same week, a similar tale was related to me by another BA captain of a common-language communications failure off the coast of North Africa involving another Aeroflot captain and a Moroccan ATC controller.

There is an ever present RISK stemming from any lack of fluency in the language of ATC in circumstances of both normality and stress.

✶ Damaging consequences of response to password-protected viruses

<Vassilis Prevelakis <vp@mcs.drexel.edu>>

Wed, 3 Mar 2004 10:47:58 -0500 (EST)

A new variant of password-protected viruses is circulating, I won't bother you with the details as you are probably well aware of them by now. What is dangerous in my mind is the response to such viruses: for example, Drexel's computer support decided unilaterally to remove all password protected

attachments:

"This morning, Drexel IRT has configured the central mail antivirus scanners to remove all attachments which require a password to open them."

Mercifully they do not do that, they only remove password protected ZIP files. However, if people just go and ahead and remove any encrypted attachment, then that will cause severe disruption to secure communications over e-mail.

I think we should resist such efforts and prevent the spammers and virus writers do to us what the government failed to do.

Vassilis Prevelakis, CS Dept. Drexel University

✶ Spring '04 Sun Outage Notification (via Mich Kabay)

<memberservices@starband.net>

Tuesday, March 02, 2004 15:15

Dear StarBand Member,

What is a sun outage? The sun never goes out! Well that is not what we are referring to. A sun outage is what happens when the sun positions itself directly behind and in line with your satellite antenna and the satellite in the sky.

How does that cause an outage? The reference to an "outage" is when your satellite antenna cannot hear the signal from the satellite. The satellite

signal did not go away, but the sun overpowered your receiver with "noise".

Look at it this way, imagine you are at a party trying to hear a story your friend is telling you, but the guy next to you is shouting. Your friend is still talking to you, but because of the shouting, all you hear is "noise".

Sun outages usually occur two times a year, in the spring and the in the fall. The time and length of the outage varies from day to day and depends upon where in the United States you live, but will occur for only a few minutes at a time.

If you live in Atlanta and your StarBand system is looking at the satellite AMC-4 (99-101 degrees) you may experience the event on March 2nd from 2:02 PM until 2:06 PM and again on the 4th, 5th, 6th, and 7th at about the same times.

Since Telstar 7 (129 degrees) is at a different place in the sky than AMC-4, the first sun outage in Atlanta when looking at this satellite will be from 3:08 PM to 3:10 PM from March 5th to March 6th.

The duration of the outage will start out short and build to a peak of about 7 to 8 minutes at a time, then diminish as the days go by. Again, this is an example based on a satellite antenna positioned in Atlanta, Georgia.

For all other StarBand customers within the continental United States, these sun outages may occur between March 2nd and March 7th. The time of day

depends upon your location in the US and which satellite your system is using. For customers in Hawaii, these outages may occur between March 8th and March 13th.

Please be patient and bear with us, as we have no control over this natural phenomenon. Thank you.

The StarBand Team

✶ SPAM Countermeasures

<Scott MacQuarrie <scott@zwcx.com>>
Tue, 02 Mar 2004 23:52:55 -0500

I am surprised at some of the ideas put forward to prevent spam and feel many of them, such as charging for e-mail, are worse than the problem itself. Ultimately, this is matter of using definitions to focus on the actual problem, rather than trying to apply massive architectural changes to "carpet-bomb" the problem.

By definition, spam is simply e-mail from unidentified sender (s). The solution is to require senders to identify themselves, either by e-mail address or domain before accepting their e-mail. There is no need to filter e-mail from people you know or domains you trust. It's strangers you need to watch.

Anti-spam lists, such as the Blackhole list and others are following this

strategy, but offering to act as an intermediary. The better, and simpler, solution is at the individual layer, using tools such as choicemail from Digiportal. (Note: I am simply a satisfied customer and, in no way represent the company). This tool filters e-mail, based on if I allowed them or their domain to e-mail me. If you are not know, you are sent an e-mail asking who you are. The response (via digiportal's website - a trusted URL) is sent to me and I can decide if I want to receive it. If you never respond, your e-mail is quietly deleted. For mailing lists, such as this one, I can authorize the domain or the individual e-mail address in advance. During the installation, It also happily reads my address file and adds anyone found there to the authorized list (since I obviously know them).

After using this tool for almost a year, I have enjoyed a spam-free existence. This has also not required a significant architectural change or additional billing models to implement. This is simply the implementation of the same process used if you ring my doorbell. If I don't know you, I may not answer it.

Of course, I still have the bandwidth of the e-mail being sent, but this is my ISP's problem, not mine.

Scott MacQuarrie, ZWCX Computer Corp.

🔥 Re: RFID tags in new US notes explode when you try to

microwave them

<mikkeles@netscape.net (Michael Borek)>

Thu, 04 Mar 2004 15:02:07 -0500

I received the following in reference to my submission in [RISKS-23.24](#).

[RISKS received a large number of similar debunkings: Most of the bills depicted were old-style, there is no RFID tag, no bump in the vicinity of Andrew Jackson's right eye, etc. I did not believe it either, but thought I'd see what responses it inspired. Thanks to all of you whose contributions I did not include. PGN]

In response, I didn't believe or disbelieve the story. The main point I intended was a risk of the rumour that one can microwave RFIDs to destroy them. Coupled with a belief that the notes contain RFIDs (I understand some countries are at least considering this), this could lead to some less than safe activities.

If, as Mr. Schleck states, a bundle of new US\$20 notes can set off anti-theft systems because of the contained metal, I can see other risks:

- * Thieves targetting those who set off an anti-theft system but who are not detained by store security (customer risk)
- * 'the boy who cried wolf' syndrome leading to only cursory checks of those who set off an anti-theft system (store risk)

What would be the effect on anti-theft systems of carrying about a handful of iron filings or chopped steel wool? Could this become an interesting version of DoS (denial of service)?

Michael Borek

"Paul W. Schleck" <pschleck@novia.net> wrote:

>It was not clear from the RISKS submission whether or not the story was
>believed by the submitter (or the editor, for that matter). Several
>people have debunked the assertion that RFID tags are in current
>U.S. currency. Even if they existed, microwaving such RFID tags (often
>with resonant frequencies much lower than microwave) might not disable
>them. Debunking links include:
>
><http://frank.geekheim.de/archives/000684.html>
><http://slashdot.org/comments.pl?sid=98942&cid=8437731>
><http://slashdot.org/comments.pl?sid=98942&cid=8438208>
>
>The explanation for what happened is that current U.S. notes, including
>the new \$20 bill, have metallic content. Stacking a large number of
>them could set off anti-theft systems, or cause large burn marks in the
>metallic regions of the notes when microwaved.
>
>Paul W. Schleck

✶ And Another E-Voting Problem (via Dave Farber's IP)

<David Bolduc>

Tuesday, March 02, 2004 12:47 PM

One that hadn't occurred to me, but should have:

<http://www.instapundit.com/archives/014431.php>

UPDATE: Athena Runner e-mails from California:

My husband and I went to vote this morning at 7 a.m. in Carlsbad, CA (San Diego County) and the new and improved *cough* electronic voting system wouldn't boot up. I went back twice and at 8 a.m., they still weren't working. Apparently it's a sporadic problem county wide.

When voter turnout is so low already, forcing people to try and come back multiple times is a huge problem. I miss my paper ballot.

Bryon Scott also e-mails:

At least the machines in Maryland are working. Here in San Diego the local radio stations are reporting that more than a dozen areas in the county can't even get the machines up and running.

Paper always works.

ANOTHER UPDATE: Reader Bruce Bender e-mails:

New voting machines were down in at my polling place in Oceanside, CA (next door to Camp Pendleton). Many people here leave for the day to work in San Diego and Orange and will either try again tonight or not vote. It is a strange feeling to be denied the chance.

Several other readers are reporting problems in various locales. You can't expect any system to work perfectly, of course, but this really doesn't seem ready for prime time.

IP Archives at: <http://www.interesting-people.org/archives/interesting-people/>

✶ Moseley Braun paper

<Peter Zelchenko <pete@chinet.com>>

Wed, 18 Feb 2004 04:31:42 -0600 (CST)

Since Carol Moseley Braun has dropped out of the presidential race, it's safe for me to put out the draft of her position paper on voting systems:

http://chinet.com/~pete/Article_11-11-03.rtf

As it was my draft, Carol didn't have an ounce of input on this paper. She was to go to Georgia with voting systems in her platform, but she never found time for it. In fact, this paper is primarily a provider of background for the public and concludes with my own prejudices about electronic voting. Therefore, it should be interesting to this community as it comes from the perspective of a technological conservative.

Over the years, after too many hours logged troubleshooting polling places in minority areas rife with both low machine competency and election fraud, and having sat in on a lot of discussions about what to do about the undervote crisis, absentee balloting, fraud, and so on, I have to say I am even more reluctant than most about the prospect of putting computers into

every booth. I am still struggling with how to express this.

As an initial exercise into these questions, I obtained some punch systems from the Chicago Board of Elections and threw together a rudimentary feedback-enhanced punch booth, employing a few flip-flops set by punching through with a micro-mini phone plug (replacing the stylus), which flip-flops drive colored LEDs on a bigboard in front of the voter. With a few pennies invested, a part of the punch feedback problem was solved.

This is obviously not a real solution, since it operates on a fundamentally flawed concept. Punch, while to a great degree implemented with astonishing elegance, loses all credibility, in my opinion, at the die-cutting operation, in which a printer must make 2,000 precise incisions into a small card. Its second major flaw is the fact that the text is not displayed on the ballot. Enough is enough: It's long since time for punch to retire. But the exercise demonstrates that the technology we need to solve the problems may be far simpler than we think.

Setting punch aside, paper as a source document should not be discarded out of hand. Obviously, the DRE companies are eager to bury paper, but my belief is that we cannot improve on it in the booth. I sat for two days with a sketch pad attempting to devise a foolproof scrolling and selection metaphor using what I felt were solid principles of industrial and interface design. This was after reviewing a spate of elegant looking but woefully

inadequate, deeply flawed interfaces by even well-funded names like Diebold and Hart. I couldn't come up with something that approached the rudiments of pen contacting paper.

I decided that a combination platform of hand-marked optical (for 90% of the population) should be coupled with computer-aided booths (for the remainder) which print out ballots for optical reading; hand-marked ballots should be scannable and reviewable by any voter if he or she so chooses, and possibly even committed to tabulation by the voters themselves. My efforts led me to conclude that a proper solution must assume a consistent rendering of the ballot, whether a voter is marking the ballot by hand, it is being displayed on a DRE, or it is being reviewed on some reviewing device. How in the world?

What is interesting about this usability problem is that it involves such surprisingly simple stimulus and feedback atoms - the basic checkbox or radio-box metaphor - but they must be executed on a potentially very complex display and selection plane, calling for either paging or scrolling. Multiple selection, deselection, reselection is a huge additional problem, possibly unsolvable in two dimensions without a dialog. The interface needs to be instantly and plainly usable by every voting-age individual. The device must be highly configurable.

Elevator, vending machine, microwave, cash station, VCR - a voting system is unprecedented in its demands, and we are attempting to solve all of the

demands in too short a period. This is not a place where experimentation should be welcome. Feeling rushed, everyone is grasping at replicating the historical experience on screen rather than coming up with something new that works.

I hope to elaborate on this when time permits.

I also want to thank David Dill, Rebecca Mercuri, Doug Jones, Avi Rubin, and Lorrie Cranor for the successful phone conference we had with Moseley Braun and Bruce Crosby back in October.

Peter Zelchenko (pete@chinet.com) 1-312-RED-BIRD <http://chinet.com/~pete/>

✶ Avi Rubin on e-voting after yesterday's primary

<"Dave Brunberg" <DBrunber@FBLEOPOLD.com>>
Wed, 3 Mar 2004 13:07:50 -0500

Avi Rubin's experiences as an election judge in Baltimore yesterday both relaxed and confirmed some of his fears about electronic voting. He came out of the experience with the impression that the Diebold systems are still flawed, but with greater faith in the other election judges he worked with.

Whole story here: <http://www.avirubin.com/judge.html>

Denial of service in criminal justice

<Dick Mills <RMills@nyiso.com>>

Wed, 3 Mar 2004 12:58:40 -0500

Elliot Spitzer, Attorney General of New York was interviewed on the radio this morning about the potential prosecution of Jason West, mayor of New Paltz, who has been performing same-sex marriages. Mr. Spitzer said, "Although this case is important, we have many other cases more important, involving violence, child abuse and so on. We can't prosecute them all."

The statement made me think immediately of denial-of-service hacker attacks. It suggests that elected officials could arrange for the prosecutor's office to be permanently overloaded so that those officials could steal without fear of being prosecuted; even if caught.

However, Mr. Spitzer's very next statement suggested the cure for the problem. He said that if abuses become serious enough that his office makes exceptions to the priorities. It might make an example of an abuser to send a signal to others. Of course, the radio interview itself was sending just such a signal.

Human institutions utilize adaptability, psychology and publicity. Try to imagine a Web server changing it's priorities, or launching retaliatory attacks, or of making public threats. That level of machine intelligence is not in the foreseeable future (thank goodness.)

There is a risk if we expect the security of unsupervised machines, regardless of design, to be comparable to human institutions.

REVIEW: "Hiding in Plain Sight", Eric Cole

<Rob Slade <rslade@sprint.ca>>

Thu, 4 Mar 2004 08:25:42 -0800

BKHDPLST.RVW 20031205

"Hiding in Plain Sight", Eric Cole, 2003, 0-471-44449-9,
U\$35.00/C\$53.95/UK#24.50

%A Eric Cole

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2003

%G 0-471-44449-9

%I John Wiley & Sons, Inc.

%O U\$35.00/C\$53.95/UK#24.50 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0471444499/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0471444499/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0471444499/>

[robsladesin03-20](#)

%P 335 p. + CD-ROM

%T "Hiding in Plain Sight"

Part one explores the world of covert communication. Chapter one suggests that covert communication is all around us, but weakens its case by providing only fictional examples. The author also states that he has detected huge numbers of files which contain embedded steganographic materials. He doesn't seem to understand that this hurts his argument: what

good is steganography if you can detect its effects? There is a confused and incomplete introduction to cryptography in chapter two. To be fair, it does make some good practical points, such as the difference between an algorithm and an implementation. The basics of steganography are provided in chapter three but the explanations and examples may not make clear the distinction between steganography and covert channels or codes. The definition and illustration of digital watermarking, in chapter four, does not present a rationale as to why the invisible marking data cannot be removed. The example is confused and unconvincing.

Part two is supposed to take us into the hidden realm of steganography. Chapter five outlines miscellaneous computer crimes and intrusions with only the most tenuous ties to steganography, fabricated by the author. A list of steganographic programs (almost all of the insertion type) are provided without details in chapter six. There are more examples of the same illustrations, a couple of related programs, and some mislabelled figures (a graphical layout of an IP header rather than the promised sniffer example) in chapter seven. Cole uses an instance of hiding a virus with steganography, but the dangers of inventing your own cases becomes evident: the virus, as described, wouldn't work anymore.

Part three purports to show you how to make your own communications secure. Chapter eight lists cryptanalytic and steganalytic techniques, but does not delineate them well. A rehash of previous ideas and weak examples

substitutes for the strategy promised in chapter nine: the main illustration has a complete failure of forward secrecy. Chapter ten pledges that steganography will get better.

Although Cole is more entertaining than Katzenbeisser and Petitcolas manage to be in their "Information Hiding Techniques for Steganography and Digital Watermarking" (cf. BKIHTSDW.RVW), his information is sketchy and suspect. In comparison, his work is little more than a pamphlet.

copyright Robert M. Slade, 2003 BKHDPLST.RVW 20031205
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

Volume 23: Issue 26

Monday 8 March 2004

Contents

- [U.S. Senate security shenanigans](#)
[Kristina Herrndobler](#) via [James Bauman](#)
- [PFIR Conference Announcement: "Preventing the Internet Meltdown"](#)
[PFIR](#)
- [Yet another worm masquerades as Microsoft update](#)
[NewsScan](#)
- [The price of e-mail is constant vigilance](#)
[Rob Slade](#)
- [Firms look to limit liability for online security breaches](#)
[Jonathan Krim](#) via [Monty Solomon](#)
- [Smartcards weren't so smart after all, says Target](#)
[NewsScan](#)
- [BBC reports card cloning scam](#)
[John Sawyer](#)
- [An interesting airplane user interface](#)
[David Magda](#)
- [Re: Legal Mercedes driver jailed for 18 months](#)
[David Gillett](#)
- [Extended Call for Papers: Voting, Elections, and Technology](#)
[Micah Altman](#)

 [Info on RISKS \(comp.risks\)](http://comp.risks)

U.S. Senate security shenanigans

<"James Bauman" <James.Bauman@safety-kleen.com>>

Fri, 5 Mar 2004 13:41:26 -0500

If an independent or Justice Department investigation occurs beyond the one by the U.S. Senate sergeant-at-arms, the security issues (and their possible accompanying illegal and/or unethical issues) should be interesting to read about. Right now, there are a lot of questions about the incident and not much clarity.

According to a **Chicago Tribune** article, a Senate Republican clerk, Jason Lundell, watched a system administrator gain access to Democratic folders on a network. Then, Mr. Lundell, repeated the administrator's actions and "downloaded more than 4,670 files" from those folders. Lundell gave the files to Manuel Miranda, who was a staffer for Majority Leader Bill Frist (R-Tenn.). Lundell said "Miranda told him that it was common knowledge that staff could access each other's files". [Then, I suppose?... Republican staffers could access Democratic files and Democratic staffers the Republican ones.]

A Question" If each side could look at each other's files, then why did Jason Lundell need special knowledge about network security to download the

files?

Regarding this: "Republican committee Chairman Sen. Orrin Hatch of Utah condemned the actions of the staff members, who no longer work for the Senate." "'I am mortified that this improper, unethical and simply unacceptable breach of confidential files occurred," Hatch said Thursday as he released the report. "There is no excuse that can justify these improper actions.'"

Later in the article is this: "Furthermore, Mr. Lundell recalled that Mr. Miranda had told him that Sen. Hatch wanted the staff to use any means necessary to support President Bush's nominees," the sergeant-at-arms reported.

Seems that the two Republican staffers took "any means necessary" in the most literal of senses, and Lundell's assertion in the previous paragraph could be an embarrassment for Hatch given Hatch's latest statements of outrage.

Anyway, it's got the earmarks of a good future read as more facts develop and the smoke clears.

Source: Kristina Herrndobler, GOP staffers accused of taking senators' files, *Chicago Tribune*, 5 Mar 2004

<http://www.chicagotribune.com/news/nationworld/chi-0403050231mar05,1,7561874.story?coll=chi-news-hed>

PFIR Conference Announcement: "Preventing the Internet Meltdown"

<PFIR - People For Internet Responsibility <pfir@pfir.org>>

Sat, 06 Mar 2004 18:14:43 -0800

PFIR Conference Announcement
"Preventing the Internet Meltdown"
Spring/Summer 2004
Los Angeles, California, USA
<http://www.pfir.org/meltdown>

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

[To subscribe or unsubscribe to/from this list, please send the command "subscribe" or "unsubscribe" respectively (without the quotes) in the body of an e-mail to "pfir-request@pfir.org".]

People For Internet Responsibility (PFIR) is pleased to preliminarily announce an "emergency" conference aimed at preventing the "meltdown" of the Internet -- the risks of imminent disruption, degradation, unfair manipulation, and other negative impacts on critical Internet services and systems in ways that will have a profound impact on the Net and its users around the world.

We are planning for this conference (lasting two or three days) to take place as soon as possible, ideally as early as this coming June, with all sessions and working groups at a hotel in convenient proximity to Los Angeles International Airport (LAX).

A continuing and rapidly escalating series of alarming events

suggest that immediate cooperative, specific planning is necessary if we are to have any chance of avoiding the meltdown. "Red flag" warning signs are many. A merely partial list includes attempts to manipulate key network infrastructures such as the domain name system; lawsuits over Internet regulatory issues (e.g. VeriSign and domain registrars vs. ICANN); serious issues of privacy and security; and ever-increasing spam, virus, and related problems, along with largely ad hoc or non-coordinated "anti-spam" systems that may do more harm than good and may cause serious collateral damage.

All facets of Internet users and a vast range of critical applications are at risk from the meltdown. Commercial firms, schools, nonprofit and governmental organizations, home users, and everybody else around the world whose lives are touched in some way by the Internet (and that's practically everyone) are likely to be seriously and negatively impacted.

Most of these problems are either directly or indirectly the result of the Internet's lack of responsible and fair planning related to Internet operations and oversight. A perceived historical desire for a "hands off" attitude regarding Internet "governance" has now resulted not only in commercial abuses, and the specter of lawsuits and courts dictating key technical issues relating to the Net, but has also invited unilateral actions by organizations such as the United Nations (UN) and International Telecommunications Union (ITU) that could profoundly affect the Internet and

its users in unpredictable ways.

Representatives from commercial firms, educational institutions, governmental entities, nonprofit and other organizations, and any other interested parties are invited to participate at this conference. International participation is most definitely encouraged.

The ultimate goal of the conference is to establish a set of *specific* actions and contingency plans for the Internet-related problems that could lead to the meltdown. These may include (but are not limited to) technical, governance, regulatory, political, and legal actions and plans. Scenarios to consider may also include more "radical" technical approaches such as "alternate root" domain systems, technologies to bypass unreasonable ISP restrictions, and a wide range of other practical possibilities.

It is anticipated that the conference will include a variety of panels focused on illuminating specific aspects of these problems, along with potential reactions, solutions, and contingency planning for worst-case scenarios. Breakout working groups will be available for detailed discussion and planning efforts. Formal papers will not be required, but panel members may be asked to submit brief abstracts of prepared remarks in advance to assist in organizing the sessions.

The ability of this conference to take place, and necessary conference details such as the specific program, costs, etc. will depend largely on the response to this announcement and particularly on the number of persons and

organizations who express a potential interest in attending.

If you may be interested in participating (no obligation at this point, of course) or have any questions, please send an e-mail as soon as possible to:

meltdown@pfir.org

or feel free to contact Lauren at the phone number below. As appropriate, please be sure to mention how many people from your organization may be interested in attending. If you express an interest in attending, you will be added to a private mailing list for upcoming announcements regarding this conference unless you ask not to be so notified.

Together, we may be able to stop the Internet meltdown. But we need to act now.

Thank you for your consideration.

- - -

Lauren Weinstein

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

Tel: +1 (818) 225-2800

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

Co-Founder, Fact Squad - <http://www.factsquad.org>

Co-Founder, URIICA - Union for Representative International Internet

Cooperation and Analysis - <http://www.uriica.org>

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

Member, ACM Committee on Computers and Public Policy

<http://www.pfir.org/lauren>

Peter G. Neumann

neumann@pfir.org or neumann@csl.sri.com or neumann@risks.org

Tel: +1 (650) 859-2375

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

Co-Founder, Fact Squad - <http://www.factsquad.org>

Co-Founder, URIICA - Union for Representative International Internet

Cooperation and Analysis - <http://www.uriica.org>

Moderator, RISKS Forum - <http://risks.org>

Chairman, ACM Committee on Computers and Public Policy
<http://www.csl.sri.com/neumann>

David J. Farber

dave@farber.net

Tel: +1 (412) 726-9889

Distinguished Career Professor of Computer Science and Public Policy,

Carnegie Mellon University, School of Computer Science

Member of the Board of Trustees EFF - <http://www.eff.org>

Member of the Advisory Board -- EPIC - <http://www.epic.org>

Member of the Advisory Board -- CDT - <http://www.cdt.org>

Member of Board of Directors -- PFIR - <http://www.pfir.org>

Co-Founder, URIICA - Union for Representative International Internet

Cooperation and Analysis - <http://www.uriica.org>

Member of the Executive Committee USACM

<http://www.cis.upenn.edu/~farber>

(Affiliations shown for identification only.)

⚡ Yet another worm masquerades as Microsoft update

<"NewsScan" <newsscan@newsscan.com>>

Mon, 08 Mar 2004 09:23:00 -0700

The latest variation on the Sober worm -- Sober.D -- tries to trick recipients into opening it by disguising itself as a Microsoft Update

message. "It arrives in an e-mail that pretends to be a patch to protect against a version of MyDoom," says a senior consultant at antivirus firm Sophos. "The e-mail appears to be a Microsoft patch so people will of course double-click on that attachment." Once a user clicks on the file, the worm scans the PC to see if it's already infected -- if not, it installs itself and uses its own SMTP engine to send copies of itself to e-mail addresses found on the victim's PC. Microsoft emphasizes that it does not send patches via e-mail and that users should ignore such messages. [ZDNet 8 Mar 2004; NewsScan Daily, 8 Mar 2004]
http://zdnet.com.com/2100-1105_2-5171243.html

✶ The price of e-mail is constant vigilance

<Rob Slade <rslade@sprint.ca>>
Sat, 6 Mar 2004 16:37:18 -0800

Peter Wilson's article on spam and viruses (on Saturday, March 6, 2004) lists a number of antispam measures that are currently being promoted. He also retails Bill Gates' confident prediction that spam will be a thing of the past by 2006. Remember that prophecy, because Bill Gates is going to be proven wrong. An examination of the measures listed in the article demonstrates why.

SPF (sender-permitted format) is currently garnering the greatest interest.

The description of SPF as a kind of caller-ID is not quite correct. All e-mail carries caller-ID in the form of the information about who the message is from, and information about the Internet Protocol (IP) address that originated the message. SPF is actually an attempt to contact the site that is supposed to have originated the message, and verify that these two pieces of information match, or, at least, are likely. Spammers, when creating spoofed addresses, don't bother to make sure that they do. Or, at least, they haven't up until now.

Microsoft's own version seems to be either an attempt to compete or an attempt to derail SPF: SPF is primarily promoted by AOL, and the two companies have never played particularly well together. Microsoft's plan is derided by the SPF camp for being proprietary. It is true that SPF uses features and functions that make more effective use of the e-mail protocols that are currently in use on the Internet. The configuration of factors is not universal, though, and some of the activities will require new programming for everyone who participates in SPF. Which may mean that the Internet might become split into the camp of those who use SPF, and those who don't.

I have seen this in action already. I have a number of accounts. (And, of course, get tons of spam.) One is through Vancouver CommunityNet, which does not have very much in the way of spam detection or prevention. Because of the volume of spam this account receives (particularly during

the Sobig
flood last summer), I forwarded the account to a service that
does spam and
virus filtering. One of the functions that the service uses is
similar to
the SPF protocol. A great deal of the spam that was being
forwarded was
unverifiable, and so the service simply refused to accept it.
This meant
that a volume of e-mail built up on Vancouver CommunityNet, to
the point that
it affected the mail system as a whole. (Vancouver
CommunityNet, despite
being informed of all the details, and my own actions to rectify
the
situation, has handled the whole matter in a very sloppy manner.)

SPF has promise, and it may be possible (unlike the Microsoft
proposal) to
provide workarounds for a variety of systems, platforms, and
applications.
However, there are a number of issues that still have to
resolved, such as
e-mail aliases, third-party services, and applications such as
mailing lists,
which operate in a wide variety of forms. The difficulties are
not
insurmountable, but an enormous amount of work still has to be
done.

Microsoft's micropayments strategy is apparently the most recent
one, but
has been raised many times over the history of the nets. (One
of the
popular programs providing Usenet news, a type of topical
discussion, used
to remind anyone who attempted to post a message that it would
possibly cost
thousands of dollars to send this to everyone: did they really
want to do
that?) Unfortunately, the issue of mailing lists comes up almost
immediately. Even if we assume one cent per message, if I send
a message to

a popular list such as the RISKS-FORUM Digest, with a possible hundred thousand subscribers, am I charged a thousand dollars for that message? Is the list moderator charged? In the case of RISKS, it is also redistributed by a number of sub-mailing lists: do those costs get charged to the accounts of the local administrators? The list moderator? Me?

(The obvious second question is: who *gets* the money? The Internet Engineering Task Force? Some bloated bureaucracy parcelling out the cash to the various national telecom carriers? Charity? Microsoft? The recipient? Hmm. Maybe I should rethink my objection to the micropayment system. At one point I was getting 8,000 [yes, eight thousand] copies of spam from one system in China. Per hour. Same message.)

And, of course, in order to provide for such a micropayment system, everybody is going to have to use a Microsoft mailer. With a Microsoft payment system. And a Microsoft account. This sounds like an attempt to resurrect the (justly derided and roundly condemned) Passport and Palladium systems.

The challenge-response system is already being used by a number of outfits providing spam filtering and other services. It is a nuisance. It can create a great deal of annoyance in a number of situations, not least being mailing lists.

It also doesn't work. The most common challenge response systems present a graphical image of a word. This word is supposed to be entered

in a field
on a web page in order to create permission for the message to
go through.
People can read the word easily, but machines have difficulty
with this type
of task, so this makes it impossible for spammers to automate
the sending of
e-mail: they have to read and respond to every challenge.

That's the theory. In fact, spammers have already been found to
be
"automating" the process--using Internet web surfers. A number
of web pages
have been set up promising access to pornography. In order to
access the
files, you have to respond to a challenge. The challenges are,
of course,
those that are being presented on the antispam filtering sites.
Those
challenges are simply extracted, presented to the surfers
wanting access to
pornographic images, solved by the user, and the solution fed
back to the
antispam site. The same problems apply to computational
puzzles: they are
simply another form of challenge-response.

In fact, most of these antispam technologies fail in the face of
the problem
of spam nets set up by viruses. Spam sent from infected
machines could
simply use the name of the owner, thus verifying the identity.
Spam sent
from infected machines could use the micropayment "wallet" on
the infected
machine, thus creating not only problems of clean-up for the
owner, but also
a real cost. Infected machines could be used to crack
computational
puzzles, or the owner could be presented with challenges to
respond to, in a
variety of ways.

Spam has passed the stage of being a nuisance. E-mail is a means of communication that is starting to rival the phone, and spam is seriously degrading the effectiveness and utility of e-mail. Antispam measures are badly needed, but we cannot accept any proposed solution uncritically. Dividing the Internet into isolated camps of incompatible (and rival) antispam technologies takes us back to the early days of online systems, when lots of people had e-mail, but nobody could talk to each other.

There is no easy fix, and there is no easy answer. Administrators have to ensure that they are not providing open relays that can be used for spam. E-mail filtering services are checking for inappropriate inbound e-mail, but must also check what is going out. ISPs (Internet Service Providers) must be more vigilant in regard to the use being made of the net to which they provide access. Computer users at all levels have to check for malicious software, unpatched vulnerabilities, open ports and services, and what is going out of their systems as well as what is coming in. Everybody needs to become more aware of what is going on, and keep up with the changes in threats around us all.

And anyone who tells you it is not going to be painful is selling something.

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>

✦ Firms look to limit liability for online security breaches (Krim)

<Monty Solomon <monty@roscom.com>>

Fri, 5 Mar 2004 09:30:15 -0500

Firms Look to Limit Liability for Online Security Breaches
Jonathan Krim, **The Washington Post**, 5 Mar 2004; Page E01

In the face of ongoing attacks by computer hackers, some companies that store their customers' personal data are adopting a new defensive tactic: If your information is stolen, they're not legally responsible. Across the Internet, retailers and other service providers that handle consumer transactions are requiring customers to agree to waive any right to sue the companies if the businesses are hacked, regardless of how secure their systems are. The waivers are contained in lengthy terms-of-use agreements that consumers often click to accept without reading closely. ...

<http://www.washingtonpost.com/wp-dyn/articles/A31874-2004Mar4.html>

✦ Smartcards weren't so smart after all, says Target

<"NewsScan" <newsscan@newsscan.com>>

Thu, 04 Mar 2004 10:33:54 -0700

Target is phasing out the computer chips embedded in its branded Visa cards

less than three years after they were first introduced, citing "limited use" by shoppers. The technology allowed cardholders to download coupons from the Internet or in-store kiosks in order to receive discounts on merchandise, but few customers took advantage of the feature. Only 3.5% of Americans 18 years or older said they had used a smart payment card like Target's, according to a survey conducted by Financial Insights in March 2004. John Gould, director of consumer lending and bank cards at TowerGroup, says Target had been on the right track with its smartcard rollout and perhaps was overhasty in its decision to curtail the program. "I don't think they gave it time to mature," he says. [Reuters, 3 Mar 2004; NewsScan Daily, 4 Mar 2004]

http://www.reuters.com/newsArticle.jhtml;jsessionid=__JPT5K1DAV2VEACRBAEKSFEY?type=technologyNews&storyID=4491160§ion=news

⚡ BBC reports card cloning scam

<John Sawyer <jpgsawyer@btopenworld.com>>
Fri, 5 Mar 2004 14:28:34 +0000 (GMT)

The BBC is reporting that a Automatic Teller Machine Scam that records card and password details to allow card cloning is spreading in Cardiff and other parts of West Wales.

<http://news.bbc.co.uk/1/hi/wales/3535473.stm>

Risks has seen this kind of thing before but perhaps not to this

level of
sophistication.

Dr John Sawyer, Department of Mechanical and Design Engineering
University of Portsmouth

✶ An interesting airplane user interface

<David Magda <dmagda@ee.ryerson.ca>>

Sat, 6 Mar 2004 08:50:20 -0500

I found the following anecdote in Edward Tufte's message board:

http://www.edwardtufte.com/bboard/q-and-a-fetch-msg?msg_id=0001G1&topic_id=1&topic=Ask%20E%2eT%2e

Alan Kay and User Interfaces

I attended the course in Boston yesterday, and enjoyed it very much. Made

me think about the following story which might spur some discussion or

comments here. It seems related to the overall theme here.

In 1985 I attended an OOPSLA (Object oriented programming languages ...)

conference. Alan Kay (PARC/Smalltalk/ Apple/Macintosh/...) gave a

presentation. Alan told the following true story:

He once flew down to Mexico on vacation, to some lonely place on the

California peninsula for surfing etc. A pilot was supposed to come in a

week to pick him up at a rural landing strip. Alan got there on time,

waited, and eventually the plane, an older DC3, came. When Alan entered

the plane he noticed that almost all the instruments had been

unscrewed

from the panels, pulled out and twisted around in various positions, and

were basically standing (or waving) on their cable hoses like flowers on

their stems. He got worried, considered exiting the plane, but decided to

stay. The pilot, a younger fellow, seemed trustworthy.

When the plane had reached cruising altitude and speed Alan suddenly "got

it" wrt. the instruments. As long as everything was operating correctly,

all the needles on the instruments was pointing in the same direction! It

was very easy to spot if anything out of the ordinary was going on, and

what that might be.

This story has stuck with me as a super example of adapting the technology

to what we people are good at, as opposed to the other way around which is

too often the case.

Enjoy, Harald

With the multitude of gauges in a cockpit this is a brilliant way to quickly

scan the status of the various components of the airplane. The display of

information is quite important in complex systems and has been discussed in

RISKS before (e.g., [RISKS-23.12](#), the whole "Bubba" debate).

★ Re: Legal Mercedes driver jailed for 18 months (Lesser, [RISKS-23.2x](#))

<David Gillett <dgillett@deepforest.org>>

Fri, 05 Mar 2004 00:13:36 -0800

A few years back, before my father retired from traffic engineering, his was one of several cars narrowly missed by a vehicle operated with excessive speed and careless disregard for others on the road. He told me that the driver, when he appeared in court, argued that as the holder of a racing driver's permit, he had been in perfect control of his vehicle at all times.

The judge ruled that it was entirely UNreasonable to assume a similar level of skill and coordination on the part of other drivers using the roadway, and imposed the maximum available sentence.

Yes, you can be liable for provoking foreseeable mis-reactions....

✶ Extended Call for Papers: Voting, Elections, and Technology

<Micah Altman <Micah_Altman@harvard.edu>>

Thu, 4 Mar 2004 19:22:28 -0500 (EST)

Due to the scheduling of other journal issues, the SSCORE editor has given us an opportunity to extend the original deadline for submissions to this special issue until June 15.

Call for Papers: *Voting, Elections, and Technology*
a special issue of Social_Science_Computer_Review

This special issue of Social Science Computer Review will bring

together a collection of high quality academic work that extends, refines and challenges our understanding of the use, state of the art, and challenges associated with voting and election technology, broadly conceived.

This special issue will bring together papers that investigate specific cases of the use of technology in voting and elections, as well as analysis of policy, and reviews of the state of the art. Papers from a broad range of social science perspectives are encouraged. Submissions can be in the form of full papers (maximum 20 printed pages) or in the form of short papers (5 printed pages). Post-graduate students are particularly encouraged to submit early work in the form of short papers.

Sample Topics: E-voting, Online voter survey methods, Technologies for election forecasting, Agent,based models of voting behavior, Web, based campaign fundraising, Redistricting technology, Policy implications

[Abridged for RISKS. For more on SCORE, see this URL:

<http://hcl.chass.ncsu.edu/sscore/sscore.htm>

]



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 27

Tuesday 16 March 2004

Contents

- [DARPA robot race is a bust](#)
[NewsScan](#)
- [Re: DARPA robot race](#)
[PGN](#)
- [Can Software Kill?](#)
[Debbie Gage and John McCormick via Dan Scherer](#)
- [P2P legal defense by separation of content and key?](#)
[Brent J. Nordquist](#)
- [PPI delayed by "computer problems"](#)
[Bill Hopkins](#)
- [Microsoft Word reveals document's author -- again](#)
[George W. Harris](#)
- [Lost e-votes could flip Napa County race](#)
[PGN](#)
- [California voters turned away](#)
[PGN](#)
- [Googling Up Passwords, Scott Granneman excerpt](#)
[Monty Solomon](#)
- [SSL is being severely stressed by phishing expeditions](#)
[Alistair McDonald](#)

- [When is a decimal point not a decimal point?](#)
[Darryl Smith](#)
 - [Merger Mania](#)
[Mike Albaugh](#)
 - [New twist to social engineering in virus transmission](#)
[John Sawyer](#)
 - [Re: An interesting airplane user interface](#)
[A.M. Passy](#)
 - [People are not as conservative as some think!](#)
[Jonathan de Boyne Pollard](#)
 - [Re: Buffer overflows](#)
[Mike Albaugh](#)
 - [2004 IEEE Symposium on Security and Privacy](#)
[Steve Tate](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **DARPA robot race is a bust**

<"NewsScan" <newsscan@newsscan.com>>

Mon, 15 Mar 2004 09:14:24 -0700

The highly touted robot race staged by the Pentagon in an effort to boost R&D in driverless vehicles has ended with all 15 self-navigating devices petering out within a few miles of the starting gate -- victims of technical glitches, barbed wire fences and rough terrain. The Defense Advanced Research Projects Agency had spent \$13 million on its Grand Challenge, which offered a \$1 million prize to the creators of the vehicle that could complete a 150-mile race across the Mojave Desert within 10 hours. Team members were not allowed to touch or steer the vehicles and most of the

robots stalled, overturned, or ran off the course shortly after taking off. Defense officials foresee using such autonomous robotic vehicles to ferry supplies in war zones. [AP 15 Mar 2004: NewsScan Daily, 15 Mar 2004]

<http://apnews.excite.com/article/20040315/D81AQ3M00.html>

✶ Re: DARPA robot race

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

Tue, 16 Mar 2004 11:12:14 PST

For RISKS readers, it should be no surprise that none of the competitors got very far in the first robotic Grand Challenge of such scope. This challenge is a fine example of an **overall system** problem where **everything** counts, not just mechanical and electrical robustness, software reliability, fault tolerance, vision processing, incredible foresight in choosing system requirements, good software engineering, sound programming languages, design for survivability, etc., but also real-time awareness of and reactivity to the surrounding physical and logical environments. Furthermore, security was not even a concern this time around -- although it would be absolutely critical in any real military deployment. In actual battle conditions, defending against and responding to all sorts of denial-of-service attacks would have to be in scope, including electromagnetic jamming, remote penetrations, sabotage, and so on. (Here, each vehicle had a

remote manual
trigger that would cause it to halt in case human lives -- or
even a
protected tortoise -- were about to be threatened. Of course,
such a
safety-contingency mechanism could also be potentially misused by
competitors, although I presume there might have been rules
against such
actions in this case -- or at least suppositions that an
eventual winner
might be disqualified for having engaged in such tactics.)

Knowing what we know about RISKS and human frailty, I am always
concerned
about people overendowing a sense of operational certainty
toward fully
automated vehicles. (For example, think about the completely
automated
highway and what might happen in the event of noncompliant
participants or
unanticipated events.) At any rate, the prize remains a Grand
Challenge for
the future -- or, actually, a kilogrand Grand Challenge, because
one grand
is *one thousand dollars*. (Note for foreign readers: American
slang!)

Incidentally, after commenting on watching the event, Paul Saffo
called it
``Woodstock for Warlords''. PGN

✂ Can Software Kill? Debbie Gage and John McCormick, Baseline

<"Dan Scherer" <dans@oz.net>>
Wed, 10 Mar 2004 00:46:58 -0800

An article out at eWeek.com that RISKS readers can relate to all
too well:

<http://www.eweek.com/article2/0,1759,1543652,00.asp?>

kC=EWNWS030804DTX1K0000599

It reviews the risks of software/human interactions that have lead to injuries or death of the human component of the equation. A fairly comprehensive summary of what has been covered here many times in the past.

✶ P2P legal defense by separation of content and key?

<"Brent J. Nordquist" <brent@nordist.net>>

Tue, 16 Mar 2004 15:55:11 -0600

Bruce Schneier's CRYPTO-GRAM for March 2004 had a pointer to this article: http://zdnet.com.com/2100-1104_2-5164413.html from which

I quote:

Spanish developer Pablo Soto, whose Blubster and Piolet software have

attracted several hundred thousand users, is taking a decidedly different tack. [...]

Information such as an MP3 song will still be downloaded from its original

source, he said. But a song will be scrambled, and downloaded simply as

raw, unintelligible data. This means that no actual copy of a song is

being exchanged, he contends.

If downloaders want to turn that data into usable music, their software

must seek elsewhere on the file-swapping network for the encryption "keys"

that will unlock the data, transforming it back into an MP3.

Separating

the download of the data and the keys may help protect file sharers from

lawsuits, making it more difficult for courts to say exactly which party

is responsible for copyright infringement, Soto said.

This reminded me immediately of my favorite RISKS article, "The source of

semantic content" (Gat, [RISKS-16.87](#)). Perhaps Gat's questions

"Has the law

been broken? Who broke it?" will soon be tested in court.

✈ PPI delayed by "computer problems"

<"Bill Hopkins" <whopkins@wmi.com>>

Fri, 12 Mar 2004 14:05:31 -0500

The Bureau of Labor Statistics (BLS) has been unable to compute the Producer

Price Index (PPI) for January or February due to delays in implementing a

change in the way data is organized. The switch of the industry classification system used has already been done for most BLS data,

according to a Reuters report, but the "PPI had to remap some 40,000

industry units and about 120,000 items before re-aggregating the data into

four indexes" in the PPI. The assistant commissioner responsible for the

PPI said "God knows when" the January numbers will be out. He blamed "aging

computers" which could not handle a dry run before pulling the plug on the

old system, and "30-year-old systems" that are not conversion-friendly.

The PPI measures wholesale prices and is an early indicator of inflationary trends, future corporate profitability and hiring, etc. A report on public radio's morning MarketPlace Report on Friday March 12 alluded to business contracts with prices based on the current PPI.

Source: Reuters, "U.S. Blames Aging Computers for PPI Delay" by Andrea Hopkins (no relation), 9 Mar 2004, found on Yahoo.

[Andrea may be no direct relation, but Bill may have many other one-hop-kins-men. PGN]

Microsoft Word reveals document's author -- again

<"George W. Harris" <gharris@mindspring.com>>
Tue, 16 Mar 2004 03:04:32 -0500

California's Attorney General circulated a document to fellow state attorneys general outlining a strategy for a legal attack on the makers of peer-to-peer software. However, the document was in Microsoft Word, and the metadata revealed that the document's actual author was "stevensonv", apparently Vans Stevenson, the MPAA's Senior Vice President for State Legislative Affairs.

[http://www.wired.com/news/digiwood/0,1412,62665,00.html?
tw=wn_tophead_1](http://www.wired.com/news/digiwood/0,1412,62665,00.html?tw=wn_tophead_1)

Lost e-votes could flip Napa County race

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

Mon, 15 Mar 2004 13:45:11 PST

One Sequoia Optech electronic machine used to count optical-scan paper absentee ballots in the 2 March 2004 California primary in Napa County failed to record votes on some ballots. This was detected by chance in a random 1% recount. As a result, the county will re-scan over 11,000 ballots, which could possibly change the results of some close local races. The machine was miscalibrated to detect carbon-based ink, but not dye-based ink commonly used in gel pens. (The pre-test was done only with carbon-based ink.) [Of course, the random test might not have noticed other machines that were similarly miscalibrated. PGN]

Kim Alexander said the county was lucky that the problem occurred on a system with a paper trail. "If the problem had occurred with their electronic ballots or with the tabulation software (which sits on the County server), they would have been hard pressed to reconstruct their election. Or, they might not have ever known there was a problem at all. If they were doing the manual count on the electronic ballots there would be no record to look at to determine what the accurate vote count should be." [Source: Kim Zetter, Wired News, 12 Mar 2004; PGN-ed]

<http://www.wired.com/news/politics/0,1283,62655,00.html>

California voters turned away

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

Mon, 15 Mar 2004 13:45:11 PST

In the 2 March 2004 California in Alameda and San Diego Counties, some voters were delayed or turned way from polling places. In Alameda County, about 200 of their 1,096 voting precincts experienced problems with the precinct-control module encoder machines that provide voters with an access card for Diebold touch-screen machines. Some voters were able to fill out provisional paper ballots. However, apparently many voting places ran out of paper ballots, and voters were turned away in at least 25 polling places.

[Sources: Ian Hoffman, Electronic-voting machine snafus leave votes in limbo

The Argus (Fremont, CA), 4 Mar 2004, and Thomas Peele and Sam Richards,

Voters turned away by encoder problems, *Contra Costa Times*, 12 Mar 2004;

PGN-ed.]

The Argus article had this quote: Alameda County elections officials ``were swamped Tuesday morning by some 200 calls for help from poll workers in all parts of the county. Diebold representatives said part of the problem seemed to be a low battery charge in the voter-card encoders, causing them to boot up into an unfamiliar Windows screen.''

As we noted earlier ([RISKS-23.07](#)), in the 17 counties in which Diebold systems were used, none of the versions of those systems actually used was the version that had been certified.

There were numerous reports in the past weeks of malfunctions and

irregularities elsewhere as well. I would have to spend more time than I have to catalogue them all in RISKS. But I think you get the idea from what we have included here that there are vastly too many problems that could influence the results of close elections, often with no recourse to find out what was really intended.

🔥 Googling Up Passwords, Scott Granneman excerpt

<Monty Solomon <monty@roscom.com>>

Fri, 12 Mar 2004 00:45:13 -0500

Google is in many ways the most useful tool available to the bad guys, and the most dangerous Web site on the Internet for many, many thousands of individuals and organizations.

By Scott Granneman, 9 Mar 2004

In my last column, I provided a checklist for Windows users that would help them secure their computers. I created that checklist because it has become increasingly and painfully obvious to me that most home users -- and most small businesses and organizations -- have substandard security practices in place, if they have any at all. The checklist was designed to help secure things on the perimeters: on client computers and at the edges of home and business networks. This week, I want to talk about servers.

Specifically, let's talk about the stuff that people are serving without

realizing it. Security pros have known about this problem for years, but most computers users still have no idea that they may be revealing far more to the world than they would want. In fact, it wouldn't be far from the truth to say that Google is in many ways the most useful tool available to the bad guys, and the most dangerous Web site on the Internet for many, many thousands of individuals and organizations. [...]
<http://www.securityfocus.com/columnists/224>

SSL is being severely stressed by phishing expeditions

<"Alistair McDonald" <alistair@inrevo.com>>
Tue, 9 Mar 2004 20:30:34 -0000 (GMT)

Netcraft reports that phishers are using real and fake SSL certificates to fool computer users into thinking that they are using the site they hope to be using instead of the phisher's site.

The report is here:

http://news.netcraft.com/archives/2004/03/08/ssl_credibility_as_phishing_defense_is_tested.html

and is worth a read even if, like me, you've been a regular RISKS reader for years. The phishers must be on to something, as they are putting a lot of research and effort into this scam.

One thing I didn't know: SSL allows a "plain text" encoding, that doesn't require a signed certificate, yet browsers show a locked padlock as a site using encryption would display. I'm not sure whether I should

whack the
browser authors, the SSL implementors or the SSL designers on
the head for
this.

My advice on phishing avoidance: never click on a link in an e-
mail from a
financial institution, always navigate from a bookmark. If
possible, avoid
typing in web addresses too, in case you misspell and a phisher
has taken
the misspelled site hoping to catch unlucky typists. And never,
ever use a
public terminal such as in a cyber cafe or library to enter
any password
at all, due to physical or software keyboard sniffers.

Alistair McDonald +44 (0)7017-467386 <http://www.inrevo.com>

✶ When is a decimal point not a decimal point?

<"Darryl Smith" <Darryl@radio-active.net.au>>

Thu, 11 Mar 2004 23:40:51 +1100

As part of a hobby, I write vehicle tracking software that plugs
into cheap
external mapping software to create an entire application
without me needing
to worry about dealing with maps - I just need to tell the
mapping program
where to display positions, and it just goes and does it.

Now, I use two interfaces to the mapping software - one using
API calls
sending the positions as parameters of the API call for adding
points to the
map. The second interface involves creating a dummy GPS data
line (starting

with \$GPRMC), and sending this to the application for use with the moving map functions.

In the last few days I have been exchanging e-mail with a user in Canada who has been complaining that the positions on the map for the mappoint are correct at about 48N and 71W, whereas the moving map functions are saying about 80N and 0W. Of course the points should be identical.

My software sends the mappoint through the API, and then generates and sends the fake GPS position. The software is written in Visual Basic version 6.

Some of my code appears below.

```
lat = Abs(lat)
nmeastring = Format(Int(lat), "00")
lat = lat - Int(lat)
lat = lat * 60
nmeastring = nmeastring & Format(lat, "00.000")
```

On most systems this correctly encodes the latitude into degrees followed by decimal minutes.

Unfortunately on systems where the locale has been changed to have a comma as a decimal place, then Visual Basic ignores the fact that I have specifically stated that I want to use a decimal point when I format the number into a string, and changes it to a comma. To be fair to Microsoft this is listed in the manual Visual Basic 6.

Of course since the NMEA sentence I am generating uses commas as field delimiters, the fields are getting totally messed up. And the mapping software is making its best effort to display the obviously

incorrect
position.

The risk: using the same character to denote decimal places as for denoting different fields is not a good idea.

Darryl Smith, VK2TDS POBox 169 Ingleburn NSW 2565 Australia
Mobile Number 0412 929 634 [+61 4 12 929 634 International]
www.radio-active.net.au - www.radio-active.net.au/web/tracking

Merger Mania

<albaugh@spies.com>

Tue, 9 Mar 2004 09:20:52 -0800 (PST)

My bank has decided that two trusts for which I am a trustee are in fact "the same", despite being "for the benefit of" different individuals, and having different Taxpayer Identification Numbers. Or, at least, the trusts have different TINs, and the accounts used to have different TINs, but the first of two lines on the bank's forms is the same for the two trusts, and my address is, naturally, the same for both, and that's "close enough" for them to decide to report all income for both trusts as being paid to one TIN.

I am now at four weeks calendar time, four hours phone-log time directly interacting with them, and three forms signed in duplicate. So far, all it has gotten me is that they issued another 1099 (report to the IRS of interest paid), now reporting all income to the other TIN.

Plus an
oddly-formatted (no spaces between words) e-mail claiming that
they would
"take care of it and issue another 1099" (note: _an_other, I
shudder to
think...) Meanwhile, April 15th is closer than it appears...

Risks? Obviously, someone, or something, at the bank was able to
change the
TIN on an account without the permission, or even notification,
of the
account holder. Yet enormous effort is required (so far
unsuccessfully) to
correct the mistake. This scheme (easy to break, hard to fix) is
breathtakingly wrong.

I would go to another, perhaps more competent bank, but every
time I do,
they get bought by the likes of these incompetents. Hence the
double meaning
to "Merger Mania".

✶ New twist to social engineering in virus transmission

<John Sawyer <jpgsawyer@btopenworld.com>>
Fri, 12 Mar 2004 08:49:34 +0000 (GMT)

It seems that the Beagle virus is doing the rounds again with a
new
interesting twist to the social engineering used previously. In
this case it
seems to send you an e-mail saying that your mailing system will
be out of
action for two days and to follow the instructions in the
attachment.

> Dear user of "Btopenworld.com" mailing system, Our main
mailing server

> will be temporary unavailable for next two days, to continue
receiving
> mail in these days you have to configure our free auto-
forwarding service.
>
> For further details see the attach.
>
> Cheers,
> The Btopenworld.com team
> <http://www.btopenworld.com>

It's fairly transparent to RISKS readers, but to someone less
savvy it might
seem quite plausible. Of course, given btopenworlds recent
conjoining of
its services with Yahoo! and the confusion that caused some
users, people
should be forgiven if they fall for this. The risk of a well-
timed and
well-written e-mail of this sort should not be underestimated.

✉ **Re: An interesting airplane user interface (Magda, [RISKS-23.26](#))**

<"A.M. Passy" <marc@passy.us>>
Sun, 14 Mar 2004 23:07:10 -0600

> With the multitude of gauges in a cockpit this is a brilliant
way to
quickly scan the status of the various components of the
airplane.

This should not be remarkable, and it is certainly not
original. When I
served aboard Nuclear Submarines more than 10 years ago, all the
instruments
in the Engineering control room were designed such that at
roughly normal
operation, all needles pointed up (all analog instruments).

There were a few that weren't pointing up, due to their nature -- we used to talk about the Beauty of analog -- you could take a mental "picture" of normal, and identify off-nominal very rapidly, much more so than if you had to process each number.

In the 1980s, the B-1 Lancer bomber was remarkable for a similar "innovation" -- they used LED bargraphs lined up next to each other for engine instrumentation, and when all was normal at cruise, there was a straight line across several (~10, I think) instruments.

⚡ People are not as conservative as some think! (Re: Maziuk, [R 23.21](#))

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

Thu, 11 Mar 2004 11:14:44 +0000

DM> On the other hand, there's no reason to believe anyone will rush to

DM> implement new and improved SMTP when/if ever that comes along.

It is "when", not "if ever". Two projects for replacing SMTP-based Internet mail, IM2000 and "mail-ng", exist right now.

DM> nobody's in a hurry to switch to IPv6, are they?

Actually, IP version 6 is a good example, because it is a bad example. It doesn't actually support that point at all. In a U.S.-centric view of the world, perhaps nobody is in a hurry to implement IP version 6.

But there are other parts of the world that are quite enthusiastic about implementing it, because they are significantly inconvenienced by IP version 4.

The same is true of a replacement for SMTP-based Internet mail. There will be those who, because they have reached the stage where SMTP-based Internet mail is simply unusable, will be enthusiastic about adopting a suitable replacement.

✉ **Re: Buffer overflows (Quayle and Hopkins, [RISKS-23.24](#))**

<Mike Albaugh <albaugh@spies.com>>

Thu, 4 Mar 2004 19:13:45 -0800 (PST)

> From: "Stanley F. Quayle" <stan@stanq.com>

> Subject: Re: Buffer overflows and VMS

> C programmers moving to OpenVMS quickly discover what the ACCVIO error

> message means.

BTW: SYS III Lint core-dumped when I first ran it on itself, under VMS :-)

> From: "Bill Hopkins" <whopkins@wmi.com>

> Subject: Re: Buffer overflows and Burroughs/Unisys

> Since C's memory abstraction is basically the hardware address, and

> addresses can be manipulated arbitrarily, [...]

Anybody else note the dissonance here? In fact the C language, while not as

"tight" as, e.g. Ada, does provide sufficient opacity of pointers to accomplish pretty good bounds-checking. Of course, not much "alleged C" code would run on such a system. I submit it is because too many implementors accepted the notion that "C has pointers that are no more than tarted-up machine addresses" and didn't even consider implementing real C pointers on machines which would support them. The original "oh, cut them some slack" led to a generation of programmers who actually believe such dreck as "packed structs" and "result of a cast is a modifiable lvalue" is part of C.

The risk: If you take a sufficiently dim view of your ability to enforce language specs, and give up at the start, you'll get, well, the current situation, and risks...

2004 IEEE Symposium on Security and Privacy

<Steve Tate <srt@cs.unt.edu>>

Tue, 9 Mar 2004 09:18:43 -0600 (CST)

2004 IEEE Symposium on Security and Privacy
May 9-12, 2004, The Claremont Resort, Oakland, California,
USA

sponsored by
IEEE Computer Society Technical Committee on Security and
Privacy

in cooperation with
The International Association for Cryptologic Research (IACR)

For more information, see <http://www.ieee-security.org/TC/SP-Index.html>

For registration, see <http://www.cics.unt.edu/ieeereg/register.php>

[Info on registration/local arrangements at www.ieee-security.org.]

Monday MORNING

Session: Attacks and Defenses

* Keyboard Acoustic Emanations, Dmitri Asonov, Rakesh Agrawal (IBM Research)

* Effects of Mobility and Multihoming on Transport-Protocol Security

Tuomas Aura (Microsoft Research), Pekka Nikander (Ericsson Research),

Gonzalo Camarillo (Ericsson Research)

* Analysis of an Electronic Voting System

Tadayoshi Kohno (UC San Diego), Adam Stubblefield (Johns Hopkins Univ.),

Aviel D. Rubin (Johns Hopkins Univ.), Dan S. Wallach (Rice Univ.)

Session: Theory of Access Control

* Access Control By Tracking Shallow Execution History

Philip W. L. Fong (U. Regina)

* A Layered Design of Discretionary Access Controls with Decidable

Safety Properties, Jon A. Solworth, Robert Sloan (U. Illinois, Chicago)

Monday AFTERNOON

Invited Talk

Session: Cryptography

* Symmetric encryption in automatic analyses for confidentiality against

active adversaries, Peeter Laud (Tartu University)

* Automatic Proof of Strong Secrecy for Security Protocols

Bruno Blanchet (Ecole Normale Supérieure)

5-minute work-in-progress talks

Tuesday MORNING

Session: Denial of service

- * An empirical analysis of target-resident DoS filters
Michael Collins (CERT), Michael Reiter (CMU)
- * Large-Scale IP Traceback in High-Speed Internet: Practical
Techniques
and Theoretical Foundation, Jun Li, Minho Sung, Jun (Jim) Xu
(Georgia Tech),
Li (Erran) Li (Bell Labs)
- * An Endhost Capability Mechanism to Mitigate DDoS Flooding
Attacks
Abraham Yaar, Dawn Song, Adrian Perrig (CMU)

Session: Access Control and Privacy

- * Safety in Automated Trust Negotiation
William H. Winsborough (George Mason Univ.), Ninghui Li
(Purdue Univ.)
- * Securing OLAP Data Cubes Against Privacy Breaches
Lingyu Wang, Sushil Jajodia, Duminda Wijesekera (George Mason
Univ.)

Tuesday AFTERNOON

Panel Session

Session: Static Analysis

- * Run-time Principals in Information-flow Type Systems
Stephen Tse, Steve Zdancewic (U. Pennsylvania)
- * Formalizing Sensitivity in Static Analysis for Intrusion
Detection
Henry Hanping Feng (U. Mass., Amherst), Jonathon T. Giffin (U.
Wisconsin,
Madison), Yong Huang (U. Mass., Amherst), Somesh Jha (U.
Wisconsin
Madison), Wenke Lee (Georgia Tech.), Barton P. Miller (U.
Wisconsin Madison)

Wednesday MORNING

Session: Network Security

- * Fast Portscan Detection Using Sequential Hypothesis Testing,

Jaeyeon

Jung (MIT), Vern Paxson (ICIR), Arthur W. Berger, Hari Balakrishnan (MIT)

* On-the-Fly Verification of Rateless Erasure Codes for Efficient Content

Distribution, Maxwell N. Krohn (MIT), Michael J. Freedman, David Mazieres (NYU)

* Multicast Authentication in Fully Adversarial Networks

Anna Lysyanskaya, Roberto Tamassia, Nikos Triandopoulos (Brown Univ.)

Session: Security Against Physical Attacks

* An Interleaved Hop-by-Hop Authentication Scheme for Filtering False

Data Injection in Sensor Networks, Sencun Zhu, Sanjeev Setia, Sushil Jajodia (George Mason Univ.), Peng Ning (NC State Univ.)

* SWAtt: Software-based Attestation for Embedded Devices, Arvind Seshadri,

Adrian Perrig (CMU), Leendert van Doorn (IBM and CMU), Pradeep Khosla (CMU)



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 28

Thursday 18 March 2004

Contents

- [House Panel Slams Federal IT Security](#)
[PGN](#)
- [JFK AirTrain passengers end up at storage yard instead of airport](#)
[Tom Lambert](#)
- [Connecticut automobile emissions tests faulty](#)
[Danny Burstein](#)
- [Diebold Opteva 520 ATM crashes exposing Windows XP Inside!](#)
[Scott A. Hissam](#)
- [The RISKS of Risk Analysis](#)
[Michael Bednarek](#)
- [Anti-spam lawsuit complaints](#)
[Monty Solomon](#)
- [Self adjusting firewalls in Longhorn](#)
[Neil Youngman](#)
- [Death of UK skydiver in Australia](#)
[Anthony Youngman](#)
- ["Special Skills draft"](#)
[Geoffrey Brent](#)
- [Risks of automated pedophilia detection](#)
[Nick Brown](#)

- [Latest e-mail worms use password trick to foil filters](#)
[NewsScan](#)
 - [CORRECTION to "SSL is being severely stressed by phishing expeditions"](#)
[Alistair McDonald](#)
 - [Re: SSL is being severely stressed by phishing](#)
[Isaac Morland](#) [Nelson Minar](#)
 - [Re: When is a decimal point not a decimal point?](#)
[John Carlyle-Clarke](#) [Nick FitzGerald](#)
 - [Throwing out the baby with the bathwater: Crypto sigs](#)
[Tim Panton](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🔥 House Panel Slams Federal IT Security

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

Wed, 17 Mar 2004 17:10:06 PST

The latest "report card" of the U.S. House Government Reform Subcommittee on Technology on cybersecurity in U.S. government agencies continues to paint a generally dismal picture. The National Science Foundation and the Nuclear Regulatory Commission received A grades, while eight other agencies had F (Failing) grades -- including the Department of Homeland Security. FOURTEEN of 24 agencies received a score worse than C. According to U.S. Representative Adam Putnam (R-Fla.), Federal agencies aren't doing enough to secure their network systems, even as documented cyber-attacks against the U.S. government continue to rise dramatically -- from 489,890 in 2002 to 1.4 million in 2003. "Our government has taken very dramatic steps to increase our physical security, but protecting our information networks

has not progressed commensurately either in the public or private sector."

Putnam closed the hearing by saying his subcommittee will seek accountability of the "highest agency official responsible for information technology investments to insure that IT security is baked into the investment decision making process." [Source: Roy Mark, *Internet News*, 17 Mar 2004; PGN-ed]

<http://www.internetnews.com/infra/article.php/3327081>

[What's New? Technology alone does not solve management problems.

Management alone does not solve technology issues. Reducing risks is a beginning-to-end, end-to-end system problem where the systems include all of the relevant technology, all of the relevant people, and all of the dependencies on and interactions with the operating environment, however flawed and complicated. But those flaws and complexities must be addressed systemically. The many lessons familiar to RISKS readers tend to be widely ignored by the folks who should most seriously be learning them. PGN]

✈ JFK AirTrain passengers end up at storage yard instead of airport

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

Thu, 4 Mar 2004 14:19:12 -0500

For the second time this year, passengers on the Kennedy Airport AirTrain

were accidentally diverted to a unused-train storage yard -- where passengers were exposed to live rails. The 12 Feb 2004 mistake prompted an internal overview of the \$1.9 billion, eight-mile long transit system to JFK. Fifteen minutes later, the train was back on course. A similar event occurred on 26 Jan 2004, with a train winding up in the same storage yard.

[Source: FreeRepublic.com, 4 Mar 2004, PGN-ed.]

<http://www.freerepublic.com/focus/f-news/1091020/posts>

Thanks to Tom Lambert at ACM for noting this one. Tom's reaction was this:

"Whenever I hear of MTA [subway system] plans to further automate subway service here in NY City, I think of events such as this one."

✶ Connecticut automobile emissions tests faulty

<danny burstein <dannyb@panix.com>>

Tue, 16 Mar 2004 18:47:40 -0500 (EST)

Lisa Chedekel, Connecticut: New Emissions Tests Faulty, DMV Says False

Readings May Have Led Inspectors To Fail Thousands Of Vehicles, (Hartford) *Courant*, 16 Mar 2004

As many as 13,000 vehicles tested under Connecticut's new emissions

inspection program may have been failed in error because the software used

to measure a critical pollutant produced false readings, state motor

vehicle officials confirmed Monday. [...] In Connecticut, state

Department of Motor Vehicle officials, working with Agbar

technicians,

discovered recently that an analyzer used to detect hexane, the main

hydrocarbon present in gasoline exhaust, was instead measuring propane levels.

<http://www.ctnow.com/news/custom/topnews/hc-agbar0316.artmar16,1,5617910.story?coll=hc-headlines-topnews>

Sigh. The usual two problems here. First, no one kept track of the expected versus the actual failure rates. And second, there's apparently no periodic quality control checks.

(and third, of course, is the entire question of the value of emissions testing, but that's a horse of a different color)

⚡ Diebold Opteva 520 ATM crashes exposing Windows XP Inside!

<"Scott A. Hissam" <shissam@sei.cmu.edu>>

Thu, 18 Mar 2004 07:27:55 -0500

Want to listen to a little Beethoven, Jazz, or even the Talking Heads

while making that ATM deposit?

* The Scene: Carnegie Mellon University

* The Event: A newly installed Diebold Opteva 520 ATM crashes, then

reboots. Surprisingly, it's vanilla-style Windows XP operating system

initialized without the actual ATM software.

* The Result: A desktop computer with only a touch screen interface is left

wide open for the amusement of the most wired university in the U.S.

Eschewing more malicious schemes, the first move was to connect to the Internet. This plan proved unsuccessful as there seemed to be no network capability. The situation was complicated in that even typing proved extremely difficult due to the lack of a keyboard. The Character Map program was used to enter text by copy-and-pasting, yet the most that was accomplished by doing so was making the text-to-voice program say, "What, do you think I'm made of money?" Windows Media Player was set up to loop a series of Beethoven, Jazz, and Talking Heads (the sample sound files included with XP) while running a full screen visualization.

[Source: <http://midnightspaghetti.com/news.htm>; 17 Mar 2004]

[Another report noted by George Michaelson in Dave Farber's IP. PGN]

✶ The RISKS of Risk Analysis

<Michael Bednarek <mb@mbednarek.com>>

Thu, 18 Mar 2004 00:02:58 +1000

A recommendation by a Government agency to allow banana imports from the Philippines is being reviewed after finding an error in its risk assessment report, reports the ABC [Australian public broadcaster]. (1)

According to the agency, Biosecurity Australia, it was a "transcription error in the electronic spreadsheet used in the estimation of

risk for this particular IRA [import risk analysis]. The spreadsheet has now been corrected." (2)

Well, it wasn't really a spreadsheet, but a MS Project file with the @Risk add-on. (3)

A quote from the ABC's coverage: (1) "The Australian Banana Growers Council says its opposition to banana imports has been vindicated. Council spokesman Tony Heidrich says a revision is not good enough and the assessment process needs to start again from the beginning. 'We just don't think you can continue to have faith in Biosecurity Australia's ability to carry out this [import risk analysis],' Mr Heidrich said. 'We think there could well be fundamental flaws going right back the first commencement of the process.' "

The RISK? Surely one of the oldest chestnuts in computerdom: don't believe something just because it's a computer printout.

(1) <<http://www.abc.net.au/news/newsitems/s1067958.htm>>

(2) <<http://www.affa.gov.au/content/output.cfm?ObjectID=DAD55B7F-9F61-49D3-9CB1B9F38F09A82F>>

(3) <http://www.palisade.com/html/risk_for_project.asp>

Michael Bednarek <http://mbednarek.com/>

[This case was also noted by George Michaelson. Incidentally, for those of you who have not seen it, you might enjoy Section 7.10 of my *Computer-Related Risks* book, pages 255--257, entitled Risks in Risk

Analysis, drawn from an earlier *CACM* Inside Risks column from June 1991,
written by Robert N. Charette. It is still very relevant.
PGN]

✶ Anti-spam lawsuit complaints

<Monty Solomon <monty@roscom.com>>

Fri, 12 Mar 2004 09:35:30 -0500

Spam Litigation

<http://news.findlaw.com/legalnews/documents/index.html#spam>

* Complaint and Exhibits (America Online, Inc. v. John Does 1-40)
(March 9, 2004)

<http://news.findlaw.com/hdocs/docs/cyberlaw/aoldoes30904cmp.pdf>

* Complaint and Exhibits (America Online, Inc. v. Davis Wolfgang
Hawke, et al. (March 9, 2004)

<http://news.findlaw.com/hdocs/docs/cyberlaw/aolhawke30904cmp.pdf>

* Complaint (Earthlink, Inc. v. John Does 1-25, et al. (March 9,
2004)

<http://news.findlaw.com/hdocs/docs/cyberlaw/elnkdoes30904cmp.pdf>

* Complaint (Microsoft Corp. v. JDO Media, Inc., et al. (March
9, 2004)

<http://news.findlaw.com/hdocs/docs/cyberlaw/msjdo30904cmp.pdf>

* Complaint (Microsoft Corp. v. John Does 1-50 d/b/a Super
Viagra Group)
(March 9, 2004)

<http://news.findlaw.com/hdocs/docs/cyberlaw/mssprviag30904cmp.pdf>

* Complaint (Yahoo!, Inc. v. Eric Head, et al. (March 9, 2004)

<http://news.findlaw.com/hdocs/docs/cyberlaw/yahoohead30904cmp.pdf>

[My unfiltered spam has gone through the roof again in the

past two weeks.

Thank you all for using the designated keyword in the subject line of your

postings. So, I have a new strategy. I delete ALL of the unkeyworded NEW

MAIL, and then check for exceptions. In the past week, I have detected

only a few legitimate messages that did not use the keyword. The result

is that even after SpamAssassin filtering, 95% of the residual e-mail is

spam. But this really simplifies my pain. PGN]

✶ Self adjusting firewalls in Longhorn

<Neil <no.spam.for.n.youngman@ntlworld.com.die.spammers>>

Wed, 17 Mar 2004 17:33:34 +0000

According to <http://www.internetnews.com/ent-news/article.php/3325631>

"Longhorn engineers are packing new technologies into the OS to check

against a central patching Web service for security holes on computers. If a

user does not have a patch installed, Longhorn's active protection

technology will kick in to adjust the firewall or PC settings"

Great if it works and it doesn't break any critical functions.

RISKS? how about blocking communication to/from a heart monitor in an

intensive care ward?

Further examples are left as an exercise for the reader ;-)

According to Robert McLaws of Interscape Technologies, an

independent
software partner of Microsoft, "if they don't care enough to
keep their
systems secure, then they have lost that right to complain,"

✶ **Death of UK skydiver in Australia**

<"Anthony Youngman" <Anthony.Youngman@eca-international.com>>
Thu, 18 Mar 2004 12:45:47 -0000

Skydiving victim Clare Barnes was doomed from the moment she
jumped from a
plane at 14,000ft, an enquiry revealed yesterday. What
appears to have
happened in this case is that all the cards have been stacked
against her
and have fallen the wrong way each time. A parachute has a
number of
components. They are largely interchangeable, but not always.

She was apparently using her own equipment, and the
incompatibilities meant
that there was no way that parachute was going to open
successfully. The
risks are obvious and, sadly, tragic.

✶ **"Special Skills draft"**

<Geoffrey Brent <g.brent@student.unsw.edu.au>>
Thu, 18 Mar 2004 10:52:18 +1100

The USA's Selective Service System has begun working on
developing
procedures and policies for a targeted military draft of

Americans with computer and foreign-language skills, although the SSS has emphasised that such a draft is not imminent.

<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/03/13/MNG905K1BC1.DTL>

(A similar plan for selective drafting of medical personnel, the HCPDS, has already been assembled. See <http://www.sss.gov/FSmedical.htm> for a brief overview, or

<http://www.livejournal.com/users/turnberryknkn/79171.html> for a friend's observations on the HCPDS - some of which may also be pertinent to this latest project.)

It has long been known that conscripts are vastly less effective and less reliable than volunteer soldiers; during the Korean War, the AP famously reported that only one in four US draftees used their weapons even when defending against enemy attack.

Computing is a field where a sloppy, unmotivated worker can all too easily achieve negative productivity without immediate detection. A disgruntled, _malicious_ worker can do far worse - compare the man-hours spent in writing malware with those spent in repairing its effects. Relying on conscripts to supply the computer expertise the US armed forces might need strikes me as an exceptionally bad idea.

⚡ Risks of automated pedophilia detection

<Nick Brown <Nick.BROWN@coe.int>>

Thu, 18 Mar 2004 16:16:49 +0100

The BBC's web site reports on a "chatbot" program which is designed to run in chat rooms oriented at children, and detect when the people chatting with it may be attempting to lure children into "inappropriate" activity.

Highlights:

'The chatbot has already been used in many chatrooms and its creator claims that, so far, no-one has caught it out.' (Nothing unsubstantiated or speculative there, then.)

'[The author of the software] said that information gathered by the Chatnannies had already helped some police investigations.' (Uh-huh.)

'"If this software works, then it would be marvelous because there is nothing like this out there," Chris Atkinson, Internet safety officer at the National Society for the Prevention of Cruelty to Children, said.' (Can you say "non-sequitur" ?)

The RISKS are left as an exercise to the reader, but to get you started:

- How will law enforcement officers tend to treat chatroom participants whose behaviour has been flagged as dubious by this program ? Will they spend large amounts of resources to trap a pedophile, only to find that all they meet is an over-eager 13-year-old boy ?

- The claims made for this software seem to amount to passing the original

Turing test. That's quite an achievement. I wonder if the software

community will be allowed to verify these claims; or will the bot be kept

secret "to protect the children"?

<http://news.bbc.co.uk/2/hi/technology/3520834.stm>

Nick Brown, Strasbourg, France

🚀 Latest e-mail worms use password trick to foil filters

<"NewsScan" <newsscan@newsscan.com>>

Tue, 16 Mar 2004 07:09:31 -0700

The most recent versions of the pesky Bagle worm -- Bagle N and Bagle O --

arrive in a compressed and password-locked .zip or .rar file with the

password included in the body of the e-mail along with a message urging the

recipient to open it right away. This latest technique is designed to foil

corporate e-mail filters that may block ordinary zipped attachments but

allow password-protected documents to pass through the network's defenses

unimpeded. Once the attachment is unlocked, the worm is then forwarded to

everyone in the victim's e-mail address book. "The worm's author is sneakily

trying to make it more difficult for antivirus products to scan inside the

password-protected files," says Graham Cluley, a researcher with U.K.

cybersecurity firm Sophos. [**New Scientist**, 15 Mar 2004;

NewsScan Daily,
16 Mar 2004]

<http://www.newscientist.com/news/news.jsp?id=ns99994777>

✦ CORRECTION to "SSL is being severely stressed by phishing expeditions"

<"Alistair McDonald" <alistair@inrevo.com>>

Wed, 17 Mar 2004 08:44:55 -0000 (GMT)

I am indebted to David Wagner for correcting me when reporting on the Netcraft News item, regarding plain-text SSL, in [RISKS-23.27](#). Those with better knowledge than I have been discussing this, and, in David's own words, the reports are "Hogwash".

David has provided a link to a newsgroup archive at Google groups:

<http://tinyurl.com/39p4h> where the matter is discussed. If you're interested, then please take a look.

The risks (to me): don't believe everything you read, even if it comes from a normally reputable source.

Alistair McDonald (+44)(0)7017-467386

✦ Re: SSL is being severely stressed by phishing ([RISKS-23.27](#))

<Isaac Morland <ijmorlan@cscf.cs.uwaterloo.ca>>

Thu, 18 Mar 2004 08:37:06 -0500 (EST)

Of course, the ultimate fix to phishing would be an end to the mixed-endian nature of URLs: The domain name and user/password are little-endian, while the rest of the URL is big-endian. So for example, a bogus url like

<http://www.microsoft.com@abcd:hacker.org/a/b/c?hack=yes&ddos=true>

would look like this in big-endian form:

<http://org.hacker:www.microsoft.com@abcd/a/b/c?hack=yes&ddos=true>

Note that even disallowing the user/password stuff would still allow an URL like this:

<http://www.microsoft.com.index.html.com/hack>

Which again is quickly revealed as a fraud in big-endian notation. So the real fix is to use big-endian notation. Of course, in real life this would never work even if the technical aspects would be worked out because people will just click on anything. But we can dream.

✶ Re: SSL is being severely stressed by phishing ([RISKS-23.27](#))

<Nelson Minar <nelson@monkey.org>>

Tue, 16 Mar 2004 16:40:03 -0800

"Alistair McDonald" <alistair@inrevo.com> writes:

>My advice on phishing avoidance: never click on a link in an e-mail from a

>financial institution, always navigate from a bookmark. If possible, avoid

>typing in web addresses too

Microsoft offered one more item to your advice: don't click on links on web pages. Or as Microsoft Knowledge Base Article - 833786 said:

The most effective step that you can take to help protect yourself

from malicious hyperlinks is not to click them. Rather, type the URL

of your intended destination in the address bar yourself. By manually typing the URL in the address bar, you can verify the information that Internet Explorer uses to access the destination

Web site. To do so, type the URL in the Address bar, and then press

ENTER.

This absurd suggestion used to appear here:

<http://support.microsoft.com/default.aspx?scid=kb;%5Bln%5D;833786>

It's since been removed and a patch for this problem has been issued.

(Search for the above quote to find many copies of the original.)

Something is seriously wrong with the state of Web security when the

approved way to verify the identity of a site is to look for a 16x16

icon in one corner of the screen and even that doesn't work in many

cases. It's not just MSIE URL display bugs or obscure SSL modes at

fault; the model is broken.

⚡ Re: When is a decimal point not a decimal point? ([RISKS-23.27](#))

<"John Carlyle-Clarke" <john.cc@euoplacer.co.uk>>

Wed, 17 Mar 2004 11:33:24 -0000

```
> Date: Thu, 11 Mar 2004 23:40:51 +1100
> From: "Darryl Smith" <Darryl@radio-active.net.au>
> Subject: When is a decimal point not a decimal point?

> Unfortunately on systems where the locale has been changed to
have
> a comma as a decimal place, then Visual Basic ignores the fact
> that I have specifically stated that I want to use a decimal
point
> when I format the number into a string, and changes it to a
comma.
> To be fair to Microsoft this is listed in the manual Visual
Basic
> 6.
```

We encounter the same problem regularly with VB software that we produce.

We have made efforts to by default use Val and Str (which are non-locale aware functions) unless a locale aware conversion is specifically needed.

We have also written our own non-locale aware Format replacement where number formatting is needed.

A RISK here is that salepeople assume that producing French and German versions of the software will be "just a matter of translating a few strings", which ignores the many pitfalls. This is before you even try more complex problems like non-Roman alphabet languages, or even right-to-left ones!

Another gotcha: if you change your locale on your development machine to test the effects, VB breaks its own source code. If the hidden part of form files (text format, but concealed by the IDE) contains any non-integer numbers, VB will save them using the locale settings. Switching

back can
make the project fail to load.

The RISK, it seems to me, is assuming that OS locale-handling functions will deal with all these problems without the developer having to worry about it, and approaching language or locale conversion as a "Phase 2" option, rather than being aware of it from the outset.

Like many others, I imagine, this was learned the hard way for us. (Perhaps this is mostly a UK/USA problem? Maybe developers in other countries tend to be more aware of this.)

⚡ Re: When is a decimal point not a decimal point? (Smith, [RISKS-23.27](#))

<Nick FitzGerald <nick@virus-l.demon.co.uk>>
Wed, 17 Mar 2004 14:16:55 +1300

"Darryl Smith" <Darryl@radio-active.net.au> wrote:

```
<<snip gory details>>  
> Unfortunately on systems where the locale has been changed to  
have a comma  
> as a decimal place, then Visual Basic ignores the fact that I  
have  
> specifically stated that I want to use a decimal point when I  
format the  
> number into a string, and changes it to a comma. ...
```

Your description of what VB is doing is incorrect. When you write and compile your program on a system whose locale settings mean "<digit>.<digit>" represents a "decimal number", VB is taking

note of the meta-information about locales, number (and no doubt, date, time and several other) formats and representing that internally in a locale-independent way.

> ... To be fair to Microsoft
> this is listed in the manual Visual Basic 6.

Precisely. VB6 is designed to be localization sensitive and to more or less automatically handle such things on behalf of the programmer (depending where in Canada your correspondent is, there is a high probability that any VB6 runtime error messages generated by your program will be displayed in French too...).

> Of course since the NMEA sentence I am generating uses commas as field delimiters, the fields are getting totally messed up. And the mapping software is making its best effort to display the obviously incorrect position.
>
> The risk: using the same character to denote decimal places as for denoting different fields is not a good idea.

This is an historic issue with "soft" data formats where field and/or record delimiters occur "in-band" (i.e. in the same transmission stream) and where the set of such delimiters contains one (or more) characters that can validly comprise part of a valid field value.

I think the greater risk you have described is that of a programmer using a tool whose complete feature set s/he was not fully aware of.

This is a class of risk that is probably much greater the "simpler" the tool is to use (assuming it is a tool of modest power, as VB6 certainly is). This is so for (at least) two obvious reasons -- if a powerful (and therefore complex) tool is made simple to use much of its complexity is necessarily hidden (at least from those of its likely users who are less widely experienced in that field), and simple yet powerful tools are likely to attract the attention (and use) of those who are otherwise prevented access to such power (because other such tools are obtuse for not disguising their complexity, etc).

(I'm not a VB user, but suspect a simple, albeit perhaps not strictly "correct" solution to the issue here might be to quote the field values, at least for those fields that can contain such "ambiguous" data values.)

And finally, there was potential for an even larger risk in this story -- had your Canadian user had a GPS device that expected "locale-correct" input and was configured for "French Canadian" language or somesuch, your program would have worked for reasons you would not have understood _nor_ been unaware of...

✶ Throwing out the baby with the bathwater: Crypto sigs

<Tim Panton <thp@westhawk.co.uk>>

Wed, 17 Mar 2004 17:32:28 +0000

What's wrong with this picture ?

```
> [demime 0.98b removed an attachment of type  
> application/pkcs7-signature which had a name of smime.p7s]
```

So in order to protect me from a potential virus, the sending system has removed the one thing that would have helped me judge the provenance of the e-mail.

To be fair, stripping cryptographic signatures isn't entirely stupid if either:

- (a) the crypto software is not sanity checking its inputs, or
- (b) the mail client can be fooled into executing an attachment that the mail gateway took to be a data, i.e., a signature.

Unfortunately both of these conditions are true for most Outlook on Windows setups (or at least were until the recent ASN1 patch).

This isn't really any different from the problems we saw with buffer overruns in the from line permitting execution of arbitrary code. In that case no one stripped from addresses as a protective measure!

We still have a prevalent mindset that sees security (in this case authentication) as optional. I suppose that's what I'm complaining about.

By the way, as an author of an ASN1 decoder (for SNMP), I know how hard it is to parse ASN1 securely. If you use the right language and design, it really isn't that hard.

The sender is a mailing list with a strict no-attachments

policy, so it could be said that they are just treating the signature like any other attachment.

However it would be a sad day if this were the norm, as signatures should be part of the solution to spam and viruses -- not part of the problem.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 29

Thursday 1 April 2004

Contents

- [Coincidental Risks -- related to electronic voting systems](#)
[Jim Horning](#)
- [Toyota music-playing robot and possible spinoffs](#)
[PGN](#)
- [April Foolproof: AT&T Alerts Consumers About the Latest Scams](#)
[Monty Solomon](#)
- [Network Solutions' "A Sucker Born Every Minute" Domain Service](#)
[Lauren Weinstein](#)
- [Fraudulent request for bank info](#)
[Ken Knowlton](#)
- [Bridge construction mismatch](#)
[Ken Knowlton](#)
- [Shuttle speed-brake gears installed backwards](#)
[Anthony Youngman](#)
- [Pontiac leap-year bug](#)
[Tom Van Vleck](#)
- [Online student election flaws](#)
[James Prescott](#)
- [Utility employees rig customer survey](#)
[Monty Solomon](#)

- [AOL unveils spam-victim sweepstakes](#)
[NewsScan](#)
 - [Wrong number leads to woman's arrest](#)
[Monty Solomon](#)
 - [Risks of confusing LAN and WAN rules](#)
[Leonard Erickson](#)
 - [Web site devoted to Word documents with unintended strikeouts](#)
[Henry Baker](#)
 - [Risks of discarded receipts](#)
[Tim Aidley](#)
 - [Exploiting Software: How to Break Code, Hoglund/McGraw](#)
[PGN](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ **Coincidental Risks -- related to electronic voting systems**

<Jim Horning <horning@acm.org>>

Thu, 1 Apr 2004 00:58:19 GMT

[The following item appears in the *Communications of the ACM*, 47, 4,

April 2004, and is reproduced here with the permission of the author,

subject to CACM copyright guidelines. PGN]

The story of the Aceville elections has received some attention in the

national press, but it is worth considering from a Risks perspective. This

column is based on reports by AP (Affiliated Press, Unusual Election Results

in Ohio Town, 2/30/04) and Rueters (Losers Question Ohio Election, 2/30/04).

The Aceville, OH, municipal elections last February -- the city's first time

using the SWERVE electronic voting system -- led to the election of the

alphabetically first candidate in all 19 races. This is an astonishing coincidence. Furthermore, every winning candidate, and Measure A, garnered 100% of the votes counted.

``I am extremely gratified by this mandate,'' said mayor-elect Neuman

E. Alfred, who received 7,215 votes in a town with 7,213 registered voters.

``This is the greatest electoral landslide since the re-election of Iraqi President Saddam Hussein.''

Byron Augusta, CEO of Advanced Automatic Voting Machines (AAVM), which

supplied the SWERVE system, denied that there was anything suspicious about

the coincidence that Alfred was also the AAVM technician in charge of the

new voting machines. ``We are confident of the integrity of our employees,

which is reflected in their unblemished record of electoral success.

Reports that Alfred installed undocumented `software patches' the day before

the election are completely unfounded. We could prove this to you, except

that the machines now contain the software upgrade that Alfred installed the

day after the election. Anyhow, our software was once certified tamper-proof by the Federal Election Commission. Any suggestion of

hanky-panky is scurrilous and un-American. We were unquestionably the low-cost bidder.''

Ohio Supervisor of Elections Ava Anheuser expressed no surprise that the

alphabetically first candidate won every race. ``Don't you believe in

coincidence?'' she asked. ``This is an example of Adam Murphy's Law: `If

it's logically possible, sooner or later it's bound to happen.'
AAVM
downloaded the totals from the voting machines three times.
There's nothing
else to recount.''

Rueters reported that several voters claimed to have voted for
losing
candidates, including mayoral candidate Zeke Zebronski, who
said, ``I know
this election was crooked. I voted for myself three times, and
still got no
votes.' ' However, the *Aceville Advertiser* conducted an
investigation and
concluded that the complaints were the work of ``a small group of
out-of-town academic Luddites with a paper fetish,' ' and ``an
even smaller
group of agitators for `alphabetic equality'.' ' ``They should
remember that
'America' starts and ends with A,' ' chided *Advertiser* Editor-
in-Chief Ada
Augusta.

Pundits are divided on whether this election was a statistical
fluke, or is
the harbinger of a statewide, or even national, trend. But many
politicians
are taking no chances. The Democratic Party is scrambling to
find an A
presidential candidate. ``We just don't see how Clark or Dean
can beat Bush
in this environment,' ' said party spokeswoman April Brown. The
newly-renamed All American Party's entire Ohio slate has filed
to legally
change their names, to Aaron Aaren, Abigail Aaren, etc. ``It's
like one big
family,' ' said party secretary Absalom Aaren, ``and we expect to
do very
well in the next election.' '

The American Association of the Mentally Challenged has pressed
for national
adoption of the SWERVE system. Spokeswoman Ada Augusta stressed

that ``This is the only available system that guarantees that your vote will be counted, whether you can cast it or not. And it will bring jobs to Aceville.''

Measure A provided tax-exempt bond funding for the Aceville Automation Park, which will house new headquarters for both AAVM and the *Advertiser*.

On a lighter note, the American Automobile Association was elected Dog Catcher, even though it wasn't on the ballot. ``This seems to be the first time a write-in candidate has been elected without any write-ins,' said an AAA insider, who spoke on condition of anonymity.

Regular readers of ``Inside Risks'' know that there is an important distinction between coincidence and causality. The fact that A preceded B does not mean that A caused B. The order of the candidates probably didn't influence enough voters to change Aceville's landslide results. However, ``out of an abundance of caution,' election officials should have followed the advice of People for Randomized Alphabetic Ballots (PRAY4Ps). Putting names on the ballot in random order preserves faith in the fairness of the election. Of course, it is still possible for a random permutation to leave names in alphabetical order. Wouldn't *that* be a coincidence? I'd be happy to Risk It.

[Jim Horning <horning@acm.org> is a member of the American Association for April Foolishness, and a co-founder of PRAY4Ps.]

✦ Toyota music-playing robot and possible spinoffs

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

Thu, 1 Apr 2004

Relating to the Toyota music-playing robot item some of you may have seen (replicated below), the extension of the concept from trumpets to other brass-family instruments is relatively straightforward: trumpets, French horns, valve trombones, and tubas all have the same basic mathematically based fingering system (relative to the fundamental of the instrument).

In order to provide a well-disciplined robotic brass band, Toyota will need to implement a real-time distributed operating system by which each robot can interoperate. This system would allow tight synchronization among the players to be controlled by a robot conductor, where all the robots are integrated into a wireless local network. Arbitrary music can be downloaded on a per-instrument-type basis with fingering plans akin to those of a remotely controlled player piano, so that the group could easily expand its repertory.

This approach would even facilitate performance of musical works such as Gabrielli's antiphonal compositions for multiple brass quartets and quintets dispersed around a concert hall or outdoor space. One of the standard problems in the past has been the acoustic delays, which tend to

create long
gaps between antiphonal responses, somewhat similar to remote
news
commentators linked by satellite communications.

The risks are numerous, although not onerous [one-rous? two-
rous?].

Perhaps other robots could also provide a chorus:

* Blue screens, smiling at me,
Nothing but blue screens do I see.
(Accidental or intentional denial of service attacks,)

* Wrong song, screeching at you,
Nothing but wrong song; you can sue.
(Given the general insecurity of wireless networking
and operating systems, and the dynamic downloadability of
music files, it is likely -- for example -- that ribald,
raucous, or otherwise inappropriate tunes might be
maliciously
substituted for liturgical music. This would be likely to
stir
up Congressional legislation to protect robot vendors from
liability under such circumstances.)

* I've got plenty of nothin',
And nothin's got plenty of me.
(Accidental deadly embraces caused by certain Trojan-horsey
note
sequences, security flaws caused by basso overflow, etc.)

This message is a trum-pet-er swan song
(inspired by a famous star of the previous century, Glorious
Swansong).

Date: Fri, 12 Mar 2004 09:38:39 -0700
From: "NewsScan" <newsscan@newsscan.com>
Subject: Toyota robot toots its own horn

Toyota has taken the wraps off its latest venture in humanoid
robotics --
a 4-foot (120cm) tall machine that plays "When You Wish Upon a
Star" on a

trumpet. The automobile company says it hopes to form a robot band to

play at the 2005 World Exposition in Japan next year. The musibot is the

latest entry in an increasingly competitive rivalry with Honda, whose

Asimo robot walks around, and Sony, whose Qrio sings, dances, and jogs.

[BBC News 11 Mar 2004; NewsScan Daily, 12 Mar 2004]

<http://news.bbc.co.uk/1/hi/technology/3501336.stm>

[I suppose that a robot text editor might perform a fontal robotomy

on this issue of RISKS. PGN]

[Important note: The NewsScan item above is not April Foolishness.

The same is true of the following items in this issue. PGN]

✶ April Foolproof: AT&T Alerts Consumers About the Latest Scams

<Monty Solomon <monty@roscom.com>>

Wed, 31 Mar 2004 17:47:16 -0500

PRNewswire: This April Fool's Day, AT&T wants to warn consumers about some of the latest scams being perpetrated on the unsuspecting public.

"Awareness certainly helps consumers from being bilked," said Robert Cruz,

consumer affairs director for AT&T. "We try to be vigilant about

detecting new fraud and alerting consumers so they won't fall prey to ever

more resourceful lawbreakers."

Beware of the following schemes:

Star-7-2, billing back to you: You receive a call from a stranger posing as a telephone technician or telling you that he has been arrested for driving with a suspended license and is in jail -- or is in a situation that requires your immediate help. "I need to reach my wife and tell her what happened so she can pick up our two kids. Would you dial *72 and then her number?"

Star-7-2 is a custom feature for call forwarding. When the customer dials *72 followed by a telephone number, it activates the call forwarding feature causing all your incoming calls to ring at another number. At the end of the other line -- whether calls have been forwarded to a landline, a cell phone or a payphone -- the original caller's partner-in-crime is able to accept all collect and third-party calls, while telling your own legitimate callers that they have the wrong number. You get billed for all calls made because your number is the one from which they are forwarded. This ingenious scam, which even overrides cell phones inability to get collect calls, may go on for several days before you become aware it has occurred.

*72, Not for you: Do not accept collect calls from individuals you don't know, regardless of who they claim to be. Also, never activate *72, the call forwarding feature, unless you yourself wish to have calls forwarded elsewhere.

Within the sound of my voicemail: Hackers can compromise your voicemail

system in order to make fraudulent collect, third party or direct-dial

calls. Hackers make use of an out-calling feature on many systems that

allows them to make the calls at your expense. It isn't until you receive

notification from your telephone company's security group, notices

something different about your voicemail greeting, or receive a large bill

that you realize you have become a victim.

To prevent this:

- * Always change the default password provided by your voicemail vendor.

- * Choose a complex voicemail password, of at least six digits, so it's difficult for a hacker to guess.

- * Don't use obvious passwords such as an address, birth date or phone number.

- * Change your voicemail password often.

- * Check your announcement regularly to ensure the greeting is indeed

yours. (Owners of small businesses should consider disabling the

auto-attendant, call-forwarding and out-paging capabilities of

voicemail (if these features are not used), because those features also can be hacked.

[...]

For these and other tips on avoiding telecommunications and Internet fraud,

visit www.att.com/consumertips . Don't be an April Fool today or any day.

- <http://finance.lycos.com/home/news/story.asp?>

[story=40974362](#)

⚡ Network Solutions' "A Sucker Born Every Minute" Domain Service

<Lauren Weinstein <lauren@vortex.com>>

Wed, 24 Mar 2004 10:25:40 -0800 (PST)

When I first heard about this my initial reaction was that it must be a joke. Sadly, it is not. It appears we not only have to worry about spammers, scammers, and other illicit fraudsters on the Net, but now the vested, 800-pound gorilla of domain name registrations, Network Solutions (recently spun-off from our friends at VeriSign) has a new plan to try fleece the masses -- a "100 Year" domain registration service! I kid you not -- they're sending out the e-mails promoting this gem as I type these words.

Yes, boys and girls, just send Network Solutions your non-refundable renewal fee in the amount of \$999, and they'll renew your domain every year for an Entire Century. Never mind that domain names and the Internet are unlikely to even exist as we know them now *long* before a hundred years have elapsed. Forget about the fact that Network Solutions itself (as well as everyone reading this message) is likely to have vanished from the scene well before 2104. For that matter, we'll be damn lucky if *civilization*

still exists by that time.

It appears that we now have a new textbook definition of greed, along with treating the entire Internet community like a pack of imbeciles. But then, anyone who falls for Network Solutions' "No worries for 100 years" service will themselves have given new meaning to the concept of a sucker.

http://www.networksolutions.com/en_US/name-it/popup-100-yr-term.jhtml

Lauren Weinstein lauren@pfir.org +1 <http://www.pfir.org/lauren>
(818) 225-2800
People For Internet Responsibility <http://www.pfir.org> <http://www.factsquad.org>

✶ Fraudulent request for bank info

<Ken Knowlton <KCKnowlton@aol.com>>

Mon, 29 Mar 2004 12:08:16 EST

On 25 Mar 2004, I received, not a surprise, but just another example of fraudulent requests for personal information. My local branch officer, after some reflection and search, said that yes, a week earlier, they were notified of the scam and that action was being taken to shut down the site (no mention of trying to apprehend the culprits). The complete e-mail to me appears below. What does surprise me is that it is so obviously a spoof.

- - - - -

Dear Member,

This e-mail was sent by the [bankname] server to verify your e-mail address. You must complete this process by clicking on the link below and entering your [bankname] ATM/Debit Card number and PIN that you use on ATM. This is done for your protection because some of our members no longer have access to their e-mail addresses and we must verify it. This is to prevent any type of online fraud. [bankname] is made to protect your identity online.

To verify your e-mail address and protect your [bankname] account, click on the link below. If nothing happens when you click on the link (or if you use AOL), copy and paste the link into the address bar of your web browser.

[URL removed. no longer valid. PGN]

Thank you for using [bankname].

✶ Bridge construction mismatch

<KCKnowlton@aol.com>

Tue, 30 Mar 2004 13:54:52 EST

German and Swiss engineers, finally connecting their respective parts of the new Upper Rhine Bridge in Laufenberg, Germany, discovered that one half had been built 54 cm lower than the other, requiring massive reconstruction.

[*Der Spiegel, 14 Jan 2004, *Salt Lake Tribune* 2 Feb 2004].

(There must be a lesson in this debacle somewhere.)

[Someone must have had No-Pfaltz insurance. PGN]

✶ Shuttle speed-brake gears installed backwards

<"Anthony Youngman" <Anthony.Youngman@eca-international.com>>

Wed, 24 Mar 2004 09:36:37 -0000

A space shuttle has risked disaster every time it flew in the last 20 years because its speed brakes were faulty, NASA said yesterday. Gears were installed backwards on the flaps in Discovery's tail. They could have failed under the stress of an emergency landing, causing a crash. Discovery has flown 30 times since 1984 without a problem. The reversed gears were found in an actuator which works the flaps -- they stick out to create drag and slow the craft in flight. NASA, which is blaming subcontractor Hamilton Sunstrand, said it would replace parts on all three shuttles before restarting missions after last year's Columbia disaster.

[Source: London

Metro, 24 Mar 2004. See also

<http://www.siliconvalley.com/mld/siliconvalley/news/8250895.htm>

Original PGN URL requires AOL login :

<http://aolsvc.news.aol.com/news/article.adp?id=20040322213609990004>

(noted by Ken Knowlton). PGN]

✶ Pontiac leap-year bug

<Tom Van Vleck <thvv@multicians.org>>

Tue, 23 Mar 2004 07:01:05 -0500

``Due to a software glitch, the computer display in the 2004 model year Grand Prix shows the wrong day of the week, Pontiac spokesman Jim Hopson said on Monday. Engineers overlooked the fact that 2004 is a leap year, with an extra day, ''

http://story.news.yahoo.com/news?tmpl=story&cid=583&ncid=583&e=4&u=/nm/20040322/od_nm/autos_gm_leapyear_dc

Jerry Saltzer's story on Multics calendar calculations is at <http://www.multicians.org/jhs-clock.html>

What worries me is, what ELSE did the GM guys overlook?

✶ Online student election flaws

<James Prescott <prescotj@telusplanet.net>>

Tue, 23 Mar 2004 17:25:50 -0700

According to the Calgary **Herald**, 23 Mar 2004, the Student Union Review Board on 22 Mar 2004 ordered a complete new election. There is apparently a higher level of appeal within the Students' Union, so the story

may not be entirely over. The *Herald* story did not add any details not already known about the flaws in the online voting software.

Excerpts from Chris Beachamp, Online voting glitches?, "The Gauntlet", the student newspaper of the University of Calgary, in Calgary, Alberta, Canada, 18 Mar 2004, regarding potential flaws in the online voting system used in this year's Students' Union General Election (PGN-ed):

Sorex Software Inc. ``discovered an issue that allows for the possibility for the system to mix up one voter for another.' ' The system slowed down due to the larger than normal ballot size and "significantly larger HTML data" in the ballot code, which was too large for the word processor software! ``The slow down may have caused some voters to leave their voting stations before their ballot was complete. This could have allowed another voter to [log in] and complete the first voter's ballot.' '

Because of the anonymity, it was impossible to trace how often this problem might have occurred. Sorex allegedly violated a number of SU election bylaws. Citing irregularities in the online voting system, including voters logging in to find their ballots already selected or even closed, the petition claims system crashes ``affected the overall integrity of the election process and compromised the election result.' '

Utility employees rig customer survey

<Monty Solomon <monty@roscom.com>>

Thu, 18 Mar 2004 13:42:08 -0500

A Southern California Edison customer-satisfaction survey was spoofed by at least 12 employees who had altered system data in order to have their friends and relatives receive survey calls and provide glowing reports.

The company apparently thereby falsely received millions of dollars based

on the survey! [Source: Reuters, 17 Mar 2004; PGN-ed]

<http://www.boston.com/news/odd/articles/2004/03/17/>

[utility_employees_rig_customer_survey/](http://www.boston.com/news/odd/articles/2004/03/17/utility_employees_rig_customer_survey/)

AOL unveils spam-victim sweepstakes

<"NewsScan" <newsscan@newsscan.com>>

Tue, 30 Mar 2004 09:20:48 -0700

America Online is launching a sweepstakes program that will award victims of

spam various assets seized from spammers. The top prize is a 2002 Porsche

Boxster S, purchased with the proceeds from a lawsuit settled with a spammer

-- one of five antispam lawsuits that AOL filed in federal court last

year. AOL executive VP and general counsel Randall Boe says the company sees

the sweepstakes program as a "great way to teach spammers a lesson, and

reward our members for their continued use of the 'Report Spam' button." The

sweepstakes started at 5:00 a.m. this morning and will run till

11:59

p.m. eastern time on April 8th. Details can be found at AOL.com. [*Internet

News*, 30 Mar 2004; NewsScan Daily, 30 Mar 2004]

<http://www.internetnews.com/xSP/article.php/3332991>

✶ Wrong number leads to woman's arrest

<Monty Solomon <monty@roscom.com>>

Thu, 18 Mar 2004 13:44:33 -0500

Using her cell phone, an Oklahoma woman mistakenly called her parole

officer. She was arrested after she tried to set up a drug deal. [Source:

Reuters, 18 Mar 2004, PGN-ed]

http://www.boston.com/news/odd/articles/2004/03/18/wrong_number_leads_to_womans_arrest/

✶ Risks of confusing LAN and WAN rules

<shadow@krypton.rain.com (Leonard Erickson)>

Wed, 31 Mar 2004 02:18:49 -0800

I'd noticed some time ago that I couldn't access files on one of the servers

used in yahoo groups (f4.grp.yahoofs.com) I figured it was down or some

such. I ran into this again a couple months ago and found that I still

couldn't get thru to that server.

Since my ISP had done a few odd things in the recent past, I

tried via
dial-up on another ISP and got thru.

After much swapping of cables and computers, I discovered that the
culprit was my router! A Multitech 550VPN.

Several exchanges of e-mail with tech support finally brought forth the info
that the server was being blocked because its IP address
(66.218.66.255)
ended in .255. Tech support informed me that meant it was a
broadcast
address.

I had to inform them that, no, it did **not**. Only **some**
addresses ending in
.255 are broadcast addresses and blocking the rest is badly
broken behavior.

They said they were turning the info over to the engineers. So
far, not
trace of a patch. And I discovered the same bug exists in the RF
500 as
well.

The risk is someone who **thought** they knew something deciding
to use it to
implement a "security" measure that amounts to a designed in
denial of
service for some parts of the Internet.

Leonard Erickson (aka shadow) shadow at krypton dot rain dot com

Web site devoted to Word documents with unintended strikeouts

<Henry Baker <hbaker1@pipeline.com>>

Tue, 30 Mar 2004 05:51:42 -0800

Even Microsoft itself can't keep its own people from publishing documents with deleted information in them.

The Web site below hoists Microsoft on its own petard:

<http://lcamtuf.coredump.cx/strikeout/>

✶ Risks of discarded receipts

<Tim Aidley <tim@planettimmy.com>>

Mon, 29 Mar 2004 23:32:01 +0100

Nowadays, most credit card receipts blank out portions of the credit card number so that discarded receipts cannot give it away to anyone who picks it up. However, the section of the credit card number that gets blanked out seems to vary between every shop. My wife was recently cleaning out her wallet of credit card purchase receipts and noticed that if someone was to get hold of several of her receipts, they would have enough information to piece the whole of her number together. Our local council provides green bins for everybody for them to put their waste paper, glass and tin in, which is collected every week. If a snooper was to collect someone's paper waste and get 3 or four receipts they would have enough information (as obviously they know the address) to make fraudulent charges to a card.

I suppose the RISK here is assuming that a security measure that works in a single situation will work well when multiple situations are

combined.

[We've probably discussed this problem before, but because the risks keep recurring, it is probably worth repeating. PGN]

✈ **Exploiting Software: How to Break Code, Hoglund/McGraw**

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

Mon, 22 Mar 2004 15:29:11 PST

Exploiting Software: How to Break Code

Greg Hoglund and Gary McGraw

Foreword by Avi Rubin

Addison-Wesley 2004

ISBN 0-201-78695-8

This book will rekindle the old argument long prevalent in RISKS about

whether vulnerabilities and their exploitation should be discussed openly or

whether such knowledge should be considered as hidden from public view

(security by obscurity). In RISKS, we have long favored the realities that

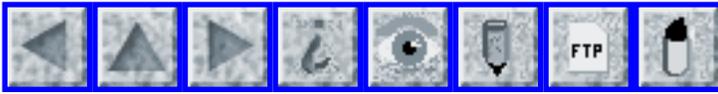
vulnerabilities do not get fixed as long as their existence is suppressed,

and that belief that supposedly hidden vulnerabilities cannot be detected by

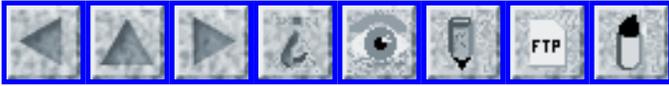
would-be attackers is simply counterproductive in the long run. The quote

from Ed Felten on the front cover sums it up nicely: ``It's hard to protect

yourself if you don't know what you are up against.'' PGN



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 30

Monday 5 April 2004

Contents

- [GM recalls Cadillac SRX](#)
[Monty Solomon](#)
- [Firetruck steers itself into tree](#)
[Caleb Hess](#)
- [800,000 cards overcharged at Wal-Mart stores](#)
[Monty Solomon](#)
- [News24's not-very-restrictive access restrictions](#)
[Cody Boisclair](#)
- [Time records often altered, job experts say](#)
[Bob Schuchman](#)
- [4.6-million DSL subscribers' data leaked in Japan?](#)
[Chiaki Ishikawa](#)
- [Pilot study of cybercrime against businesses](#)
[Michel Kabay](#)
- [Risks of broadband upgrades](#)
[Jeremy Epstein](#)
- [Too Many Pips!](#)
[Andrew Watkins](#)
- [Fighting back at spam, viruses, etc.?](#)
[Neil Youngman](#)
- [Risks of malicious code in MIDI instruments/robots](#)
[Kenji Rikitake](#)
- [Net hoaxes snare fools all year](#)

[Monty Solomon](#)

- [Re: Bridge construction mismatch](#)
[Stephen Poley Darryl Smith](#)
 - [Re: AT&T Alerts Consumers About the Latest Scams](#)
[Pekka Pihlajasaari](#)
 - [Netsky.P and iframe src=??cid variant](#)
[Rob Slade](#)
 - [Latest Citibank scam...](#)
[Cody Boisclair](#)
 - [Who's in charge of the e-mail virus war, and are we losing?](#)
[Steve Summit](#)
 - [Re: Buffer overflows and Burroughs/Unisys](#)
[Crispin Cowan](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **GM recalls Cadillac SRX**

<Monty Solomon <monty@roscom.com>>

Fri, 2 Apr 2004 17:57:08 -0500

General Motors Corp will recall 12,329 Cadillac SRXs equipped with all-wheel drive, following two reports of a software anomaly that causes a one-second delay in the anti-lock brakes activating to stop the vehicle -- reportedly only in the first few seconds of driving when the SUV is moving slowly. One owner crashed his SRX into his garage wall following the brake delay, but was uninjured. (Buick Rendezvous SUVs are also being recalled because of a faulty latch on the liftgate.) [Source: Reuters, 2 Apr 2004; PGN-ed] <http://finance.lycos.com/home/news/story.asp?story=40999216>

⚡ **Firetruck steers itself into tree**

<Caleb Hess <hess@cs.indiana.edu>>

Fri, 02 Apr 2004 13:31:39 -0500

A major US manufacturer of firefighting apparatus has begun offering an electronically controlled all-wheel steering option for its large trucks. The system offers three driver-selected operating modes, in which the rear wheels are either locked in straight-ahead position, or angled with or in opposition to the front wheels.

One such truck, owned by the town of Natick, Massachusetts, was recently involved in a collision with a tree. Firefighter union President Danny Hartwell said the truck's rear axles turned on their own as the truck traveled to a call. "The back end wrapped around a tree and there was nothing the guys could do about it," Hartwell said. The truck manufacturer examined an onboard computer and determined the accident was not caused by a mechanical error. However, the analysis also showed human error was not a factor.

Quoting from the manufacturer's description, "The entire system is designed for fail-safe operation. System interlocks and a self-diagnostic troubleshooting system are in place to enhance safety and reliability."

<<http://cms.firehouse.com/content/article/article.jsp?sectionId=46&id=28508>>

✶ 800,000 cards overcharged at Wal-Mart stores

<Monty Solomon <monty@roscom.com>>

Sun, 4 Apr 2004 22:30:53 -0400

[Source: Dan D'Ambrosio, Associated Press, 4 Apr 2004; PGN-ed]

A computer hardware problem caused more than 800,000 credit and debit

card transactions to be double- or triple-billed last week at Wal-Mart stores nationwide, according to officials at First Data Corp., which handled the electronic payments. The excess Visa and Mastercard charges, which occurred on 31 Mar 2004 and were posted on 1 Apr 2004, have been reversed, First Data spokeswoman Staci Busby said Sunday. [...]
<http://finance.lycos.com/qc/news/story.aspx?story=200404050213_APO_V3173>

First Data says glitch hit card users at Wal-Mart
4 April 2004, 4:57pm ET, Reuters
<http://finance.lycos.com/qc/news/story.aspx?story=200404042057_RTR_N04362746>

Wal-Mart Customers Affected by Computer System Disruption at First Data; Toll-Free Number Open for Consumer Inquiries
2 April 2004, 10:31pm ET, PR Newswire
<http://finance.lycos.com/qc/news/story.aspx?story=200404030331_PRN_LAF044>

News24's not-very-restrictive access restrictions

<"Cody B." <cody@zone38.net>>
Sun, 04 Apr 2004 19:38:12 -0400

Oh, my. This one ought to win some sort of award for brazen cluelessness about how the web works...

News24.co.za, a popular news site in South Africa, has begun to limit access to articles by international users-- in the same vein as the London Times' Web site, for instance-- allegedly due to "escalating international bandwidth costs". Foreign users of the site must pay a monthly registration fee in order to read the latest news from South Africa.

One minor oversight, though: users are forwarded to the registration form in question by means of a Javascript redirect. Thus, foreigners can read all of News24's articles in full, at absolutely no cost, *simply by turning Javascript off*.

I don't even think I need to point out the many things that are utterly wrong with this.

Cody "codeman38" Boisclair <<http://www.zone38.net/>> cody@zone38.net

⚡ Time records often altered, job experts say

<Bob Schuchman <schuchmanr@ieee.org>>

Sat, 03 Apr 2004 12:23:07 -0800

Here's another data modification risk: a manager altering computerized time-card records to "shave time" -- reducing the hours worked by employees,

"secretly deleting hours to cut their paychecks and fatten his store's bottom line." [Source: *The New York Times* 4 Mar 2004; PGN-ed]

<<http://www.nytimes.com/2004/04/04/national/04WAGE.html?hp>>

⚡ 4.6-million DSL subscribers' data leaked in Japan?

<Chiaki <ishikawa@yk.rim.or.jp>>

Sun, 21 Mar 2004 01:54:11 +0900

By now, the scope of the leak of 4.6 million name has been confirmed.

That is basically Yahoo/BB, the ADSL company operated by SoftBank and the

police sources admitted that the list is part of the genuine current active

users save for the subscribers who have stopped the subscription.

SoftBank

kept these names in case some inquiries were made from former subscribers.

Now, regarding the problematic data handling policy, the following is widely reported in the Japanese press.

Access logs to the data server which held the name of the subscribers were removed after one week : this makes the tracing of the route via which the leak was made almost impossible, it seems. SoftBank claims that it has lengthened the life of log files now.

There were too many people with authorized access : one account I read in a magazine stated 135 people could access it inside the company.

Adding insult to the injury, the password and ID pairs for these authorized personals seemed routinely be handed out whoever "needed" to access the list at the whim of the moment. That is, only about 40 pairs of account and password pairs were issued among 135 people. Now how can anyone reasonably figure out where the leak was?

Really a good example of what one should NOT do in handling sensitive information and seeing it at an large ISP is rather disappointing and disgusting.

Yahoo BB, the ADSL service company decided to send coupon worth 500 YEN (slight less than 5 dollars) to people whose name was leaked as a gesture of apology. I have no idea where this 500 YEN figure came from. It seems to too cheap to me.

One irate customer of Yahoo/BB did quite a striking opinion piece by selling his "personal information", exactly the info which was believed to be in the mentioned DVD, on non other than Yahoo auction site.

He started the bid at the same 500 YEN which Yahoo/BB seems to regard it to be worth, but then after 150 bids, the price went up to more than 1.5

million YEN. I have not followed it and so I don't know if the auction item was removed from the site since it is "anti-social", etc..

This incidence is a really good example of what we should not do and many organizations seem to take this example seriously.

In that sense, it is a good thing, but I have no idea what bad things may happen due to the leaked list.

✦ Pilot study of cybercrime against businesses

<"Michel Kabay" <mkabay@norwich.edu>>

Thu, 1 Apr 2004 21:40:54 -0500

"Cybercrime against Businesses: Pilot Test Results, 2001 Computer Security Survey" (12 pp.) (NCJ 200639) describes the history, development, and implementation of the pilot Computer Security Survey conducted during the last half of 2002. It provides recommended improvements to be incorporated in the final questionnaire, which BJS anticipates fielding in FY 2004. (BJS) [National Criminal Justice Reference Service <<http://www.ncjrs.org>>, 1 Apr 2004, Vol 10, No 7] <<http://www.ojp.usdoj.gov/bjs/abstract/cb.htm>>

✦ Risks of broadband upgrades

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Fri, 2 Apr 2004 12:40:50 -0500

Cox Communications is currently (8:45am EST 2 Apr 2004) suffering from a

widespread outage among Virginia customers who have Toshiba 1100 series cable modems. As best as I've been able to find out from their "support" people and web page, it was an upgrade gone bad. The outage at this point has been 22 hours, and there's no estimate for when it will be fixed.

At this point there are more questions than answers, including:

- * Why is this only impacting customers with Toshiba cable modems (which, incidentally, is the brand Cox recommends!)
- * What specifically did they change that's causing the problem?
- * Why is it only impacting Virginia Cox customers?
- * Why wasn't there a recovery plan in place before pushing out a change like this?

On the positive side, this is an example of where diversity really **does** make the system more resilient: customers with other brands of cable modems are (for whatever reason) apparently immune to whatever went wrong.

[For anyone tempted to get useful information from the Cox web page, it incorrectly claims that the outage started at 7:45pm, when in fact it started no later than 2pm, and probably earlier than that.]

Update at 12:45amEST: A (purported) Cox representative reported <<http://www.dslreports.com>> that "we have an outage on a subset of our Toshiba cable modems in Northern Virginia. While performing software upgrades (DOCSIS 1.1) some of our Toshiba PCX1100 modems went off-line and are not able to come back up. [...] [we have performed this identical upgrade to many other Toshiba modems in other cities, so we're trying to determine what was unique in the NOVA case.]" I haven't gone back and read the terms of service to see if they have the right to update the software in a modem that I own....

⚡ Too Many Pips!

<"Andrew Watkins" <andrew@newlandsoftware.ltd.uk>>

Thu, 1 Apr 2004 09:51:13 +0100

BBC Radio 4 is the primary news and current-affairs Radio service in the UK.

The Greenwich Time Signal (The Pips) is a sequence of 5 short pips spaced 1

second apart followed by a longer pip, marking the turn of the hour. This

'official' time check allows people to set their watches accurately. On

23rd Mar 2004 the pips were heard on air at 12:14:55 and 17:14:55.

According to a source at the BBC, "We generate pips every 15 minutes, and

the Studio Manager has to press a button to select the pips in the 14 minutes before the pips are needed. In the old Radio 4 studio, once a set

of pips went through, they self-cancelled (unless the SM had put them on a

channel of the desk and faded them up, which they might do for operational

reasons) ... but they don't self-cancel in the new studio. We seem to have

had two Studio Managers that day who had completely forgotten that they don't self-cancel. Sadly, as more and more new systems come on line over

the next year or so, the inability of those designing the systems to properly evaluate and mitigate the risks and the lack of experience of those

using the systems will inevitably lead to an increase in such errors."

Andrew Watkins, Newland Software ltd. tel: +44 1926 640073 (01926 640073)

<<http://www.newlandsoftware.ltd.uk>>

✈ Fighting back at spam, viruses, etc.?

<Neil <no.spam.for.n.youngman@ntlworld.com.die.spammers>>

Tue, 30 Mar 2004 17:43:43 +0100

According to [esecurityplanet.com](http://www.esecurityplanet.com), a company called Symbiot is planning to launch a network security tool offering countermeasures "graduated from blocking and quarantining to more invasive techniques"

<http://www.esecurityplanet.com/prodser/article.php/11166_3327391_2>

The article points out many of the risks associated with aggressive counterattacks.

Also *The Register* claims that a Trojan is being distributed on file sharing networks, masquerading as pirate software. "The programs have circulated disguised as activation key generators and cracks for Unreal Tournament 2004, Pinnacle Studio 9, Norton Antivirus, TurboTax"

<<http://www.theregister.co.uk/content/55/36391.html>>

While this Trojan appears not to carry a dangerous payload, there's no doubt that something like this could be used to carry out some seriously malicious actions.

✦ Risks of malicious code in MIDI instruments/robots (Re: PGN, [R 23 29](#))

<Kenji Rikitake <kenji.rikita@acm.org>>

Thu, 1 Apr 2004 20:03:15 +0900

On music-playing robots: the MIDI protocol specification defines System Exclusives, which allows sending almost any kind of data without any authentication, directly to the instrument's memory. Without performing proper sanitization, any sort of System-Exclusives data can cause unexpected problems, rhythms, notes, and tunes. I hope the music-playing robots were well-protected from such attacks. [Seems unlikely. PGN]

⚡ Net hoaxes snare fools all year

<Monty Solomon <monty@roscom.com>>

Wed, 31 Mar 2004 23:14:36 -0500

<<http://wired.com/news/culture/0,1284,62794,00.html>>

⚡ Re: Bridge construction mismatch (Knowlton, [RISKS-23.29](#))

<Stephen Poley <sbpoley@xs4all.nl>>

Thu, 01 Apr 2004 15:22:41 +0200

> one half [of the bridge] had been built 54 cm lower than the other

My off-the-cuff reaction to this was to wonder if the problem was caused by

a difference in datum sea-level height between Germany and Switzerland [calculated at the North Sea and the Mediterranean, respectively] -- and to

wonder how civil engineers would fail to think of that. [See PGN note.]

Well, according to <http://www.kopa.ch/img_upload/az_bruecke.htm>, that was

indeed the cause. But the difference between Germany and Switzerland is not

54cm, but 27cm! I don't think I need to spell out the rest to RISKS readers.

Incidentally the discrepancy is not between the two halves of the bridge,

but between the bridge and the roadway on the German side, so it appears the

bridge itself was (sensibly) all surveyed from the same baseline.

[Indeed, the engineers had thought of the difference, as it is widely known in their community, but unfortunately they corrected it in the *wrong* direction, as also noted by Pete Kaiser and Markus Fleck-Graffe.

PGN]

✉ Re: Bridge construction mismatch (Re: Knowlton, [RISKS-23.29](#))

<"Darryl Smith" <Darryl@radio-active.net.au>>

Thu, 1 Apr 2004 16:33:31 +1000

Unfortunately, this is not as uncommon as it would appear. Here in Australia, Wallerawang Power Station was built over a period of about 40 years or so using two or three height datums. They started with the 'A' station, followed by the 'B' and 'C' stations. Then removed most of the 'A' and 'B' stations.

The problem was that the original site works were done on the 'A' datum which was about a meter different from the 'C' datum. This did not matter until they wanted to build a non-local coal conveyor system to replace bringing coal in by truck. Some of the design was done for the 'C' datum and some at the 'A' datum - without the knowledge of the designers.

This was only discovered once construction started, and the resulting dispute ended up in court.

Darryl Smith, VK2TDS POBox 169 Ingleburn NSW 2565 Australia
Mobile Number 0412 929 634 [+61 4 12 929 634 International]
www.radio-active.net.au - www.radio-active.net.au/web/tracking

✉ Re: AT&T Alerts Consumers About the Latest Scams ([RISKS-23.29](#))

<"Pekka Pihlajasaari" <pekka@data.co.za>>

Fri, 2 Apr 2004 22:03:14 +0200

This RISK was not at all clear until I recalled that in the United

States

many cellular calls are mostly charged to the recipient. In many networks, GSM included, the caller is charged for the full cost of the call and the recipients only pay for routing calls while the subscriber is roaming across networks.

The RISK is assuming that business models and technical constraints are globally applicable.

Pekka Pihlajasaari, Data Abstraction (Pty) Ltd pekka@data.co.za

🔥 Netsky.P and iframe src=??cid variant

<Rob Slade <rslade@sprint.ca>>

Thu, 25 Mar 2004 12:31:27 -0800

I assume that everyone is, by now, well aware of the Bagle.Q virus that used an interesting trick to spread a virus via e-mail without an attachment.

Netsky, in its latest incarnation, appears to reverse that in an intriguing twist.

I have noted, in the past few days, the sudden spurt of Netsky.P messages, and, simultaneously, queries about messages containing the string "iframe src=??cid:" in the body. (In the samples I've got the ?? has been 3D, but I don't know if this is the same in all cases.)

In the Netsky.P infected messages as they are described in the virus encyclopedias (I have checked F-Secure and Sophos in detail), the message carries a standard attachment, in the normal MIME format as:

```
Content-Type: application/octet-stream;
             name="photo.zip"
```


Content-ID:<031401Mfdab4\$3f3dL780\$73387018@57W81fa70Re>

Note that, in a reverse of the Bagle.Q trick, the URL does not actually point to an external Web site, but to a subsequent part of the same message.

(In all the samples I have received the filename used is message.scr.) The structure of the message appears to use two different known vulnerabilities in Outlook. (Given the numbers of Netsky.P that I am receiving, it is rather depressing to note that vulnerabilities that were known, in general terms, as far back as 1997, and specifically patched as early as 2001, are still effective. People, if you must use MS products, please keep them patched!)

Because of the use of the iframe vulnerability, users of mailers other than Outlook may see the message appear in various ways. In Pegasus (which I use) the message has no body, but does have a normal attachment. (In most viruses that use iframe to directly invoke the attachment, Pegasus doesn't show any attachment.)

I note that neither the Sophos nor the F-Secure encyclopedias mention this version of the message. The Trend advisory does mention the iframe vulnerability (without giving details) but not the second, and also does not mention the non-iframe version of the messages. (Having two radically different forms of messages appears to be similar to Swen.A and Swen.B, both of which produce two different types of messages, each of which is somewhat polymorphic within the version.)

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>>

🔥 Latest Citibank scam...

<"Cody B." <cody@zone38.net>>

Sat, 27 Mar 2004 13:05:43 -0500

I just received yet another one of those Citibank scams. Normally my attitude toward these things is simply one of annoyance, because they use old tricks that *should* be well-known by now, such as the fact that anything before an @ sign in the first part of a URL is interpreted as a username-- but this one was a bit more devious than most of the scams I've seen so far.

Reminiscent of the PayPal scam reported by Jacob Palme in [RISKS 23.13](#), this particular scammer eschewed using the username-in-URL trick, and instead registered a vanity domain name with 'citibank' in it! Specifically, the domain was securecitibank.us, which is registered to one Wayne Stanford in Marina, CA according to a whois lookup.
<http://www.whois.us/whois.cgi?TLD=us&WHOIS_QUERY=securecitibank.us>

Just as in the scam Palme reported, the actual URL used http rather than https, but gave the appearance of 'security' to the untrained eye because of the rather deceptive domain name used.

I wasn't fooled, of course, for a number of reasons-- most significant probably being the fact that I have no Citibank account because they have no branches in my state-- but I can see how someone who knew a bit less about the workings of the Internet and who actually had an account with the bank in question could easily be fooled by such trickery...

Cody "codeman38" Boisclair cody@zone38.net <<http://www.zone38.net/>>

🔥 Who's in charge of the e-mail virus war, and are we losing?

<Steve Summit <scs@eskimo.com>>

Thu, 25 Mar 2004 10:54:02 -0500

Three or four big virus outbreaks ago, there was a disturbing sentence in a Boston Globe article by Hiawatha Bray, along the lines of, "Clearly, computer experts still don't know how to stop these outbreaks." My immediate thought was, "Of course we do! Don't write e-mail clients that make it easy to execute untrustworthy, received, executable content!" But then I imagined a likely riposte to my assertion: "Sure, lots of problems can be solved if you're allowed to go back and rewrite and replace everything, but how can we solve the problem given the e-mail programs that are out there?"

This imaginary conversation got me to thinking: what is the general consensus, not just among RISKS readers, but across the computing industry as a whole, as to the appropriate strategy for dealing with e-mail viruses? I'm certainly not alone here in assuming that the best way, and in fact the only way, of truly eliminating the problem is to eliminate the e-mail clients -- all of them, even if it takes a while --

which do make it easy to execute untrustworthy, received, executable content. But lately I'm not so sure that this solution is so self-evident to the industry at large.

Whenever a new one of these viruses hits, the visible reactions are always the same: hasty updates to "antivirus" software, new exhortations to end users not to open suspicious attachments, new ad-hoc rules implemented in corporate e-mail gateways which block certain potentially-dangerous filename patterns (also known as "file types") in attachments.

Notice how these responses are all reactive, and dance around the real problem.

My fear, then, is that the fundamental enabling mechanism for most of these e-mail viruses -- namely, the fact that a user of a popular graphical e-mail client need only click on an executable attachment to run it -- is being or has already been tacitly reclassified. I would have blandly asserted that this aspect of those e-mail clients is and

has always been a bug, but: what if it's now, so help us, an *axiom*?

If the world at large, and those portions of the computer industry that cater to the world at large, believe that any solution to the virus problem must be designed around the "fact" that users must be able to click on executable attachments and have them run, then I'm afraid the battle is lost. That assumption concedes a huge and tragically unnecessary upper hand to the virus writers, an upper hand which is basically unbeatable.

If this assumption is, in fact, in the process of being ordained, what can we (who assume otherwise) do about it?

[If you wish to take Steve's bait and respond, PLEASE send your comments directly to him. He will summarize the responses for RISKS. TNX. PGN]

⚡ Re: Buffer overflows and Burroughs/Unisys (Hopkins, [RISKS-23.24](#))

<Crispin Cowan <crispin@immunix.com>>

Thu, 04 Mar 2004 17:07:51 -0800

> Heck, software can always make up for hardware deficiencies, right?

That's a perspective, but I disagree. Burroughs was not the only lab to experiment with language support on chip. Intel also tried this, with the i432. The result was that the RISC processors produced *crushing* performance wins over chips with complex semantics, due to the ability to heavily pipeline and thus ramp up the clock on simple instruction sets.

Thus hardware semantics enforcement ended because the hardware people discovered that it was easier to do in software.

Continuing this tradition, software semantics enforcement more or less ended when software people discovered that it was easier to do in marketing :)

[Crispin, in the business of software semantics enforcement]

[To which Bill Hopkins retorted:]

> Hardware semantics enforcement is impossible unless programs have
> enforceable semantics. C doesn't provide them, so Crispin has a
business.

Hey! C provides the semantics of a PDP11 quite well :) C is not a
programming language. C is God's Own Portable Macro Assembler. Never
forget

that, and you'll know when it is appropriate to write code in C.

CTO, Immunix <<http://immunix.com>> <<http://immunix.com/~crispin/>>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 31

Friday 9 April 2004

Contents

- [Chinooks again](#)
[Neil Youngman](#)
- [Blackout computer failure analysis](#)
[Stephen Cohoon](#)
- [Malware, auto-reply, and non-native languages](#)
[Drew Dean](#)
- [Risks in Google's New "Gmail" Service](#)
[Lauren Weinstein](#)
- [Risks in Network Solutions' domain information masking](#)
[Lauren Weinstein](#)
- [Seeing the Light might just *not* show the right contamination](#)
[Bob Heuman](#)
- [Re: Buffer overflows](#)
[Jon A. Solworth](#)
- [Re: iAPX 432](#)
[Robert I. Eachus](#)
- [Re: 4.6-million DSL subscribers' data leaked in Japan?](#)
[Curt Sampson](#)
- [Re: News24's not-very-restrictive access restrictions](#)
[Curt Sampson](#)

- [Yet another version of the Beagle social engineering](#)
[John Sawyer](#)
 - [REVIEW: "Cybersquatters Beware", Chantelle MacDonald Newhook](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ **Chinooks again**

<Neil <no.spam.for.n.youngman@ntlworld.com.die.spammers>>

Thu, 08 Apr 2004 06:42:36 +0100

The Royal Air Force bought 8 Chinook Helicopters for 259M pounds. The helicopters were supposed to be in service 6 years ago, but problems with radar systems, mean they can not fly in cloud. According to the BBC

"The Chinooks were originally supposed to be in service in 1998 but radar systems and software developed under a separate contract would not fit in the cockpit, the report said."

<http://news.bbc.co.uk/1/hi/uk/3606325.stm>

[The Chinooks are hiding in Chicrannies. PGN]

✈ **Blackout computer failure analysis**

<Stephen Cohoon <stephen.cohoon@voxpath.com>>

Fri, 9 Apr 2004 17:19:34 -0500

Kevin Poulsen of Security Focus reports on the analysis of the

Great

Northeast Blackout of August 2003 in

http://www.theregister.co.uk/2004/04/08/blackout_bug_report/
<http://www.theregister.co.uk/2004/04/08/blackout_bug_report/

> . Much is

made of the fact that the Energy Management System built by GE had a very obscure, difficult to test race condition that caused it to fail during the early stages of the blackout thus denying the operators at FirstEnergy much of the information they needed to prevent or limit the blackout.

I would agree that this is a difficult bug to root out, but there are several extremely important risks that need to be noted.

- * The alarm system failed silently - the operators did not know that it had failed and was displaying stale data.

- * The alarm queues backed up causing that host to fail - bad design that does not handle queue overflows.

- * The backup alarm queue processor kicked in and quickly failed - bad design of an allegedly high-available system

These 3 points prove that the system suffered from much more than an obscure race condition. It had truly bad design problems. Clearly, when GE created an energy management system that processed alarms they would have benefited from the experience of the telecom world where we have been building alarm monitoring systems for years. We made these mistakes years ago and they should have known that.

The best part of the article:

"But Peter Neumann, principal scientist at SRI International and moderator of the Risks Digest, says that the root problem is that makers of critical systems aren't availing themselves of a large body of academic research into how to make software bulletproof.

"We keep having these things happen again and again, and we're not learning from our mistakes," says Neumann. "There are many possible problems that can cause massive failures, but they require a certain discipline in the development of software, and in its operation and administration, that we don't seem to find. ... If you go way back to the AT&T collapse of 1990, that was a little software flaw that propagated across the AT&T network. If you go ten years before that you have the ARPAnet collapse.

"Whether it's a race condition, or a bug in a recovery process as in the AT&T case, there's this idea that you can build things that need to be totally robust without really thinking through the design and implementation and all of the things that might go wrong," Neumann says."

✶ Malware, auto-reply, and non-native languages

<Drew Dean <ddean@csl.sri.com>>
Wed, 07 Apr 2004 11:51:54 -0700 (PDT)

I received the (excerpted, redacted) following piece of mail.

```
> From: ABCDEF HIJKLM <HIJKLM.ABCDEF@WXYZ.co.in>
> Subject: Out of Office AutoReply: good morning
>
> Hallo
> Your mails have not been received by me.
> Please send all your mail to HIJKLM.ABCDEF@NOPQRST.com.
```

My first thought was that this was a phishing expedition. Interestingly enough, all of the Received: headers in the mail seemed to be valid, and the mail was routed through NOPQRST's mail servers.

Then it hit me: NOPQRST is a large, German multinational. I'm not familiar with WXYZ, although ABCDEF HIJKLM's name sounds Indian, so that's reasonable. It must have been the case that some piece of malware (spreading its garbage) forged my name in the From: header. "Hallo" is typically German. "Please send all your mail to" is fluent, close to correct, but decidedly not idiomatic English -- easily explained if he's not a native speaker.

So we have the confluence of malware, auto-reply agents, and non-native speakers of human languages.

I decided not to forward all my spam to him. :-)

Meta-RISK: I'm not using string's of X's for redaction -- as usual, in an attempt to get through spam filters.

Drew Dean, Computer Science Laboratory, SRI International

⚡ Risks in Google's New "Gmail" Service

<Lauren Weinstein <lauren@vortex.com>>

Fri, 02 Apr 2004 07:48:14 PST

Google (or ISPs) getting into the business of routinely scanning users' e-mail for "interesting" keywords is of staggering import, even if the reason is "merely" to insert ads (or spam control, for that matter, though Google's plan to act as a massive long-term e-mail repository ups the risk ante considerably over e-mail pass-through ISPs).

What would Google's legal responsibilities and actions be if they "stumbled" across discussions of apparently illegal activity (everything from overdue library books to adultery to murder...), or terrorism, or illicit pornography? Since they've apparently opened the surveillance box, it's quite possible they'd be legally required to report everything that might even potentially fall into questionable categories.

This of course would include all the false alarms that would be generated by innocent messages that only looked suspicious but really weren't, not to mention purposely faked messages spiked with likely nasty keywords to try upset the system. Even with the best of motives, do we really want Google or ISPs becoming the commercial equivalent of Total Information Awareness? We all want to prevent crime and terrorism, but is the creation of massive surveillance machines in the guise of free e-mail services the proper way to do so in our society?

And what of the proprietary information that will inevitably find its way

into Google's scannable e-mail treasure chest? "Innocent" scanning could reveal all sorts of goodies. (I've thought in the past about all those new product names and future trademarks that first drop into Google's logs when initial searches are performed...) Can we trust Google not to abuse this potentially lucrative power? For now the answer is probably yes, but market forces make the future anything but certain.

Don't get me wrong. I like Google -- a lot. I think overall they've got a good attitude, and a superb search engine (though the privacy implications of their search logs have long been a matter of concern, as I noted). But I fear that they have not fully thought through the ramifications of their new e-mail project, and how it can, even with the best of intentions, be rapidly turned to the Dark Side. That risk won't only result from Google's decisions, but also from actions by government, lawyers, law enforcement, courts, and even ISPs and Google's competitors.

E-mail is arguably the most sensitive form of Internet communications, and deserves the highest possible levels of protection. Mere trust or good faith aren't enough.

In the classic (and highly recommended) satirical film "The President's Analyst," the protagonists gradually come to the realization that every phone call in the country is being tapped. The 1967 film has been prescient in numerous ways, and doesn't seem quite so funny anymore.

Centralized scanning of e-mail (even for ostensibly innocent commercial purposes), the push for expanded surveillance of conventional and VoIP telephone systems, and many other moves, together point towards a future where all use of telecommunications is monitored through close alliances of commercial enterprises and government, and where encryption will be banned or tightly controlled.

Even if one assumes completely benign motives on the part of these firms and governments today, what of the future? Will the incredibly powerful and pervasive monitoring infrastructures now being woven always be in the hands of such trustworthy entities?

History suggests that we have a lot to worry about in these regards.

[Incidentally, it is now being reported that Google's terms of service for

Gmail (or whatever it ends up being called if there are really trademark

problems) apparently say they can KEEP your e-mail even after you close

your account! That's what's being reported!]

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>

⚡ Risks in Network Solutions' domain information masking

<Lauren Weinstein <lauren@vortex.com>>

Mon, 29 Mar 2004 10:22:41 PST

Network Solutions (and other registrars in various ways) have begun offering services to bypass ICANN's requirement for accurate domain holder information being listed in WHOIS.

While the issues of WHOIS information accuracy and availability vs. privacy are complex and controversial, NetSol's particular approach appears to trigger a number of interesting legal questions.

For an extra charge, NetSol will mask the contact e-mail address with an aliased address that changes at intervals, list their own po box for the physical address, and list a phone number that leads to a "no calls accepted" recording.

I do not see an obvious problem with their e-mail alias approach. However, their intercepting and opening of physical mail is a different matter, since it makes it impossible for senders of certified mail to be assured that the material ever reached the actual registrant, and of course privacy of such mailings is lost. If confidential legal materials were involved, the issues could get very dicey.

Lack of an accurate phone number is of great concern. In cases of network disruptions (either intentional or not) often the only recourse to restore normal services is to pick up the phone and call the person at the domain in question. Physical mail is too slow, and if systems are disrupted e-mail often won't work.

One also must wonder if NetSol really wants to interject themselves into the middle of legal and related communications involving spammers,

pornographers, and others with less than pristine motives for wanting to hide their contact info -- the John Smith family who wants to protect their home address is not the major issue.

Finally, what actions will ICANN take to enforce both the letter and spirit of their rules in this regard, while these issues are being hashed out in various policy forums?

Lauren Weinstein lauren@pfir.org <http://www.pfir.org/lauren> +1 (818) 225-2800
Co-Founder PFIR <<http://www.pfir.org>>, Fact Squad <<http://www.factsquad.org>>

✶ Seeing the Light might just *not* show the right contamination

<"R.S. (Bob) Heuman" <rsh@idirect.com>>
Tue, 06 Apr 2004 11:01:11 -0400

The real risks with the following "New Technology" are that it depends on the light source remaining at the correct 'frequency' throughout its lifetime AND somehow letting you know when it is NOT working correctly. Until the bulb burns out you simply will not have a clue that it is not working correctly should the light wave used shift frequency or the 'marker' detection fail. There is no discussion of failure mode, unfortunately, so we could all end up deep in what the product is intended to detect.

New technology could detect dirty hands, Associated Press, 5 Apr 2004

<http://edition.cnn.com/2004/TECH/ptech/04/05/cleanhand.technology.ap/index.html>

With just a flicker of blue light, little Johnny's mother one day may know for sure whether her son washed his hands before dinner. New light-scanning technology borrowed from the slaughterhouse promises to help hospital workers, restaurant employees -- one day, even kids -- make sure that hand washing zaps some germs that can carry deadly illnesses. A device the size of an electric hand dryer detects fecal contamination and pinpoints on a digital display where on a person's hands more scrubbing is needed.

✶ Re: Buffer overflows (Cowan, [RISKS-23.30](#))

<"Jon A. Solworth" <solworth@cs.uic.edu>>
Tue, 06 Apr 2004 10:17:33 -0500

I'll take issue with Crispin Cowan's assertion that ([RISKS-23.30](#)):

"Thus hardware semantics enforcement ended because the hardware people discovered that it was easier to do in software."

The issue is not whether there is hardware semantics enforcement. All modern architectures do have hardware enforcement via privilege modes, trap instructions, and memory protection. Rather the issue is of what form they take, whether they provide only mechanism (and hence are policy neutral) and

what level of semantics they provide.

The problem of layering (whether to put the mechanism in the architecture, operating system or application is exacerbated by two issues. The first is pushing to lower levels special purpose mechanisms. The second is pushing to higher levels issues we don't understand and making them more complex. The latter is every bit as much of a problem as the former, and thereby following Hoare's dictum:

"I conclude that there are two ways to constructing software design: One way is to make it so simple that there obviously no deficiencies and the other way is to make it so complicated that there are no obvious deficiencies."

The higher levels of necessity depend on the lower levels for their security. So the question is how, not whether, the protection is provided at the various levels.

Jon A. Solworth, Computer Science Dept., University of Illinois at Chicago
Chicago, IL 60607-7053 <http://parsys.cs.uic.edu/~solworth> 1-312-996-0955

✉ **Re: iAPX 432 (Cowan, [RISKS-23.30](#))**

<"Robert I. Eachus" <rieachus@comcast.net>>
Mon, 05 Apr 2004 19:48:51 -0400

>> Heck, software can always make up for hardware deficiencies, right?

> That's a perspective, but I disagree. Burroughs was not the only lab to
> experiment with language support on chip. Intel also tried this, with the
> i432. The result was that the RISC processors produced *crushing*
> performance wins over chips with complex semantics, due to the ability to
> heavily pipeline and thus ramp up the clock on simple instruction sets.

The death or rather non-success of the iAPX-432 had very little to do with language support. It had a lot more to do with the fact that customers were not willing to pay for security--the iAPX-432 had very good hardware support for security.

But the devastating decision was a decision not to fix a "bug" in the initial version of the chip. The net effect was to make every instruction owned by a user take two memory cycles longer to complete, and every OS instruction took one more memory cycle when working with user data. It is an instructive lesson in how software fixes for hardware problems may be counterproductive.

The iAPX-432 was a capability based architecture. All resources, in particular memory were accessed through capability descriptors. The chip kept track of whether or not something was a capability, so they were not easily forged. However, in the final preproduction version of the chip, there was a glitch. As a result, the only way to expand the top-

level
capability table was to do a hardware reset. (Ouch!) Of course,
the
workaround that the developers used was to have a fixed set of
top-level
descriptors, which pushed all user owned descriptors one level
lower.

On a day when I was there for a job interview in the compiler
department,
the decision was made to ship the current version of the chip,
and fixed
this problem in a later mask release. At lunch the discussion
was not about
how bad this decision was, but where people were going to go
when they left
Intel. Needless to say, I didn't take the job. (I probably
should have --
the actual result of that decision by Intel was the founding of
two
companies: Rational and Verdix. Rational eventually bought
Verdix, and was
then acquired by IBM.)

Why was the decision by Intel so bad? Because it meant that
almost anyone
designing products around the iAPX-432 made the same workaround
decision.
Once you made that decision it didn't matter if 99.9% of the
chips your
software ran on had the fix. You had to design your software
one way or the
other. There was one company in England, High Integrity
Products was the
name I think, who instead decided not to support the first batch
of iAPX-432
chips. They had quite a good business for years. But that was
it. Well,
BiiN, a joint venture between Siemens and Intel was developing a
trusted
operating system, and there was no reason for them to support
the original
buggy chips. But Intel discontinued the 432 and disbanded the

company
before they shipped product.

It is interesting to speculate what would have happened if
absent that
decision, the 432 became the future of computing. Certainly
most viruses
would never have existed.

🔥 Re: 4.6-million DSL subscribers' data leaked in Japan?

<Curt Sampson <cjs@cynic.net>>
Tue, 6 Apr 2004 14:16:03 +0900 (JST)

> Date: Sun, 21 Mar 2004 01:54:11 +0900
> From: Chiaki <ishikawa@yk.rim.or.jp>
> ...
> Really a good example of what one should NOT do in handling
sensitive
> information and seeing it at an large ISP is rather
disappointing and
> disgusting.

It may be disappointing and disgusting, but it's my opinion that
this
is going to happen again and again. I have friends who work as
computer
technicians in various companies here, and there are other
companies
that keep similar personal information and take just as little
care
with it. Not only have the managers been informed by tech folks
time
and time again over the years that this risk exists, but even
after
management has seen this whole Yahoo brouhaha they still have
done
nothing whatsoever to make the information more secure.
Honestly, not

one single step.

I myself in the past have been in a similar position and have tried to convince managers that they should spend a little to reduce the level of risk they were undertaking, and have always had little luck.

> This incidence is a really good example of what we should not do and
> many organizations seem to take this example seriously.
> In that sense, it is a good thing...

It would be interesting to find out how many organizations have taken this example seriously, and how many have not. I can't think of any way to do this, of course; everybody's going to say, in public, that this can't happen to them. The only way to find out, if you're not part of the organization itself, is to know someone in the right place in the organization who's willing to tell you about it over a beer. And needless to say, that kind of information, when handed to someone, is probably not going further. I'm left with anecdotal evidence.

Possibly being able to buy insurance against these sorts of things would help; insurance companies would presumably then be able to come in and inspect for such situations, giving companies a direct financial incentive to fix this stuff. And I would certainly be much more inclined to use a company that had insurance that would pay me directly, say, \$250 should my personal information be compromised.

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

✈ **Re: News24's not-very-restrictive access restrictions ([RISKS-23.30](#))**

<Curt Sampson <cjs@cynic.net>>
Tue, 6 Apr 2004 14:15:38 +0900 (JST)

```
> From: "Cody B." <cody@zone38.net>
> Thus, foreigners can read all of News24's articles in full, at
> absolutely
> no cost, *simply by turning Javascript off*.
> I don't even think I need to point out the many things that
> are utterly
> wrong with this.
```

It would help me if you would do so. I have often done things in a similar style, after doing a risk and cost analysis. In those cases, the conclusion that the programming team and the customer came to, after discussion, was that a few users getting by the access restrictions was not a big problem, and the cost of that was less than the cost of modifying the system so that no users got by the access restrictions.

For a case like this, I can easily conceive of the following scenario:

1. Modifying the back-end software to deal with this would be expensive because they would have to bring in an external developer to do the work and to retest. There's also additional risk in that should a bug be introduced, they have to call in the external developer again. (They use

an external developer to do the development work on this part of the system because it doesn't change often enough to warrant hiring a full-time programmer to do the work internally.)

2. Doing the javascript redirect is very cheap, because they already have a full-time HTML guy with the expertise to do this, and the system is designed to let him easily add such things to the requisite pages in the system.

3. They currently have in place and use a system for analyzing their web logs that can tell them how many users are getting around the restriction.

None of the above points are particularly uncommon at many web-publishing organizations, and I could certainly see this being a situation where you might say, "the extra bandwidth charges for a few foreign users are not going to be substantial and there seems to be no other risk of us suffering from something we're not already suffering from now; let's do it the cheap way, and only re-implement it the more expensive way when we see that more than a certain percentage of our foreign users are getting around the restrictions."

I didn't see any indication in your message that you have sufficient information to do the analysis above and have done this analysis, and found that this javascript course was not the best one to take.

The RISK here? Perhaps it's assuming you have all the information you

need to do an analysis of whether something is a smart or stupid move.

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

✶ Yet another version of the Beagle social engineering

<=?iso-8859-1?q?John=20Sawyer?= <jpgsawyer@btopenworld.com>>
Tue, 6 Apr 2004 08:52:10 +0100 (BST)

Following up from my recent report on 16 Mar in [RISKS-23.27](#) of social engineering to get the Beagle virus onto people's systems, here is yet another attempt.

```
>Dear user of Btopenworld.com gateway e-mail server,  
  
> Some of our clients complained about the spam (negative e-mail  
content)  
> outgoing from your e-mail account. Probably, you have been  
infected by a  
> proxy-relay trojan server. In order to keep your computer  
safe, follow the  
> instructions.  
>  
> Further details can be obtained from attached file.  
>  
> Have a good day,  
> The Btopenworld.com team  
>  
> http://www.btopenworld.com
```

This time they interestingly attempt to scare people into opening the attachment by accusing them of already having had their computer compromised

and being responsible for spam. An old con trick but not one I have seen in this context before. Another interesting feature is that the message doesn't seem to have any gross grammatical errors this time something that seemed to be standard in these things before.

John Sawyer, University of Portsmouth

REVIEW: "Cybersquatters Beware", Chantelle MacDonald Newhook

<Rob Slade <rslade@sprint.ca>>

Wed, 7 Apr 2004 08:19:07 -0800

BKCYBSQT.RVW 20031118

"Cybersquatters Beware", Chantelle MacDonald Newhook, 2002, 0-07-090579-7, U\$19.95/C\$24.99

%A Chantelle MacDonald Newhook chantelle@disputewinners.com

%C 300 Water Street, Whitby, Ontario L1N 9B6

%D 2002

%G 0-07-090579-7

%I McGraw-Hill Ryerson/Osborne

%O U\$19.95/C\$24.99 905-430-5000 800-565-5758 fax: 905-430-5020

%O <http://www.amazon.com/exec/obidos/ASIN/0070905797/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0070905797/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0070905797/>

[robsladesin03-20](#)

%P 290 p.

%T "Cybersquatters Beware"

The introduction talks about branding, and the fact that companies can do it very inexpensively on the Internet. Chapter one explains

trademarks, as well as the domain name system. The Uniform Domain name dispute Resolution Process (UDRP) is outlined in chapter two (along with other similar mechanisms), and key elements necessary to winning a dispute are noted.

Successive chapters present a number of cases involving different types of principals and principles: companies (in three), institutions and individuals (in four), celebrities (five), sex (six), complaints and comments (in seven), generic names (eight), and an amalgam, in chapter nine, of airlines, banks, wineries, and other companies that have not prepared for the disputes. Chapter ten deals with the process of going to court with domain name disputes. Trends and indications in decisions are reviewed in chapter eleven.

The book does provide a good compilation of advice on a complex and poorly understood topic. There is one proviso: the text frequently makes the point that the race is not always to the justified, nor the legal battle to the prepared. However, as current wisdom has it, the prepared side is the one to bet on.

copyright Robert M. Slade, 2003 BKCYBSQT.RVW 20031118
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

Volume 23: Issue 32

Thursday 15 April 2004

Contents

- [Republicans walk out of Federal hearing on voting machines, Lynn Landes](#)
 - [USB "square" plugs](#)
[Henry Baker](#)
 - [Re: Who's in charge of the e-mail virus war ...](#)
[Steve Summit](#)
 - [Radar guns, again](#)
[Adam Shostack](#)
 - [Wireless hacking](#)
[NewsScan](#)
 - [Citibank data compromised without using it?](#)
[Art Mellor](#)
 - [Re: Chinooks again](#)
[Peter B. Ladkin](#)
 - [REVIEW: "Ethics and Technology", Herman T. Tavani](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Republicans walk out of Federal hearing on voting machines, Landes

<VoteFraud2@aol.com>

Thu, 15 Apr 2004 12:02:17 EDT

Republicans Walk Out Of Federal Hearing On Voting Machines,
While Some Civil Rights Groups Support "Paperless" Elections
by Lynn Landes www.dissidentvoice.org April 13, 2004
<http://www.dissidentvoice.org/April2004/Landes0413.htm>

As the battle over voting machines rages across the country, the U.S.

Commission on Civil Rights met on 9 Apr 2004, to examine the "Integrity, Security and Accessibility in the Nation's Readiness to Vote." Two scientists and four representatives of civil rights organizations were invited to brief the Commission.

But, before the panelists had a chance to share their views, three Republican commissioners and one (notably conservative) Independent commissioner walked out, ostensibly over a personnel dispute. But, others are not so sure.

It appears that voting technology is a topic that the Republican leadership wants to tightly control. It is without doubt that Republicans own most of the companies that manufacture, sell, and service voting machines. And President Bush and the Republican Congress appear determined to control and limit oversight of the elections industry. The Bush Administration has stacked the Election Assistance Commission with supporters of paperless voting technology, while the National Institute of Standards and Technology's (NIST) got walloped with a \$22 million budget cut in fiscal

2004, which means that NIST will have to cut back substantially on its cyber security work, as well as completely stop all work on voting technology for the Help America Vote Act.

With no mandatory federal standards or certification in place and no funding available, the Bush Administration and Republican-controlled Congress have ensured that their friends in the elections industry maintain control of voting technology and, in effect, election results.

So, at Friday's hearing, Republican members of the Commission of Civil Rights decided that the issue of voting -- the lynchpin of democracy -- should take a back seat to employee contract buyouts. Chairperson Mary Frances Berry, a Professor of History and Adjunct Professor of Law, at the University of Pennsylvania, decided to soldier on with the hearing.

And that's when the second big disappointment of the hearing became apparent. Some of America's largest civil rights organizations have lined up with the Republicans on this subject. They support 'paperless' voting technology. No fuss, no muss.

They are: Meg Smothers, Executive Director of the League of Women Voters of Georgia, Wade Henderson, Executive Director of the Leadership Conference on Civil Rights, Jim Dickson, Vice President, American Association of People with Disabilities, and Larry Gonzalez, Director, National Association of Latino Elected and Appointed Officials.

Only one panelist at Friday's hearing spoke out against paperless elections, Dr. Rebecca Mercuri, one of the nation's leading experts on computer voting security. It's a familiar muddle for Mercuri. Last year she was the only election official kicked out of the annual conference of the International Association of Clerks, Recorders, Election Officials, and Treasurers (IACREOT). The complaint was that she wasn't really an election official, which she really was. So, it was perverse justice that at Friday's hearing Mercuri found herself the only panelist invited in to defend the voter's right to verify their own paper ballot.

Make that, "alleged" ballot. Since a machine-processed ballot can only produce circumstantial evidence of the voter's intent. There was no one at the hearing to represent the point of view that only voters have the right to vote, not machines; that only voters can produce real evidence of their own intent, not machines; and that with voting machines there is no effective ability to discover vote fraud, no ability to enforce the Voting Rights Act, no real integrity or security to the voting process, at all.

The hearing was a replay of many meetings this writer has attended on the subject of voting machines. The focus was on regaining the voters' trust and confidence in voting machines, while blaming poll workers for machine "glitches" and malfunctions, and blaming the public for not being computer savvy.

The overall request of the panelists was for increased education of poll workers and the public.

Jim Dickson continued to insist that the blind could not vote without touchscreen machines, despite the fact that the paper ballot template with an audiocassette (a combination that is used in Rhode Island, Canada, and around the world), is a simpler and easier solution. As I have written in previous columns, if election officials want a fast ballot count, they can limit the size of the voting precincts or increase the number of election officials. If more elections officials are needed they can be drafted into public service as is done all year around for jury duty. Likewise, voters who don't understand English could order ballots in their own language in advance of an election.

Then there was the incredulous argument put forward that voting machines save money, as reports filter in that some communities already need to replace their 3-year-old touchscreen voting machines due to rampant equipment malfunctions, costly millions more in taxpayer dollars.

Most of the panelists insisted to Commission members that paperless touchscreen technology is the best performing voting system. But, how could they know? And performing at what? Accuracy, accessibility, vulnerability? What about performing under the U.S. Constitution and the law?

Incredibly, there has been no comparative study conducted of all voting systems on any level. The lack of comprehensive studies or

standards is an issue that the General Accounting Office (GAO) complained about in an October 2001 report. The GAO report states, "Voting machines do not have effective standards...The standards are voluntary; states are free to adopt them in whole, in part, or reject them entirely."

Forgetting for a moment about the Constitutional issue, even if there was a comprehensive technical analysis of all voting systems, it is "vulnerability" -- the ease at which votes can be manipulated or lost -- that should trump concerns about accuracy and accessibility. Let's just assume that picking up the phone and calling-in our votes was the most accurate and accessible way to vote. Can anyone reasonably argue that it would be a secure voting method?

Logic dictates that even if lots of people incorrectly fill out their ballots and lots of election officials incorrectly count up the ballots, the ability to move massive numbers of votes through technology (whether deliberately or by accident), cannot compare to simple ballot box stuffing or similar petty election crimes.

Even when we do look at the limited studies done on technical performance (overvotes and undervotes), voting machines take a back seat to hand marked, cast, and counted paper ballots. The latest Massachusetts Institute of Technology (MIT) study actually puts hand counted paper ballots at the top of the list for voting system performance for overvotes and undervotes. "The difference between the best performing and worst performing

technologies is as much as 2 percent of ballots cast. Surprisingly, (hand-counted) paper ballots -- the oldest technology -- show the best performance." This is the finding of two Massachusetts Institute of Technology (MIT) political science professors, Dr. Stephen Ansolabehere and Dr. Charles Stewart III, in a September 25, 2002 study entitled, Voting Technology and Uncounted Votes in the United States. This study was an update of a previous CalTech/MIT study.

Some of the panelists misrepresented the results of the California Recall election, once again claiming that touchscreens performed the best, when in fact, they did no such thing.

Dr. Mercuri, who has extensively studied that particular election, says, "Essentially, what the California Recall Election showed was that it was not the type of (voting) system (that matters), in other words, DREs (direct recording electronics)/touchscreen, optical scan, or punchcard, but rather the models within each of the types that could be either good or bad. For example, the second best performing system in terms of residual votes (undervotes or overvotes) was actually one of the punchcard systems. But, (it was) the type that sucks the chad out rather than leaves it hanging there. Even within particular systems, it (performance) could also be good or bad. For example, the Diebold touchscreen, which outperformed all of the systems in the yes/no California Recall question, was the eighth worst in the candidates selection. This demonstrates that it is

inappropriate to characterize an entire family of systems, or even a particular system, as good or bad just on the basis of their type. Further research has been needed for a long time on improving the usability of voting systems, but to date, funding has been lacking in comparison with the purchasing allocations."

Again, it doesn't take a PhD in computer science to conclude that vote fraud or system failure in a machine-free election simply cannot compare to the unlimited damage technology can do to the voting process. It is really a question about how risk should be managed. Should the risk of election fraud or system failure be spread out among millions of voters and thousands of poll watchers, or should it be concentrated in the hands of a few technicians - otherwise known as "putting all your eggs in one basket"?

On a personal note, having been informed by the Commission staff a few days before the hearing about the composition of the panel, that the deck was going to be stacked against voters and in favor of machines, I called and offered to testify. As one of the lead journalists covering this subject, I thought my contribution would help round out the testimony. Although my offer was declined, a member of the Commission indicated that there might be room for me at the next meeting, on May 17th. I sure hope so. Apparently, that's when the voting machine manufacturers will be speaking.

Fundamentally, it doesn't really matter if corporations or government officials control voting technology. The real issue is that

99.4% of Americans aren't really voting, machines are. But, if C-SPAN covers the hearing, perhaps the public will finally get the picture - that voting machines aren't some passive technology designed to 'assist' with the voting process. Instead, voting machines constitute a grab for power, a grab for our votes. Having voting machine manufacturers appear before the Commission could put a face on the farce that is voting in America today. And I'd sure like to be there to help that process along.

Lynn Landes is the publisher of EcoTalk.org and a news reporter for DUTV in Philadelphia, PA. 1-215-629-3553 lynnlandes@earthlink.net.

⚡ USB "square" plugs

<Henry Baker <hbaker1@pipeline.com>>

Thu, 15 Apr 2004 08:49:58 -0700

I just discovered to my dismay that the USB "square" plug does plug in backwards, although it requires a bit more pressure. I also notice that some manufacturers install the female connectors backwards, so that the roundy side is down/back, rather than up/front. Unless you actually look at the plug before you put it in, this arrangement would lead you to install the plug backwards.

So far, I haven't actually destroyed any equipment, but have cause a large number of reboots until I discovered what the problem was.

BAD USER INTERFACE!

✦ Re: Who's in charge of the e-mail virus war ... (Summit, [RISKS 23.30](#))

<Steve Summit <scs@eskimo.com>>

Tue, 13 Apr 2004 12:54:12 -0400

In [RISKS-23.30](#), I mused about whether easily clicked-to-execute attachments had reached some kind of irreversible inevitability, and inquired of RISKS readers whether we could do anything about the resulting virus infestation.

The response was gratifyingly quick and voluminous, and based on it I can state a conclusion which is not quite so gratifying: there isn't much consensus.

Several readers argued that combinations of existing strategies -- disallowing certain file types, scanning for known virus patterns, correlating sending users and systems with DNS records, etc. -- are effective. Some observed that it's an economic and/or political problem as well as a technical one, and suggested that legal remedies might be required. Several more did agree that clickable executable attachments are the root of the e-mail virus problem and that easy clickability for these attachments must be specifically removed. Others missed that point and objected that users wouldn't tolerate losing *all* their

clickable
attachments (i.e. including the non-executable, pure data
ones). But still
other readers advocated getting rid of all non-text attachments,
clickable
or not.

Perhaps the largest class of responses pointed out various
reasons why
disabling easily-clickable .exe attachments won't halt **all** e-
mail viruses.
Some virus recipients will still be tricked into installing (or
doing
whatever it takes to authorize) an executable attachment and
running it
anyway. Some non-directly-executable data types (such as Word
documents and
Excel spreadsheets) can contain macros which can carry viruses.
In light of
these difficulties, some readers conclude that the problem is
insoluble,
while others place their hopes in considerably more elaborate
proposals,
such as strong sender authentication, or safe "sandboxes" for
untrusted
code, or tiered capability-based execution environments, or a
complete
overhaul and replacement of the entire SMTP-based e-mail
infrastructure.

My purpose here was not to enter any debates about all the
various proposals
which have been floated, but I will make the observation that we
can't
afford to sit on our hands waiting for some evanescently perfect
100%
solution which either hasn't been invented yet, or would take
years to
deploy. The e-mail virus problem is **big**, so if we've got any
workable
solutions that would "only" address 90% of the problem, those
would be well
worth pursuing soon; they'd be an awful lot better than doing

nothing.

In light of the varied responses I received, I'm less sure than I was that focusing on easy clickability of executable attachments is the obvious short-term approach. But in closing, I must acknowledge David F. Skoll and Erling Kristiansen, who both made the excellent point that, quite aside from any technical solutions, we desperately need to work harder at educating people that e-mail viruses are **not** inevitable, that they neither need to be put up with nor merely reacted to. It **is** possible to eradicate them, mostly if not completely, proactively rather than reactively, and without rendering e-mail (or even attachments) useless in the process. Perhaps if more users can be made aware of these facts, they'll insist that the responsible vendors do something real, comply with some of these suggestions, to eliminate the glaring, unnecessary, not-inevitable-after-all vulnerabilities.

✶ Radar guns, again

<Adam Shostack <adam@homeport.org>>

Sat, 10 Apr 2004 09:15:04 -0400

A Belgian motorist received a speeding ticket for traveling in his Mini at three times the speed of sound. The ticket claimed the man had been caught driving at 3379 kph (2,100 mph) - or Mach 3 speed - in a Brussels suburb according to Belgian newspaper La Dernière Heure.

The police claim that human error was to blame for sending out the ticket and have since apologized to the man and promised to fix the radar.

(Interestingly, different newspapers report the ticket as being different speeds.)

<http://news.bbc.co.uk/2/hi/americas/3613715.stm>

[http://www.iol.co.za/index.php?](http://www.iol.co.za/index.php?click_id=29&art_id=iol11081526736236M522&set_id=1)

[click_id=29&art_id=iol11081526736236M522&set_id=1](http://www.iol.co.za/index.php?click_id=29&art_id=iol11081526736236M522&set_id=1)

<http://www.dhnet.be/> (but I can't find the original article)

[Suppose they had put a bounds check that was somewhat greater than

maximum that any vehicle was capable of attaining, thus preventing the

system from issuing tickets for such obviously ridiculous speeds.

Unfortunately, then if the radar was the culprit rather than the software,

the real speedsters would all get tickets for going exactly the same

default speed of the bounds check. PGN]

[So the questions are: 1) what are the failure modes of these things,

and 2) how often does the unit clock cars at mach 3? Is it easier to

filter the failure, or fix it? Are failures often enough to bother

fixing, or should we accept a silly-season story once in a while? Adam]

Wireless hacking

<"NewsScan" <newsscan@newsscan.com>>

Tue, 13 Apr 2004 06:54:28 -0700

Pointing to a rise in wireless hacking, security expert Joshua Wright of the SANS Institute warns: "All the money you've spent to protect your corporate network is moot if someone hacks your laptop at a wireless access point."

And Don LeBeau of security firm Aruba Wireless Networks says that at least one Silicon Valley company suspected it was the target of corporate espionage when it found an unauthorized device surreptitiously establishing a hot spot from a conference room. Shai Guday, group program manager for wireless at Microsoft, urges companies to take the wireless hacking threat seriously: "Wireless is happening. They can't bury their heads in the sand.

Wireless is great, but security is more important." [*USA Today*, 13 Apr

2004; NewsScan Daily, 13 April 2004]

<http://www.usatoday.com/tech/wireless/data/2004-04-13-hackers-wireless_x.htm>

✶ Citibank data compromised without using it?

<Art Mellor <art@scumpa.com>>

Sat, 10 Apr 2004 10:30:06 -0400

The other day I got a call from the Fraud Alert department at Citibank. When I called, they informed me that my Citibank card had been compromised when data was stolen from BJ's (a big discount club like CostCo and Sam's). They

noted I had probably heard about this in the news (which I had).

They said they were cancelling my card for my protection, and issuing me a new one. While I am a customer of BJs, I have never used my Citibank card there. I exclusively use my Discover card. I asked how my credit card number could be at BJs if I have never used it there. The service rep said that maybe it was some other info that had been taken, such as my birth date, SSN, etc. When I asked how issuing me a new card would protect me given that "they" already had my sensitive information, I was reprimanded for not appreciating them doing all they could to protect my identity.

I told them to cancel the card, but not issue a new one - I'd use another bank. I called Discover to ask if my information had been compromised, and according to them, my information was not on the BJs list of compromised accounts.

So what's going on here? Is there really some information that isn't the card number that can compromise the card and by getting a new card make me safe? Is Citibank pulling a scam to get me a new card with undoubtedly a new set of conditions? Did Citibank share information including my card number with BJs for some reason?

Art Mellor : Support the Cure for MS : <http://www.scumpa.com/~art/>
art@scumpa.com : <http://www.bostoncure.org> : 617/899-2360

Re: Chinooks again (Youngman, [RISKS-23.31](#))

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

Sat, 10 Apr 2004 07:44:37 +0200

Neil Youngman said in [RISKS-23.31](#), concerning the recent purchase by the UK MoD of Chinook helicopters, that are sitting on the ground because of severe restrictions on flight, that

The helicopters were supposed to be in service 6 years ago, but problems with radar systems, mean they can not fly in cloud.

This is an incorrect attribution of cause. As far as I know, there are no indications of actual system problems. The cause of the flight restrictions may be found in paragraphs 3.39-3.43 of the UK National Audit Office report "Battlefield Helicopters", 7 April 2004, available from http://www.nao.org.uk/publications/nao_reports/03-04/0304486.pdf

The report says that problems with the Chinook HC3 procurement are fourfold:

1. There is a certification problem with the software.
2. The contract did not specify that all the military requirements should be fulfilled. It was assumed that certain capabilities could be retrofitted. They haven't all been, yet.
3. The HC3 has a unique configuration, necessitating additional testing.
4. Capabilities need to be enhanced to deal with a changing operational environment.

The NAO estimates an in-service date of at least mid-2007 for a machine at

least as capable as the current HC2/2a variant used by British forces, providing additional funding (about 50% of procurement costs) is found.

The procurement contract apparently did not specify that the system software documentation and code shall be analysed according to military procurement standards on software integrity. It was apparently thought that an adequate safety case could be constructed on the basis of similar systems procured by the Royal Netherlands Air Force. This turned out not to be so.

There are two main reasons why an adequate safety case cannot easily be constructed retrospectively. One is restricted access to the source code and other development data. The other is that "legacy software is not amenable to the techniques required to confirm the robustness of software design". It is going to cost a lot and there is no guarantee of success.

"Consequently, the Chinook HC3 is currently restricted to day/night flying above 500 feet in weather clear of cloud, and where the pilot can fly the aircraft solely using external reference points without relying on the flight displays. These restrictions mean that the helicopters cannot be used other than for limited flight trials." (NAO)

Thanks to David Tombs, of the University of Queensland, for the reference.

Peter B. Ladkin, University of Bielefeld, <http://www.rvs.uni-bielefeld.de>

✶ **REVIEW: "Ethics and Technology", Herman T. Tavani**

<Rob Slade <rslade@sprint.ca>>

Mon, 12 Apr 2004 08:09:21 -0800

BKETHTCH.RVW 20031025

"Ethics and Technology", Herman T. Tavani, 2004, 0-471-24966-1, U
\$56.80

%A Herman T. Tavani

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2004

%G 0-471-24966-1

%I John Wiley & Sons, Inc.

%O U\$56.80 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0471249661/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0471249661/robsladesinterne)

<http://www.amazon.co.uk/exec/obidos/ASIN/0471249661/>

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0471249661/robsladesinte-21)

%O <http://www.amazon.ca/exec/obidos/ASIN/0471249661/>

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0471249661/robsladesin03-20)

%P 344 p.

%T "Ethics and Technology"

The preface states that this is a textbook on ethical issues in
cyber

(computer and possibly communications) technology for computer
science, philosophy, sociology, and library science students.

Chapter one is an introduction to cyberethics, providing the
concepts,

perspectives, and a methodological framework. There is more
detailed

examination of the structure of, and practical approach to,
ethics

than in any other computer ethics book I've reviewed. The
questions

at the end of the chapter are mostly simple, but some call for
analysis and judgment. Establishing a moral system, in chapter
two,

contemplates using ethics to review consequences, dealing with duty-, contract-, and character-based theories. The material is detailed but, disappointingly after the good start in chapter one, breaks no new ground. Critical thinking, logical argument, and the problems with fallacious arguments are considered in chapter three. Professional ethics are in chapter four. Chapter five has a basic but fairly complete review of privacy, better than some books on the topic (although it does retail the data mining/diapers and beer myth). Chapter six is a general introduction to security, with almost no mention of ethics. Cybercrime, in chapter seven, buys into the myth of the "evil teenage genius," and, again, has almost no mention of ethics. Chapter eight's discussion of intellectual property deals with ethics of copyright and related concepts, but is not as rigorous as chapter one. Regulation of cyberspace, in chapter nine, is similar. There is fairly standard coverage of equity, access, and employment, in chapter ten, and community and identity, in eleven.

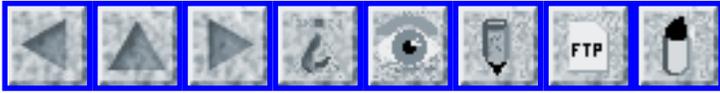
One could have hoped for a book that delivered on the promise of chapter one, but, even without, this is a worthwhile addition to the computer ethics bookshelf.

copyright Robert M. Slade, 2003 BKETHTCH.RVW 20031025

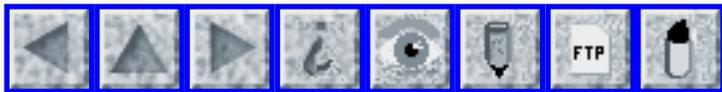
===== (quote inserted randomly by Pegasus Mailer)

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

Volume 23: Issue 33

Saturday 24 April 2004

Contents

- [University supercomputers attacked by vandals](#)
[NewsScan](#)
- [Risk of automatic updates](#)
[Geert Jan van Oldenborgh](#)
- [Runaway car from hell](#)
[Ken Knowlton](#)
- [Unfortunate MTA behavior](#)
[Drew Dean](#)
- [User interface anecdote, ATMs and voting machines](#)
[David Crooke](#)
- [Global Domination](#)
[Lauren Weinstein](#)
- [Former anti-piracy 'bag man' turns on DirecTV](#)
[Monty Solomon](#)
- [Expecting browser-side code to implement security](#)
[Derek Ziglar](#)
- [MiniDV Firewire connectors](#)
[Ron Erwin](#)
- [Risks of tax-preparation software](#)
[Toby Douglass](#)

- [Re: Cancer treatments and radiation detectors](#)
[Rob Slade](#)
 - [Squeezing the pips until they squeak](#)
[Andrew Yeomans](#)
 - [Re: Radar guns, again](#)
[Derek Ziglar](#) [Sean Sosik-Hamor](#) [Arthur T](#)
 - [Web Sites ignore the law, think it applies only to Federal Government](#)
[Bob Heuman](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **University supercomputers attacked by vandals**

<"NewsScan" <newsscan@newsscan.com>>

Wed, 14 Apr 2004 08:28:32 -0700

Network vandals have infiltrated supercomputers at as many as 20 colleges, universities and research institutions in recent weeks, disrupting the TeraGrid, a network of computers funded by the National Science Foundation and used in support of such scientific projects as weather forecasting and genome sequencing. The vandals have not been identified. None of the systems was permanently damaged, but the intruders gained the ability to control the various networks for short periods of time, prompting TruSecure security expert Russ Cooper to warn, "This could be a wake-up call to what should be very, very secure computing environments, because these machines should never have been compromised." The attacks were made against Unix machines. Stanford University computer security officer Tina Bird comments: "This incident is definitely giving us an opportunity to reevaluate the maintenance and protection we provide to our Unix systems. When you're completely focused on widespread attacks on Windows systems, it's certainly startling." [*The Washington

Post*,

13 Apr 2004; NewsScan Daily, 14 Apr 2004]

<<http://www.washingtonpost.com/wp-dyn/articles/A8995-2004Apr13.html>>

✶ Risk of automatic updates

<"Geert Jan van Oldenborgh" <oldenborgh@knmi.nl>>

Fri, 23 Apr 2004 14:47:38 +0200

At a recent workshop one of the authors presented his latest insights in seasonal predictability using his laptop connected to the beamer - not unusual. However, he was not aware that his computer also surreptitiously connected itself to the wireless network of the university, and worse, that it had determined that it was vulnerable to attack! So, suddenly a notice propped up, informing him that the latest Windows update had been installed successfully, that a reboot was necessary, and asking him whether he would like to reboot now. The only option available was [Yes], and a timer announced it would reboot anyway within three minutes. Rushing through his conclusions he just finished his presentation before this unexpected deadline.

Geert Jan van Oldenborgh <<http://www.knmi.nl/~oldenbor>>

✶ Runaway car from hell

<Ken Knowlton <KCKnowlton@aol.com>>

Sat, 17 Apr 2004 20:04:51 EDT

Source: Sarah Huntley, *Rocky Mountain News*, 2 Feb 2004,
starkly PGN-ed]

Angel Eck, driving a 1997 Pontiac Sunfire found her car racing at high speed and accelerating on Interstate 70 for 45 minutes, heading toward Denver -- with no effect from trying the brakes, shifting to neutral, and shutting off the ignition. To make a long story short, she eventually gained cell-phone coverage and called a co-worker airliner mechanic, whose suggestions failed but who then had another colleague call 911. Recalling a 1980s CHiPs TV show, police then cleared the highway into Denver, and while she was going 80 mph, a cruiser was positioned just in front of her and -- after a light initial impact -- eventually brought her car to a halt. The car was awaiting review by a GM rep to see what caused the malfunction.

✶ Unfortunate MTA behavior

<Drew Dean <ddean@csl.sri.com>>

Fri, 16 Apr 2004 11:36:02 -0700 (PDT)

I recently received a typical phishing scam. I'm reproducing the poorly done (NB: by SRI's MTA) Received: headers below.

Received: from localhost (HELO mailgate-external11.SRI.COM)
(127.0.0.1)

by mailgate-external1.sri.com with SMTP; 11 Apr 2004 14:31:00 -
0000

Received: from ibank.barclays.co.uk ([80.98.63.110])

by mailgate-external1.SRI.COM (SAVSMTP 3.1.2.35) with SMTP id
M2004041107305827172

for <DDean@CSL.sri.com>; Sun, 11 Apr 2004 07:30:59 -0700

As I'm not a Barclays customer (how many Americans are?), I
wasn't

fooled for a minute. But note the last Received: header.
Ibank.barclays.co.uk has 2 IP addresses: 62.172.239.139 and
193.128.3.139. An inverse lookup on 80.98.63.110 yields
catv-50623f6e.catv.broadband.hu.

I included the 2nd header so you can see what things should look
like.

Why it didn't note the mismatch between claimed domain and and
inverse

IP mapping is beyond me. RISK: If someone was trying to
determine the

legitimacy of this message and looked at the Received: headers,
nothing appears to be wrong. (Anyone sophisticated enough to
look at

headers hopefully won't fall for a phishing scam, but that's
another
story.)

Drew Dean, Computer Science Laboratory, SRI International

⚡ User interface anecdote, ATMs and voting machines

<David Crooke <dave@convio.com>>

Thu, 15 Apr 2004 18:14:10 -0500

I used an ATM the other day which had been upgraded with a new
touchscreen system. Judging by the UI and the design of its
overlaid
peripatetic mouse pointer, the underlying OS is an elderly MS-
Windows

variant. It was very slow to repaint the screen, and made no acknowledgement of touchscreen input whatsoever, leading to me stabbing at the touchscreen repeatedly with my finger. There was no fallback to choose options from the keypad instead of the touchscreen. I noticed that the alignment between where I touched and where the mouse pointer would gravitate to on the screen was quite a bit off. When I finally got to the screen for choosing the amount of money to withdraw, I stabbed 7 or 8 times at the \$100 button. After some delay, and still no on-screen acknowledgement, the machine dispensed \$70 - just as I was about to explode, there followed a receipt for the same amount, proving at least that it could count. I looked up, and suddenly I understood why the UI was so horrible - there before me was a little badge that said "Diebold ix".

The issues had it been a voting machine I leave to the reader.

David Crooke, Chief Technology Officer, Convio Inc.
11921 N Mopac Expy, Austin TX 78759 1-512-652 2600

✶ Global Domination

<Lauren Weinstein <lauren@vortex.com>>
Fri, 16 Apr 2004 15:49:03 -0700

The latest "Reality Reset" satire column explores the potential for manipulation of hi-tech voting systems (touch-screen voting, Internet voting, etc.).

It's in the form of a "progress report" titled:
"Global Domination Via Voting Manipulation"

and resides at:

<<http://www.vortex.com/reality/2004-04-16>>

Unfortunately, the technological scenario it postulates is far from impossible.

Lauren Weinstein lauren@pfir.org lauren@vortex.com Tel: +1 (818) 225-2800

<http://www.pfir.org/lauren> <http://www.pfir.org> <http://www.factsquad.org>

✶ Former anti-piracy 'bag man' turns on DirecTV

<Monty Solomon <monty@roscom.com>>

Fri, 16 Apr 2004 22:19:37 -0400

Former anti-piracy 'bag man' turns on DirecTV

By Kevin Poulsen, SecurityFocus, 16 Apr 2004

A one-time enforcer in DirecTV's anti-piracy campaign is suing his ex-employer for wrongful discharge, after he allegedly resigned rather than continue to prosecute the company's controversial war against buyers of hacker-friendly smart card equipment.

John Fisher, a former police officer, alleges in a complaint filed in Los Angeles County Court late last month that he joined DirecTV as a senior investigator in July, 2002, expecting to serve a legitimate investigative role tracking signal pirates. He wound up instead "as little better than a 'bag man for the mob,'" the lawsuit claims. He's

seeking unspecified damages, and an end to DirecTV's tactics.

At issue is DirecTV's end-user campaign, aimed at shutting down and collecting money from TV watchers who use smart card programmers and other equipment to get free or expanded satellite TV service. Because there's no way to trace people who are passively receiving DirecTV's signal, the company turned to a strategy of physically raiding equipment sellers that cater to pirates, using the authority of the Digital Millennium Copyright Act. The company then sends out threatening letters to everyone on the seized customer lists. ...

[<http://www.securityfocus.com/news/8472>](http://www.securityfocus.com/news/8472)

✦ Expecting browser-side code to implement security

<"Derek Ziglar" <newsletters@dziglar.com>>

Thu, 15 Apr 2004 19:06:03 -0600

I have access to the press-only section of the website for a particular company. As one would expect, it requires a login and password assigned by the manufacturer and given only to people with appropriate press credentials or equivalents. The login combination I received from them was pretty cryptic and hard to guess.

They have recently added a new feature to update your profile online. One of the fields on the form -- inside a colored box marked Admin Only -- is a drop-down selector for the login. Naturally, some programmer

foolishly populated it with their entire database of authorized logins. The supposed protection to keep one authorized user from selecting the login of another is implemented with client-side JAVA Script that pops up a message and resets the field to its original value.

The RISKS are pretty obvious. By merely selecting View/Source in your browser, you have access to a list of all their authorized logins. But even worse, since the 'security' on this field is implemented in client-side code, all one has to do is turn JAVA Script off in the browser and then there are likely no restrictions to overwriting the profile of any other authorized user.

Oh, and one of their authorized logins is 'x' -- I wonder if the password to that one would be hard to guess?

MiniDV Firewire connectors

<Ron Erwin <ronerwin@u.washington.edu>>

Fri, 16 Apr 2004 10:54:00 -0700 (PDT)

I work at the UW business school and we have been recording, editing and producing video for instructional use for over two years. Recently all of our video equipment failed connecting thru our firewire/1394 cables.

We found only one explanation for this failure, one cable was connected in

reverse to our dell workstation(with front 1394 connectors).
From this
evidence, we surmised that switching the cable at one end would
put power to
data lines and data to power lines.

This affected all our equipment like a virus, we had a few key
components
that failed and put our video production to an abrupt halt.

Consulting with our IT group and other video production areas as
the UW
brought no help. We've sent our minidv/vhs vcr to the shop for
repair,
they estimate a 600 dollar repair bill with new motherboard
etc.. Our
cameras (2) are now reduced to s-video or composite use. Last
year our vcr
also broke and required a 600 dollar repair in california. Our
dell
computer 1394 interface card still has weak protection against
installing
this cable backwards.

Why is the firewire technology so fragile? This technology
needs solid
re-engineering.

Ron Erwin, Business School, University of Washington
Ethnic Cultural Center 543-4635 Business School Technology
Center 616-9049

⚡ Risks of tax-preparation software

<Toby Douglass <toby.douglass@summerblue.net>>
Sat, 17 Apr 2004 18:38:41 +0100

I'm British and I live in England.

I've had the extreme misfortune of recently having to fill in my income tax declaration.

There is a Government web-site, www.inland-revenue.gov.uk, which does it's best to hide contact information from you, but nevertheless from which I finally managed to find a page where I can search for local tax offices, from whom I can obtain advice filling in aforementioned tax form from hell.

To find your local tax offices, there is a form into which you can enter your post code (zip code to you American types). Now things get interesting. This form returns a page which contains a map centered on your postcode and a table containing the details (address, phone, distance to, etc) of your nearest few tax offices.

This page, with the map and table, actually comes from www.multimap.com, who have a custom interface for the Inland Revenue.

Now, the problem is this; when you view the page in IE, it looks fine. When you view the page in Mozilla, the font for the table contents is **minute**. One or two pixels per character.

Now, there's no reason for this at all. Table contents are **not** hard to get right and there's no reason for this to be browser dependent. So, I felt annoyed about this, so I contacted Inland Revenue and told them about the problem.

This was six months ago.

I had to look at the page again recently, still the same problem.

I contacted Inland Revenue again. This time I received a response; to wit, the site is IE only, and that this is a browser issue, so nothing is going to be done.

I was not happy about this, because given the nature of the fault, I felt it was a case of bad or lazy programming rather than and genuine browser dependency.

So I examined the page closely and found the bug.

The DOCTYPE for the page is;

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.1 Transitional//EN">
```

This is interesting, because this *is* no HTML 4.1. The final HTML version was 4.01, release in 1998.

The consequence of this is that Mozilla renders the page in Mozilla-mode, rather than in IE-compatibility-mode.

When the DOCTYPE is corrected, to;

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
```

Mozilla renders the page correctly.

There are a number of issues here.

1. Developer mind-set; thinking "IE-only" and attributing, without investigation, all bugs in other browsers to the fact they are not IE. In fact, making a site multi-browser is an excellent way of achieving robustness, since different browsers will highlight different errors in

your code.

2. Browsers providing minimal feedback for page errors and very generously rendering broken HTML. If a browser supports broken HTML, given the quality of the mass of page writers, broken HTML will become the norm.

3. DOCTYPE syntax being sensitive, high-impact and both silent and non-obvious as the cause, in failure.

✶ Re: Cancer treatments and radiation detectors

<Rob Slade <rslade@sprint.ca>>

Fri, 16 Apr 2004 01:15:18 -0800

Radioactive prostate sets off security alert
Margaret Munro, CanWest News Service, 13 Apr 2004

In an unexpected and embarrassing complication from prostate cancer therapy, a Canadian was recently pulled aside by guards at a major airport and interrogated after radioactive "seeds" near his private parts set off security alarms.

The man, who frequently travels to the U.S., was passing through customs at an international airport late last year when he was approached by a guard, according to a report on the incident in the Canadian Medical Association Journal today.

"He was taken into a separate room where he was asked to stand against the wall and refrain from speaking while workers examined his luggage," says the report by Hamilton doctors involved in his treatment. "Eventually, he was asked why he kept setting off the radiation detector."

The man explained it might have something to do with the radioactive iodine "seeds" implanted in his prostate gland, which is tucked inside the body under the penis. The seeds emit radiation and are implanted to kill cancerous cells.

"The agents had not heard of such a procedure and called for their superior. Fortunately, the superior's brother-in-law had recently undergone an implantation procedure, and our patient was released," report doctors Ian Dayes, Jink Sathya and Ian Davis at the Hamilton Health Sciences Centre.

The amount of radiation leaking from the seeds is "minute," say the doctors, who have never heard of a patient setting off security alarms at an airport before. They believe the episode "probably occurred because of the use of increasingly sensitive radiation detection devices, especially in relation to the recent Code Orange security status invoked in the United States."

Hamilton doctors now provide a letter to patients undergoing the radioactive seed implantation which they can show to security agents.

The Edmonton Journal 2004

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>

✶ Squeezing the pips until they squeak (Watkins, [RISKS-23.30](#))

<Andrew Yeomans <andrew_yeomans@yahoo.com>>

Fri, 16 Apr 2004 11:35:17 +0100 (BST)

Andrew Watkins' article on the Greenwich Time Signal reminds me of another technology-induced risk with the pips.

The digital broadcasts of the time signal on DAB (Digital Audio Broadcasting) and Freeview are no longer accurate, due to the delays introduced by compression at the BBC and decompression at the receiver. So you might be setting your clocks about one second slow using the latest technology.

The BBC confirm this on

<http://news.bbc.co.uk/1/hi/magazine/3462079.stm>

✶ Re: Radar guns, again

<"Derek Ziglar" <newsletters@dziglar.com>>

Thu, 15 Apr 2004 19:06:17 -0600

> Date: Sat, 10 Apr 2004 09:15:04 -0400
> From: Adam Shostack <adam@homeport.org>
> Subject: Radar guns, again
>
> [Suppose they had put a bounds check that was somewhat greater than
> maximum that any vehicle was capable of attaining, thus preventing the
> system from issuing tickets for such obviously ridiculous speeds.

But the even scarier possibility is that they 'fix' it by merely

capping the maximum, so an obviously false data reading of 3000 MPH gets translated into a 'reasonable' maximum of 120MPH -- for which the automated ticket is written. Then it becomes phenomenally harder for the driver to prove he wasn't driving that speed. In effect, the system would be masking clearly erroneous data by translating it into seemingly valid data.

⚡ Re: Radar guns, again

<Sean Sosik-Hamor <sean@trunkmonkey.com>>

Thu, 15 Apr 2004 22:08:42 -0400

On Apr 15, 2004, at 06:39 PM, Adam Shostack wrote:

> A Belgian motorist received a speeding ticket for traveling in his
> Mini at three times the speed of sound.

A few months ago, I was pulled over when I was driving home from a motorsports event. The vehicle I was driving was a fully-prepared Subaru Impreza rally car, complete with SCCA ClubRally graphics, roll cage, composite seats, 6-point harnesses, and coilover suspension that's worth more than the chassis. What was I pulled over for? 137 MPH in a 65 MPH zone while traveling in a pack of traffic. Riiight.

I fully admit that I (along with everyone else) was going a little faster than I should have but, after giving me the third degree because I should "know better", the officer insisted that his radar

was correct and he would be citing me for reckless endangerment.

As

calmly as I could, I informed him that the ECU of my vehicle hard limited me to around 115 MPH, and that I'd be more than happy to fight

the ticket with the assistance of my factory service manual that listed the exact full cutoff speed.

He stuck to his guns. I stuck to my guns. Eventually, logic got the

better of him as he admitted that it was highly unlikely that the two

or three cars in front of and behind me were also traveling at 137

MPH. Especially since it took him less than a mile to catch up to me

from a dead stop on the side of the road.

I got away with a warning. ;)

The kicker? Seconds after letting me go and pulling around me into

traffic, he painted someone else and pulled them over...knowing full

well that his radar gun was throwing less than accurate readings.

Re: Radar guns, again ([RISKS-23.32](#))

<"Arthur T." <ar23hur "at" speakeasy "dot" net>>

Fri, 16 Apr 2004 02:40:42 -0400

[RISKS-23.32](#) mentioned the mini that was clocked by radar at mach 3.

Someone once said something like, "The thirteenth strike of a clock is

not only obviously wrong, but it throws great doubt upon the previous

12."

How many of the tickets generated were for believable speeds, but were bogus nonetheless? The risk of NOT sending out a mach 3 speeding ticket is that the general public would not have proof that the radars could be wildly mistaken.

Web Sites ignore the law, think it applies only to Federal Government

<Bob Heuman rsh@idirect.com>>

Fri, 16 Apr, 2004 00:18:42 -0400

I extract briefly from a 1996 paper as it seems that business AND Educational institutions and State Government units are ignoring the laws/policies that cover accessibility to their web sites.

They are therefore are risking their Federal Funding or are risking being sued for their 'violation' of the rights of the disabled.

The US Federal Government has Section 508 requirements, and the W3C has its accessibility standards.

[Note: Australia's Federal Government has legislated the W3C standards into its own requirements re Web Site accessibility, and Canada has a similar set of requirements. I believe EVERY US State has these requirements on their books as well, but there MAY be some that have ignored the issue.

1996 paper and extract

http://www.icdri.org/CynthiaW/applying_the_ada_to_the_internet.htm

United States Department of Justice Policy Ruling, 9/9/96: ADA Accessibility Requirements Apply to Internet Web Pages:

"The policy ruling states that ADA Titles II and III require State

and local governments and the business sector to provide effective

communication whenever they communicate through the Internet. The

effective communication rule applies to covered entities using the

Internet for communications regarding their programs, goods or services since they must be prepared to offer those communications

via an accessible medium...

Applying the ADA to the Internet: A Web Accessibility Standard

Therefore, as government and businesses increasingly depend on the

convenience of the Internet as a vehicle for programs, goods or services, the more it is important that accessible web design be

addressed. Accessible web design enables effective communication and

saves government resources since documents can be readily available,

requests for ADA Alternate Document Formats can be satisfied, and

Internet/Intranet access for employees with disabilities can be provided." [End of Extract]

I have found that these requirements are ignored far more than they are

met. While the business sector is specifically named in the policy from

1996 above, business seems NOT to know that. Instead they seem to feel

the rules only apply to Federal Government web sites.

In addition, there are rules clearly applying to ALL universities receiving Federal Funding in the United States, but not all schools of higher learning meet them. They apply to the State Government agencies, but I have found them not being met by one US state's Office of the CIO, Governor's Office web site. This office is now aware that they fail, and I will not name the state.

I tested the web page for Peter G. Neumann at SRI and it failed at W3C Priority 2, when I used Cynthia to do a quick test.

Verified File Name: <http://www.csl.sri.com/users/neumann/neumann.html>

Date and Time: 4/15/2004 11:14:25 PM
Failed Automated Verification

I tested the entry page for the University of Southern California, and it too failed at W3C Priority 2

Verified File Name: <http://www.usc.edu/>
Date and Time: 4/15/2004 11:19:57 PM
Failed Automated Verification

I tested Firstgov.gov and IT passed:
Verified File Name: <http://firstgov.gov/>
Date and Time: 4/15/2004 11:57:34 PM
Passed Automated Verification

BUT the National Transportation Safety Bureau failed!
Verified File Name: <http://www.nts.gov/>
Date and Time: 4/16/2004 12:00:51 AM
Failed Automated Verification

<http://www.cde.ca.gov/webstandards/access/> specifically discusses the requirements from the California Department of Education and require USC to meet all W3C priority 1, 2 and 3 accessibility rules.

To sum up, the vast majority of web page I have tested in the United States have failed to meet US requirements for accessibility.

There are both legal and societal risks in failing to accommodate the visually disabled. I leave it to those responsible for web sites to address the issue, and to PAY for fixing their problems.

There is a risk that few in the US even know of these requirements.

<http://www.access-board.gov/sec508/508standards.htm> is clearly limited to the Federal Government itself. However, some US States have legislated so that it applies at the state level as well. Various states have legislated W3C into their own accessibility requirements in addition to 508 or instead of 508.

This has been done at different levels of W3C priority application and the coverage varies widely re the state's business and businesses.

Therefore one needs to find out the laws that specifically apply to their own web site and web pages.

Even if NO law applies, it likely is a good idea to meet the needs of the disabled. Over 20% of the population in the US and in Canada is suffering from some form of visual disability, from simply being near or far sighted to being color blind to being totally blind, or having macular degeneration, etc.

Check with your own lawyer, but keep in mind that (s)he may not

have
any idea of the issue or the laws that apply, and may have a web
site
that also violates the rules.

Tests can be run at <http://www.cynthiasays.com/> or other sites if
anyone is interested.

My signature below shows I have a vested interest in the
subject. I
also admit that it is NOT a popular topic with webmasters.

A reminder: if anyone suspects their site does NOT meet the
requirements, have an INDEPENDENT auditor or expert do the
testing. The web site maintainers and designers do NOT make good
checkers of the web site they designed or work on.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 34

Wednesday 28 April 2004

Contents

- [EFF Pioneer Awards for 2004](#)
- [Fire trucks collide](#)
[Russ Perry Jr](#)
- [Innocent Brits labelled as crooks](#)
[Fuzzy Gorilla](#)
- [UK firms face weekly attacks](#)
[Graeme Wearden via Keith A Rhodes](#)
- [Quizzed upon sending e-mail](#)
[Dan Jacobson](#)
- [Aussie banking group scales up against 'phishing'](#)
[Keith A Rhodes](#)
- [Sans-serif font hides phishy text](#)
[Andrew Collier](#)
- [Risks of tax-preparation software](#)
[Paul D. Smith](#)
- [Automated Copyright Notice System](#)
[Steve Klein](#)
- [Automotive "black box" data used in trial](#)
[Fuzzy Gorilla](#)
- [Earthlink SpamBlocker](#)

[Paul Wexelblat](#)

● [Re: Unfortunate MTA behavior](#)

[Drew Dean](#)

● [Boy trapped in public bathroom](#)

[Fuzzy Gorilla](#)

● [Re: Runaway car from Hell](#)

[Bernard W Joseph](#) [Carl Fink](#)

● [REVIEW: "Network Security Essentials", William Stallings](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

EFF Pioneer Awards for 2004

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

Mon, 26 Apr 2004 9:06:20 PDT

The three winners of this year's EFF Pioneer Award (announced at Computers, Freedom, and Privacy 2004 on 22 Apr 2004) are Kim Alexander, David Dill, and Avi Rubin. The three were honored for their "pioneering work spearheading and nurturing a popular movement for integrity and transparency in modern elections."

Relating to the question of whether the vendors' claims that pre-testing and post-testing demonstrate that nothing can go wrong during an election, Kim Alexander's acceptance speech cited this quote: 'An extra bias routine could be added to the vote-counting program that would have certain characteristics to make it undetectable by the official "logic and accuracy" test. This routine could be arranged so as not to go into effect until a larger number of ballots had been counted than were in the logic

and
accuracy test sample, or could be prevented from being operative
during the
test and be activated by a computer operator only for the
official count.'

Her speech continued as follows:

"It sounds like something Dave Dill, or Avi Rubin or David
Jefferson,
or Rebecca Mercuri or any number of computer scientists might
have
said in the past year or two. But it dates back to 1970, when
computer experts, working with civil rights leader Dr. James
Farmer,
first sounded the alarm over computerized vote counting risks.

"When I first read this passage in a 1975 study by Roy Saltman,
I had a
sinking feeling. People have been warning of the potential to
accidentally
or deliberately alter election results through computer software
for
decades, ever since we started using software to count punch
card ballots in
the 1960's.

"This is not a new problem. It's an old problem that never got
solved. But
I'm optimistic we will solve it. And the reason is because we
have the
tools to do so. We have the Internet. We have the ability to
share
information, to connect with each other, and to make a public
problem so
apparent that it can no longer be ignored.

"The history of this country has been one long struggle for
freedom. It
continues today through the efforts being made by thousands of
people across
this country who are working to ensure we have voting systems
which produce

results which can be verified."

Fire trucks collide

<Russ Perry Jr <slapdash@rcn.com>>

Tue, 27 Apr 2004 21:01:11 -0500

Melrose Park, IL, was recently (today) the scene of a collision between two fire trucks heading to the same fire. There may be an inherent risk just in emergency vehicles not following the standard rules of the road in which one vehicle should have yielded, or possibly going too fast to an intersection despite being an emergency vehicle and having the right of way over normal traffic.

But more interesting is that the intersection has the Opticon (assuming I heard that right on the news) system, which changes the light to green for emergency vehicles, and no one is (yet) sure what happened as the two vehicles approached the intersection from perpendicular directions -- might it have changed to green both ways? We'll hopefully know soon, but I hope not -- shouldn't there be a failsafe that wouldn't allow two greens no matter what?

Russ Perry Jr 2175 S Tonne Dr #114 Arlington Hts IL 60005
1-847-952-9729 slapdash@rcn.com

✶ Innocent Brits labelled as crooks

<Fuzzy Gorilla <fuzzygorilla@SoftHome.net>>

Sun, 25 Apr 2004 14:42:09 -0400

193 Brits have been wrongly labelled as criminals because of mistakes in records between Jan 2003 and Feb 2004. By incorrectly linking these people to various crimes recorded on the police national computer (PNC), the Criminal Records Bureau (CRB) may have inadvertently blighted the employment prospects of scores of innocent individuals. (The CRB vets the records of people hoping to work with children or vulnerable members of society, and made over 2.5M queries during 2003.) Some of the mistakes are the result of clerical error while others are the result of offenders giving false details to police in an attempt to avoid getting a criminal record.

[Source: John

Leyden, *The Register*, 16 Apr 2004; PGN-ed]

http://www.theregister.co.uk/2004/04/16/criminal_records_snafu/

✶ UK firms face weekly attacks (Graeme Wearden)

<"Keith A Rhodes" <RhodesK@GAO.GOV>>

Wed, 28 Apr 2004 07:38:22 -0400

The UK business sector is suffering more hacking attacks, viruses and network breaches than ever before, with large companies typically being compromised every week, according to this year's official survey of British

IT security. The DTI Information Security Breaches Survey 2004 (ISBS 2004), published in full on 27 Apr 2004, showed that two-thirds of firms fell victim to a network attacks in the last year. The average cost of a serious breach has actually fallen to 10,000 pounds (\$17.900), compared to 30,000 pounds (\$53,600) in 2002, but with the number of malicious incidents on the rise the overall cost of IT security breaches remains broadly static. The results from ISBS 2004 show that many major firms are losing millions through failed IT security. The average cost of a serious break to a large company is 120,000 pounds (\$214,500), and these large firms are suffering around four breaches a month--compared to one a month for all businesses. According to e-commerce minister Stephen Timms, "We can't yet say on the base of this survey that risks are being well-managed by UK companies."

[Source: Graeme Wearden: UK firms face weekly attacks, ZDNet (UK), 27 Apr 2004]

<http://zdnet.com.com/2100-1105-5200649.html>

✶ Quizzed upon sending e-mail

<Dan Jacobson <jidanni@jidanni.org>>

Thu, 29 Apr 2004 02:54:30 +0800

I found a misspelled word on a web page so sent e-mail to the author.

I got back a message with an https address for me to confirm my mail,

Being Dan 'Batch Jobs' Jacobson, I rigged up a batch job to fetch that page, as I am not going to be hurried into clicking on things during my brief modem sessions. But no, there lay a further quiz with Enter the text you see below into the box to its right. This step is for added security. Visually impaired? Click here My batch job did not retrieve their image... and alas too late, dwindling resources upstairs say I'm no match for this.

In other news, Mom will be proud of me as I receive lots of "VIP conference invitation" spam whereas others certainly just get regular spam.

🔥 Aussie banking group scales up against 'phishing'

<"Keith A Rhodes" <RhodesK@GAO.GOV>>

Wed, 28 Apr 2004 07:40:17 -0400

The Australia and New Zealand Banking Group has reinforced its commitment to fighting online fraud and beefed up its scrutiny of large and high-risk technology projects. The "growing trend in electronic fraud" has forced it to focus very heavily on fraud prevention and detection, in response to incidents such as hoax e-mails, false Web sites and computer viruses.

[Source: Iain Ferguson and Kristyn Maslog-Levis, ZDNet Australia, 27 Apr 2004; PGN-ed]

<http://zdnet.com.com/2100-1105-5201041.html>

✶ Sans-serif font hides phishy text

<Andrew Collier <lists@intensity.org.uk>>

Tue, 27 Apr 2004 19:05:33 +0100

I recently was e-mailed an obvious (to me) phishing attempt, which is nothing new in itself but what raised my eyebrows was the way the URL was hidden. Not by exploiting browser display bugs, not by clever use of username syntax or any of the unusual URL formats, but by hiding all the information in plain sight.

To anyone using a sans-serif font, that URL might look completely genuine -- even if that person carefully reads the source code of the incoming html e-mail. In fact, throughout the whole message each lower case "l" was replaced with capital "I" (so even if the mailer draws those characters in a slightly different way, there is no discrepancy in the way they are written in the URL, so the visual cue is lost).

Risk? Throwing information away by mapping different characters onto excessively similar glyphs (though used to great effect in endless obfuscated contest entries, no doubt).

Andrew Collier <http://www.intensity.org.uk>

[It was a real glyph-hanger! PGN]

⚡ Risks of tax-preparation software

<"Paul D.Smith" <paul_d_smith@hotmail.com>>

Mon, 26 Apr 2004 08:37:45 +0100

I'm British and fill in a UK tax form. My wife is American and fills in both UK and US tax forms.

A British tax form is typically 20-odd pages, large type, lots of whitespace, with an instruction booklet that is pretty simple to comprehend. My wife's "simple" US tax form and instructions looks like a badly written, small font, thin paper telephone directory for a small city.

Having seen the two, I can't imagine how anyone can describe the UK form as difficult. Now the standard of the UK Inland Revenue's website and support? That really is another matter! Last year it was impossible to determine whose electronic software had been validated for use, unless you first registered with the website. Problem was I wanted to at least investigate the options before deciding whether to bother with electronic filing.

BTW, electronic filing will do the calculation for you. In the UK, the Inland Revenue will do this for you anyway but I was interested to know and the "do it yourself calculation guide" is always cryptic.

⚡ Automated Copyright Notice System

<Steve Klein <steveklein@mac.com>>

Mon, 19 Apr 2004 15:42:38 -0400

Vivendi Universal Entertainment and Universal Music Group have developed a software solution to automatically disable net access for people accused of illegally sharing copyrighted material.

According to the description found here:

<http://news.com.com/2100-1027_3-5194341.html?tag=macintosh>

the software, called ACNS (Automated Copyright Notice System) would be

run by universities. When a notice of copyright infringement is received, the system automatically cuts off network access for the accused.

The ACNS software is open source. The claims of infringement are submitted in a special XML-format, also open source.

There is no apparent attempt to verify the accuracy of the claim. Which means that presumably anyone can be denied net access simply by accusing them of piracy. RISKS aplenty.

Steve Klein, Phone (248) YOUR-MAC-EXPERT (or 248-968-7622)

⚡ Automotive "black box" data used in trial

<Fuzzy Gorilla <fuzzygorilla@SoftHome.net>>

Sun, 25 Apr 2004 14:37:23 -0400

The Montreal Gazette recently reported that a man was convicted in a recent traffic accident case based on data from an automotive "black box".

"Eric Gauthier, 26, was sentenced yesterday [April 14, 2004] to 18 months...." "...police [used] information culled from the data recorder, better known as a black box, from Gauthier's car." "The recording device, which stores data on how a car is driven in the last five seconds before a collision, showed four seconds before impact, Gauthier had the gas pedal to the floor. He didn't brake before impact."

References:

<http://www.canada.com/montreal/montrealgazette/news/story.html?id=6a58a759-3fb5-4862-bbc0-39238d048874>

Earthlink SpamBlocker

<Paul Wexelblat>

Mon, 26 Apr 2004 10:59:43 -0400

Stupidity/cluelessness = Risk?

I sent off an e-mail message to an acquaintance, and got, as a response a message that said that the recipient was using spamBlocker and gave me a URL to go to. When I got there I saw a form with the following (in pretty HTML}
(Asterisk strings mine)

Please complete the short form below. If mj*****@earthlink.net

chooses to allow e-mail from your address, the message(s) that have

been intercepted will be delivered immediately, and any future message(s) will be delivered without delay.

Your First Name: P&G M.I. Your Last Name: W*****

Enter your additional e-mail addresses here:

Address 1: w**@*****.com

Add other addresses (if you have more than one).

Please type a short message to mj*****@earthlink.net.
(100 characters, max.)

This step is for added security. Enter the text you see below into the box to its right.

[the usual large, but distorted anti-OCR text]

Visually impaired? Click [here](#)

I duly filled out the form, clicked submit and was told that the name field had illegal characters - only alphas, - and _ were permitted. i. e. although the & was in the e-mail as part of my name, Earthlink would not send the request message to the recipient. There was no indication as to whether this screening actually used the name in incoming e-mail messages to filter or not. (there's nothing in the standard that would limit & from the name).

The insensitivity/cluelessness issue is that, although the distorted text is quite large, the "Visually impaired? Click here" option is in their normal, small text - only a bit of thinking would have made them realize that increasing the size of a message to a visually impaired person might help.

The RISK - there may be no way for an unsophisticated Internet user (who has

an "illegal" character in their name) to get a message to the spamBlocker subscriber to add their name to the pass list.

✉ Re: Unfortunate MTA behavior (Dean, [RISKS-23.33](#))

<Drew Dean <ddean@csl.sri.com>>

Wed, 28 Apr 2004 15:01:33 -0700 (PDT)

I've received a number of replies, and so thought it might be helpful to summarize.

Peter Ladkin points out this problem is all too common. Ben Kamen points out that Sendmail can do reverse DNS (user configurable), but many domains have messed up DNS records that make this less useful.

Przemek Klosowski says: "I believe Drew is misinterpreting the Received: header. I don't know if it is written up somewhere, but in practice, most Received: headers are of the form:

```
Received: from <claimedDomain> (<lookedUpDomain>
[<observedIP>]) ..."
```

[<claimedDomain> comes from the remote MTA's SMTP HELO command.]

Uh, no, I'm not. 16 years of SMTP mail has conditioned me fairly well. I'm complaining that the MTA in question (a commercial, "anti-virus" MTA), is doing nothing to note that the <claimedDomain> may have absolutely nothing to with the numeric IP address displayed next to it. In fact, this happens

all of the time -- the same is true of legitimate mail that I receive. In Przemek's terminology, <lookedUpDomain> is always the empty string. It should do forward and/or reverse DNS lookup(s), and it would be really nice if it noted discrepancies when they occur. That this MTA is suboptimal in its use of DNS is a common RISK -- improper DNS use was one of the first bugs we (Dan Wallach, Ed Felten, and I) found in Sun's early JVM.

Patrick LoPresti points out that the behavior I observed is all too common, and probably the reverse DNS lookup failed. It worked immediately the next morning (when I first read the mail), but I can't rule out a transient failure. The really clever spammer might even launch a DoS attack against the appropriate DNS servers to try to hide their tracks. Patrick also notes experience similar to Ben's (above), that things often aren't configured properly, and goes on that he found too many false positives when he tried to use this as a spam filter.

Malcom Pack received 2 copies of the mail (from very different places), and starts along the same line as Przemek Klosowski. However, he goes on to give a concrete example where a mismatch is actually legitimate. I do, however, rather like how the MTA he uses handled the phishing mail:

```
| Received: from barclays.co.uk (wbar1.nycl-4.15.213.240.nycl.
| elnk.dsl.genuity.net [4.15.213.240])
|   by smtpserver.homeip.net with SMTP (Mailtraq/2.5.0.1568)
| id SMTPF3B8F140
|   for n@by-users.co.uk; Wed, 21 Apr 2004 08:58:38 +0100
```

Now that's what I'd like the Received: header to look like. (If you notice in the headers I provided earlier, a different SRI mail server, running a different MTA, does something similar.) And if the reverse DNS lookup fails, (as it apparently did for my mail server), I'm just asking for a warning (e.g., (reverse DNS failed [w.x.y.z])). Is that really too hard?

Jonathan de Boyne Pollard also replied. His reply starts along the same lines as Malcom Pack's, and points out that at one point this was meant for loop detection, although that has many related problems. He goes on to say:

But that's not the risk here at all. The risk here is erroneously assuming that the "HELO"/"EHLO" domain names recorded in "Received:" headers tell one anything at all, let alone that they tell one something about the legitimacy of messages. In other words: The risk is that of false conclusions being drawn from the mis-use of a protocol element for something other than its actual purpose.

Of course, the way to check a mail message, purporting to come from Barclays Bank (or anyone else), for legitimacy is the same as it always has been (both for SMTP-based Internet electronic mail and for physical mail): check that the message is signed and that the signature is valid.

These are certainly reasonable points. However, I still believe that the

observed MTA behavior I originally reported is just about the worst possible thing to do. I'm not necessarily asking for information to judge the validity of the mail message (after all, someone could break into the target's mail server, or an insider could launch a phishing scam, etc.), but to give me all observable information about the mail servers a message traversed. There are simple improvements (already present in other MTAs) that would significantly mitigate the RISK I observed.

Alas, S/MIME is still not widely deployed: I note that Jonathan's message wasn't signed. :-) And yes, I do have it (mostly) working on my end, although only in the last week or so.

My thanks to all who took the time to respond.

🔥 Boy trapped in public bathroom

<Fuzzy Gorilla <fuzzygorilla@SoftHome.net>>

Sun, 25 Apr 2004 14:18:30 -0400

The Register and the BBC recently covered a story about a boy who was trapped in an automated public bathroom.

"A young boy [thought to be 10 or 12] had to be freed by the Fire Service after becoming trapped inside an automated public lavatory in Devon... in Plymouth's Central Park on Saturday [April 17, 2004]."

They do not yet know why the boy was trapped, but apparently there is some

sort of weight sensor to detect if someone is present or not.

References:

http://www.theregister.co.uk/2004/04/22/cyberloo_kidnaps_kiddie/
<http://news.bbc.co.uk/1/hi/england/devon/3648633.stm>

✶ Re: Runaway car from Hell

<Bernard W Joseph <k8lix@arrl.net>>

Sat, 24 Apr 2004 18:05:21 -0400

I was the project manager for high speed testing for one of the Big 3 car makers. I was driving home in a company car on an Interstate highway under cruise control when a similar thing happened. Fortunately, my driver training enabled me to make my way through traffic until I found a clear spot where I could safely turn towards the median and turn off the ignition. We towed the car back to the garage.

Our garage manager told me that the small, plastic, speed-transducer gear in the transmission had disintegrated. The computer thought that the car was slowing down and moved the pedal to the metal. Now here's the risk: The computer didn't understand what the problem was. As the manager explained to me, stepping on the brake should have reset the computer speed control. But through a programming glitch, the computer did not obey the brake signal because it thought that I was already stopped. What was obviously needed was a hard electrical-reset, not a signal to reset if the program

indicated that
conditions are suitable.

This was an early production of a new transmission model. When investigation showed several similar failures, the manufacturer went back to the powdered-metal drive gear. I don't know if the software was corrected.

Thank goodness, for other drivers' sakes, that the police have learned the blocking technique to stop runaway vehicles. According to several news stories over the years since my misadventure, they have used it several times. It leads me to think that there are still glitches in drive-by-wire schemes.

Bernard W. Joseph

<http://www.appliedgrammar.com>

⚡ Re: Runaway car from hell -- or fantasyland? (Knowlton, [RISKS-23.33](#))

<Carl Fink <carlf@panix.com>>

Sat, 24 Apr 2004 17:40:07 -0400 (EDT)

I read the original coverage of this, and I don't believe it. Reports at the time also claimed the car later attacked a mechanic and pinned him to the wall of the garage.

Can anyone in RISKS-land come up with a malfunction that would simultaneously interfere with the car's ignition, transmission, and both braking systems, including the parking brake, WHICH IS

MECHANICAL AND HAS NO
LINKS TO ANY OTHER SYSTEM?

I strongly suspect this of being a hoax/urban legend.

Carl Fink, carlf@dm.net, Manager, Dueling Modems Computer Forum
<http://dm.net>

⚡ REVIEW: "Network Security Essentials", William Stallings

<Rob Slade <rslade@sprint.ca>>
Wed, 28 Apr 2004 08:41:44 -0800

BKNTSCES.RVW 20031210

"Network Security Essentials", William Stallings, 2000, 0-13-
016093-8,

U\$48.00/C\$75.81

%A William Stallings ws@shore.net

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

%D 2000

%G 0-13-016093-8

%I Prentice Hall

%O U\$48.00/C\$75.81 201-236-7139 fax: 201-236-7131

%O [http://www.amazon.com/exec/obidos/ASIN/0130160938/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0130160938/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0130160938/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0130160938/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0130160938/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0130160938/robsladesin03-20)

%P 366 p.

%T "Network Security Essentials: Applications and Standards"

The existence of this book is a bit odd, particularly in view of
the

fact that it shares so much material with Stallings'

"Cryptography and

Network Security." The (clear and structured) preface, however,

states that the intent is to provide a practical survey of network security applications and standards, particularly those in widespread use. As with the earlier work, this book is intended to serve both as a textbook for an academic course of study, and as a self-study and reference guide for practicing professionals. There is reduced detail in regard to cryptography.

Chapter one is an introduction, and provides a good list of basic concepts and vocabulary. It may not be completely apparent to all readers that the emphasis is on threats to data transmissions and there is limited review of attacks on functioning systems.

Part one deals with cryptography. Chapter two covers symmetric block ciphers in fundamental but sound terms, illustrated by an explanation of DES (Data Encryption Standard). The logic is heavily symbolic at times, but that should not be an impediment to the reader. It is interesting that chapter three views asymmetric cryptography as an extension of message authentication codes, but the explanations are articulate, including both algebraic and numeric examples, although the numeric illustrations could be fuller.

Part two deals with network security applications. Chapter four looks at authentication applications, concentrating on Kerberos and X.509. The examples of e-mail security systems given in chapter five are PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extension). Security provisions for the Internet Protocol (IP) itself

are reviewed in chapter six. Web security, in chapter seven, discusses SET (Secure Electronic Transaction) and SSL (Secure Sockets Layer). Chapter eight reviews SNMP (Simple Network Management Protocol) both in terms of network management for security purposes, and in regard to cryptography for authentication of the application itself.

Part four outlines general system security. Intruders and malicious software are lumped together in chapter nine, with a reasonable outline of the types of malware, but not dealing as well with viruses themselves. (Activity Monitors are referred to as "third generation" tools, when they actually predate both signature scanners ["first generation"] and heuristics ["second generation"].) Chapter ten finishes off the book with a description of firewalls, but has a rather odd inclusion of basic access control and trusted systems.

Each chapter ends with a set of recommended readings and problems.

Many chapters also have appendices giving additional details of specific topics related to the subject just discussed.

A very reasonable guide, although possibly less practical than it intended to be.

copyright Robert M. Slade, 2003 BKNTSCES.RVW 20031210
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

Volume 23: Issue 35

Tuesday 4 May 2004

Contents

- [Computer glitch grounds Atlanta flights](#)
[Fredric Rice](#)
- [TurboTax electronic filing option fails to send AMT Form 6251](#)
[Richard Mason](#)
- [California bans e-vote machines](#)
[Kim Zetter via Monty Solomon](#)
- [Ireland scraps electronic voting plans](#)
[Brent M.P. Beleskey](#)
- [Sydney trains disrupted by software glitch](#)
[John Colville](#)
- [Self-referential Patriot Act suppression of law suit](#)
[PGN](#)
- [Millions of lost revenue from faulty speed cameras](#)
[Bertrand Meyer](#)
- [Sasser worm is latest threat](#)
[NewsScan](#)
- [Antivirus software prolongs viral life](#)
[Geoff Kuenning](#)
- [Sasser eyed over train outage](#)
[NewsScan](#)

- [New identity-theft scam](#)
[Geoff Kuenning](#)
 - [Gas explosion creates confidential litter](#)
[Sarah Hollins](#)
 - [Hybrid vehicles may be hazardous to rescuers' health](#)
[Joe Thompson](#)
 - [TCP, BGP, DoS, and BS](#)
[Rob Slade](#)
 - [Florida sues AT&T for billing errors](#)
[Frank Carey](#)
 - [Re: Traffic Signal Controllers](#)
[Jay R. Ashworth](#)
 - [FREEDOM 2.0, Washington, DC, 20-22 May 2004](#)
[EPIC](#)
 - [REVIEW: "Non-Repudiation in Electronic Commerce", Jianying Zhou](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Computer glitch grounds Atlanta flights

<fredric.rice@invensys.com>

Tue, 4 May 2004 10:27:35 -0700

http://news.yahoo.com/news?tmpl=story&cid=509&u=/ap/20040501/ap_on_bi_ge/delta_computers&printer=1

A computer glitch kept Atlanta-bound Delta Air Lines flights on the ground

for about two hours Saturday, but the company was gradually restoring service to its main hub.

http://news.yahoo.com/news?tmpl=story&cid=562&u=/ap/20040502/ap_on_hi_te/delta_computers&printer=1

Delta told the Federal Aviation Administration it had a

problem with

dispatch computers, which calculate weight and balance and handle

information related to preparation for flight, plus gate information, FAA

spokeswoman Kathleen Bergen said.

Sounds reassuring.

✶ TurboTax electronic filing option fails to send AMT Form 6251

<"Richard Mason" <mason@unr.edu>>

Tue, 4 May 2004 10:31:45 -0700

For taxpayers who do not owe Alternative Minimum Tax (AMT), but may have sufficient items on their tax returns to require the preparation of Form 6251, TurboTax when using the electronic filing option does not send the Form 6251. This has prompted refund delays and letters from the IRS requesting the Form 6251 to be faxed or mailed. The number of taxpayers that have this problem is not known, but may be significant.

Richard Mason, Assistant Professor, MAcc Program Director, University of Nevada, Reno, College of Business Administration Reno, NV 89557
1-775-784-6886

✶ California bans e-vote machines (Kim Zetter)

<Monty Solomon <monty@roscom.com>>

Sat, 1 May 2004 00:40:39 -0400

[Source: Kim Zetter, wired.com, 30 Apr 2004]

California Secretary of State Kevin Shelley ended five months of speculation and announced on 30 Apr 2004 that he was decertifying all electronic touch-screen voting machines in the state due to security concerns and lack of voter confidence. He also said that he was passing along evidence to the state's attorney general to bring criminal and civil charges against voting-machine-maker Diebold Election Systems for fraud. "We will not tolerate deceitful tactics as engaged in by Diebold and we must send a clear and compelling message to the rest of the industry: Don't try to pull a fast one on the voters of California because there will be consequences if you do," he said. Shelley said the ban on touch-screen machines would stay in effect unless and until specific security measures could be put in place to safeguard the November vote.

<http://www.wired.com/news/evote/0,2645,63298,00.html>

✶ Ireland scraps electronic voting plans

<"Brent M.P. Beleskey" <voterscoalition@rogers.com>>

Tue, 4 May 2004 13:14:49 -0400

The Government has been forced to make an embarrassing U-turn on its electronic voting plans. Environment Minister Martin Cullen issued a statement saying that plans to introduce electronic voting in all

constituencies for the local and European elections this June were being scrapped, after the independent Electronic Voting Commission said the system was open to potential interference and its accuracy could not be guaranteed, and said it could not recommend the introduction of such a system.

[Source: PGN-ed from 30 Apr 2004 item]

<http://212.2.162.45/news/story.asp?j=125409434&p=yz54yxz97&n=125410377>

✶ Sydney trains disrupted by software glitch (Joseph Kerr)

<colville@it.uts.edu.au>

Mon, 3 May 2004 09:09:20 +1000

[Source: CityRail gremlin could strike any day, Joseph Kerr, Transport

Reporter, *Sydney Morning Herald*, 3 May 2004: PGN-ed]

<http://www.smh.com.au/articles/2004/05/02/1083436476114.html>

A mysterious computer software glitch halted half of Sydney's rail fleet on 2 May 2004. Rail officials admit they do not know what caused the breakdown in the system that keeps train drivers connected through a radio network, but it left as many as 50,000 of the usual 300,000 Sunday train travellers stranded for up to two hours. While the computer network was fixed by 1.50pm, the gremlin wasn't found, leaving open the possibility of a repeat performance on any given weekday -- when up to 950,000 commuters could be thrown into chaos.

The Glenbrook rail disaster inquiry recommended that all trains needed radio communication. According to a CityRail spokeswoman, Jane Lavender, the radios on most suburban trains are connected to a central computer so rail control and other workers can be constantly aware of the location of every train.

Red-eyed technicians had worked through Saturday night and much of yesterday to repair the computer fault. But CityRail train drivers arriving at work in the morning found their radios would not communicate properly with central control. Realising this, RailCorp officials decided about 5am to switch to alternative communications: the mobile phones and pagers carried by every train guard.

RailCorp's chief executive officer, Vince Graham, admitted it took some time to switch over and this caused train delays, and that the impact would have been much more grave on a weekday. CityRail called in 109 buses to replace the cancelled trains yesterday. It made announcements through the morning calling on passengers to avoid trains if they could, delay their journey or "make their own arrangements".

John Colville, Dept of Computer Systems, University of Technology, Sydney,
PO Box 123, Broadway NSW Australia 2007 +61-2-9514-1854
colville@it.uts.edu.au

Self-referential Patriot Act suppression of law suit (Dan Eggen)

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

Tue, 4 May 2004 11:46:52 PDT

The American Civil Liberties Union disclosed on 28 Apr 2004 that it filed a lawsuit on 6 Apr 2004 challenging the FBI's methods of obtaining many business records, but the group was barred from revealing even the existence of the case until now, to avoid violating secrecy rules contained in the USA Patriot Act. The ACLU was allowed to release a redacted version of the lawsuit only after weeks of negotiations with the government. The ACLU alleges that a section of the act is unconstitutional because it allows the FBI to request financial records and other documents from businesses without a warrant or judicial approval. The group also says such requests are being used much more broadly than they were before the Patriot Act. [Source: Patriot Act Suppresses News Of Challenge to Patriot Act Dan Eggen, *The Washington Post*, 29 Apr 2004 (Page A17); PGN-ed] <http://www.washingtonpost.com/wp-dyn/articles/A51423-2004Apr28.html>

⚡ Millions of lost revenue from faulty speed cameras

<Bertrand Meyer <Bertrand.Meyer@inf.ethz.ch>>

Sat, 01 May 2004 14:44:42 +0200

Given the attention this story has been commanding in Australia, I was surprised to find no record in RISKS. The country is proud of its strictness

in enforcing speed rules, sometimes fining motorists for driving one kilometer above the posted limit (however absurd that sounds). The state of Victoria has numerous speed cameras. Last year their accuracy was questioned after reports that a truck with a maximum speed of 140 km/h was caught traveling at 164 km/h, and other similar incidents. After the first such report the Assistant Commissioner said (Melbourne Age, 11 Nov 2003):

"There's no evidence to support that any of the other cameras are malfunctioning [...] in any other way,"

but he later had to change to:

"It's embarrassing for everybody... Technology is technology and I think we have had indications where it doesn't say the right thing."

The state government then ordered tests of all the cameras in the system, and had to suspend fines from all fixed cameras. According to the Age of 29 April 2004, the problems were supposed to "take six weeks to fix" but:

almost six months after the State Government suspended the issuing of fines from Victoria's fixed speed cameras, problems with the cameras are still unresolved [...] A State Government spokesman confirmed yesterday that the 47 fixed cameras were still under review. He was unable to say when the issue would be resolved.

More than 40,000 fines notified to motorists have been suspended until the results are in. This represents a total sum of over six million

Australian
dollars.

For details:

<http://theage.com.au/articles/2004/04/29/1083224516563.html>

(30 Apr 2004)

<http://theage.com.au/articles/2004/04/28/1083103551024.html>

(29 Apr 2004)

<http://www.theage.com.au/articles/2003/11/10/1068329487082.html?from=storyrhs>

(11 Nov 2003)

Bertrand Meyer

ETH Zurich / Eiffel Software

<http://www.se.inf.ethz.ch> -- <http://www.eiffel.com>

✶ Sasser worm is latest threat

<"NewsScan" <newsscan@newsscan.com>>

Mon, 03 May 2004 09:57:37 -0700

A fast spreading worm known as "Sasser" surfaced over the weekend and is making its way around the globe, warn computer security experts at Finland's F-Secure. The worm shares many characteristics with the Blaster worm that infected hundreds of thousands of PCs last year, says F-Secure antivirus research director Mikko Hypponen, who notes that both worms exploit relatively new holes in the Windows operating system and frequently cause computers to repeatedly reboot. However, this time more companies appear to

be ready to take preventive action, which may mitigate Sasser's damage potential. "With Sasser it seems that companies are (using software) patches better and more quickly than last year (with Blaster), but for those that are hit, they are hit hard," says Hypponen, who adds that he believes Sasser originated in Russia. The worm does not need to be activated by double-clicking on an attachment and can strike even if no one is using the PC at the time. [Reuters/*The Washington Post*, 3 May 2004; NewsScan Daily, 3 May 2004]
<http://www.washingtonpost.com/wp-dyn/articles/A62063-2004May3.html>

✶ Antivirus software prolongs viral life

<Geoff Kuenning <geoff@cs.hmc.edu>>
Mon, 3 May 2004 16:03:38 -0700 (PDT)

I was reading up on the Sasser worm this afternoon and came across the following rather interesting recommendation on Symantec's Web site:

2. To disable System Restore (Windows XP) If you are running Windows XP, we recommend that you temporarily turn off System Restore. Windows XP uses this feature, which is enabled by default, to restore the files on your computer in case they become damaged. If a virus, worm, or Trojan infects a computer, System Restore may back up the virus, worm, or Trojan on the computer.

Windows prevents outside programs, including antivirus programs, from modifying System Restore. Therefore, antivirus programs or tools cannot remove threats in the System Restore folder. As a result, System Restore has the potential of restoring an infected file on your computer, even after you have cleaned the infected files from all the other locations.

Also, a virus scan may detect a threat in the System Restore folder even though you have removed the threat.

For instructions on how to turn off System Restore, read your Windows documentation, or "How to turn off or turn on Windows XP System Restore"

Note: When you are completely finished with the removal procedure and are satisfied that the threat has been removed, re-enable System Restore by following the instructions in the aforementioned documents.

Clearly, the "System Restore" feature has not been carefully thought out!

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

***S*asser eyed over train outage**

<"NewsScan" <newsscan@newsscan.com>>

Tue, 04 May 2004 08:17:36 -0700

In Australia, RailCorp has dispatched software engineers to find the source

of the outage that left up to 300,000 commuters stranded yesterday, saying the new Sasser worm, which has already spawned two variants, is being evaluated as a possible cause. A RailCorp spokesman confirmed that software engineers were investigating the problem, which prevented drivers from talking to signal boxes. A virus attack was one possibility being investigated. RailCorp was unable to confirm when the investigation would be complete. RailCorp chief executive Vince Graham raised the possibility of a virus attack at a press briefing yesterday: "There is no evidence that hacking is an issue here, the viral infection could have been introduced by one of our own people not taking sufficient care." [*The Australian*, 3 May 2004 (Received from John Lamp, Deakin Univ.); NewsScan Daily, 4 May 2004]
<http://australianit.news.com.au/articles/0,7204,9455677%5E15306%5E%5Enbv%5E,00.html>

✶ New identity-theft scam

<Geoff Kuenning <geoff@cs.hmc.edu>>
Thu, 29 Apr 2004 16:50:54 -0700 (PDT)

Our campus just received word of a sophisticated new identity-theft scam:

- > The other night, a woman was outside Collins Hall offering pre-paid phone
- > cards and T-shirts to students who filled out and signed a form and let her
- > take a digital picture of their drivers' licenses. Apparently, when Campus

> Safety arrived, she told them she was from the Alumni
Association. One
> student later pressed her about it and she left, but he
believed she had
> gotten information (including photos of licenses) from several
students by
> that point.

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

Gas explosion creates confidential litter

<Sarah Hollins <sara@iec17799.com>>

Sun, 2 May 2004 06:37:54 -0700

Both the Disaster Recovery Guide and the ISO 17799 Newsletter report a story of a major banking group getting major business continuity issues right, but the small details badly wrong. There's an irony to it somewhere.

They had been diligent in spending time and money on their disaster recovery planning operation. Indeed, it went swimmingly well when a gas explosion occurred in their offices on a Sunday afternoon.

Recovery from the actual damage was swift, but not from the fall out from, of all things, staff leaving papers and documents on desks! These, which included confidential information on customer accounts, were scattered throughout the streets for days afterwards.

The risks of not locking away sensitive materials manifested themselves in a

most unexpected and spectacular way.

References:

<http://www.disaster-recovery-guide.com/stories.htm>

<http://www.isol7799-web.com/issue5.htm>

✶ Hybrid vehicles may be hazardous to rescuers' health

<"Joe Thompson" <kensey_news@linuxmail.org>>

Wed, 05 May 2004 02:44:20 +0800

As reported by CNN from AP, hybrid vehicles pose special concerns for accident responders:

<http://www.cnn.com/2004/TECH/05/04/hybrid.rescues.ap/index.html>

"Chris Peterson, a service training instructor for Toyota, said the Prius' electric system should shut down if anything goes wrong. 'There should not be high voltage in those cables, but I'm not going to stand up and say there isn't,' he said."

Apparently various hybrids run high-voltage power cables through places rescuers normally use to disassemble vehicles in emergencies, like doors.

Also, there appears to have been no or little thought given to the necessity to quickly cut power for such purposes -- the standard advice noted in the article is to turn off the key and disconnect the battery, but if you can't do that, no one seems to have any good ideas besides "watch where you put that thing."

Can anyone in the audience with auto-engineering experience give an idea of the extent to which making things easy for rescuers is incorporated into vehicle design? -- Joe

[Joe added a note just as this issue was going out:]

Slashdot picked up the story later this afternoon and in all the discussion, the following points emerged:

* Many people, some Prius owners and some not, assert that the high-voltage does not actually run through the doors, but along the frame rails.

* Many people point out that the biggest hazard in hybrid cars is the risk of delayed airbag detonation while rescuers are cutting apart the car.

This risk exists for modern non-hybrids just as much as hybrids.

The question I ended with, though, still seems relevant in light of that last point: when designing vehicles, how much, if any, thought is given to the safety of everyone involved *after* an accident? -- Joe

References:

[http://slashdot.org/article.pl?](http://slashdot.org/article.pl?sid=04/05/04/1923240&mode=thread&tid=126)

[sid=04/05/04/1923240&mode=thread&tid=126](http://slashdot.org/article.pl?sid=04/05/04/1923240&mode=thread&tid=126)

http://www.toyota.com/web/vehicles/prius/safety/prius_erg_2.pdf

<http://www.gizmodo.com/archives/hybrid-cars-may-send-gods-electrical-wrath-to-punish-oilhating-pinkos-015878.php>

[last url split:

<http://www.gizmodo.com/archives/hybrid-cars-may-send-gods-electrical-wrath-to-punish-oilhating-pinkos-015878.php>]

✶TCP, BGP, DoS, and BS

<Rob Slade <rslade@sprint.ca>>

Thu, 22 Apr 2004 13:07:33 -0800

The sky is falling! We're all going to die!

No, it's not. No, we're not

The latest "death of the net" rumour has to do with a recent paper that discusses the fact that something called "session hijacking" can be used to force an end to a specific connection (connected sessions over the Internet use an arrangement called TCP). If the session is ended or disconnected, you will be effectively denied the service you were attempting to obtain. Connected sessions are used for everything from transferring files to connecting to the Internet in special ways to virtual private networks. Sometimes they are used to transfer information between the machines that decide where Internet traffic goes (called routers). If the routers can't keep up to date, the Internet will not be as effective as it should be.

So you will have heard that there is a new threat to the Internet, that it is a denial of service attack, that it can disconnect you from the net, that it can kill your sessions, that it affects the routers (and a router protocol called BGP), and that sessions can be hijacked.

None of this is new. What is new is a paper that was originally presented

in England, caught the attention of the media there, and has spread, kinda like a hoax virus warning, from media outlets to bandwagon jumpers in the security field and back to the media, around the world.

Denial of service attacks are not new. Session hijacking is not new. Using TCP resets and session hijacking in combination has not been used in specific attacks before, but all the parts of this attack are well known to people who deal with such things. There are even ways to protect against this attack, and some institutions use them.

So, rather than talking about the death of the net, and "The Man Who Saved the Internet":

Net not dead, but was coughing up blood last night. Phlegm at 11.

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>

✶ Florida sues AT&T for billing errors

<Frank Carey <Carey1938@aol.com>>

Sat, 1 May 2004 19:52:31 EDT

Florida Attorney General Charlie Christ is suing AT&T, accusing the giant of overcharging for long distance service and billing people who are not even AT&T customers. A week ago Christ issued a consumer alert urging all telephone customers to check their bills carefully for possible

billing
errors by AT&T. Since the alert was issued, more than 600
Florida residents
have contacted Christ's office. Christ is seeking up to \$10,000
restitution
for each allegation of wrong billing. He also said the company
violated the
state's unfair and deceptive business law. Company officials
have
acknowledged that a computer problem erroneously assessed long
distance
charges on the bills of one million people nationwide. [Source:
Associated
Press, *Florida Today*, 1 May 2004, p. 10B]

✶ Re: Traffic Signal Controllers (Perry, [RISKS-23.34](#))

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

Sat, 1 May 2004 11:30:28 -0400

> shouldn't there be a failsafe that wouldn't allow two greens
no matter what?

And the answer, of course, is yes. When I was growing up, my
dad was a
traffic and parking coordination officer for the City of Boston,
Massachusetts. Among his duties was interacting with
contractors who did
sign and signal work for the city, which, in addition to
resulting in some
pretty cool tchotchkes for a 10 year old, gave me the
opportunity to feed
the Elephant's Child, and that was one of the questions I asked.

At least in that (late 70's) generation of controllers, yes,
there was a
physical interlock: the clocked drum on those motor-driven
controllers

switched the light heads through relays, as opposed to directly, and the wiring of the relays was such that it was not physically possible to cause the controller to display opposing greens, unless you managed to have *two* stuck relays -- it might even have been three.

Jay R. Ashworth, Member of the Technical Staff Baylink The Suncoast Freenet
Tampa Bay, Florida <http://baylink.pitas.com> +1 727 647 1274
jra@baylink.com

✶ FREEDOM 2.0, Washington, DC, 20-22 May 2004

<EPIC News <alert@epic.org>>
Mon, 3 May 2004 18:24:37 -0400

Freedom 2.0: Distributed Democracy, Dialogue for a Connected World
The Washington Club in Washington, DC, 20-22 May 2004

Information: <http://www.epic04.org>
Registration: <http://regmaster.com/epic04.html>
(Early registration deadline deadline 5 May.)
Schedule: <http://www.epic04.org/schedule/index.htm>
Special conference events include
SWIPE <http://www.we-swipe.us/about.html>
and Spy Museum <http://www.spymuseum.org/index.asp>

Confirmed speakers include: Anita L. Allen, David Banisar, Ann Bartow, Francesca Bignami, James Boyle, David Burnham, Vinton G. Cerf, Enrique Chaparro, David Chaum, Julie E. Cohen, Lillie Coney, Amitai Etzioni, David J. Farber, David H. Flaherty, Oscar H. Gandy, Deborah Hurley, Jerry Kang,

Ian R. Kerr, Judith F. Krug, Elizabeth Longworth, Gary Marx,
Pedro Mendizábal, Mary Minow, Peter G. Neumann, Stephanie Perrin,
Katitza Rodriguez, Pamela Samuelson, Paul M. Schwartz, Bruce Schneier,
Barbara Simons, Brooke Singer and Jamie Schulte (SWIPE), Robert Ellis
Smith, Daniel J. Solove, Edward G. Viltz, Paul Wolfson.

⚡ REVIEW: "Non-Repudiation in Electronic Commerce", Jianying Zhou

<Rob Slade <rslade@sprint.ca>>
Tue, 20 Apr 2004 08:46:21 -0800

BKNNRPDT.RVW 20031205

"Non-Repudiation in Electronic Commerce", Jianying Zhou, 2001,
1-58053-247-0, U\$89.00/C\$131.95
%A Jianying Zhou
%C 685 Canton St., Norwood, MA 02062
%D 2001
%G 1-58053-247-0
%I Artech House/Horizon
%O U\$89.00/C\$131.95 617-769-9750 800-225-9977 fax: +1-617-769-
6334
%O [http://www.amazon.com/exec/obidos/ASIN/1580532470/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1580532470/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/1580532470/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1580532470/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/1580532470/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1580532470/robsladesin03-20)
%P 200 p.
%T "Non-Repudiation in Electronic Commerce"

The preface outlines non-repudiation as a security service in
its own right,

with supporting requirements, rather than an effect of another security mechanism. This position is in rather interesting contrast to most works that tag non-repudiation onto the list of functions that can be accomplished by asymmetric (public key) cryptography: a benefit, but a bit of an afterthought.

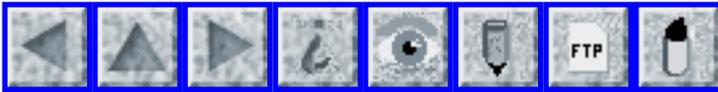
Chapter one gives us an introduction to the basics of non-repudiation, in both electronic mail and electronic commerce. Various parties to a transaction, the means, requirements, and forms of evidence all make up the fundamentals of non-repudiation in chapter two. Digital signatures are the traditional, but not the only way to prevent repudiation of a message, and chapter three examines four approaches for maintaining their validity. Chapter four investigates the concept of fairness in a non-repudiation system, ensuring that where the transaction is not completed neither side is able to obtain an advantage over the other. In general, fairness requires either gradual disclosure (in an ad hoc situation) or the involvement of a trusted third party. Specific "Fair" protocols are reviewed in chapter five. Chapter six looks at the ISO's (International Standards Organization) non-repudiation mechanisms. Case studies of the detailed requirements and proposed protocols for an online lottery (which also involves anonymity) and mobile (wireless) billing are in chapter seven. Chapter eight has a summary of the main points in the book, and appendix A deals with formal verification of non-repudiation.

A detailed and interesting account of a rather neglected but important topic.

copyright Robert M. Slade, 2003 BKNNRPDT.RVW 20031205
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

Volume 23: Issue 36

Friday 7 May 2004

Contents

- [Computer glitch gives out free gasoline](#)
[Jack Christensen](#)
- [U.S. blunders with China, Iran keyword blacklist](#)
[Declan McCullagh](#)
- [Risks of prisoner abuse vs. digital cameras](#)
[Lauren Weinstein](#)
- [Auto-Blacklisting is a bad idea](#)
[Drew Dean](#)
- [Re: Computer glitch grounds Atlanta flights](#)
[Tron Smith](#)
- [Corrupted virus definition load blocks re-load](#)
[George Michaelson](#)
- [Antivirus software prolongs viral life](#)
[Matthias Heiler](#)
- [Challenge/response standards](#)
[Brent Laminack](#)
- [Aus vs. Swiss speeding](#)
[Ivan Reid](#)
- [Re: ... lost revenue from faulty speed cameras](#)
[Anthony Youngman](#) [Michael Smith](#) [Bertrand Meyer](#)

● [MDT and a Fatal accident: a possibility?](#)

[Nick Lindsley](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Computer glitch gives out free gasoline

<"Jack Christensen" <j.christensen@sbcglobal.net>>

Wed, 5 May 2004 17:28:12 -0400

Some Michigan college students discovered that swiping their driver's license instead of a credit card in pay-at-the-pump gasoline pumps allowed them to fill up for "free." What they evidently didn't count on was that information from their driver's licenses, sufficient to trace them, was in fact read and stored by the system.

The exact mechanism of the "glitch" isn't detailed, but there are at least a couple Risks here, including:

- (1) Insufficient testing/robustness, with regard to unexpected input, can lead to retail losses and/or expenses to recover the losses, and
- (2) Failure to understand that ignorance (in this case, of the workings of embedded systems, and of their failure modes,) is insufficient reason to assume a best-case scenario.

I know nothing of the specific technology involved, but I'm at least a little surprised at the interchangeability of different types of cards. I would think one of the first checks would be to determine if you

were
reading a credit card, or something else that you didn't want to
process
(driver's license, video store card, etc.)

Strictly from personal observation when using these pumps, there
is usually
some sort of authorization that happens before you can dispense
gasoline.
If this authorization fails, as I assume it would when given a
driver's
license, then I would not think the transaction should proceed.

[Source: Associated Press item, 5 May 2004]

[http://story.news.yahoo.com/news?tmpl=story&cid=817&e=1&u=/ap/
free_gas](http://story.news.yahoo.com/news?tmpl=story&cid=817&e=1&u=/ap/free_gas)

Jack Christensen j.christensen@sbcglobal.net

✶ U.S. blunders with China, Iran keyword blacklist (Politech)

<Declan McCullagh <declan@well.com>>

Mon, 3 May 2004 11:20:10 -0500

Declan McCullagh: U.S. blunders with keyword blacklist, 3 May
2004

<http://news.com.com/2010-1028-5204405.html>

The U.S. government concocted a brilliant plan a few years ago:
Why not give
Internet surfers in China and Iran the ability to bypass their
nations'
notoriously restrictive blocks on Web sites?

Soon afterward, the U.S. International Broadcasting Bureau (IBB)
invented a
way to let people in China and Iran easily route around
censorship by using

a U.S.-based service to view banned sites such as BBC News, MIT and Amnesty International.

But an independent report released Monday reveals that the U.S. government also censors what Chinese and Iranian citizens can see online. Technology used by the IBB, which puts out the Voice of America broadcasts, prevents them from visiting Web addresses that include a peculiar list of verboten keywords. The list includes "ass" (which inadvertently bans usembassy.state.gov), "breast" (breastcancer.com), "hot" (hotmail.com and hotels.com), "pic" (epic.noaa.gov) and "teen" (teens.drugabuse.gov). [...]

Politech mailing list Archived at <http://www.politechbot.com/>
Moderated by Declan McCullagh (<http://www.mccullagh.org/>)

✶ Risks of prisoner abuse vs. digital cameras

<Lauren Weinstein <lauren@vortex.com>>

Fri, 7 May 2004 08:23:31 -0700 (PDT)

Perhaps understandably lost in the furor over Iraqi prisoner abuse is the role that technology has played in moving this story from "footnote" to "international firestorm" status. Without a doubt, the digital camera has played a central role.

It's these relatively inexpensive cameras, producing vast numbers of high-quality shots at essentially zero cost per photo, images that can be

easily stored and e-mailed, that have inspired the visual recording of scenes that otherwise would have been reduced to dry, easily ignored, textual descriptions at the most.

Note the brief, sterile, vacuous January press release from CENTCOM, that Rumsfeld is touting as proof that everyone was already informed about possible "detainee" abuse problems in Iraq: (<http://www.vortex.com/centcom-abuse-release.html>).

Now contrast the stark, full-color realities of the photos, most from a massive digital archive obtained by *The Washington Post* (and subjected to "appropriate" cropping and blurring -- it's OK to show all manner of visual horrors to the public, but you don't want to offend them with naughty body parts).

The photos *are* the story, and apparently there are lots more to come.

President Bush says that such abuses are aberrations that don't reflect the true nature of our society. In the "Reality Reset" column referenced by (<http://neon.vortex.com/blog/lauren/archive/000051.html>) I question this premise, but without a doubt the digital camera and related technologies are creating a sea change, the effects of which we cannot even begin to realistically predict.

Lauren Weinstein +1 (818) 225-2800 <http://www.vortex.com>
<http://www.pfir.org> <http://www.factsquad.org> <http://www.uriica.org>

✂ Auto-Blacklisting is a bad idea

<Drew Dean <ddean@csl.sri.com>>

Thu, 06 May 2004 12:49:28 -0700 (PDT)

I recently received a challenge from someone's challenge-response spam filter. Alas, I had not sent the original message. Unfortunately, said challenge-response system warned that it was going to automatically blacklist my e-mail address if I didn't respond. But I didn't want to respond, because the original message was either malware (most probably, see below) or spam.

Milgram's famous "six degrees of separation" turns out to make auto-blacklisting a really bad idea: many types of e-mail-based malware propagate via random choices from the victim's address book. As it's an awfully small world, there's a good chance that someone knows two people with common interests, who may not have exchanged e-mail before. (Lots of people seem to have my old e-mail address in their address books, even though I've never heard from them, or sent them mail, other than indirectly via a mailing list (or USENET posting).)

If auto-blacklisting challenge-responses systems become the norm, there will be interesting risks related to the combination of forged mail, and auto-blacklists: what happens if you follow the challenge-response protocol to avoid being on someone's blacklist (the only obvious option),

and said
person (e.g., your research sponsor) receives a highly
inappropriate piece
of mail nominally from you? Other denial of service attacks are
also
possible: seed your competitors (auto-)blacklists with the e-
mail addresses
of your (mutual) funding agency. I'm sure the clever will have
even more
ideas about risks here.

Auto-whitelisting, by contrast, has none of these problems.

Drew Dean, Computer Science Laboratory, SRI International

⚡ Re: Computer glitch grounds Atlanta flights ([RISKS-23.35](#))

<Tron Smith <ziggart57@yahoo.com>>

Tue, 4 May 2004 19:47:14 -0700 (PDT)

Talk within the airline industry has it that Delta's problems on
1 May 2004
were the result of systems not patched and hit by the Sasser.b
virus.

⚡ Corrupted virus definition load blocks re-load

<George Michaelson <ggm@apnic.net>>

Fri, 7 May 2004 09:55:20 +1000

The desktop virus scanner we use appears to update windows
registry, or some
other record of load, *before its verified the integrity* of the
loaded virus

definitions. And, it refuses to re-load them if its recorded them as loaded.

We have just had at least one host which fell over during the virus load phase off the net, and then spend an hour or more trying to find where to remove on-disk data to allow a reload of the file.

The risk here is pretty obvious: a virus could quite easily be written to corrupt the virus definition state in registry and prevent you from downloading the current patches to remove the virus...

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

✦ Antivirus software prolongs viral life (Kuenning, [RISKS-23.35](#))

<Matthias Heiler <surname@gmx.de>>
05 May 2004 09:56:54 +0200

> Clearly, the "System Restore" feature has not been carefully thought out!

"System Restore" is a functionality of Windows XP, not of any Antivirus software. So the header should read "Windows XP prolongs viral life".

✦ Challenge/response standards

<Brent Laminack <ibrent@alltel.net>>
Wed, 5 May 2004 21:05:32 -0400

What is your favorite color? Blue.. No, Yellow! Aaaargh!!

Security professionals are well aware of password restrictions. ISO 17799 says that passwords should be at least six characters in length and free of consecutive identical characters or all-numeric or all-alphabetical groups. (Section 9.3.1) There are a number of variations on the theme: requiring internal numerics, mixed upper and lower case, etc.

Here is a recent encounter I had where an organization tried to apply such a rule to a non-password.

I was signing up for on-line bill-payment from our local ILEC PSTN telephone provider. I chose my user name and password, and was asked to provide a question and answer to re-set my password. Such challenge/response systems are fairly common. I liked that I could choose my own question. Some systems have a small set of pre-defined questions that are, unfortunately, matters of public record "What is your mother's maiden name?", "In what city where you born?" etc. They suggested using a question like "What is your favorite color?" I decided that that particular information was not easily found in government databases so I entered it as the question. I then entered my favorite color as the answer. I submitted the form and got an error message saying that the answer had to be at least six characters. Odd. Let's see.. common colors of at least six characters: Blue? Red? Green? White? Black? Cyan? Beige? Aqua? Gray? Pink? Navy? Olive? Peach? Rose?

Tan? Teal?

Clearly they have disallowed a number of valid responses. I finally picked a compound color name (which really isn't my favorite color) and finished the registration process.

What think ye? Is it proper to apply password standards to challenge/response responses, or are other criteria (such as: not a matter of public record) more valid? I've looked, but can find no body of work setting forth standards for challenge/response questions similar to those standards which govern password creation and use. Clearly, this should be addressed if such challenge/response dialogs are used to reset passwords. This because authentication by strong passwords is for naught if the password reset mechanism is weak or flawed.

✶ **Aus vs. Swiss speeding ([RISKS-23.35](#))**

<Ivan.Reid@brunel.ac.uk>

Wed, 5 May 2004 07:46:40 +0100

> The country is proud of its strictness in enforcing speed rules, sometimes
> fining motorists for driving one kilometer above the posted limit (however
> absurd that sounds).

That's a little ironic, given that I was twice fined in Switzerland for "injuring the speed laws" by riding 1 km/h too fast, after a 5 km/h tolerance (86 in an 80 and 56 in a 50; for completeness my other fine was

for four over at 59 in a 50 -- each fine was CHF 20 [since tripled] but no points accrue in the Swiss system).

Ivan Reid, Electronic & Computer Engineering, CMS
Collaboration,
Brunel University. Ivan.Reid@brunel.ac.uk Room 40-1-B12, CERN

✶ Re: ... lost revenue from faulty speed cameras (Meyer, [RISKS-23.35](#))

<"Anthony Youngman" <Anthony.Youngman@eca-international.com>>
Wed, 5 May 2004 09:19:26 +0100

"Last year their accuracy was questioned after reports that a truck with a maximum speed of 140 km/h was caught traveling at 164 km/h, and other similar incidents."

I don't know how failsafe the UK system is, but UK fixed cameras take a double image with a time interval of maybe a second. Coupled with markings on the road, it's possible to work out the distance covered between photos, and hence calculate the speed. I'm fairly certain that on several occasions this has been used to prove the camera was faulty. The only thing I don't know is how the time gap is proven -- hopefully the time is stamped on the photo based on the national Radio Time Signal.

Re: ... lost revenue from faulty speed cameras (Meyer, [RISKS-23.35](#))

<Michael Smith <emmenjay@zip.com.au>>

Wed, 05 May 2004 03:26

> The country is proud of its strictness in enforcing speed
> rules, sometimes fining motorists for driving one
> kilometer above the posted limit (however absurd that sounds).

That sounds like an extraordinary claim to me. I've lived in Australia all of my life (over 40 years) and I've never heard of a speeding ticket being given for one km/h over the limit. Speed cameras are normally calibrated for between seven and 12 km/h above the limit.

As for "The country is proud of its strictness in enforcing speed rules", I'm not sure how you would define "the country". Most official sources attribute a significant proportion of road deaths to excessive speed. (e.g. <http://www.rta.nsw.gov.au/roadsafety/speedandspeedcameras/>) and such sources normally describe the anti-speeding initiatives as being successful in reducing the number of road deaths. However there is a quite vocal "pro speeding" group. I don't have data to estimate the group's size, but they get significant media attention. They claim that speed limit enforcement is merely "revenue raising" (which is presumed to be a bad thing) and that speeding has little effect on accident rates -- suggesting that road improvements and driver training are preferable ways of reducing the number of road deaths.

Mr Meyer's comments on the faulty speed cameras are, sadly, all too accurate. However I would be interested to know his sources on the comments outlined above -- for they contradict my own personal experience.

Michael J Smith <emmenjay@zip.com.au>

✶ Re: ... lost revenue from faulty speed cameras (Smith, [RISKS-23.36](#))

<"Bertrand Meyer" <Bertrand.Meyer@inf.ethz.ch>>

Wed, 5 May 2004 07:25:51 +0200

I have been a frequent visitor to Australia (the equivalent of a month and a half a year) for the past ten years and this may be the most dangerous stage, at which you start believing that you know enough about the place even if you're still basically a tourist.

Both of the claims that Michael questions are based on numerous conversations with diverse people. The fear of being fined for going 1 KM/H over the limit is prevalent among my acquaintances; As to being "proud" of the policy this is a general impression, which may be biased by the kind of people I meet -- typically, urban professionals.

This illustrates the risks of voicing generalities about "the country", whatever that country is. Fortunately the other points in my note are, as you observe, factual, not a matter of opinion or impression.

✶ MDT and a Fatal accident: a possibility?

<"Nick Lindsley" <nicklindsley@beethoven.com>>

Fri, 7 May 2004 00:10:50 -0400

----- Original Message -----

From: fist <fist@ozemail.com.au>

Reply-To: fist@ozemail.com.au

Date: Fri, 07 May 2004 11:04:39 +1000

>Nick, One suggestion would be to send a short version of this
>to the Risks
>Digest, asking if anyone had seen similar reports and pointing
>out the
>dangers of drivers not watching the road I find this digest has
>some of the
>most intelligent IT people around, and it might generate enough
>commentary
>to give you something more to send along to the authorities.
On 8 Sep
>2002, Wayne Duncan (a colleague of mine) rolled his taxi with
>fatal
>results on Airport Drive, Brisbane. It was unwitnessed and skid
>marks
>indicated that he had swerved, possibly to avoid something in
>his way.

For sometime before and after this accident, I had considered the
possibility that using and reading the on-board computer system
could
contribute to an accident. It had nearly happened to me, looking
up just in
time to avoid a pedestrian. Wayne was not a bad driver, not
always within
the speed limit, but not outlandishly beyond it either.

Black and White's taxi computer system is supplied by and
maintained online
by Raywood Communication of Melbourne, and works in conjunction

with a GPS
in the taxi which transmits its position (latitude and
longitude) and other
relevant data to the cab base.

I figured that if I knew the position of the crash by driving to
the
accident site and using my own GPS, I could perhaps find out if
it coincided
with the last transmission from Wayne's taxi, proving at least
the
possibility that he had been using the on-board computer close
to the time
of his death. After perhaps three months I visited Const Kelly
Donahue at
Boondall Police Centre, who was investigating the cause of the
crash. I
explained how we physically worked the on-board computer,
roughly measured
time with eyes off the road, reaction time, distance traveled
therein and so
on.

As stated previously, Wayne's accident was unwitnessed. As luck
-- if that's
the word -- would have it, the first person on the scene was a
doctor who
declared him dead at 20:44. He probably had been killed
instantly.

Constable Donahue had a report from Black and White purporting
to have come
from Wayne's taxi timed at 20:40 (about 4 minutes before he was
found dead),
and printed shortly after the accident (I am not sure when or by
whom).

At that time, according to the report, Wayne had indicated his
preferred
work area as Eagle Farm and other details. Most interesting for
me was the
latitude and longitude. I was looking for something close to
27deg 23.6mins

South and 153deg 06.8mins East (about 300 to 400 metres before the tall control tower on the way to the Domestic Airport), roughly the site of the accident and marked nowadays by two small white crosses in the median section.

Everything appeared to be in order EXCEPT for the latitude and longitude. This indicated a position 1400 kms to the SW, near Melbourne, approximately 38 deg South and 145 deg East. When I pointed this out to Const Donahue she had no explanation. In fact she had been unaware that the report contained the current position of the taxi when it transmitted details at 20:40 even though she had been in possession of the report for some months.

Now this could be seen as another simple computer glitch. Having an IT background and having spent many years using GPSs for navigating boats, I find this extremely unlikely. After all, everything else transmitted from the taxi to the cab base at 20:40 appeared correctly, so why not the latitude and longitude? Const. Donahue had no explanation.

Now over one year later I am still without an explanation. I have repeatedly asked the police, the coroner, offered my own experience, just to be basically ignored. I have even had the Freedom of Information act mentioned.

Recently Constable Donahue phoned me from Landsborough, her new posting, to tell me that the coroner has decided not to have an inquest into the accident. I may not in fact have a right to know exactly what the reason

for the false latitude and longitude on the report was. My main concern is that the police and/or coroner are acting on the advice of B&W and Raywood Communications who obviously have an invested interest in a non controversial outcome. Additionally, if the position in the report was wrong, has the real position been saved? And was it close to the accident site?

UPDATE SINCE THE ABOVE WAS WRITTEN

There will be no inquest and I have received copies of the police report and witness statements. The following is a copy I have just sent to the Deputy Coroner here in Brisbane:

C A Clements
Deputy State Coroner
179 North Quay
Brisbane 4000
Your Ref#COR 472/02

30 April 2004

Dear Mr/Ms Clements

Thank you for sending me some of the details concerning the fatal accident to Clifford Wayne Duncan at Airport Drive, Brisbane Airport on the 8 September 2002.

As you are probably aware, I knew Duncan on a passing basis and I was curious why a driver with his experience would suddenly swerve to the right through about 170 degrees, initiating a roll that killed him when his taxi collided with a steel pole. I had considered the possibility

that his on-board computer (and back lit at the time 2041hrs) had distracted his eyes a moment too long, and when he looked up he desperately -- and suddenly -- swerved to avoid something in his lane (possibly a fox or another car). Unfortunately too late.

Having read the reports and witness statements that you sent me, I am still unconvinced that the on-board computer was not a contributory factor in the accident. I noticed towards the end of Report Number 02/22444, Senior Constable Donohue recommended (and I quote from page 11):

``1. that Queensland Transport conduct a safety audit into the feasibility of taxi drivers operating the MDT safely whilst the vehicle is in motion. The operation of the MDT whilst the vehicle is moving may be akin to the use of mobile phones.''

It is the only recommendation that she makes.

On page 9 of the same report she mentions in further information 1(b):

``I visually observed each of the drivers to take their attention from the road ahead for a period of at least 2 seconds at a time. Furthermore, conversations with the Black and White taxi drivers suggested that they are all of the opinion it is a safety risk, as monitoring requires the driver to take his/her eyes away from the road ahead, relying on peripheral vision. This risk was particularly enhanced during nighttime hours, as the illumination of the MDT was distracting when trying to refocus ahead. They all likened the operation of a MDT to a mobile phone.''

The Statement of Witness Greg Whitney (Service manager for Raywood

Communications at the time of the accident) contains an analysis of how the

GPS/On-board MDT work. Page 4 of that witness' statement contains the

following:

``I have an MDT and radios fitted to my vehicle for testing purposes. I

admit that in times past, I have been accessing the data screens whilst

driving. When I have looked up, I have been surprised at how far I have

traveled and admit that if a car was slowing down or stopped in front of me,

or a pedestrian was to walk in front of my vehicle, my ability to stop

safely may have been compromised.''

Coming from the manufacturers themselves, this is rather significant.

Mr Whitney also mentions a software engineer with Raywood called Karl Leake

(now based in North Sydney). On the report given to the police, the current

location of Duncan is given in and around Melbourne (an error offset 1400km

south west of the actual position). I discussed this matter with Mr Leake

and Mr Whitney today and it appears that this ``error'' is well known

and deliberate and used for their ``own internal purposes''. Neither

could explain why this known error would be maintained in software that had

been in use for some years with B&W Brisbane. Interestingly, Mr Leake told

me that the actual correct position would have stayed on B&W hard disk as

the ``error'' is only induced by the report generator. In

theory the

correct position should still be on B&W's computer system unless it has been

deleted. Considering the severity of the accident, one can only hope that

it hasn't been deleted as it will show quite conclusively where the Wayne

Duncan was at 2041 hrs on the day he died -- and, more importantly, if he was

closing in on the accident site (27 23.6South 153 06.8East). He would

probably been looking at the screen just after his final transmission at

20:40:09 hrs to check the stats.

I do not know if you felt a need for an independent technical witness

(unrelated to the companies involved) but, considering the importance of the

matter (it could happen again, if it happened at all) why will there be no

inquest? Is it because you feel that there is absolutely no chance that the

on-board MDT computer system contributed to the accident, and if so, where

is the evidence for that side of the argument?

Additionally, I would like to request copies of the following:

Data Printout for B&W Taxi #682 for the 8 Sept 2002

Data Printout for Statistics for B&W taxi #682 for 1 Sept 2002 thru to

(and including) 8 Sept 2002.

Yours Sincerely

Nick Lindsley

Thank God for cut and paste.

I have been around all the state govt houses -- police, transport, justice

and, it seems, I am going around in circles. I am not 100% exactly how the

driver was killed, but I do think the subject needs further attention.

Interestingly, I belong to a Yahoo discussion group (Oz Cabs) and I put a post on this issue about a year ago to try and engender some interest in the matter. Yesterday the moderator -- a David Gawthorn (Melbourne) -- e-mailed to say that someone in Qld had called him to "moderate" my posts on this particular subject ("moderate" in this context means censor) quite a few months ago. I also cannot find my original posting.

If you find this interesting, please contact me on 0418-727.727 Australia



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 37

Tuesday 18 May 2004

Contents

- [Las Vegas monorail delayed due to computer glitch](#)
[Chuck Weinstock](#)
- [False Positive Risks](#)
[John Lettice via R.G. Newbury](#)
- ['Blue Screen of Death' on hotel TV screen](#)
[Henry Baker](#)
- [New UK Driving Licence puts Identity at risk](#)
[Adam Laurie](#)
- [Forrester speeds up timeline on white-collar offshoring](#)
[NewsScan](#)
- [Researchers find WiFi flaw](#)
[NewsScan](#)
- [Sasser creator turned in for the reward](#)
[NewsScan](#)
- [German Toll-Collect announces another delay...](#)
[Debora Weber-Wulff](#)
- [Listen to your CPU and break RSA?](#)
[Gadi Evron](#)
- [Banks don't understand phishing social risks](#)
[Samuel Liddicott](#)

- [Fines reimbursed, drivers reinstated; faulty speed camera](#)
[Bertrand Meyer](#)
 - [Re: Hybrid vehicles may be hazardous to rescuers' health](#)
[Stephen Fairfax](#)
 - [Re: Auto-Blacklisting is a bad idea](#)
[Kyler Laird](#)
 - [Formal Methods for Industrial Critical Systems CFP](#)
[Diego Latella](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Las Vegas monorail delayed due to computer glitch

<Chuck Weinstock <weinstock@sei.cmu.edu>>

Tue, 11 May 2004 09:46:17 -0400

The Las Vegas strip \$650M 3.9-mile monorail project is months behind schedule. The opening, which had been scheduled for 20 Jan 2004, was first postponed to March, and now to the summer. In January, a train drive-shaft fell off in a test. In February, a glitch was detected in the computer control system that keeps trains spaced safely while moving at 50mph. Bombardier (Canada) and Granite Construction Co. (Watsonville, California) are paying about \$85,000 a day in penalties. The control system uses Alcatel's SelTrac S40 Automatic Train Operating System. Source: Associated Press, 11 May 2004

⚡ False Positive Risks (John Lettice)

<"R.G. Newbury" <newbury@mandamus.org>>

Tue, 11 May 1982 13:25:18 -0400

Roger Benson and Miguel Espinoza brought a lawsuit against Identix and California and Oregon because Identix's Livescan 10-print fingerprint scanner assigned each of them an ID that was also assigned to someone else who had a criminal record.

Benson was imprisoned for 43 days for carrying a firearm after he was stopped in California for a traffic violation; the ID derived from his fingerprint scan (incorrectly) matched that of someone with a completely different name (William Lee Kellogg) who had been convicted for three felonies in Oregon. Records show that Benson's and Kellogg's biometric fingerprint records are completely different -- with Benson having only nine fingertips! Similarly, Espinoza claimed his restaurant business was destroyed because his ID was shared by someone with a criminally negligent homicide conviction.

The ability of this system to generate duplicate IDs has been known since 1996, but evidently not corrected. In fact, Oregon has a list of 97 such cases. As usual, there is significant blame to go around -- the system itself, and the rather unimaginative use of it by law enforcement. (On 11 May 2004, Identix sought to have the suit dismissed in San Jose Superior Court.)

Incidentally, the Department of Homeland Security has a contract

for
Identix's fingerprint system, reportedly worth \$27M. The UK
Passport
Service is also using this system.

[Source: John Lettice, DHS and UK ID card biometric vendor in
false ID lawsuit,

The Register, 11 May 2004; PGN-ed]

http://www.theregister.co.uk/2004/05/11/identix_false_id_suit/

'Blue Screen of Death' on hotel TV screen

<Henry Baker <hbaker1@pipeline.com>>

Wed, 12 May 2004 05:59:35 -0700

I'm staying in New York City at the Mandarin Oriental Hotel, where every room has a 'high definition' flat panel TV screen powered by a PC running Windoze XP Media edition. This is massive overkill, since the 'web' feature of the setup is no better than what you would get with a 'thin' web browser. (The quality of the TV picture also left a lot to be desired, indicating that the \$\$ spent on the PC would have been better spent on the TV itself, but that is a different story.)

Unfortunately, the PC malfunctioned in the middle of the night, and completely froze -- not responding to the IR wand, or even trying to power cycle the various components using the power on/off button.. Note: on this system, the power buttons are all software interpreted, so when the software screws up, there's no easy way to even power cycle it.

I was forced to pull a very heavy dresser away from the wall so I could get access to the power plug and power cycle the system in this way. It's only a matter of time before hotels will disable this option as well, by hard wiring the power to the system.

The risks of disabling the power buttons are clear -- what if

the system
were melting down and starting a fire?

⚡ New UK Driving Licence puts Identity at risk

<Adam Laurie <adam@algroup.co.uk>>
Wed, 05 May 2004 08:29:39 +0100

To obtain the new UK photocard driving licence, you are required to provide proof of your identity (see item 6 here):

http://www.dvla.gov.uk/drivers/photocard_licences.htm

My wife recently applied for one, and submitted her passport as proof of identity. In due course, the licence arrived, but not the passport. When she contacted the DVLA, she was told that they were always sent separately, and the passport should have come first.

Given the following story, showing that the post office is losing 14.4M letters a year, and the fact that the DVLA take no special precautions such as registered post, we assumed the worst:

<http://news.bbc.co.uk/1/hi/uk/3681547.stm>

Fortunately, the passport eventually arrived, but a system that sends crucial documents through a service that is losing such vast quantities of its charges is clearly putting valuable documents, and thereby identities, at grave risk, which seems to me to be criminally irresponsible of those in

charge of the DVLA.

Adam Laurie, A.L. Digital Ltd., The Stores, 2 Bath Road, London
W4 1LT UK

+44 (20) 8742 0755 <http://www.thebunker.net> [http://www.](http://www.aldigital.co.uk)

[aldigital.co.uk](http://www.aldigital.co.uk)

✦ Forrester speeds up timeline on white-collar offshoring

<"NewsScan" <newsscan@newsscan.com>>

Mon, 17 May 2004 10:10:36 -0700

Forrester Research says the export of [U.S.] white-collar jobs is happening faster than it had first predicted back in 2002, but that its long-term outlook for offshore outsourcing hasn't changed much since that report, which estimated that a cumulative 3.3 million white-collar jobs would be shifted to other countries by 2015. Forrester's revised numbers project a total of 830,000 jobs offshored by 2005, up from its earlier estimate of just under 600,000. Ironically, Forrester analyst John McCarthy says the media's focus on the issue has encouraged more companies to experiment with offshore outsourcing. "While the press visibility has spurred offshoring's emergence as a political third rail, it has also fostered an increase in overall offshore alternatives," says Forrester's revised report. [*Wall

Street Journal*, 17 May 2004; NewsScan Daily, 17 May 2004]

<http://online.wsj.com/article/0,,SB108474869663912901,00.html>

(sub req'd)

✶ Researchers find WiFi flaw

<"NewsScan" <newsscan@newsscan.com>>

Fri, 14 May 2004 08:23:38 -0700

Researchers at Queensland University of Technology in Australia have discovered an easily-exploited vulnerability that can be used to take down most 802.11 wireless networks. The flaw operates at lower network layers than most previously-discovered security flaws in 802.11 networking, and affects any network operating at the 2.4GHz frequency -- which is the sole frequency used by the most popular wireless protocol, 802.11b.

[*The

Australian*, 13 May 2004; NewsScan Daily, 14 May 2004, rec'd from John Lamp, Deakin U.]

<http://australianit.news.com.au/articles/0,7204,9549723%5E15306%5E%5Enbv%5E,00.html>

✶ Sasser creator turned in for the reward

<"NewsScan" <newsscan@newsscan.com>>

Mon, 10 May 2004 08:45:38 -0700

The German teenager who created the computer worm Sasser was identified by acquaintances seeking a \$250,000 reward from Microsoft. The young man was arrested in the village of Waffensen, near Bremen, and appeared shaken by

the extent of the damage his program had caused around the world. He faces charges of computer sabotage, which under German law could mean his imprisonment for five years. If the teenager is convicted, Microsoft will make good on its pledge for the full \$250,000 reward. [*The Washington Post*, 9 May 2004; NewsScan Daily, 10 May 2004]
<http://www.washingtonpost.com/wp-dyn/articles/A11160-2004May8.html>

★ German Toll-Collect announces another delay... (Re: [RISKS-23.21](#))

<Debora Weber-Wulff <weberwu@fhtw-berlin.de>>
Tue, 11 May 2004 12:47:13 +0200

... but in newspeak it is, of course, not announced as such. The public-private partnership Toll Collect, which was to have helped the German Government rake in tolls starting last year, has kept posting delays. This led to the Transport Secretary throwing them out in February 2004 but reinstating them the beginning of March because they promised to start testing in the summer and would have the first stage fully functional by Jan 1, 2005.

Experts laughed, but the government reinstated the consortium, and they got to work. AP reports (quoting the *Berliner Zeitung* from 10 May 2004) that testing will not commence until October or November. [Well, I guess that's Indian Summer... dww] The company is currently looking for

errors in the individual systems, the head of Toll Collect, Christop Bellmer, announced.

"The recent tests of the on board units are promising. The error rate was just under 3%, about 2% of that are software and 1% are hardware problems. "

[Translation dw]. [typo corrected in archive copy. PGN]

THREE PERCENT error rate? For a security system of this size? But reading a snippet from the proposal makes it clear where the error rate is coming from [my translation]:

<http://www.heise.de/tp/deutsch/special/eco/16684/1.html> (in German)

TollChecker measures the vehicles three-dimensionally and determines a geometric vehicle model. With this, the number of axles are determined and trailers are recognized. From this data, the system determines the class of vehicle, in order to determine the appropriate fee. In addition, pictures of the vehicles and the license plates are taken with an infrared flash lighting that is invisible to the driver. With this, the license plate can be automatically determined.

The information from the control system is then compared by way of the communication interfaces [satellite!] with the data from the on-board unit and the data that was registered with the central computer system. Should it appear that some sort of falsification has occurred, the data will be stored as evidence.

All this computational effort to determine how many axles the

vehicle has?

No wonder they are having problems! It seems to me that it would be a lot easier to have the trucks buy stickers and police the use of the stickers! For this they have built ugly toll station information collectors over all the autobahns, have installed terminals that don't work in rest stops, and are using satellite technology.

It seems that the assumption is that people are hell-bent on deceiving the system, so they are trying to solve the social problem with technology, and that is not working. Germany is suffering from this wild scheme because the money was planned for repairing roads for the World Cup in 2006. Oh well, anyone for a train? Just a few minor signalling and switching problems there.....

[Added note from Debora: Here's a later followup on the Toll Collect:]

There are reports (for example <http://www.pcwelt.de/news/vermischtes/40102/>) that 3 high school students have developed a toll collection system as part of the "Jugend forscht" (Young Scientist Award given every year in Germany). They spent only 1300 Euros on their system which uses WLAN technology and broadcasts information on the number of axles to access points mounted over the autobahns. The data are then sent to a central computer, and when the truck leaves the highway via an exit ramp, a bill is automatically sent to the owner. This is similar to the toll system used, for example, on the bridge between Denmark and Sweden.

The students won first prize in the Geosciences division. They were invited to speak with TollCollect (the consortium that has not actually produced a toll system yet but is burning money by the hayloads), but TollCollect said that they would not use the technology because so much has already been invested in the method that they are using.

I would give TollCollect first prize in the "Never-admitting-we-were-wrong" category....

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB4, Treskowallee 8, 10313 Berlin
GERMANY +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

⚡ Listen to your CPU and break RSA?

<Gadi Evron <ge@linuxbox.org>
Sat, 08 May 2004 18:46:09 +0200

A story hit slashdot today about a research done by Adi Shamir and Eran Tromer on how you can perhaps break RSA keys by listening to a CPU.

The idea by itself is not new. If you are interested you can look up information on DPA and SPA as well.

I won't talk about how and what, you can find more information on the following URL's, and they are pretty easy to read and understand.

/. article at:

[http://slashdot.org/article.pl?
sid=04/05/08/117242&mode=thread&tid=126&tid=172](http://slashdot.org/article.pl?sid=04/05/08/117242&mode=thread&tid=126&tid=172)

Original article at: [http://www.wisdom.weizmann.ac.il/~tromer/
acoustic/](http://www.wisdom.weizmann.ac.il/~tromer/acoustic/)

As much as this technology is a risk and therefore a potential threat, unless you are of the really paranoid (which would mean this interests you considerably) there are far easier ways of attacking a computer.

This attack came to show how to attack the key, which is why it interests these folks, I suppose, but it would be much easier to use TEMPEST if you get access to actually install some tool to hear && (record || transmit) the audio. Then again, if you get that close you could always install a Trojan horse (which doesn't have to be software).

I would suggest TEMPEST would also be more reliable, but some testing is in order and the POC is impressive in its simplicity and efficiency. I would think a lot of research would be required for every CPU you intend to attack, but I am apparently wrong (?).

Cost vs. benefit? I can't really see it. But it works!

This is pretty cool though! I have to admit that!
(adding another mark on my paranoia list).

+972-50-428610 (Cell) ge@linuxbox.org. Backup: ge@warp.mx.dk.

[See also an article by Dmitri Asonov and Rakesh Agrawal, Keyboard Acoustic Emanations, 2004 IEEE Symposium on Security and Privacy, pages 3--11. PGN]

✶ Banks don't understand phishing social risks

<"Samuel Liddicott" <sam@liddicott.com>>

Mon, 17 May 2004 10:48:38 +0100

[This post has been edited slightly since being sent to the Co-operative Bank (UK). No response had been received from the bank after 4 weeks]

Normally there are subtle differences between the way a bank operates and the way phishing scams operate; typically any client initiated contact with the bank is safe (typos aside).

Phishing scams generally work by initiating a fake contact from the bank that directs users to transactions that scam the user.

The Coop bank is engaging in marketing practices indistinguishable from those practiced by phishers, encouraging customers to believe that callers claiming to be from the bank are indeed from the bank, making it easy for phishers to impersonate the bank for the purposes of obtaining customers security information.

Scammers would also need account number and sort code information that could be had from disposed receipts, personal cheques, stolen/found wallets etc, or obtained from the same phone call used to obtain the answers to security questions.

A few times in this past year I have received a telephone call from the bank (I suppose). The caller would identify themselves as being from the Coop bank, and that before they could proceed, would I have any objection to answering some security questions? I always refused to do so, not being able to tell that they were really from the bank and not some fraudster currently online to my bank and needing some help to answer my personal security questions.

Recently, within the last few weeks, out of curiosity I took the call a little further.

I told the caller that I would not answer the questions, for how could I tell she really was from the Coop bank.

She assured me she was a genuine caller from the bank, and seemed to think this assurance held some weight.

I suggested that for all I knew she was a fraudster who was on the line to my bank that very moment and asking me the same security questions the bank was asking her.

She finally understood my concerns enough and offered to let me call the bank number given on the bank website and then ask for her extension, which I did. When I then spoke to her, she said the call was just to make sure that I knew, that since the Coop bank and Coop insurance had merged, they could offer me combined products! For some reason "making sure I knew" needed me to answer personal security questions.

What is more concerning is not how sure the bank wanted to be that they were talking to me, but that they put their customers into the habit of believing that callers claiming to be from the bank are indeed from the bank.

And after all, what's the difference TO THE CUSTOMER between an e-mail purporting to be from the bank (typical phishing scam) and a phone call claiming to be from the bank?

I'll tell you the answer: On the bank website the customer is warned not to believe e-mails from the bank. There are no such warnings about telephone calls (yet).

Fortunately, while this sort of behaviour makes the banks customers more susceptible to believing man-in-the-middle phishers, it doesn't affect me.

It is admirable that the bank authenticates its customers, but before it does so the customers need to authenticate the caller as being the bank; I don't know how many customers are competent enough to do this, and while this is the case I think the bank should be careful what sort of expectations they instill into their customers.

[Fines reimbursed, drivers reinstated; faulty speed camera \(R-23.35\)](#)

<"Bertrand Meyer" <Bertrand.Meyer@inf.ethz.ch>>
Sun, 16 May 2004 17:22:03 +0200

New developments on the Victoria (Australia) defective speed cameras affair (see my note in RISKS 23:35):

Almost 165,000 motorists caught by fixed speed cameras will have their

finer waived or be paid compensation, costing the State Government \$26

million. This includes waiving \$6.1 million in fines. Hundreds of drivers

who lost their licenses for speeding may be back on the road. The State

Premier Steve Bracks said that every one of the 90,000 speeding fines ever

issued because of Western Ring Road fixed cameras would be repaid.

(Sums in Australian dollars. Summarized from the Melbourne Age, 15 May 2004,

<http://theage.com.au/articles/2004/05/14/1084289885456.html>.)

"Wear and tear, poor installation and electromagnetic interference were

blamed for faulty readings on ring road cameras". The State Government is

blaming the supplier, now in "administration", which says it's being

scapegoated and was not in charge of camera maintenance.

The opposition criticizes the State Government for not releasing the full

report and is threatening to go to court to get it published

(<http://theage.com.au/articles/2004/05/16/1084646060721.html>).

-- Bertrand Meyer

ETH Zurich <http://se.inf.eth.ch> -- Eiffel Software <http://eiffel.com>

Re: Hybrid vehicles may be hazardous to rescuers' health (R-23.35)

<Stephen Fairfax <fairfax@mtechnology.net>>

Sat, 08 May 2004 16:10:21 -0400

My wife owns a Toyota Prius, and as an engineer interested in power electronics and reliability I purchased and studied all the available shop manuals and other technical documentation available for the vehicle.

The hybrid voltage battery is located in the trunk. The Prius DC cables are colored bright orange for visibility and easy identification. Unlike power cables in 12 VDC systems, where the car chassis serves as the return circuit, two cables carry the + and - DC to the power electronics. This means that a person would have to accidentally touch both terminals to be shocked. In the unlikely but conceivable instance where damaged cable insulation connects one cable to the metallic chassis, a ground fault detection circuit would open the main DC relays (there are two, normally open) and de-energize the cables. Any collision that activates the front airbags will also cause the main DC relays to open and de-energize the cables and power electronics.

Prius service technicians are taught about an easily accessible bright orange plastic plug inside the trunk that can be pulled to physically disconnect the battery and remove all power from the high voltage electronics and cables. First responders are trained not to

touch anything colored bright orange in the Prius. There is also a control relay under the hood that can be removed to open the main DC relays and de-energize the cables. I found instructions for removing that relay in about 15 seconds of google searching using the search ("toyota prius" hazmat) at www.firehouse.com. As I am not a first responder I cannot comment on how many read firehouse.com.

Using the search ("toyota prius" "high voltage" site:toyota.com) I found the Toyota Emergency Response Guide (ERG), a 26-page PDF document explaining the operation of the vehicle, roadside assistance, and emergency response procedures. During a fire, the car is treated as any other car fire. As the ERG notes, firefighters can not be expected to notice that the car is a hybrid until after the fire has been knocked down. The battery electrolyte is potentially hazardous as it is a caustic alkali. The electrolyte is confined in a gel and will not normally leak even if the hybrid battery case is cracked.

The DC cables do NOT run through the doors. Many automobile wires, brake hydraulic, and fuel lines run in or near the frames surrounding the doors, as these are typically heavily reinforced and so offer good protection from both normal wear and accidents.

While the dangers posed by hybrid batteries are real, in context they are not very large, and Toyota seems to have done a commendable job of anticipating and mitigating the hazards. The new RISK arises

from the fact
that this is new technology for automobiles and there is a
transition period
where not all first responders have received appropriate
training. During
that transition period, uninformed speculation and
misinformation could
result in unwarranted delays extracting an injured person or in
controlling
a fire.

The greatest hazard in a damaged and motionless vehicle is
almost always the
tank of gasoline. Can you imagine the safety, environmental,
and other
regulatory hullabaloo that would arise if we were trying to
introduce
gasoline into vehicles for the first time today?

✶ Re: Auto-Blacklisting is a bad idea ([RISKS-23.36](#))

<Kyler Laird <Kyler@news.Lairds.org>>

Mon, 10 May 2004 14:08:08 GMT

> ... challenge-response system warned that it was going to
automatically
> blacklist my e-mail address if I didn't respond.

Anyone know when auto-blacklisting would be beneficial? I'm not
getting it.

If the message truly is spam, the sending address is probably
bogus. (I use
TMDA and I think I have the data to back up that assertion.)
Either the
address belongs to an innocent user (in which case auto-
blacklisting has
negative value, as demonstrated above) or the address points

into a bit
bucket somewhere (in which case blacklisting of any sort has
little or no
value).

On the rare occasion that a spammer sends a message with a
legitimate sender
address, the challenge will be sent to the spammer. It would be
easy enough
for that spammer to respond to the challenge (even, as we've
already seen,
if it requires some thought such as the image-based challenges)
and the auto-
blacklisting is not engaged.

So now we're down to the tiny chance of a spammer sending a
message with a
legitimate sender address from which he does not respond. Now
the auto-
blacklist engages and kills further messages from that address.
So? The
effect seen by the intended recipient is the same as if auto-
blacklisting
had not been used; either way, no messages are passed.

It's a stretch, but I'm willing to say that there is *some*
benefit to not
sending challenges to the same (unresponsive) address
repeatedly. That
benefit is so tiny that it disappears in the noise compared to
the problems
caused as a result. Also, there is no benefit to the intended
recipient
unless bandwidth has a very high cost.

Anything I'm missing?

[PGN asked Drew Dean if he wanted to answer that question, and
his response was evidently NO, Kyler has it right, although
Drew
added this counterquestion as to what might be added:

That people often assume that things are linear and

symmetric even

when they aren't?

Granted, much of the real world is linear and symmetric, so it's hard

to fight against a large number of years of "life experience." DD]

[typo corrected in archive copy. PGN]

✶ Formal Methods for Industrial Critical Systems CFP

<Diego Latella <Diego.Latella@isti.cnr.it>>

Mon, 10 May 2004 11:56:15 +0200

The 9th ERCIM "Formal Methods for Industrial Critical Systems" Workshop will be held in Linz, Austria (EU) on 20-21 September 2004

The aim of the FMICS <<http://www.inrialpes.fr/vasy/fmics/>> workshops is to provide a forum for researchers who are interested in the development and application of formal methods in industry. In particular, these workshops are intended to bring together scientists who are active in the area of formal methods and interested in exchanging their experiences in the industrial usage of these methods. These workshops also strive to promote research and development for the improvement of formal methods and tools for industrial applications.

Submissions are due by 21 June 2004. Further information at <http://www.fmics04.cclrc.ac.uk/>

Dott. Diego Latella, Consiglio Nazionale delle Ricerche

Ist. di Scienze e Tecnologia dell'Informazione - ISTI

Via G. Moruzzi, 1 - I56124 Pisa, ITALY

phone: +39 0503152982 or +39 348 8283101

fax: +39 0503138091 or +39 0503138092

Diego.Latella@isti.cnr.it [http://www.isti.cnr.it/People/D.](http://www.isti.cnr.it/People/D.Latella)

[Latella](#)



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 38

Thursday 27 May 2004

Contents

- [Paris Airport collapse: Analogy collapses](#)
[Marshall D Abrams](#)
- [FBI fingerprint screwup: Brandon Mayfield no longer a suspect](#)
[PGN](#)
- [GAO looked at DoD and off-shored software](#)
[James Paul](#)
- [So what's new with Pittsburgh Verizon DSL](#)
[David Farber](#)
- [The lighter side of electronic voting](#)
[Jason T. Miller](#)
- [Florida law bans deceptive subject lines in e-mail](#)
[NewsScan](#)
- [Spam being rapidly outpaced by 'spim'](#)
[Nico Chart](#)
- [Another method of password theft](#)
[James Renken](#)
- [Window smashed, data lost](#)
[David Lazarus via Monty Solomon](#)
- [Spamming the referrer logs](#)
[Diomidis Spinellis](#)

- [And a Mac Sniffer in a Pear Tree ...](#)
[Paul Kedrosky via Dave Farber](#)
 - [Speed cameras: fines refunded, licenses restored](#)
[Stuart Lamble](#)
 - [Re: Radar Gun Follies](#)
[Chris Meadows](#)
 - [Re: New UK driving licence puts identity at risk](#)
[Chris Malme](#)
 - [Re: Challenge-response is a bad idea](#)
[Jonathan de Boyne Pollard](#)
 - [REVIEW: "Beyond Fear", Bruce Schneier](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Paris Airport collapse: Analogy collapses

<Marshall D Abrams <abrams@mitre.org>>

Mon, 24 May 2004 09:39:17 -0400

In decrying the state of software quality we often make analogy to [the more solid engineering disciplines in] other professions. Years of experience have not made these other professions free from occasional catastrophic failure. The collapse of a 'Showcase Jewel' building is sobering.

A 98-foot section of the vaulted roof of the new \$890M terminal at the Paris Charles de Gaulle Airport collapsed just before 7am on 23 May 2004, killing at least five people and forcing authorities to revisit problems that preceded the fanfare opening of Terminal 2E less than a year ago. Cracks in the ceiling began to be noticed appearing only a few minutes before the

collapse -- which affected outerwalls and several cars parked below. The terminal opened 25 Jun 2003, and is referred to as a "showcase jewel". In the past, a huge light fixture had fallen in the departure area as inspectors were checking the facility before its opening, and there had been leaks in the ceiling. [Source: Jocelyn Gecker, Roof at Paris Airport Collapses, Killing 5; Terminal Described as 'Showcase Jewel', Associated Press, 24 May 2004; PGN-ed]

Marshall D. Abrams, The MITRE Corporation, 7515 Colshire Drive
McLean, VA 22102-7508 1-703-883-6938

✶ FBI fingerprint screwup: Brandon Mayfield no longer a suspect

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

Tue, 25 May 2004 09:11:34 -0700 (PDT)

After the Madrid train bombings that killed 191 people, a partial fingerprint was found in Spain on a plastic bag of detonators. Spanish authorities were unable to make a match on the print, and sent a digital copy to the FBI. The FBI claimed "100 percent" confidence that the fingerprint was that of Brandon Mayfield, a lawyer in the Portland Oregon area, although this was doubted by the Spanish authorities (who more recently fingered an Algerian national as the actual bearer of the print). Mayfield was arrested on 6 May and jailed for two weeks. (FBI agents were subsequently in Madrid on 21 Apr, meeting with Spanish investigators, but

reportedly did not check the original print.) FBI officials indicated digital matching was not unusual and within accepted policies and procedures, although this is reportedly being reconsidered. [Sources: Spain Had Doubts Before U.S. Held Lawyer in Madrid Blasts, Sarah Kershaw and Eric Lichtblau, *The New York Times*, 26 May 2004, and Oregon Lawyer Speaks Out About His Ordeal Behind Bars, Associated Press, 25 May 2004; PGN-ed]

[In past issues, RISKS has reported various cases of mistaken identities resulting from false biometric identifications, but also cases in which biometrics were successful in identifying culprits. In Mayfield's case, certain Muslim associations seem to have added circumstantial credibility to the confidence associated with the presumed match. Once again, some caution is needed in believing in digital evidence -- especially with only partial prints. PGN]

GAO looked at DoD and off-shored software

<"James Paul" <James.Paul@mail.house.gov>>
Tue, 25 May 2004 14:27:02 -0400

The U.S. General Accounting Office has released the following report:

Defense Acquisitions: Knowledge of Software Suppliers Needed to Manage Risks. GAO-04-678, 25 May 2004:
<http://www.gao.gov/cgi-bin/getrpt?GAO-04-678>

Highlights:

<http://www.gao.gov/highlights/d04678high.pdf>

[Interesting report. PGN]

⚡ So what's new with Pittsburgh Verizon DSL [IP]

<David Farber <dave@farber.net>>

Thu, 27 May 2004 09:18:04 -0400

Nothing. As of 0830 this am, access to some (maybe a large number) of Pittsburgh Verizon DSL customers has been down for 34 hours. When I called them I asked whether such service outages are appropriate for a communications company. After all there would be a major headline event if the telephone service was out that long due to human error. I was told that "after all, there is a federal requirement on telephone service not on data service.

I wonder what will happen as VOIP gets larger and outages like this take place.

Archives at: <http://www.interesting-people.org/archives/interesting-people/>

⚡ The lighter side of electronic voting

<"Jason T. Miller" <jasomill@theoneview.com>>

Wed, 19 May 2004 15:48:15 -0500 (EST)

It's a serious topic. One of the Onion items on foreseen problems [such as the possibility of electronic voting machines electing a robot president] at

<http://www.theonion.com/infograph/index.php?issue=4020>

is this:

"Not enough outlets in most high-school gymnasiums to plug in machines",

This made me think. Obviously the number of *plugs* isn't much of an issue

[nor the age of the students], but forgetting to check the capacity of the

electrical infrastructure is exactly the kind of bird-brained planning

failure that would surprise no one on RISKS.

Lamponing serious topics is of course *The Onion*'s raison d'etre

(for example,

<http://web.archive.org/web/20010927221133/http://www.theonion.com/>

was considered for a Pulitzer prize), and they do it so well.

One View, Inc., The Document Archiving Company, 8531 Bash Street Indianapolis, IN / 46250 <http://theoneview.com> 1-317-915-9039 x302

[This item was PGN-ed.]

✶ Florida law bans deceptive subject lines in e-mail

<"NewsScan" <newsscan@newsscan.com>>

Wed, 26 May 2004 08:17:14 -0700

Legislation signed by Florida Governor Jeb Bush will allow the state's attorney general to bring civil action against anyone in Florida

who sends
spam e-mail with a subject line intended to give the message
recipient a
false idea of what the message is about. [AP/*USA Today*, 26
May 2004;
NewsScan Daily, 26 May 2004]
<http://tinyurl.com/2jj6l>

✶ Spam being rapidly outpaced by 'spim'

<"Nico Chart" <NicholasC@ParadigmGeo.com>>
Thu, 27 May 2004 10:58:39 +0100

We have seen a lot of discussion about spam in RISKS lately, but
no mention
of spim, the instant messaging equivalent, said to be outgrowing
spam at the
present time. See this **New Scientist** article:
<http://www.newscientist.com/news/news.jsp?id=ns99994822>
"While the torrent of unsolicited spam e-mails continues to
rise, it is being
far outpaced by the surge in unwanted messages sent to the users
of instant
messaging programs, analysts have warned."

✶ Another method of password theft

<James Renken <jrenken@sandwich.net>>
Fri, 21 May 2004 18:24:40 +0000 (UTC)

Yesterday, I discovered that one of my Web hosting customers had
placed a
directory full of (copyrighted) MP3s on his site, open to
everyone. In

addition to the usual warnings and removals, we added basic HTTP password protection to the directory.

The MP3s had been around for a few months, long enough to make it onto some search engines, so we're still seeing quite a few visitors - many of whom are trying to log in using their own ISP/e-mail usernames and passwords. I haven't tested the passwords, of course, but I'm almost certain that this is the case, especially where people are entering their full e-mail addresses.

Although financial information isn't involved, this suggests a method of password theft that I haven't yet seen mentioned. One could easily post some MP3s, wait for search engine listings, and then record the passwords submitted. Human factors strike again!

James Renken, System Administrator Sandwich.Net Internet Services

<http://sandwich.net/> 1-760-729-4609 jrenken@sandwich.net

🔥 Window smashed, data lost (David Lazarus)

<Monty Solomon <monty@roscom.com>>

Thu, 13 May 2004 00:21:29 -0400

David Lazarus: Window smashed, data lost, *San Francisco Chronicle*,
12 May 2004

A thief smashed the rear window of Larry Saltzman's Saab not long ago and

stole his gym bag, a gold watch, credit cards, a few hundred dollars and the names, addresses and Social Security numbers of about 95,000 Bay Area residents. At issue -- yet again -- is the question of whether people's personal information can ever be truly safe once it's handed to an outside contractor, as a local insurer did with Saltzman.

A series of thefts involving confidential data in recent months suggests that no matter how extensive a company's security measures may be, they can be easily undone by human error, negligence or random circumstances. Consumers, in turn, face the very real possibility of their personal info falling into the wrong hands. ...

<http://sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/05/12/BUG806JPV71.DTL>

Spamming the referrer logs

<Diomidis Spinellis <dds@aueb.gr>>
Tue, 25 May 2004 11:49:54 +0300

A new form of spamming pollutes web server referrer logs, tricking Web sites to publish pages with links to unrelated commercial content.

Every day I receive an e-mail report summarizing the activity at my personal Web site. This allows me to see how the day's activities, such as the release of a new software update, or a new blog entry, contribute to the

popularity of various areas. It is also a security monitoring tool: an unexpected surge in traffic could mean something was amiss in its content.

Over the last year the contents of this report were becoming less reliable as a proliferation of different distributed crawling engines began taking up a noticeable percentage of the site's traffic. A bit of filtering corrected that issue: a "user agent" trying to read the robots.txt file could safely be excluded from the site's statistics.

Over the last days a more sinister form of noise has made its appearance. Part of the report I receive contains a listing of the top-10 referrer sites: the foreign URLs that were followed to land on my site. This is a useful feature, because it allows me to see which foreign links contribute to the traffic. Here is an example, from the day I announced a new release of UMLGraph, an open-source declarative UML diagramming tool, on freshmeat.org:

Top 10 Referrals:

77

http://freshmeat.net/projects/umlgraph/?branch_id=48663&release_id=160174

59 <http://javanews.jp/>

63 <http://www.cafeaulait.org/>

50 <http://www.ibiblio.org/javafaq/>

33 <http://freshmeat.net/daily/2004/05/09/>

23 <http://freshmeat.net/projects/umlgraph/>

15 <http://www.javanews.org/>

14 <http://www.freebsd.org/ports/sysutils.html>

[...]

Yesterday, following one of the links in the day's referral list, landed me on a typical popup window-infested porn Web site. It was the first time I had to enable Mozilla's popup window blocking feature to escape from the deluge of popups. The same happened with another site appearing in the referral list. Scanning the content of both referring pages confirmed my suspicion: none of the two did in fact contain a link to my Web site. The referrals were generated by Web server log entries like the following:

```
66.230.218.66 - - [15/May/2004:23:10:54 +0300] "GET / HTTP/1.1"
200 3132
"http://www.mixtaperadio.com/" "Mozilla/4.0 (compatible; MSIE
6.0;
Windows NT 5.1; .WONKZ)"
```

A Google search for a .WONKZ user-agent predictably showed more than a hundred entries, typically containing Web site usage statistics. With many sites automatically generating lists of referring sites and posting them on-line, the spamming of a site's referrer log is apparently an easy way to increase the number of links pointing to a Web site, and thereby increase the site's performance in search query results that base their results on this number (e.g. pagerank). An entry in an article on "spamdexing" at <http://www.tutorgig.com/encyclopedia/getdefn.jsp?keywords=Spamdexing> refers to this practice as "Referrer log spamming" and gives a similar rationale.

The risk: the ability to crawl the Web generating millions of spammed referrer entries will further diminish the utility of two up to

now useful

data sources: referrer logs, and incoming link counts as a measure of a site's importance.

Diomidis Spinellis - <http://www.dmst.aueb.gr/dds>

✶ And a Mac Sniffer in a Pear Tree ... (From Dave Farber's IP)

<Paul Kedrosky <pkedrosky@hotmail.com>>

Sun, 16 May 2004 09:21:41 -0700

The following is a laundry list of just some of the wireless network attacks and shenanigans that went on at this week's Networld + Interop trade show in Las Vegas. It is from an AirDefense press release (http://www.airdefense.net/newsandpress/05_13_04.shtm):

- 189 separate attacks on different devices
- 112 separate MAC spoofing attacks
- 89 Denial of Service attacks
- 42 authentication attacks, likely due to brute force attacks or misconfigured clients
- 20 separate AirSnarf attacks
- 4 separate Hotspotter attacks
- 3 large Ad-Hoc mesh networks were re-established on day two with an average of 10 stations connected.
- Another association was made with the Sear Service Toolbox (SST-PR-1) and the - network was attacked twice
- One Virtual Routing Redundancy Protocol (VRRP) attack, a routing tool attack to redirect traffic
- 165 BlueJack attacks
- 12 Blue Snarf attacks

✶ Speed cameras: fines refunded, licenses restored ([RISKS-23.35,36](#))

<Stuart Lamble <Stuart.Lamble@its.monash.edu.au>>

Fri, 14 May 2004 20:00:48 +1000

The Victorian (Australia) government is set to spend over \$AU19 million (approx \$US13 million) in compensation and refunding speeding funds for those affected by recent speed camera "glitches": \$13.7 million in refunding fines paid, and \$6 million in compensation for those who have suffered financial loss through loss of their driving licenses.

The fines being refunded are those on the Western Ring Road, from the date the fixed speed cameras were installed (2002), and those on the city's tollway and South Eastern (aka Monash) Freeway during the period that the cameras were being tested (from November last year).

Details at the Melbourne Age's Web site:

<http://www.theage.com.au/articles/2004/05/14/1084289868873.html>

and at the ABC News Web site:

<http://www.abc.net.au/news/newsitems/s1108467.htm>

Both reports were published on the 14 May 2004.

✶ Re: Radar Gun Follies

<Robotech_Master <robotech@eyrie.org>>

Sun, 2 May 2004 02:10:48 -0500

The comments in [23.33](#) (about the incorrectness of the radar gun for one stop casting doubts on its correctness for subsequent stops) are quite correct.

In point of fact, even when a radar gun is working *correctly*, it is fairly easy to cast doubt upon its efficacy. There are plenty of "How to beat a speeding ticket" tracts available on the Internet, and the typical "beat a ticket" tract includes a lengthy section on questions to ask in cross-examination to throw doubt upon the radar reading. How well was the officer trained, when was the unit calibrated, and so forth.

A typical such document can be found here:

<http://www.jesbeard.com/29ab.htm>

and makes interesting reading irrespective of the Risks issue.

One noteworthy quote, which relates to the "137 miles per hour" story from [23.33](#), comes from Section 9 on Cross-Examinations:

| NOTE: While it probably should become painfully obvious to both the officer and the court that he is simply unqualified to use a radar gun or to testify regarding its use.... the reality is that the officer and the judge are both likely to think the radar gun is just a magic gizmo you simply point and shoot....

Chris Meadows aka Robotech_Master <http://www.eyrie.org/~robotech>

⚡ Re: New UK driving licence puts identity at risk (Laurie, [R-23.37](#))

<Chris Malme <cim001@filklare.co.uk>>

Wed, 19 May 2004 00:31:36 +0100

The DVLA already give an option where for an admin fee of 4GBP, you can have your passport (or other ID) inspected without risking it to the post. This is actually detailed on the DVLA site the original poster referred to:

"Premium Service at Post Office Branches: If you are applying for your

first photocard driving licence, or already have a paper driving licence

in your present name, and you do not wish to send your identity documents

through the post, you may be able to use the premium service available at

selected Post Office branches. Your application will then be checked and

your evidence of identity will be returned to you immediately."

✶ Re: Challenge-response is a bad idea (Dean, [RISKS-23.36](#))

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

Mon, 17 May 2004 09:17:15 +0100

DD> If auto-blacklisting challenge-responses systems become the norm,

DD> there will be interesting risks related to the combination of

DD> forged mail, and auto-blacklists: [...]

That depends from one's publicly stated policy on responding to challenge-response Internet mail messages. If one has the publically stated

response policy of the RISKS List ("SPAM challenge-responses will not be

honored."), or the publically stated (or implicit) response policy of only responding to challenges where the original message really was one that one sent oneself, then this particular situation is a problem (especially with respect to the latter policy).

However, and somewhat ironically, other publically stated response policies do not cause the problems alluded to in this situation. Challenge-response systems, and their impacts upon unsolicited bulk mail, have been discussed at length in the "comp.mail.misc" and "news.admin.net-abuse.email" Usenet newsgroups (where it has been pointed out that such challenge messages *themselves* fulfill the criteria for being defined as "unsolicited bulk mail"). One poster has been so persuaded by the arguments that he has publically stated that he will now respond to *all* such challenges, whether for messages that he sent or not, on the grounds that (JdeBP précis - all misrepresentations are mine) since challenge-response systems are essentially reflecting all UBM forged in his name to him, the way to stop them doing so is to confirm the challenge and thereby ensure that the challenge-response system allows the UBM through to the original recipient without forwarding it to him (or simply sending the UBM that is the challenge messages themselves) any more.

That person in this situation can thus point to his publically stated policy and assert to any recipient of mail with his name in the headers that the fact that a message passed a challenge response system does *not* imply that

he actually originated it.

Of course, the tool for proving whether someone did or did not write a message is not challenge-response at all, and (as the preceding demonstrates) it is erroneous to assume otherwise. As I pointed out back in [RISKS-23.23](#) (with respect to the SPF, which flawed system is also falsely labelled as a means for stopping forgery), the tool for proving *that* has long since been invented, and is signed message bodies.

✈ REVIEW: "Beyond Fear", Bruce Schneier

<Rob Slade <rlade@sprint.ca>>
Tue, 25 May 2004 14:05:57 -0800

BKBYNDFR.RVW 20031219

"Beyond Fear", Bruce Schneier, 2003, 0-387-02620-7, U\$25.00/C
\$38.95

%A Bruce Schneier schneier@counterpane.com

%C 115 Fifth Ave., New York, NY 10003

%D 2003

%G 0-387-02620-7

%I Copernicus/Springer-Verlag

%O U\$25.00/C\$38.95 800-842-3636 212-254-3232 fax: 212-254-9499

%O <http://www.amazon.com/exec/obidos/ASIN/0387026207/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0387026207/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0387026207/>

[robsladesin03-20](#)

%P 295 p.

%T "Beyond Fear"

It is instructive to view this book in light of another recent

publication.

Marcus Ranum, in "The Myth of Homeland Security" (cf. BKMYHLSC.RVW)

[See Rob's review in [RISKS-23.02](#) and Marcus's response in [RISKS-23.14](#). PGN]

complains that the DHS (Department of Homeland Security) is making mistakes, but provides only tentative and unlikely solutions. Schneier shows how security should work, and does work, presenting basic concepts in lay terms with crystal clarity. Schneier does not tell you how to prepare a security system as such, but does illustrate what goes on in the decision-making process.

Part one looks at sensible security. Chapter one points out that all security involves a balancing act between what you want and how badly you want it. An important distinction is also made between safety and security, and the material signals the danger of ignoring the commonplace in order to protect against the sensational but rare. Fundamental security concepts are outlined as well as risk analysis. Chapter two examines the effect (usually negative) that bias and subjective perceptions have on our inherent judgment of risks. Security policy is based on the agenda of the major players, and chapter three notes that we should evaluate security systems in that light.

Part two reviews how security works. Chapter four introduces systems and how they fail. "Know the enemy," in chapter five, is not just a platitude: Schneier shows how an understanding of motivations allows you to assess the likelihood of different types of attack. Chapter six is less

focused than those prior: it notes that attackers reuse old attacks with new technologies, but it is difficult to find a central thread as the text meanders into different topics. Finding a theme in chapter seven is also difficult: yes, technology creates imbalances in existing power structures, and, yes, complexity and common mechanisms do tend to weaken security positions, but the relationships between those facts is not as lucidly presented as in earlier material. The point of chapter eight, that you always have to be aware of the weakest link in the security chain, even when it changes, is more straightforward, but the relevance of the illustrations surrounding it is not always obvious. Resilience in security systems is important, but it is not clear why this needs to be addressed in a separate chapter nine when it could have been discussed in eight with defence in depth (or "class breaks" and single-points-of-failure in seven). The hurried ending is also very likely to confuse naive readers in regard to "fail-safe" and "fail-secure": Schneier does not sufficiently stress the fact that the two concepts are not only different, but frequently in conflict. Chapter ten notes that people are both the strongest and weakest part of security: adaptable and resilient but terrible at detail; frequently surprisingly intuitive but often randomly foolish.

At this point the book is not only repetitive, but loses some of its earlier focus and structure. Detection and prevention are examined, in chapter eleven, not as part of the classic matrix of controls, but as

yet another example or aspect of resilience. Most of the rest of the types of controls in the preventive/detective axis are listed in chapter twelve, lumped together as response. Chapter thirteen looks at identification, authentication, and authorization (but not accountability, which was seen, in the form of audit, in chapter eleven). Various types of countermeasures are described in chapter fourteen. Countermeasures with respect to terrorism are examined, in chapter fifteen, both in general terms and in light of the events of 9/11. What works is discussed, as well as what does not, and there is an interesting look at the different roles of the media in the US as contrasted with the UK.

Part three, entitled "The Game of Security," is not clear as to purpose. Chapter sixteen starts off by pointing out that the five step assessment process is constant and never-ending--which begs the question of how to determine when diminishing returns start to set in on assessment itself. However, there is good material in regard to the actions you can take to influence decisions about security. A concluding editorial, in chapter seventeen, encourages the reader to move beyond fear and think realistically about security and the tradeoffs you are willing to make.

Some of the terms Schneier uses or invents may be controversial. His use of "active" and "passive" failures for the concepts more commonly known respectively as false rejection (false positive) or false acceptance (false negative) is probably much clearer, initially, to the naive

reader. The concept is an important one, and so the presentation of it in this way could be a good thing. On the other hand, does "active failure" completely map to what is meant by "false acceptance," and, if not, how much of a problem is created by the use of the new term? Similarly, "class break" does indicate the importance of new forms of attack, but the concept seems to partake aspects of defence in depth, single point of failure, and least common mechanism, all important constructs in their own right. Schneier's invention of "default to insecure" is not really any more understandable than the more conventional terms of fail-safe or fail-open.

I recommend this book. Unlike Ranum's, "Beyond Fear" has a more significant chance of informing and educating the public on vital issues of security. Security educators will find a treasure trove of ideas and examples that they can use to explain security concepts, to a variety of audiences. Security professionals are unlikely to find anything new in this material, but Schneier's writing is always worth reading, and this work is refreshingly free of the grating of erroneous ideas.

copyright Robert M. Slade, 2004 BKBYNDFR.RVW 20031219
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

Volume 23: Issue 39

Friday 28 May 2004

Contents

- [Air Force radios jamming garage-door openers in FL Panhandle](#)
[Paul Wexelblat](#)
- [Boa triggers blackout in Honduras](#)
[M. Barnabas Luntzel](#)
- [Online satire reported as truth](#)
[Jean L. Palmer](#)
- [*Reason Magazine* custom covers](#)
[Charles Shapiro](#)
- [New GAO Report on Government Data Mining](#)
[Barry Steinhardt via Dave Farber](#)
- [Coming Soon: A Cellphone Directory](#)
[Jube Shiver Jr. via Monty Solomon](#)
- [Maryland governor signs tough anti-spam law](#)
[Andy Sullivan via Monty Solomon](#)
- [The Fight Against Spam, Part 3](#)
[F.J. de Kermadec via Monty Solomon](#)
- [Now, two-thirds of all e-mail is spam](#)
[Bob Sullivan via Monty Solomon](#)
- [Poor fallbacks on automated systems](#)
[Geoff Kuenning](#)

- [Re: Ireland scraps electronic voting plans](#)
[Erling Kristiansen](#)
 - ['Pirate Act' raises civil rights concerns](#)
[Declan McCullagh](#)
 - [Re: New UK driving licence puts identity at risk](#)
[John Sawyer](#)
 - [Crash data recorders in cars](#)
[Fuzzy Logic](#)
 - [Re: FBI fingerprint screwup](#)
[Scott Miller](#)
 - [Risks of believing in testing, Re: GAO report](#)
[Chris Jewell](#)
 - [Re: Another method of password theft](#)
[A J Stiles](#)
 - [Banks don't understand phishing social risks](#)
[Michael Bacon](#)
 - [REVIEW: "The Teeth of the Tiger", Tom Clancy](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Air Force radios jamming garage-door openers in FL Panhandle

<Paul Wexelblat <wex@cs.uml.edu>>

Wed, 19 May 2004 20:31:15 -0400

A new \$5.5M military two-way radio system being tested at Eglin Air Force

Base in Florida is preventing garage doors from opening in the neighboring

communities of Niceville, Valparaiso and the Crestview area.

Motorola said

it will try to minimize the problem, altering the frequencies for the next

tests. However, a news report suggests that homeowners "may have to change

the frequencies" on their remote controllers because the FCC

indicates the
Air Force is operating within its licensed frequencies. The
problem is also
likely to propagate further: a similar system has been requested
for the
Pensacola Naval Air Station and other bases. [Source: AP item,
*South
Florida Sun-Sentinel*, 19 May 2004; PGN-ed]

Gee, if the avionics are jamming the garage door mechanisms,
ya gotta
wonder what the garage door openers are jamming. PW

⚡ **Boa triggers blackout in Honduras**

<"M. Barnabas Luntzel" <mark@luntzel.com>>

Wed, 19 May 2004 16:44:58 -0700

A boa constrictor triggered a 15-minute nationwide blackout when it
slithered into a generator at a major hydroelectric plant that
supplies 60%
of Honduras' electricity. Power outages are common in Honduras;
a failure
at the same dam left the nation without power for three hours in
Sep 2003.
[Source: AP item from Tegucigalpa, 19 May 2004; PGN-ed. Yes,
the boa was
electrocuted, but earns the RISKS-archives size prize for animal-
inspired
outages -- beating out the raccoons, rats, and 6 SRI squirrels.]
[http://www.sfgate.com/cgi-bin/article.cgi
?file=/news/archive/2004/05/19/international1934EDT0786.DTL](http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2004/05/19/international1934EDT0786.DTL)

⚡ **Online satire reported as truth**

<"Palmer, Jean L." <jean.palmer@ngc.com>>

Fri, 28 May 2004 08:35:02 -0700

On 6 May 2004, the online satire magazine *The Daily Farce* ran a tongue-in-cheek story saying that US Secretary of Defense Donald Rumsfeld had banned the use of digital cameras in Iraq: "Donald Rumsfeld told reporters in a press conference "those found guilty of following my orders, I mean, of performing these acts will be tried and prosecuted by a jury as effective as the one that prosecuted O.J. Simpson." He continued "Further, to protect the Iraqi prisoners from any future abuses; any digital cameras, camcorders, or cell phones with cameras are strictly prohibited anywhere in any military compound in Iraq."

http://www.thedailyfarce.com/world.cfm?story=2004/05/world_moreabusepictures_05200400006

A few weeks later, someone picked this up and ran with it, rather than recognizing it as a satire piece. It reproduced and began appearing in news media all over the world, especially overseas, as an established fact. A search of Google News found it on at least 40 news sites, and a web search found it on more than 4,000 sites.

Risks:

1. News organizations assuming that everything they read online must be true
2. Reporters using questionable sources for facts
3. (perhaps) Non-native english speakers not recognizing satire
4. Humans assuming that everything reported by a newspaper -- especially an online newspaper -- is fact.

Jean Palmer, Northrop Grumman jean.palmer@ngc.com 1-410-993-

2627

[5. Some folks might think it true, and are happy to pass it on as such.

6. Some folks, knowing it is bogus, want to poke at the underlying situation.

7. Some folks get fooled even on April Fools' Day.
and lots more. PGN]

***Reason Magazine* custom covers**

<Charles Shapiro <cshapiro@nubridges.com>>

28 May 2004 09:58:34 -0400

Reason Magazine (<http://reason.com>) got some coverage in both slashdot and the New York Times for their May cover, which was tailored individually to feature an aerial photo of the residence of and the name of each subscriber. Alas, it looks like someone screwed up the columns in one of their SQL queries. The article on the inside of the cover was intended to give some more entertaining facts about the subscriber, but for me it said "...the same information networks that tell me that 1.82% of your neighbors have college degrees or that Rep Denise percent of the kids in your ZIP code are cared for by their grandparents...". I cannot tell whether the 1.82% number is accurate, but I have my doubts. Denise Majette is my representative, but I think they really wanted a number there. They also mixed up the column headings on the table of demographic data printed at the bottom of the inside cover, although the nature of the data there makes it

possible to sort out what number goes where. I'm most curious to know how general these problems were in the print run, which featured close to 40,000 different covers.

This illustrates one of the many ways that you can screw up while using a database to characterize your customers, clients or suspects. In this case the consequences are minor, but a supermarket which guesses too wrong will lose a lot of money, and a government could victimize exactly the wrong people.

✈ New GAO Report on Government Data Mining (via Dave Farber's IP)

<Barry Steinhardt <Bsteinhardt@aclu.org>>

May 27, 2004 1:10:03 PM EDT

A new report on "data mining" , which is being released today by the General Accounting Office, reveals that practice is widespread in the the Federal government and that there are, at least, four programs that may be accessing and analyzing private-sector databases in ways that are reminiscent of the Pentagon's Total Information Awareness Program. The report was prepared at the request of Senator Daniel Akaka of Hawaii.

The GAO's investigation uncovered 199 government uses of the statistical analysis techniques known as data mining, 54 of which use private-sector

data. Such information could include any data held in corporate or other private hands, including credit-card records and Internet logs.

In an appendix to its report, the investigators listed those programs, providing a brief description of each and indicating its purpose and whether it contained personal information, or made use of private-sector data and data from other government agencies.

The 4 programs of special concern are:

- * Verity K2 Enterprise - Defense Intelligence Agency (DIA). Mines data "to identify foreign terrorists or U.S. citizens connected to foreign terrorism activities." (Page 30 of GAO report)
- * Analyst Notebook I2 - Department of Homeland Security. "Correlates events and people to specific information." (p. 44)
- * PATHFINDER - DIA. "Can compare and search multiple large databases quickly" and "analyze government and private sector databases." (p. 30)
- * Case Management Data Mart - DHS. "Assists in managing law enforcement cases" Using private-sector data. (p. 44)

According to the GAO descriptions, all four programs draw on private-sector databases, contain personally identifiable information, and appear to constitute dragnets on the general population.

Of course, many of the other programs listed by the GAO raise questions about how they are using information, including private-sector information -- and the GAO's list did not include programs run by the Central Intelligence Agency and the National Security Agency, which did not respond to its requests for information.

The ACLU, together with the Electronic Privacy Information Center and the Center for Democracy and Technology, today sent a joint letter to Senator Akaka praising his efforts and the report.

The joint letter to Sen. Akaka is online at <http://www.aclu.org/Privacy/Privacy.cfm?ID=15858&c=130>

The GAO [report] should be on their Web site shortly at <http://www.gao.gov/>.

Barry Steinhardt, Director Technology and Liberty, American Civil Liberties Union (ACLU), 125 Broad Street, NYC 10004 www.aclu.org

IP Archives: <http://www.interesting-people.org/archives/interesting-people/>

Coming Soon: A Cellphone Directory (Jube Shiver Jr.)

<Monty Solomon <monty@roscom.com>>

Fri, 21 May 2004 10:19:35 -0400

Privacy advocates fear consumers will face a flood of unwanted calls and junk e-mail, Jube Shiver Jr., **Los Angeles Times**, 20 May 2004:

After years of anonymity, the numbers of most of the nation's mobile phones will be compiled later this year in the first wireless directory. The database being assembled by the Cellular Telecommunications and Internet Assn. is expected to include about 75% of the 163 million mobile phones in the United States, making looking up a wireless number as easy

as dialing
411. ...

<http://www.latimes.com/la-fi-cellphones20may20,1,3236420.story>

[NO OPT OUT??? Beware! PGN]

⚡ Maryland governor signs tough anti-spam law (Andy Sullivan)

<Monty Solomon <monty@roscom.com>>

Fri, 28 May 2004 08:59:37 -0400

[Source: Andy Sullivan, Reuters, 26 May 2004; PGN-ed]

Internet "spam" purveyors who hide behind false e-mail addresses could face

up to 10 years in jail and fines of \$25,000 per day under The Maryland Spam

Deterrence Act signed on 26 May 2004 by Maryland Governor Robert Ehrlich.

The law allows state officials to arrest and fine those who engage in a variety of deceptive tactics to send junk e-mail.

But one anti-spam activist said it would do little to stop the unsolicited

bulk messages that now account for up to 83 percent of all e-mail, because

most of those already violate anti-fraud laws. ...

<http://finance.lycos.com/home/news/story.asp?story=41660480>

⚡ The Fight Against Spam, Part 3

<Monty Solomon <monty@roscom.com>>

Mon, 24 May 2004 12:06:18 -0400

The Fight Against Spam, Part 3, by Francois Joseph de Kermadec,
21 May 2004

Editor's note: In part one, F.J. focused on laying the foundation for an anti-spam strategy and he covered how to block most of your unwanted mail. Then in part two, he fine-tuned this strategy, plus he took a closer look at the technologies inside of Mail.app. Now in part three, the conclusion of this series, F.J. covers rules and additional tools and techniques you can use to avoid becoming buried in spam. ...

http://www.macdevcenter.com/pub/a/mac/2004/05/21/spam_pt3.html

✶ Now, two-thirds of all e-mail is spam (Bob Sullivan)

<Monty Solomon <monty@roscom.com>>

Sat, 22 May 2004 12:59:56 -0400

According to MessageLabs Inc., in its monitoring of e-mail traffic for 8500 customers in April 2004, spam accounted for two-thirds of all e-mail traffic, and 80% of e-mail the United States. The first figure was 50% a year ago, and MessageLabs predicts 90% in another year.

[Source: Bob

Sullivan, MSNBC, 21 May 2004; PGN-ed]

<http://msnbc.msn.com/id/5032714/>

✂ Poor fallbacks on automated systems

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

25 May 2004 01:33:20 -0700

I pay my bills through Paytrust.com. They have a "feature" called "SmartBalance", which attempts to infer the balance in your checking account including allowances for outstanding checks. Of course, this is possible only if you never use an ATM, write a check outside their system, incur bank service charges, etc., but that doesn't seem to bother them. The SmartBalance system requires that you provide them with the password to your online banking account so that they can fetch current information.

A recently added misfeature tries to warn users if they are writing a check that would overdraw their account. So far, so good, despite the glaringly unavoidable inaccuracies. But if you haven't given them a password for your bank account, they assume it's zero -- and then make you walk through a "Please click OK" screen to "protect" you from the consequences of an overdraft.

The RISKS are numerous:

- * Assuming that you can make a valid calculation with partial information.
- * Continuing with a calculation when some data is unavailable.
- * Warning the user of an error condition when it is impossible to avoid false positives.
- * Teaching the user to depend on an error warning when it is impossible to

avoid false negatives.

They would almost have been better off to hook the whole system up to a random number generator; the accuracy would have been roughly the same, and they would have saved an immense amount of programming time.

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

★ Re: Ireland scraps electronic voting plans (Beleskey, [RISKS-23.35](#))

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>

Sat, 22 May 2004 21:07:11 +0200

There is an interesting additional twist to this story:

The voting machines purchased by the Irish authorities are produced by the Dutch company Nedap. Essentially the same machines have been used in The Netherlands for several years, and did not attract much attention, at least not in the general press, until the Irish rejection.

When questioned in the Dutch parliament, the responsible minister De Graaf declared that "he found the machines reliable". This statement seemed to suffice to avoid debating the matter further.

It has also transpired from the discussion that the machines have been tested by an independent test lab, TNO. The reports were, however, kept secret. Until the problems started in Ireland. The Dutch TNO reports have

now been released in Ireland! It turns out that "The reports by KEMA Quality BV and TNO were not concerned with either the accuracy or the security of the machines". The tests seem to have mainly addressed robustness of the machines, not the voting or counting itself.

The whole affair has gotten very little media coverage in The Netherlands so far, most of the available information comes from newsletters of privacy groups like Bits of Freedom (in Dutch) (<http://www.bof.nl/>) and EDRI (in English) (<http://www.edri.org/>).

So it looks like what was rejected in Ireland is happily being accepted in The Netherlands, without attracting much attention, neither by the government nor by the media.

✶ 'Pirate Act' raises civil rights concerns (Declan McCullagh)

<Monty Solomon <monty@roscom.com>>

Fri, 28 May 2004 01:42:52 -0400

Declan McCullagh, Staff Writer, CNET News.com, 26 May 2004

File swappers concerned about getting in trouble with record labels over illegal downloads may soon have a major new worry: the U.S. Department of Justice.

A proposal that the Senate may vote on as early as next week would let federal prosecutors file civil lawsuits against suspected

copyright infringers, with fines reaching tens or even hundreds of thousands of dollars. The so-called Pirate Act is raising alarms among copyright lawyers and lobbyists for peer-to-peer firms, who have been eyeing the recording industry's lawsuits against thousands of peer-to-peer users with trepidation. The Justice Department, they say, could be far more ambitious.

One influential proponent of the Pirate Act is urging precisely that. "Tens of thousands of continuing civil enforcement actions might be needed to generate the necessary deterrence," Sen. Orrin Hatch, R-Utah, said when announcing his support for the bill. "I doubt that any nongovernmental organization has the resources or moral authority to pursue such a campaign."

The Pirate Act represents the latest legislative priority for the Recording Industry Association of America (RIAA) and its allies, who collectively argue that dramatic action is necessary to prevent file-swapping networks from continuing to blossom in popularity. ...

<http://news.com.com/2100-1027-5220480.html>

✦ Re: New UK driving licence puts identity at risk (Malme, [R-23.38](#))

<John Sawyer <jpgsawyer@btopenworld.com>>
Fri, 28 May 2004 09:53:54 +0100 (BST)

Chris Malme in [RISKS-23.38](#) noted that the UK Post Office offers the option of checking your documents for you and indeed they do, unless you are exchanging a drivers license from a foreign country. In this case you have no option but post your Passport, the foreign drivers license to the DVLA. Your Passport is then returned to you via normal postage. Even if you include a postage paid recorded delivery self address envelope.

This Risk of having to include all your identification documents in the same envelope should be evident for all and to require it on someone's arrival in the country seems somewhat dangerous. The only truly safe option seems to be to go down to Swansea to submit your documents in person but event then you can not collect them in person. (Swansea isn't exactly central to most of the UK population either as nice a part of the country as it surely is.)

For a government so intent on introducing ID cards to prevent immigration fraud to have an agency acting in this manner is to my mind amazing.

✶ Crash data recorders in cars

<Fuzzy Logic <bob@arc.ab.ca>>
Fri, 28 May 2004 11:30:53 -0600

I recently watched a repeat of a consumer show called Market Place. This one was on crash data recorders in cars and how they are being

used more
and more by police and insurance companies. The transcript of
the show can
be found here:

<http://www.cbc.ca/consumers/market/files/cars/blackboxes/index.html>

Apparently they are installed in over 25 million North American vehicles.

My concern is the accuracy of these devices (odds are there are going to be a few duds) and the likelihood that they will win out in court over the drivers' word. Honest I wasn't speeding, black box says otherwise. Claimant refused insurance claim and probably has their insurance canceled.

✶ Re: FBI fingerprint screwup (PGN, [RISKS-23.38](#))

<Scott Miller <SMiller@unimin.com>>

Thu, 27 May 2004 16:37:34 -0400

[... In Mayfield's case, certain Muslim associations seem to have added circumstantial credibility to the confidence associated with the presumed match. Once again, some caution is needed in believing in digital evidence -- especially with only partial prints. PGN]

My read on the "circumstantial credibility" is that it was flimsy in the extreme. He married a Muslim and once defended someone accused of a terrorism-related crime. Not to mention that apparently the Spanish

authorities almost immediately informed the FBI the fingerprint was definitely not Mayfield's, but the FBI did not act until a positive match was found (by Spain). I also must wonder if what you cited is the true extent of the risk? The reliability of fingerprint and DNA evidence seems to go pretty much uncontested in criminal trials, and the examples of which I am aware are largely those in which the defendant can afford an adequate defense. I wonder how many persons could possibly be incarcerated on evidence no stronger than that on which Brandon Mayfield was detained? Particularly in cases where the defendant was represented by a public defender or other hired gun of less than top caliber? Combine this possibility with the sort of prosecutorial misconduct that seems to be all too common, and the imagination can conjure up some scary scenarios. I think that this might be worthy of further investigation...

✶ Risks of believing in testing, Re: GAO report ([RISKS-23.38](#))

<Chris Jewell <chrisj@puffin.com>>
27 May 2004 16:20:10 -0700

What jumped out at me from the first page of the GAO report referenced in [RISKS-23.38](#) was ...

> As the amount of code on weapons systems increases, it becomes more
> difficult and costly to test every line of code.

Can it possibly be that the GAO (and DOD procurement people) have not yet noticed that testing every line of code is a completely inadequate way to demonstrate the correctness of a software system, and that testing can demonstrate the presence of errors, but never the absence?

How long ago was Edsger Dijkstra railing against the folks who didn't realize that a program can contain errors even though each line of code has passed a test? I think that was in the 1970s, yet many people still haven't heard the message.

✦ **Re: Another method of password theft (Renken, [RISKS-23.38](#))**

<A J Stiles <ajs2@adyx.co.uk>>

Fri, 28 May 2004 10:58:00 +0100

I work for an ISP and, for a while, we had a Web mail system running on our servers; and we used to get all sorts of what we could only assume were AOL and Hotmail logins and passwords being entered.

Given the human tendency to re-use passwords across services -- or at least, to use minimal munging between uses -- I suspect that anyone putting up a form with the appropriate fields could get a lot of passwords, as long as they got listed on the search engines. As the original poster says, the promise of MP3s, porn, pictures of pop stars &c. is a powerful motivating

factor.

I'm sure I remember something similar to this, dating back to the BBS days of the early '90s; it may even have cropped up in RISKS.

✶ Banks don't understand phishing social risks

<"Michael (Streaky) Bacon" <himself@streaky-bacon.co.uk>>

Fri, 21 May 2004 07:03:06 +0100

In [RISKS-23.37](#), Samuel Liddicott reported that "Banks don't understand phishing social risks". I reported a similar instance in Risks 21:59 in regard to another UK bank, but without comment on the "phishing" aspects. The banks are making a rod for their own backs by their approach to authentication, and their systems designers appear ignorant of the basic security that needs to be applied. Of course, many of their customers are still trusting of the bank ... but sadly these contain a number who "trust" the phishers and scammers.

The bank in question in my original posting has recently changed the log-in process for their e-banking Web site. Previously, in addition to other identification, one had to type in two randomly requested letters from a "password". These were entered in a form box with the usual asterisks being displayed instead of the letters. A redesign (in the interests of improving security) now forces the user to select the letters from two

drop-down

boxes, and the actual letters remain displayed on the screen.

Yet another example of Hutber's Law: "Improvement means deterioration".

The RISKS are inherent.

✶ REVIEW: "The Teeth of the Tiger", Tom Clancy

<Rob Slade <rslade@sprint.ca>>

Fri, 28 May 2004 08:41:49 -0800

BKTTHTGR.RVW 20040306

"The Teeth of the Tiger", Tom Clancy, 2003, 0-399-15079-X,
U\$27.95/C\$40.00

%A Tom Clancy

%C 10 Alcorn Ave, Suite 300, Toronto, Ontario, M4V 3B2

%D 2003

%G 0-399-15079-X

%I Penguin Putnam

%O U\$27.95/C\$40.00 416-925-2249 Fax: 416-925-0068

service@penguin.ca

%O [http://www.amazon.com/exec/obidos/ASIN/039915079X/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/039915079X/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/039915079X/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/039915079X/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/039915079X/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/039915079X/robsladesin03-20)

%P 431 p.

%T "The Teeth of the Tiger"

It is interesting to note, reading the reviews on Amazon, that even

die-hard Clancy fans are starting to lose faith. Clancy has moved

from curmudgeon to outright maverick in this work. The plot doesn't

just depend on bending the rules, but by going completely outside them and playing God. (In which regard, I'm fairly sure that quite a few Catholics would take issue with the assertion that as long as you *think* you are doing the right thing, God can't say anything about it.) The "good guys" luck out a lot, but are extremely sloppy, and any group that did operate in this manner would tend to kill a lot of innocent people. Despite crises of conscience (very brief ones), none of the characters in this tale are attractive or sympathetic: they all seem to be pretty thin. But that isn't what we are here to talk about.

Clancy demonstrated in "The Bear and the Dragon" (cf. BKBRDRGN. RVW) that he didn't understand cryptography, and he proves his lack of comprehension again here. Sun makes good workstations, but they aren't supercomputers. Single pass DES (Data Encryption Standard) has fallen to brute force attacks, but serious users have plenty of algorithms to choose from that haven't. Clancy has moved the myth of the NSA providing encryption standards with backdoors built into it slightly out of the house, but it's still a myth. (Yes, the NSA does have smart people, but the one time they did really try it, with the Clipper/SKIPJACK key escrow system, it failed. Ironically, the failure didn't lie in their ability not to get caught, since they were completely open about it, but in a weakness that meant the escrowing system could be broken.) As far as getting everyone to buy into a proprietary, unreviewed encryption system and use it pretty much universally for several years without anybody twigging as to what was

going on, forget it. There are a number of players in the crypto market, everybody serious enough to study the field knows not to buy snake oil, and anyone following the security field at all knows that backdoors get found every day.

Just because you use the same accounting system as someone else doesn't mean that you can read all their files. (In fact, if you are breaking in to someone's system, it is often easier to grab the data files themselves and process them with your own tools.) There is no discussion about getting access to files on remote systems at all:

Clancy just seems to assume that it can be done. Admittedly, he is assuming a backdoor into Echelon, and assuming that Echelon can, in fact, collect all the transmission of voice and data anywhere in the world. (We'll leave that tall order for the moment, since it isn't inherently impossible, however unlikely.) The data under investigation, however, isn't in transit: it resides on a bank computer.

This book has annoying errors in technology, flat characters, a shaky premise, and very little of the old Clancy flair.

copyright Robert M. Slade, 2004 BKTTHGTGR.RVW 20040306
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

Volume 23: Issue 40

Thursday 3 June 2004

Contents

- [Problems due to misfiled fingerprints](#)
[PGN](#)
- [Building the A380: Just Like Software](#)
[Rex Black](#)
- [eVoting standards and testing](#)
[Rebecca Mercuri](#)
- [Re: Risks of believing in testing](#)
[Ken Knowlton](#) [Spencer Cheng](#)
- [Users, learning from history, social engineering, planning](#)
[Gadi Evron](#)
- [Detectives follow the money trail to tackle spam](#)
[NewsScan](#)
- [Are passwords passe'?](#)
[NewsScan](#)
- [Re: Boa triggers blackout in Honduras](#)
[Ralph Barone](#)
- [The lighter side of electronic voting](#)
[Marcus L. Rowland](#)
- [Re: New GAO Report on Government Data Mining](#)
[Robert I. Eachus](#)

● [Data Mining: Federal Efforts Cover a Wide Range of Uses](#)

[Monty Solomon](#)

● [Daft security questions](#)

[Ian Chard](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Problems due to misfiled fingerprints

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

Wed, 2 Jun 2004 00:12:10 GMT

If you Google "Sanchez Rosario fingerprints", you get a remarkable case of a man named Rene Ramon Sanchez who bore absolutely no resemblance to Leo Rosario, a drug dealer and deportation candidate, but whose fingerprints seemingly matched those of Rosario. To make a long story very short, the problem was that Rosario's fingerprints had been substituted for Sanchez's. A judge insisted that fingerprints never lie, causing Sanchez an enormous amount of grief. In fact, Sanchez was arrested three times for Rosario's crimes, spending two months in custody and threatened with deportation. Thus, a single error propagated and the justice system failed to correct it. [Source: Benjamin Weiser, Can Prints Lie? Yes, Man Finds to His Dismay, *The New York Times*, 31 May 2004; PGN-ed]

[Please dig up the full text. This is a grueling parable for our times, as was the Brandon Mayfield case noted in [RISKS-23.38](#) and [39](#). PGN]

✶ Building the A380: Just Like Software

<Rex Black <rexblack@ix.netcom.com>>

Sun, 30 May 2004 18:10:49 +1200

I don't have the references right now, but I read an article in the **Asian Wall-Street Journal** on 28 May 2004 that talked about the A380 development project. (The A380 is Airbus' superjumbo, doubledeck jet.) Apparently, lots of new, previously-unused technologies and materials are involved. The project management methodology: Commit to fixed delivery deadlines for major clients like Singapore Airlines before the composite wing struts and supports were fully tested.

Hey, if it's good enough for software that ends up in critical information infrastructure, it's good enough for a 500+ passenger airplane, right?

Rex Black Consulting Services, Inc., 31520 Beck Road, Bulverde, TX 78163 USA

www.rexblackconsulting.com +1-830-438-4830

rex_black@rexblackconsulting.com

✶ eVoting standards and testing

<"R. Mercuri" <notable@mindspring.com>>

Mon, 31 May 2004 07:54:35 -0400

On eVoting Standards and Testing, see two articles from 30 May

2004:

Elise Ackerman of the *San Jose Mercury News* reported on CA Secretary of State Kevin Shelley's difficulties in obtaining information about the voting systems' so-called "federal testing" by the so-called "independent" testing authorities:

<http://www.mercurynews.com/mld/mercurynews/news/politics/8797832.htm>

The New York Times also ran an editorial pointing out the lack of transparency in the election system testing process.

<http://www.nytimes.com/2004/05/30/opinion/30SUN1.html>

It is important to note that the U.S. Federal government does NOT oversee the testing of election equipment, this is a privatized process paid for by the voting system vendors. Nor are there any true Federal "standards" for election systems -- the FEC's guidelines are not Federally required and have not been mandated by all of the states. Opposers to voter verified paper ballots (VVPB) claim that the ballot printers are not implementable because there are no "Federal standards" -- yet there is NOTHING in the FEC guidelines that PREVENTS a state (or a vendor) from ADDING security features (such as VVPB) -- so this argument is just a smokescreen! In fact, the FEC declined to include such guidelines in their 2002 VSS document, despite having been alerted to the necessity of independent auditability for electronic voting systems by numerous scientists who had been requested to provide formal remarks (see my comment at www.notablessoftware.com/evote.html). California, thankfully, is

creating its own VVPB standards -- other states should be encouraged to do likewise.

(Note that there are FEC guidelines for optically scanned ballots, which are VVPB.)

The new Election Assistance Commission has yet to establish its technical commission -- the group that was supposed to create a new set of standards, presumably BEFORE states were to rush out and spend their HAVA money on voting equipment -- but now the \$3B in HAVA funding is a true cart-before-the-horse porkbelly (to mix metaphors!) and the \$30M that NIST was supposed to receive for their participation in the formation of the HAVA standards has yet to materialize. The IEEE is working on a voting system standard, but it is currently limited to vote casting equipment and the committee is heavily vendor controlled.

<http://grouper.ieee.org/groups/scc38/index.htm>

Voting system standards are of increasing concern, because vendors and election officials claim that products are safe because they have been

"Federally certified" yet investigations have revealed uncertified software used in equipment in California, Indiana, and Georgia. The standards lack security controls that would enable tracking of software changes, but even so, they are being ignored in blatant violation of state election laws.

This situation will bear monitoring, and it is helpful that some major press agencies have now begun to give it a closer look.

✶ Re: Risks of believing in testing (Jewell, [RISKS-23.39](#))

<Ken Knowlton <KCKnowlton@aol.com>>

Sat, 29 May 2004 21:30:29 EDT

Well, I've turned "store" into a macro that redundantly puts data in the intended location and those before and after it, just to be super-safe -- because some other part of the program may contain an off-by-one error when trying to fetch it. It has tested perfectly. Could I still be in trouble?

[Certainly. The data you are storing could be already corrupted.

This is a problem with voting machines whose vendors claim that there

are THREE INDEPENDENT VERSIONS OF YOUR VOTE, when all three come from

the same possibly erroneous program. PGN]

✶ Re: Risks of believing in testing (Jewell, [RISKS-23.39](#))

<Spencer Cheng <spencer@morphbius.com>>

Fri, 28 May 2004 22:36:02 -0400

While Chris Jewell is quite correct, the state of the industry on S/W testing is very inadequate today. I would be very happy to have any S/W that has actually being tested properly for functionality even if there are latent errors in the S/W.

There is at least one testing technology available which can do

proper
functional testing by generating optimally minimal test suites
using
formal interface specification but the acceptance by industry
has been
very slow.

I have looked long and hard at proof of correctness in a
previous job
but other than safety critical systems, the cost is difficult to
justify. In addition, proof of correctness is not very useful if
the
implementation changes even slightly.

I have become a firm believer over the years in proper black box
testing since -

1) it is the only way I know to establish that mythical S/W
contract
that people have been talking about for the last 20 years.

2) Properly done, it can shield the applications from changes in
the
underlying system. A complete and optimal set of black box test
cases
IS the S/W contract since it defines the semantics. Any
implementation changes that changes interface behaviour would
fail the
black box tests.

3) Requirement traceability can be satisfied by tracing the
requirement
to the interface specification and onward to the test cases.

⚡ Users, learning from history, social engineering, planning

<Gadi Evron <ge@linuxbox.org>>

Sun, 30 May 2004 20:29:40 +0200

Apparently, although the security industry came a long way and proper working procedures, risk analysis and billions of USD in products every year do exist, we still didn't find a way to effectively attack the simplest of problems.

Any problem can be addressed, but usually running a firewall or running after a virus outbreak take precedent over methodology and planning. Security professionals many times ignore the simplest of issues, being over-whelmed by work and believing the basics are covered.

Here are a few examples.

Although different policies are being implemented in many organizations, as well as many organizations do extensive security planning, users still find ways to get by any restriction and go with the easiest solution which would allow them to circumvent security and work in ease.

I truly believe that if we provide solutions that a user won't find easy to use and integrated into the day-to-day job, the user will give us hell and do anything and everything to compromise the security that is set in place.

Why should users circumvent our security? Not because we have malicious users (or do we?) but rather because the average user does not understand the risks. Nor should he/she. Finding solutions to problems is our job (see comment on user education below). The average user wants to work, and if security gets in the way... users will find a way around

our solutions.

Security should be implemented in such a way that a user can do his or her work as they always do and if that is not possible and security **must** take precedence then the easiest solution for the user to work with must be found.

Social engineering is another serious risk which usually doesn't get addressed very well, if only for the difficulty in trying to address it. However, I'd think we have learned something since the 1960's, apparently they had the very same problems, only with different systems (see below).

Educating users to understand the risk would in the long run save serious investment in damage control and extra security measures. As I mentioned, users want to do their jobs but I doubt that users would chose to become a security risk if things are explained to them.

I am partially contradicting myself. Should or shouldn't user education be implemented? Absolutely, yes. Should we rely solely on education? No! But education or not, if we work against the user we'd lose every time.

A third issue I'd like to discuss is learning and implementing conclusions. Nowadays we are facing security issues on our cell phones and printers, 5 years ago it was the beginning of the real problems with the Internet and 10 years ago it was the Personal Computer and the BBS's (I can't sign on the exact years, but you get my drift).

Security issues follow us around to whatever systems we use, and it always seems like we run around putting out fires rather than build systems secure from the get-go (naturally, I'm generalizing, not everybody goes "live the moment" with security. Generalizing is wrong but I think you see where I am going with this).

Not everybody implements security planning and procedures. As a matter of fact, most don't. Those who try many times face immense bureaucratic barriers as well as budget and time-frame issues that have to be dealt with and taken into consideration.

The very basics of security [such as choosing a good password] are still the biggest issues we have to deal with as security professionals.

Although this was discussed before, here is a paper which recently hit

/.: <http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf>.

Side note: how many of us use the same passwords for many different applications?

Here is a very recent /. story about a widely known "password" used in

nuclear silos in the 1960's (00000000):

<http://www.cdi.org/blair/permissive-action-links.cfm>

("1, 2, 3, 4, 5? That's the exact same combination on my luggage!")

To make a long e-mail short, I believe the very basics, while not being ignored, are not given enough attention thus leading to very serious security issues and incidents.

Also, to state the obvious even if only for the simple reason it

keeps
being over-looked; as long as we do not plan our future services
and
projects with security in mind (not to mentions learning from
lessons in
history), we are doomed to keep repeating our mistakes.

Oh. And educate users and try to find solutions they'd find easy
to use.
Nearly forgot that one after my overzealousness.

🔥 Detectives follow the money trail to tackle spam

<"NewsScan" <newsscan@newsscan.com>>
Tue, 01 Jun 2004 11:10:11 -0700

It seems like spammers have been working overtime since the
federal antispam
legislation took effect Jan.1, and the government is now turning
away from
technical fixes offered by software engineers in favor of private
investigators' expertise to boost their efforts to stem the
deluge of
unsolicited e-mail. In an unusual arrangement, the Direct
Marketing
Association has paid \$500,000 to hire 15 investigators to work
alongside the
FBI agents and other government officials in a program known as
Project
Slam-Spam. The project has built a case against 50 spammers,
mostly by
following the money trail and relying on informants. "Spammers
are more than
willing to rat each other out," says Microsoft investigator
Sterling
McBride. "The most useful information is who pays for various
aspects of the
spam operation," says attorney David Bateman, who represents
Microsoft in

spam cases. "To spam, you need four or five things -- a hosting service, a domain name, mailing software, mailing lists and so on. Each one you have to purchase from someone." Microsoft has filed 53 civil cases against spammers in the last 15 months, based on the work of its investigation team. "The real key is trying to figure out how to connect the virtual world" with "someone you can hold responsible for this," says McBride. Once you've nailed that down, "you can use all the tools of a normal investigation."

[*The New York Times*, 31 May 2004; NewsScan Daily, 1 June 2004]
<http://www.nytimes.com/2004/05/31/technology/31spam.html>

✶ Are passwords passe'?

<"NewsScan" <newsscan@newsscan.com>>
Tue, 01 Jun 2004 11:10:11 -0700

Scandinavian countries are at the forefront of a movement to ditch conventional passwords in favor of so-called two-factor authentication. These "password-plus" systems use things like disposable cards with scratch-off codes in conjunction with the usual four-digit PIN for online banking and other secure transactions. Each code is used once, and the bank replenishes the supply by sending a new card when the customer is running low. "A password is a construct of the past that has run out of steam," says Identix CEO Joseph Atick. "The human mind-set is not used to dealing with so

many different passwords and so many different PINs." Other "password-plus" options include Vasco Data Security International's pocket-sized device that issues a random second code each time you type your regular password in. Or MasterCard International's system, which requires swiping your "smart" credit card through a special reader and entering your PIN to obtain a single-use password good at Office Max, British Airways and a dozen other merchants. And while U.S. banks are well aware of the perils of password theft, they're "all afraid of making the first step," says a Gartner analyst. "They don't want consumers going to other banks because it's too hard." [AP/*The Washington Post*. 1 Jun 2004; NewsScan Daily, 1 June 2004]

<http://www.washingtonpost.com/wp-dyn/articles/A5693-2004Jun1.html>

RE: Boa triggers blackout in Honduras (Luntzel, [RISKS-23.39](#))

<"Barone, Ralph" <Ralph.Barone@bchydro.bc.ca>>
Mon, 31 May 2004 09:33:30 -0700

Of course, the humourous aspect of this is that the "Ads by Google" section below the article contains three advertisements for feather boas. Ad selection by algorithm has a way to go yet...

[So have automatic pun detectors and pun generators! PGN]

⚡ The lighter side of electronic voting (Miller, [RISKS-23.39](#))

<"Marcus L. Rowland" <forgottenfutures@ntlworld.com>>

Fri, 28 May 2004 20:58:59 +0100

> forgetting to check the capacity of the electrical
infrastructure is
> exactly the kind of bird-brained planning failure that would
surprise no
> one on RISKS.

The number of outlet sockets isn't necessarily an indication of capacity.

I work as a technician in a London school. Two weeks ago we ran our AS level physics practical exam; it's an important qualification, one of the last exams before university.

One of the questions called for the use of boiling water, and suggested providing one kettle between two students doing the experiment. We had twelve students and it was one of two experiments, so at any given time six students would need hot water. So we followed their advice and provided three kettles.

We then found, as the exam started, that if all three were switched on simultaneously the main breaker for the lab blew. Repeatedly. Somehow a lab with 60+ 13A mains sockets had all of its electricity connected to one 16A circuit breaker, and couldn't take three 10A kettles. In fact three out of four labs on that floor are like that, the smallest of the four has a 32A breaker. Amazingly none of these labs has ever tripped a main

breaker
before.

In the end we ran extension cables in from the corridor and the adjoining lab and gave the students a few extra minutes. Our report to the examiners will make interesting reading.

Marcus L. Rowland

<http://www.forgottenfutures.com/>

LJ:ffutures

<http://homepage.ntlworld.com/forgottenfutures/>

[Re: New GAO Report on Government Data Mining \(Steinhardt, R-23.39\)](#)

<"Robert I. Eachus" <rieachus@comcast.net>>

Sat, 29 May 2004 14:09:06 -0400

If these are worrisome to the ACLU, my reaction is to say go away and stop bothering me. Let's turn the scare quotes around, and see what the purpose of these programs is.

Verity K2 Enterprise seems to be reorganizing information on foreign terrorism activities so that it can by looking up the name of one of the individuals involved. Yes, there is a potential for abuse where individuals share the same name, but at the same time it can also be used to exculpate such individuals. If your namesake was in Botswana in February, and you were in Cedar Rapids, then either the investigator or your lawyer should twig to the fact that there are two individuals involved.

Incidentally, in today's environment, it is a very good idea to "Google" yourself occasionally to find out what your namesakes are up to. As a case in point, one of my friends found a parole violation by a murderer in Alabama of the same first and last name, but much younger...

Analyst Notebook I2, "Correlates events and people to specific information."

This seems to be the reverse of the above. If a suspect was in Botswana in February were there events of interest such as terrorist meetings that he might have been involved in? Again, yes, subject to misuse, but the purpose is clearly not prosecutorial, but alert analysts to POTENTIAL correlations, when an individual is a suspect for other reasons.

PATHFINDER: This is clearly a metadata tool. Its purpose is to help understand the structure and data dictionary of existing databases. Here I probably need to preach a bit as well. There is an issue in some people's minds that government access to sophisticated computer resources could have serious adverse consequences. However, there are lots of public resources available to me as a person, such as on-line databases, and data searching tools such as Google. To say that citizens can use these resources, but to try to prevent the government from using the same resources is ridiculous.

What does make sense is to limit or restrict the government's ability to use its powers to collect data which individuals would prefer to keep private. Or when such data is needed by a government, to restrict sharing of the data

to its original purpose.

If this tool were being used to say, integrate state driver's license databases, that would be one thing. But given the agency involved (the Defense Intelligence Agency) I have to believe that the intent is to integrate public (and possibly non-public) data on weapon systems, and who currently owns them.

Case Management Data Mart - DHS. "Assists in managing law enforcement cases"
Sounds scary taken out of context, but legal proceedings today can get very complex, in part due to privacy laws. If you do have privacy concerns, you do want the government to do a good job of tracking data involved in a case, especially otherwise private data that was revealed in response to a subpoena. Again, the risk is not in having tools to manage the data, but when the government or others does a bad job of managing it.

Realize that part of the job of managing data is to ensure that all copies are destroyed when that is appropriate. And no, I am not talking about white collar crimes here. For example, if the government subpoenas your bank or phone records, wouldn't you rather that all of the copies they made were destroyed when the case was closed? If really necessary, the originals can be subpoenaed again.

🔥 Data Mining: Federal Efforts Cover a Wide Range of Uses

<Monty Solomon <monty@roscom.com>>

Tue, 1 Jun 2004 11:11:51 -0400

Excerpt from Recent GAO Reports and Testimony

Data Mining: Federal Efforts Cover a Wide Range of Uses. GAO-04-548, 4 May.

<http://www.gao.gov/cgi-bin/getrpt?GAO-04-548>

Highlights - <http://www.gao.gov/highlights/d04548high.pdf>

Both the government and the private sector are increasingly using "data mining" -- that is, the application of database technology and techniques (such as statistical analysis and modeling) to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results. As has been widely reported, many federal data mining efforts involve the use of personal information that is mined from databases maintained by public as well as private sector organizations. GAO was asked to survey data mining systems and activities in federal agencies. Specifically, GAO was asked to identify planned and operational federal data mining efforts and describe their characteristics.

Federal agencies are using data mining for a variety of purposes, ranging from improving service or performance to analyzing and detecting terrorist patterns and activities. Our survey of 128 federal departments and agencies on their use of data mining shows that 52 agencies are using or are planning to use data mining. These departments and agencies reported 199 data mining efforts, of which 68 are planned and 131 are operational. Of the most common

uses, the Department of Defense reported the largest number of efforts aimed at improving service or performance, managing human resources, and analyzing intelligence and detecting terrorist activities. The Department of Education reported the largest number of efforts aimed at detecting fraud, waste, and abuse. The National Aeronautics and Space Administration reported the largest number of efforts aimed at analyzing scientific and research information. For detecting criminal activities or patterns, however, efforts are spread relatively evenly among the agencies that reported having such efforts. In addition, out of all 199 data mining efforts identified, 122 used personal information. For these efforts, the primary purposes were improving service or performance; detecting fraud, waste, and abuse; analyzing scientific and research information; managing human resources; detecting criminal activities or patterns; and analyzing intelligence and detecting terrorist activities. Agencies also identified efforts to mine data from the private sector and data from other federal agencies, both of which could include personal information. Of 54 efforts to mine data from the private sector (such as credit reports or credit card transactions), 36 involve personal information. Of 77 efforts to mine data from other federal agencies, 46 involve personal information (including student loan application data, bank account numbers, credit card information, and taxpayer identification numbers).

<http://www.gao.gov/new.items/d04548.pdf>

⚡ Daft security questions

<Ian Chard <ian@chard.org>>

Wed, 02 Jun 2004 16:18:10 +0100

I recently registered with (yet another) online banking service, and it seems that the quest for 'secure' authentication challenges is generating some very odd decisions.

As part of the registration process, as is commonplace these days, I had to think of an answer to four security questions, and was instructed only to give answers that would be known to me and 'not, for example, to a member of your family'. The questions were:

- Memorable place?
- Memorable date?
- Memorable name?

These three 'memorables' are difficult to answer with things that aren't memorable to anyone else I might know. The first thing that occurred to me is "birthplace, mother's date of birth, mother's maiden name", i.e. questions that other institutions commonly ask. I'm sure that plenty of people would assume that was what was wanted.

- Favourite singer?

This is fatally flawed as (a) there are lots of singers I like, (b) everyone knows my tastes in music, and worst of all (c) they change over time. You

might as well ask 'what did you have for breakfast this morning?'

- Secret question / answer? (for password resets)

I'm not a secretive kind of guy, and with the 20 character limit on the question I just had to give an arbitrary answer, hoping that I'd never forget any of this other stuff.

The risk here is that, in an attempt to make the sign-in process more secure, this institution has made it all but impossible to provide secure responses. The only other forms of authentication used at sign-in are the username and password, making all of this messing about with 'memorable' responses a bit pointless. Ironically, the only opportunity the user has to set something **really** secure (the secret question and answer) is wasted, as this isn't used by the sign-in process. Asking the user to set several question/answer pairs would need more thought on his part, but ultimately it would be far more secure.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 41

Thursday 3 June 2004

Contents

- [Computer breakdown in England affects air traffic](#)
[Debora Weber-Wulff](#)
 - [Privacy and Security Risks in Rampell's E-Mail Surveillance Service](#)
[Lauren Weinstein](#)
 - [France Telecom voice mail espionage](#)
[David F. Gallagher](#)
 - [USB risks](#)
[Gadi Evron](#)
 - [Whom do I tell?](#)
[Jerry James](#)
 - [An anatomy of a PGP Joe Job](#)
[Gadi Evron](#)
 - [Netgear/UWisc NTP mess](#)
[Hal Murray](#)
 - [Selling Web bugs](#)
[Neil Youngman](#)
 - [Re: Spam being rapidly outpaced by 'spim'](#)
[Gadi Evron](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Computer breakdown in England affects air traffic

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

Thu, 03 Jun 2004 18:43:42 +0200

tagesschau.de has an in-depth update on the software failure at http://www.tagesschau.de/aktuell/meldungen/0,1185,OID3328786_REF1_NAVSPM1,00.html

(in German), here my synopsis/translation:

NATS (National Air Traffic Control Service) was supposed to move from West Drayton to Swanwick near Heathrow in 1996 and 1997 with a completely modernized technology for air traffic control. The system cost 623 million Pounds Sterling (940 million Euros) and was not delivered by Lockheed Martin until 2002. It will take until 2007 for the move to be completed.

Four months after the system was initiated, there was a large breakdown in May 2002 that caused an air traffic outage over England. "Experts" decided that the problem was the technical communication between the ancient computers in West Drayton and the new ones at Swanwick.

The current misfortune is attributed to an attempt on the night of 2 Jun 2004 to update the system. The update did not work, and the mainframe could not be restarted. Two hours were needed to get the backup system functional. In the course of the day, it was disclosed that the computer in question is 30 years old. [actually, sometimes I trust older systems more than I do these modern WinTel boxes... -dww]

The update that was to have been installed was ordered after an incident in Jan 2004 in which there was almost an in-air collision in British airspace. The air traffic controller had told two large passenger machines to move apart. The data came into the system reversed, so that the machines actually moved closer to each other. The error was recognized in time by pilots and by the air traffic controller.

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Treskowallee 8, 10313 Berlin
Tel: +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

✶ Privacy and Security Risks in Rampell's E-Mail Surveillance Service

<Lauren Weinstein <lauren@vortex.com>>
Thu, 27 May 2004 13:00:00 PDT

PRIVACY Forum Digest Friday, 28 May 2004 Volume 13 : Issue 03
(<http://www.vortex.com/privacy/priv.13.03>)

Greetings. There's been a lot of publicity over the last few days about Rampell Software's DidTheyReadIt.com service. There have been other software tracking systems introduced before, but this one, by including features that attempt to determine how long a message is kept open (as well as whether it was received, who you forwarded it to, etc.) is worthy of particular disdain and concern.

There's more than just basic privacy issues involved. Many individuals, businesses, and particularly government entities may have serious security issues regarding capabilities that can expose information about when a particular person has read a message, and perhaps potentially even if they are still actually sitting there reading the message right now. The possible dangers are fairly obvious -- knowledge of the hours a person works, when they tend to be in their office, etc. can be easily abused in sensitive environments.

Some of these features not only depend upon invisible image "Web bugs" used in a "conventionally invasive" manner, but also reportedly feed a slow stream of data to your system during the entire interval you're reading a message (that's how their "how long were you reading the message" function apparently operates).

Luckily, there are several ways to protect yourself not only from Rampell and their customers but also from other mail tracking services:

- Use a text-based e-mail reader, not an html mail reader, for most mail.

Do you really need to see all the fonts and associated frills in most

e-mail? What kind of mail is most likely to be full of such stuff?

Spam of course! When you need to display image or document attachments

they can still be processed externally. Text-based e-mail systems also

can provide essentially complete protection against all virus, worm, and

related attacks that use e-mail as their vectors. I use a

text-based

e-mail system for 99.9% of all my mail quite successfully.
And I get a
lot of e-mail.

- Turn off image display in your html mail reader. E-mail tracking systems that claim to work regardless of where mail is sent typically depend upon the recipient retrieving images (often invisible images) from central servers. One way to stop that process is of course to read your e-mail offline, though that isn't practical for most of us. But various html mail reading systems allow you to turn off image display (and typically retrieval as well) for e-mail messages (you can turn it back on when you really need it for particular items). If you don't retrieve the images or Web bugs, e-mail tracking systems that need them won't work. And of course, you should never allow javascript in e-mail messages to be processed, nor allow attachments to be executed.

- Server blocking. System administrators and others may choose to determine (from viewing e-mail raw source data) the names and/or IP numbers related to the servers used by Rampell or others to serve the tracking images. If these servers are blocked at firewalls or other filters the tracking systems will be rendered impotent.

Until legislation and the legal system recognize the risks in such e-mail tracking and provide appropriate restrictions and remedies, you need to protect yourself.

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

✶ France Telecom voice mail espionage

<"David F. Gallagher" <<http://lightningfield.com>>>

Sun, 30 May 2004 13:15:21 -0700 (PDT)

France Telecom, by far the largest phone company in France, offers its customers a free voice mail service called Top Message. Users of the service can sign up to receive an e-mail letting them know when they have new voice mail -- useful for people with dial-up Internet connections. You activate this feature by sending an e-mail to a designated address with your phone number in the subject line.

I've found that France Telecom makes no apparent effort to determine whether a particular person has the right to be receiving these alerts, which include the phone number of the caller and the time they called. I was able to activate alerts for the phone in my apartment in Paris even though the phone bills are in the name of a previous tenant. It also worked when I used the phone number of some friends here who also use the voice mail service. The online instructions for the service say you're supposed to receive confirmation by voice mail and e-mail when the alert

service is
activated. When I signed up I found that this was not the case
-- the alerts
just started arriving.

There are no doubt thousands of jealous ex-lovers in France who
would love
to know who has been leaving voice mail for the objects of their
obsession. Perhaps France Telecom should start charging stalkers
for this
service? (Following through on the promise to notify users when
the alerts
are turned on would provide a minimal level of protection
against this
potential creepiness.)

Top Message online help (in French):

[http://www.agence.francetelecom.com/vfrance/esav/fixe/pages/
services/3103/etre_averti_du_depot.shtml#3](http://www.agence.francetelecom.com/vfrance/esav/fixe/pages/services/3103/etre_averti_du_depot.shtml#3)

USB risks

<Gadi Evron <ge@linuxbox.org>>

Tue, 01 Jun 2004 17:24:30 +0200

I got the idea of writing about this from a recent pen-test
mailing list
thread I replied to.

In that thread, someone asked about the risks of using USB. The
guy
described how he plugged in a USB device and was surprised to
see it
auto-run. He was particularly worried about the potential theft
of
information that can be caused by the malicious usage of USB
devices.

Indeed.

This has been covered and demonstrated on several occasions, on TV shows (Threat Matrix), Sci-Fi TV shows (Jake 2.0) and in actual real security discussions. I believe this was brought up before in both Slashdot and Full-Disclosure, but only with actual solutions. I haven't personally seen anyone discuss the risks.

Disabling auto-run might not be the solution for USB (although that is always a good idea when hardening a Windows system). USB auto-run installs a driver for itself on plug-in. A driver which is essential for the device to operate. Auto-run on CD drives for example is not necessary, one can always access the CD and execute whatever program is there (or even the auto-run), manually.

On USB, there are a few concerns when it comes to drivers. The driver can be:

1. Messed with, i.e. made to do things it shouldn't (Reverse Engineering, manipulation).
2. Built from scratch with one of **many** SDK's out there.

USB brings the threat of any user, maid, cleaner or hostile "whoever" to plug it in, covertly gather whatever information/perform whatever action they wish, and leave. They might not even have to be covert about their actions as USB devices are more than legitimate in many organizations and aside to not being notices for using a USB device one could alter the driver for any USB device they usually use.

This brings up the issue of what hardware should be allowed in an organization and whether users can bring their home hardware to work, but that is beyond the scope of this write-up.

USB technology is both fast and convenient. More and more computer services and devices move to work over USB as a fast-growing trend. It has been this way for several years, and the technology usage is still showing signs of growth.

I feel threatened enough by the fact that such small devices with such a huge data capacity exist and can be smuggled into a building in so many ways, automatic operations done "on-plug-in" or "on-connect" are just a plus. You don't really need many tools other than copy, but I suppose tools can be created.

There are many ways in which the exploitation of this technology can progress, from simply connecting a USB drive and copying information as I've mentioned above, through PDA's which would allow you to chose what you want to steal and map the network, all the way to wireless devices which can be remotely controlled by a laptop or through, say, a cellular device, whether temporary for the sake of one illegal operation, or permanently, providing an hidden backdoor to a network.

Disabling USB all-together, virtually, by domain policy or removing the USB devices themselves, maybe even just filling the plugs with silicon or glue physically are some more drastic options which some organizations *might*

take, but I don't see it as a very viable option for most.

As always when it comes to security, it all depends on your risk analysis.

Cost vs. benefit. Is it worth it?

Do you have an opponent that could threaten you in this way? Do you have anything to hide and how much do you care about hiding it?

There exist several tools to monitor a domain for when and if a USB device is connected to any remote machine, and of what kind. A simple web search should help you find some examples.

I suppose simple tools could be easily created, but as there are several commercial options it might be worth a look.

The security risks of USB are more than this short email can convey, but I think I gave you enough to get started and to think about. This issue is of paramount importance and I don't see much *noise* about it.

Thoughts, anyone?

ge@linuxbox.org gadie@cbs.gov.il +972-50-428610 (Cell).

⚡ Whom do I tell?

<Jerry James <james@eecs.ku.edu>>

Tue, 01 Jun 2004 15:08:15 -0500

I've had two telephone annoyances over the past year that are RISKS related.

First, a major home improvement chain came to town about a year ago. While the store was still under construction, I started receiving telephone calls at my home number, with the caller asking for this particular store. Upon questioning the callers, I found that someone in the construction trailer was giving out my number. I called up the construction trailer and had a "Did, too!", "Did not!" type of conversation with the person who answered. Even after construction finished, the calls continued. Now the callers claimed to be getting my telephone number from the store's web site. I confirmed this. The telephone book shows that the first 5 digits of the correct number are the same as mine. The last two digits are completely different. This is not a case of transposition or accidentally repeated digits. Someone got the last 2 digits completely wrong. This should be easy to fix, right? I sent e-mail to the webmaster. No response. I called up the store. "We don't manage the web site. Our corporate office does that." Nobody knows how to fix the problem. A year later, I am still receiving calls for this store. I have taken to telling callers that this store is so badly managed that they can't even figure out how to fix a wrong telephone number. We'll see if that gets any action.

Second, something is amiss with my telephone company's software. I have two pieces of evidence to support this claim.

- Two or three times a week, when I dial a number I know is good, I get the message that I am calling a disconnected number. When that

happens, I

just hang up, then hit redial, and the call usually goes right through.

- I get a lot more wrong numbers than I did at my last place of residence.

When I ask the callers what number they were attempting to call, I get the

usual transpositions and repeated digits, but I also get a fair number of

answers that have no obvious connection with my telephone number. I

usually suggest to these callers that they try hitting redial, and I've

never had any of them ring back.

(Oddly enough, I don't seem to be calling wrong numbers myself, unless that is what is causing the "disconnected number" messages. But then why am I not hitting valid, but wrong, numbers as well?)

So I called the operator and told her about it. She had absolutely no idea

what to do. "Surely there is some way to report problems of this nature?" I

asked. She didn't know. She didn't even know who to ask. The telephone

book yielded no clues.

In both cases I, a member of the public, knew about a problem, tried to

report it, and found that those responsible either have no problem reporting

mechanism in place, or have successfully hid its existence from their own

employees.

Jerry James <http://people.eecs.ku.edu/~james/> james@eecs.ku.edu
jamesj@acm.org

An anatomy of a PGP Joe Job

<Gadi Evron <ge@linuxbox.org>>

Sat, 29 May 2004 09:47:51 +0200

How my PGP signature ripped off, and for what purpose

On May first I e-mailed a couple of mailing lists, announcing a new spam research related mailing list.

Due to knowing that many viruses and kiddies spoof my e-mail address on a regular bases, I signed the post.

So far I received about one e-mail a day from people who Googled the PGP signature that was in a SPAM they got (right through their filters).

That signature was my signature from the spam mailing list.

Irony? Attempted Pay-back? Oh well.

As the e-mails don't stop and as it happens with Joe Jobs, you must reply and be nice while you do it.. I decided I'd put this in a short write-up describing:

1. What happened (the story).
2. A few of my opinions on the subject.
3. A full analysis of the SPAM message. Quite interesting, although
there is nothing completely new there.

PGP is used exactly for this purpose. Even if my signature was ripped, it should be pretty obvious it wasn't made by me. Still, this is a risk (which isn't completely new either

What is new is the very targeted nature of this PGP Joe Job.

Here is the write-up that was supposed to be sent as e-mail. I figured that with all the spam elements quoted in it though - it might get caught in filters:

"An anatomy of a PGP Joe Job"

<http://www.math.org.il/PGP-JoeJob.txt>

ge@linuxbox.org gadie@cbs.gov.il +972-50-428610 (Cell).

⚡ Netgear/UWisc NTP mess

<Hal Murray <hmurray@suespammers.org>>

Mon, 10 May 2004 02:54:17 -0700

There is a category of bugs that can be summed up as (re)try too hard.

They are much more interesting when they involve positive feedback. Suppose some networking code works fine normally but an environmental problem causes retransmissions. If those retransmissions make the problem worse they will cause more retransmissions which will...

Last summer, Netgear demonstrated a spectacular example of this type of bug. I'm surprised it hasn't been covered here yet.

Dave Plonka has an excellent writeup at:

<http://www.cs.wisc.edu/~plonka/netgear-sntp/>

He has links to several media web pages at the end.

Here is a highly abridged summary:

Netgear added an NTP client to some of their routers so log

entries would have the correct time. They hardwired the IP address of the NTP server at UWisc into their code. They shipped many many thousands of those routers. The total load was too much for the NTP server and/or network at UWisc so packets started getting lost. The code had a bug. If it didn't get an answer, it retransmitted once per second. (One request per hour would be reasonable.) The UWisc network collapsed on May 14th, 2003. In early June, they were discarding 250K packets/second, 150 megabits of NTP traffic! That's an impressive load for such a simple protocol.

A similar bug in SMC routers knocked the NTP server at CSIRO (Australia) off the net.

<http://mailman.anu.edu.au/pipermail/link/2003-April/049684.html>

I know of a few other examples of try-too-hard bugs:

Consider a UDP request/response protocol running over a slow phone line. Suppose that requests are tiny, the response takes a 1/2 second on the phone line, and the retransmit timer is 1 second. If there is no other traffic, things work cleanly. Suppose some other traffic causes an additional 1/2 second of delay. The retransmit timer goes off and that puts a second copy of the response in the queue. The client will continue when it receives the first (delayed) response. If the client generates more work for the server, that response will be delayed by the retransmission that is still in progress. A little more shared traffic can cause things to snowball. Note that once a few retransmissions are in the pipeline the system

doesn't need

any more outside traffic to cause troubles. It's own queued up retransmissions will keep causing more retransmissions.

That's just a simple example of a retransmit/retry timer being set too

short. Variations involve the server having to do a lot of work and not

being smart enough to cache the answer.

The next two examples don't involve any positive feedback.

Consider the typical client-server setup that uses several servers for

reliability. What happens if a particular data pattern issued by a client

finds a software bug that crashes a server? If the client retries again

using another server, that one will crash too. If the client keeps retrying

it can kill all of the servers - embarrassing if you thought you were

building a reliable system.

When forwarding mail, some servers retry right-away on a temporary error.

That turns into a denial-of-service attack if the receiving server returns a

temporary error. Anti-spam defenses sometimes return temporary errors

because that gives the operator of a mis-configured server a chance to fix

things without any bounced mail.

RISKS related issues:

* Why didn't Netgear learn from the SMC/CSIRO event? Why didn't that event get more publicity? (I can't find any reference in RISKS.)

* If you are outsourcing work or hiring contractors/consultants, how can you tell if they are good enough to avoid problems like this? How

would you
write a contract to avoid bugs like this? Is requiring "good
engineering
practices" good enough?

* Could you explain this issue to your management? What would
they do if
this bug was discovered when the product was about to ship? How
much would
it cost your company to recover from a bug like this? (Looks to
me like
Netgear got off lightly on the bad-PR area.)

* Should specifications mention this problem? Or would that
just be clutter
and distract from the main purpose of the spec? Note that
"specifications"
includes RFCs, product specifications, and contracts. Does the
answer
change if the protocol/product is widely deployed, or likely to
be widely
deployed?

* How do you update implementations out in the field when
problems like this
are discovered? You can't even contact most of the owners
because people
don't fill out product registration cards. (Probably because
they get too
much junk mail when they do.) In this case, the ISPs should know
which of
their customers are using these routers. Even if you could
contact the
owners, would they bother to update their firmware? They don't
see the
symptoms of any problem.

* How can we uncover bugs like this? The Netgear bug is
somewhere between
very hard and impossible to find by traditional testing. The
lab gear
required is too extensive/expensive. You could probably provoke
it in a

lab, if you already knew about it so you could build an artificial environment that would be more sensitive. Would that type of testing be cost effective? (Or should that testing effort be devoted to other areas?)

* How can schools teach students about this type of problem? Is repeating this war story in a lecture good enough for somebody to get it? Where should this come on the priorities? [I hope this event becomes required reading for a CS degree, but I'm a network geek.]

* Hardwiring some parameters is asking for troubles. How can we recognize (and teach) which parameters are OK to hardwire and which ones require configuration? Is there a middle ground where a parameter has a sensible default as long as configuration is possible?

* What responsibility do corporations have to the Internet community as a whole? How can we encourage them to do the right thing when it costs a little more? Corporations includes hardware manufacturers, software vendors, ISPs/ASPs, web site operators... (Maybe we should include home users too, but I think it makes sense for their ISP to be responsible for their actions.) For example, why didn't somebody at Netgear do the back-of-envelope calculations and figure out how many routers their customers (ISPs) could install before they should install NTP servers too?

* ISPs should be running time servers for their customers rather than freeloading off the net.

The suespammers.org mail server is located in California. So are all my other mailboxes. Please do not send unsolicited bulk e-mail or unsolicited commercial e-mail to my suespammers.org address or any of my other addresses. These are my opinions, not necessarily my employer's. I hate spam.

✈ Selling Web bugs

<Neil Youngman <n.youngman@ntlworld.com>>

Fri, 28 May 2004 20:27:33 +0100

The latest LWN security section (<http://lwn.net/Articles/86022/>) discusses a service called DidTheyReadIt.com. In short, the service adds web bugs to e-mail to try to determine whether the e-mail has been read.

(NOTE: that link is currently subscription only. It will probably become freely available when the next edition is published on Thursday. Ed Felten also comments at <http://www.freedom-to-tinker.com/archives/000607.html>)

To me the key excerpt is

"This, of course, has some not-so-pleasant implications for personal privacy. While the company assures its potential customers that it respects their privacy, nothing is said about the privacy of the recipient who may not wish to divulge whether or not they've read a particular e-mail or

where they've read it from. On the company's About Us page, they identify what kinds of people might want to find out whether an e-mail has been read -- including some that make DidTheyReadIt sound like a must-have for potential stalkers:

Users of online dating services such as match.com who want to know if their potential dates are reading their messages...or ignoring them."

The articles do a good job of identifying the RISKS.

⚡ Re: Spam being rapidly outpaced by 'spim' ([RISKS-23.39](#))

<Gadi Evron <ge@linuxbox.org>>

Fri, 28 May 2004 00:30:07 +0200

"Spim" is nothing new, but it is indeed a growing concern.

In recent years we have seen more and more security issues that we've encountered before repeat themselves on different mediums and technologies. Spam is no different.

In this case, though, it is much simpler. As asked by many people in the past: Would you stay with a service that you get 40 SMS spam messages every day with?

No. You'd switch a provider.

I am much more concerned with other security issues regarding cell phones, which are rapidly changing from privacy and eavesdropping concerns to Trojan

horses and buffer overflows. That is an issue to be discussed in a different post, though.

As to spam, there is no danger of it disappearing. In fact MessageLabs came out with some interesting statistics this week saying that 70% of all e-mail is spam:

<http://news.bbc.co.uk/1/hi/technology/3746023.stm>.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 42

Saturday 19 June 2004

Contents

- [Whose Data Is It, Anyway?](#)
[Matt Silberstein](#)
- [E-mail needs a makeover](#)
[NewsScan](#)
- [India's outsourcing business in trouble](#)
[NewsScan](#)
- [Autorun considered evil](#)
[Peter da Silva](#)
- [Stuck between the 2G and 3G networks](#)
[Henry Skoglund](#)
- [Verity K2 is data mining?](#)
[Aahz](#)
- [HTML Mail-readers](#)
[Mike Albaugh](#)
- [Re: Risks of believing in testing](#)
[David Crocker](#) [Peter B. Ladkin](#) [Fred Cohen](#)
- [Re: Daft security questions](#)
[Brian Reynolds](#) [Lou Katz](#) [Antonomasia](#)
- [British ATC slowdown](#)
[Peter B. Ladkin](#)

 [Info on RISKS \(comp.risks\)](http://comp.risks)

Whose Data Is It, Anyway?

<Matt Silberstein <matts2@ix.netcom.com>>

Thu, 3 Jun 2004 14:13:19 -0400 (GMT-04:00)

Encrypt your data and deprive you beneficiaries. *The New York Times* has an interesting article on password protection on a deceased person's computer. What will happen when biometrics become prevalent?

"When Tomm Purnell's uncle, Keith Cochran, died last year, Mr. Purnell's mother received two of Mr. Cochran's computers. One of them, a laptop, is password-protected, and even though Mr. Purnell considers himself somewhat of a computer geek, "the really obvious passwords," he said, like the names of Mr. Cochran's cats and combinations of his Social Security number, have failed."

<http://www.nytimes.com/2004/06/03/technology/circuits/03data.html?8dpc>

For an additional risk further on we get this gem:

"Mr. Purnell said that some of his uncle's files are gone forever. Mr. Cochran stored digital photos on two computers that used the Linux operating system. The machines were given to his brothers, "who are Windows guys, so they erased and reformatted them," Mr. Purnell said."

A little knowledge is a terrible thing.

✈ E-mail needs a makeover

<"NewsScan" <newsscan@newsscan.com>>

Thu, 03 Jun 2004 08:41:40 -0700

Forget about spam -- even your "wanted" e-mail is clogging your in-box now, right? E-mail is "broken," says Eric Hahn, former CTO of Netscape and current CEO of antispam firm Proofpoint. "We need to make metaphoric changes. The [file-folder] metaphor was designed back when we were talking about getting five messages a day." Today, many folks receive 10 to 20 times that number and filing each one just takes too much time. "People hate filing. They hate it in paper. They hate it in e-mail. Could you imagine what it would be like to have to file Web pages just to get back to them?" Hahn suggests that in addition to overhauling the filing function, software developers should find a way to combine instant-messaging software with e-mail software. "Doesn't it seem odd that IM is separate from e-mail? Why are those conversations so fundamentally different?" he asks. Ben Gross, a researcher at the University of Illinois-Urbana-Champaign, says that in addition to incorporating IM, e-mail software developers need to integrate RSS readers into their products, so that users can view updates to a Web page without having to download the whole Web page into a browser. Some e-mail software developers are already experimenting with new

approaches:

Microsoft's Outlook 2003 and Google's Gmail service include a "group by conversation" feature that enables users to view related e-mails sent to and from a single person. [Wired.com 3 Jun 2004; NewsScan Daily, 3 June 2004]

<http://www.wired.com/news/technology/0,1282,63692,00.html>

India's outsourcing business in trouble

<"NewsScan" <newsscan@newsscan.com>>

Tue, 15 Jun 2004 07:47:39 -0700

High labor attrition, poor infrastructure, and lack of data protection laws could derail India's booming outsourcing industry, says Nandan Nilekani, the CEO of Indian software giant Infosys Technologies. Noting that business process outsourcing (BPO) is based on reputation, Nilekani has urged the industry to deliver quality work: "Every year, about 70,000 jobs are added and the main challenge is how to attract people. The challenge is also how to retain the pool. It's a collective challenge. We require a holistic approach to expand the pool and train people. The question here is how to retain the manpower to deliver quality and value." Analysts say outsourcing labor attrition rates vary 20-40% in some companies while at top firms it averages at least 15%. [*The Age*, 11 Jun 2004; NewsScan Daily, 15 June 2004]

<http://theage.com.au/articles/2004/06/10/1086749833478.html>

✶ **Autorun considered evil (Re: Evron, [RISKS-23.41](#))**

<Peter da Silva <peter@abbnm.com>>

Thu, 3 Jun 2004 16:58:28 -0500 (CDT)

Any device that requires an operating system to load and install a custom driver on its say-so without verification or even alerting the user SHOULD be disabled and tossed on the garbage-heap of history.

Autorun must not be the default behaviour for any hot-pluggable device, media, class of devices, downloaded content, anything, anywhere. If there is some hardware design specification that requires it, that design should be abandoned immediately, and any device that requires it considered obsolete.

Who thought this was a good idea, and why weren't they on their meds?

This is of course a much bigger issue than USB. Apple's Internet-enabled disk images, Microsoft's plethora of "active content" mechanisms, anyone's autorun media... anything that isn't specifically requested by someone who has verified authority for it (a locally logged in user, a network administrator, ...) that can't be run in a failsafe sandbox must not be run at all.

✶ **Stuck between the 2G and 3G networks**

<"Henry Skoglund" <henry@tungware.com>>

Thu, 3 Jun 2004 23:40:46 +0200

In May this year I purchased the new SonyEricsson Z1010 mobile phone here in Sweden, and after replacing my old SIMcard for a new one, I can make videocalls with it as well. Provided you're in an area covered by the 3G network, of course. Turns out my particular residential area (Bromma, a suburb of Stockholm) has only a spotty coverage at best, if I venture outdoors I might obtain a 3G-network connection, but indoors all bets are off.

The problem is that my Z1010 phone is optimistic and switches to the 3G-network ("Sweden 3G") at every opportunity it gets. And, in theory, should gracefully revert back to my old 2G provider ("Telia") when outside 3G coverage.

But what happens instead is that, every time I return home from the city, the telephone having merrily been connected to a good 3G-network all day, finds itself in a non3G area and grudgingly switches back to Telia. But wait, there is a faint 3G signal, let's switch back to that network. But no, we lost it... Yes, you might guess what's happening, the phone gets confused, instead of a connection the display reads "Only SOS calls available". And people calling me end up at my answering service.

If I then succeed in bringing the phone back online and dial my

own mobile
number (this is a good old GSM network test, BTW), I mostly end
up at my
answering service. No busy signal. Time to go down into the
basement
(luckily out of 3G-reach) and reboot the phone there to get it
properly
online.

When I called Telia customer service the other day to complain,
a helpful
person told me that to fix this, I needed to upgrade the
software in the
phone. Because the current software has some early version
bugs, it turns
out (!).

The risk here? This stuff has obviously only been tested in a
lab, where the
3G-transmitter is either on or off. My home, barely in 3G-
coverage, was
obviously not in the specifications...

P.S. Otherwise I like my new phone, I've downloaded some of my
DV-camcorder
videos into it, makes a good show at the pub.

✶ Verity K2 is data mining?

<Aahz <aahz@pythoncraft.com>>
Thu, 3 Jun 2004 16:39:59 -0400

In [RISKS-23.39](#), Barry Steinhardt refers to a GAO report about
government use
of data mining that mentions Verity K2 Enterprise as one of the
programs. I
wonder what definition is being used for "data mining" that
covers Verity?

I ask this as someone who first used Verity software in 1990 and worked for Verity from 1994 to 1997; judging by what I see on Verity's Web site today, the technology hasn't changed much.

Fundamentally, the Verity technology that's being used here is precisely equivalent to Google's News Alerts: you specify a search that gets run against a series of documents. When a document matches, you get some kind of feedback. The only difference is that Verity's query language is enormously more powerful and flexible than Google's, with more operators and the ability to weight sub-queries with different strengths. (It's fairly common in heavy-duty Verity queries to end up with queries that have more than fifty terms and operators.)

Obviously, Verity technology can add a lot of value to a data mining operation by pre-categorizing data very precisely. But I'm concerned that labeling Verity as data mining software could lead to focusing in the wrong direction, similar to the way it's important to differentiate between viruses, trojan horses, and worms.

Aahz (aahz@pythoncraft.com) <http://www.pythoncraft.com/>

✶ HTML Mail-readers (Weinstein, [RISKS-23.41](#))

<albaugh@spies.com>

Thu, 3 Jun 2004 13:59:03 -0700 (PDT)

Lauren Weinstein makes the reasonable suggestion:

> Use a text-based e-mail reader, not an html mail reader, for most mail.

If one does, and also periodically samples the Spam-bucket, one will see that many spams (especially the fake mailer-daemon ones) start out by chiding the reader to switch to an HTML mail-reader. If the social engineering has been done correctly, the user will do just that, to get the promised benefit (e.g. error notification).

The risks of trusting a burglar to recommend a lock seem obvious to me, but apparently are not.

Another suggestion, to turn off javascript, is similarly a good idea, but runs afoul of some widely used software (Outlook Web Agent, Oracle Workflow, ...) that `_require_` javascript to function. Oracle at least snarks at you about it. OWA simply silently fails to work.

RISKS: Your boss (or IT) may require you to compromise the security of your system, even if it's the company's network being put at risk.

✶ Re: Risks of believing in testing (Cheng, [RISKS-23.40](#))

<"David Crocker" <dcrocker@eschertech.com>>

Fri, 4 Jun 2004 08:05:18 +0100

Spencer Cheng wrote:

<< I have looked long and hard at proof of correctness in a previous job but other than safety critical systems, the cost is difficult to justify.

That may be true of some techniques, but not all. We routinely generate proof of correctness, even for non-critical software. The keys to making proof of correctness practical are:

1. Use a notation that is designed to facilitate proof of correctness. This unfortunately rules out most standard programming languages. Better results are obtained by using languages designed for expressing the software specification and some of the implementation details. The full implementation can be generated in a conventional programming language (we use C++) by a code generator.
2. Use automated reasoning (AR) to generate the proofs. This technology has become practical at last due to advances in the theory of AR and improvements in processor power. We are getting successful automated proof rates of 95% to 100% depending on the problem domain, before we provide any hints to the prover (normally this is done by way of extra assertions). On our current commercial project we are getting 99.89%. So nearly all proof failures indicate either incomplete specifications or bugs.

<< In addition, proof of correctness is not very useful if the implementation changes even slightly.

Using AR, this is not a big problem - just re-run the proof generator. Ditto when the specification changes and the implementation is

adjusted to suit.

<< A complete and optimal set of black box test cases *IS* the S/W contract since it defines the semantics. Any implementation changes that changes interface behaviour would fail the black box tests. <<

I don't see how a set of black box test cases can be known to be complete, unless the system has no internal state and the set includes all possible combinations of inputs. Even if the system itself has no state variables (i.e. it just computes an output for some inputs), unless you test with all possible inputs, you don't know that the output will always be correct. The programmer might have "optimised" the calculation for certain values of the input variables (i.e. defined a different path in the program), and the optimisation may generate incorrect results. How would you have defined a "complete and optimal" set of test cases for IEEE double-precision floating point division, such that the Pentium FP DIV bug would have been found, other than by testing with all 2^{128} possible inputs?

If the system has a complex internal state, it is even harder to devise good test data, unless the software provides an interface to examine the state. Consider e.g. a word processor with an "undo" button which is good for undoing the last 100 changes you made to the document since opening it. How do you devise a "complete and optimal" set of test data for correct operation of that button? OTOH it is not difficult to formally specify.

BTW I'm not against testing - until we have provably-correct compilers, linkers, provers, code generators and hardware, testing will still be needed even when correctness proofs are produced.

Dr. David Crocker <http://www.eschertech.com>
Consultancy & contracting for dependable software development

✶ Re: Risks of believing in testing (Cheng, [RISKS-23.40](#))

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Sat, 05 Jun 2004 09:25:44 +0200

While I might share Spencer Cheng's enthusiasm for properly-designed tests, I regret that some claims he seems to be making exceed the known mathematical limits of the efficacy of testing.

Basic observations by Littlewood and Strigini (Bayesian) and Butler and Finelli (frequentist) in the 1990's established the limits of testing, at least for systems whose failure rates must be lower than one failure in a million hours of operation. Many safety-critical systems, for example, have requirements for failure rates that are up to three orders of magnitude lower than this. Those unfamiliar with this literature may find it easily on the WWW.

It is conceivable (not necessarily practical or even possible, but conceivable) that requirements on systems which may fail once in ten thousand to one-hundred thousand hours could somehow be reduced

to a requirement on results from specific tests, as Cheng suggests by his startling phrase "A complete and optimal set of black box test cases *IS* the S/W contract since it defines the semantics." However, for systems whose failure rates are required to be lower than this, such a suggestion regrettably contradicts established science.

Peter B. Ladkin, University of Bielefeld, Germany
<http://www.rvs.uni-bielefeld.de>

✶ Risks of believing in testing (Cheng, [RISKS-23.41](#))

<Fred Cohen <fred.cohen@all.net>>
Thu, 3 Jun 2004 22:42:59 -0700 (PDT)

There are many problems with proof of correctness - perhaps the biggest one being that "correctness" may not be the property of interest to the task at hand. For example, I would like to prove that programs designed to run forever don't stop. And I would like to prove that the green lights will not be on in non-parallel directions at traffic lights. And I would like to prove that my programs properly respond to all error conditions (into known and safe failure modes). None of these have to do with program correctness - per se.

> I have become a firm believer over the years in proper black box
> testing since -

Except that there are too many states. So you can't do much of a test.

This is a big problem for me in forensics cases. I just wrote a report in such a case in which I would love to have been able to say that some piece of data means some particular thing, but I cannot do so because I cannot know for certain that that is the only thing the data represents in the particular circumstance without either (1) access to the source code, or (2) the ability to reverse engineer it. The former is protected by copyright and the latter prohibited by the DMCA. So it will remain a question and not an answer for the court system charged with determining the freedom or incarceration of a defendant.

> 1) it is the only way I know to establish that mythical S/W contract that people have been talking about for the last 20 years.

Huh?

> 2) [...] Any implementation changes that changes interface behaviour would fail the black box tests.

Not hardly. There are other behaviors of programs than "interface" behavior unless you are very careful about the definition of interface. How do I black box test for performance-related covert channels?

> 3) Requirement traceability can be satisfied by tracing the requirement to the interface specification and onward to the test cases.

And what interface specifications are those? Most products on the market

today don't have such things. And to the extent that they do, they only partially specify real behavior. Can a complete specification be written? I don't think so.

Fred Cohen - <http://all.net/> - fc at all.net - fc at unhca.com - 925-454-0171

Fred Cohen & Associates - University of New Haven - Security Posture

✦ Re: Daft security questions (Chard, [RISKS-23.40](#))

<Brian Reynolds <bfr@murphy.com>>

Thu, 3 Jun 2004 16:15:48 -0400

After all, this is a method for identifying you, not a method for acquiring correct answers.

When I am forced to use something like this (or the ubiquitous "State your mother's maiden name") I make sure to give answers that have no relation to the question asked (even when I'm also asked to provide the question).

This leads to the further problem of remembering which non-sense answer goes with which (non-sense) security system, but at least others would have a harder time guessing my answers based on knowledge about me. The only time there is a problem is when some over zealous programmer tries to enforce formatting on the answer (e.g., requiring a valid date in answer to the example "Memorable date" question).

Brian Reynolds bfr@murphy.com (212)618-0999

✶ Re: Daft security questions (Chard, [RISKS-23.40](#))

<Lou Katz <lou@metron.com>>

Thu, 3 Jun 2004 14:31:55 -0700

The flaw in the poster's reasoning is to answer the 'question' correctly.

Why? What you have here, is in effect, another password. The system collecting your 'answers' cannot verify their correctness. Why not use other strings? 'f7u00Hngq' is just as good an answer as 'Boston' to the first question, etc.

One should ask, when presented with a question or a blank to fill out:

a: Do I really have to fill this out at all? Why does the asker need to

know this information?

b: If (a) is true, then is there a legal requirement for truthfulness?

Wherever possible, don't answer the questions. Otherwise generate random answers and write them down, if you think you will ever need to refer to them again. If your wallet is lost or stolen and contains such gibberish, the correct association with where they might be needed is in your brain and hard to deduce.

"Your mother's maiden name" need not be a name, need not have a female association. I have found that 'blue-green algae' or

'discombustable'
work equally well.

⚡ **Re: Daft security questions (Chard, [RISKS-23.40](#))**

<ant@notatla.org.uk (Antonomasia)>
Thu, 3 Jun 2004 23:17:15 +0100 (BST)

A daft answer fits a daft question. Your memorable place might be "Ronnie Barker"; your memorable date might be "Paris Hilton" and your mother's maiden name might be "355/113". It's really a matter of how well you can remember these.

Carl Ellison has suggested (I think accurately) that events of early childhood are the ones you won't forget. How you make daft answers from that is the problem each user needs to solve in his own way.

⚡ **British ATC slowdown (Weber-Wulff, [RISKS-23.41](#))**

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Mon, 07 Jun 2004 17:59:27 +0200

Here is some background information to the British ATC slowdown incident on 3 June 2004 reported by Debora Weber-Wulff ([Risks 23.31](#)).

The Tageschau report appears to confuse NATS, which is the company

called National Air Traffic Services, which runs ATC in Britain, with NAS, the National Airspace System, located at West Drayton, which is a couple of miles from Heathrow.

I believe what happened is that Swanwick went to Manual Mode. That is Stage 2 of a four-stage graceful degradation of air traffic control (see below). Let me explain what that means, and what it entails.

Swanwick is a place and a facility. It is not near Heathrow (by English standards of "near"), but on the south coast near Southampton. The London Area Control Centre (LACC) is the main system there, but there are others.

I shall refer to LACC below because that is the system involved. LACC controls the London Flight Information Region (FIR), which extends from borders with continental airspace up to the Scottish border. The LACC system is relatively new, having come on-line in January 2002 after a ten-year development (planned: 4 years. Search the Risks archives for "NERC").

NAS is at least 30 years old. It has been rehosted, so I think we can probably guess that the Tageschau also confused the system with the kit that runs the system.

NAS provides the master flight data planning for British airspace. This includes flight plans, predicted tracks and control sector boundary crossings for aircraft in the airspace system. I do not know if the primary and secondary radar data normally used by LACC comes through NAS as well, or whether LACC in normal mode generates its own radar data. In any case, LACC does have a radar data feed from

its own
direct connection with RadNet, which distributes that data from
the
radars throughout the ATC system. "Radar data" here means
current 2-D
position, "squawk" code (a 4-octal-digit temporary ID assigned
dynamically
by ATC), and aircraft pressure altitude.

Now, flight planning, and "handoffs" between sector controllers
as aircraft
cross sector boundaries, using the info on the "flight data
strips", is a
very important part of air traffic management. Wendy Mackay
studied this in
Paris with the French controllers, and found that the rituals
involved with
handing off and passing data strips were crucial to successful
operations,
which might help to explain why attempts to move to automatic
systems for
flight data passing and handoffs have often failed (Is Paper
Safer? The
Role of Paper Flight Strips in Air Traffic Control, ACM TOCHI 6
(4):311-40,
Dec. 1999).

LACC does have a partly automated and predictive system to aid
controllers
with passing the flight data and handing off (autocoordination).
When NAS
goes down, most of the predictive data feed goes away. The data
on the
screen at Swanwick starts to "age", and the colors start to
change to
indicate how old the data is. Controllers can work with aging
data up to a
certain point, but then it would become misleading and ultimately
dangerous. There has to be a point at which a decision is made
to ignore
the aging data and perform the flight planning locally in LACC.
This point
is well-defined. At this point, LACC turns autocoordination off

and starts
manual coordination, called Manual Mode.

In Manual Mode, the controllers at LACC work with their radar data and their voice contact only. They have lost automatic track and handoff prediction, and they have to perform this function explicitly using the old-style handoff routines between sector controllers. This is resource-intensive, as is the switch to Manual Mode itself.

When LACC switches to Manual Mode, they also impose flow control to conform with the resources now available. Inter alia, continental controllers with flights whose destination lies within or which are to transit the London FIR and which are not yet airborne are to hold those flights on the ground. Traffic already in the air continues, but is controlled to conform with the reduced flow into and in the London FIR (lots of holding!). Manual mode is intense work for the LACC controllers, and it continues until

- * NAS comes back up (obviously!), and
- * the traffic flow has reduced to a stable maintainable level, and
- * the controllers are rested enough to perform the reversion to the NAS flight-planning-data feed (which is itself a non-trivial operation akin in resource consumption to the Manual Mode change), and
- * somebody decides everybody's up for it.

So, no matter how quickly NAS comes back up, once the decision is made to go to Manual Mode, LACC is there for a while. There seems to me to be no obvious way around this feature.

The NAS has a failure-recovery strategy which is reasonably

effective,
considering when it was designed, and many NAS failures are
recovered
without LACC having to go into Manual Mode. It is moderately
loosely-coupled.

So there is graceful degradation. First stage: NAS failures are
recovered
without LACC noticing. Second stage: LACC goes to Manual Mode,
which means
it works as a typical control center usually does, but has to
impose flow
control because there is simply too much traffic to work in the
traditional
way. Third stage: if LACC loses its secondary radar data things
get hairier
(primary returns, that is, radar bounces off the airplane without
transponder data, provide only two-dimensional positional data,
and
that not as accurately). Fourth stage: if all radar data is lost,
controllers revert to voice-only. Fifth stage: there isn't one;
voice-only
does not fail, on pain of going to bed without its supper. The
whole
process is quite well layered.

So what about replacing NAS? Well, sure, but recall it is a
system that
works, and has done for 30 years. And recall that attempts to
replace
old systems with newer ones, such as Swanwick LACC replacing the
area
control function of LATCC at West Drayton, often end in tears
(op. cit.).
So the people responsible for replacing NAS would be wise to
proceed
vveeeerrrry carefully.

I thank Martyn Thomas for catching myriad mistakes in an earlier
version of
this note. Its accuracy is largely owing to him, and remaining
inaccuracy
still to me. He also pointed out to me NATS's statement on the

slowdown, at

http://www.nats.co.uk/news/news_stories/2004_06_03.html

Peter B. Ladkin, Bielefeld, Germany 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

Volume 23: Issue 43

Monday 28 June 2004

Contents

- [AOL worker sold customer list for spam, US charges](#)
[via Monty Solomon](#)
- [Swedish social insurance computers disabled by virus](#)
[Peter Håkanson](#)
- [Terror over Internet Protocol?](#)
[NewsScan](#)
- [Canada's largest bank has "processing disruption"](#)
[Yves Bellefeuille](#)
- [PFIR "Preventing the Internet Meltdown" Conference Info Online](#)
[Lauren Weinstein](#)
- [Attacking the attackers: maybe not a good idea](#)
[NewsScan](#)
- [Shocking laptop horror stories](#)
[Aahz](#)
- [Hacker hits South Korean defense](#)
[NewsScan](#)
- [/Not/ keeping security information up to date](#)
[TFB](#)
- [Wyoming woman arrested on false federal charges](#)
[Dirk the Daring](#)

- [Exploding vending machine emits phosgene gas](#)
[Cheryl Hoefelmeyer](#)
 - [Irresponsible traffic announcement](#)
[Steve Friedman](#)
 - [Who am I?](#)
[Erann Gat](#)
 - [Re: Autorun evil?](#)
[Thomas Wicklund](#)
 - [Risks of testing](#)
[Thomas Wicklund](#)
 - [Re: Whom do I tell?](#)
[Chris Brand](#)
 - [REVIEW: "Security Warrior", Cyrus Peikari/Anton Chuvakin](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ AOL worker sold customer list for spam, US charges

<Monty Solomon <monty@roscom.com>>

Fri, 25 Jun 2004 13:37:21 -0400

An America Online employee, Jason Smathers, has been charged with stealing AOL's list of 92-million customers and selling it to an

Internet spammer/marketer/online-gambling purveyor Sean Dunaway (who then resold it for \$52,000 a pop). Dunaway was also charged. Smathers has been fired.

[Sources: Monty provided several items, which were PGN-ed.]

Reuters, 23 Jun 2004

- <http://finance.lycos.com/home/news/story.asp?story=42133939>

Andrew Orlowski, 24 June 2004, UNITED STATES v. JASON

SMATHERS, SEAN DUNAWAY

<http://news.findlaw.com/hdocs/docs/cyberlaw/ussmthrs604acmp.pdf>

http://www.theregister.com/2004/06/24/aol_spam_insider/

]

⚡ Swedish social insurance computers disabled by virus

<Peter Håkanson <peter@hk.ipsec.se>>

Wed, 23 Jun 2004 18:38:32 +0200

Today Riksförsäkringsverket (the central authority that pays all social benefits and illness-related salary-supplements) was disabled by virus attacks.

This concerns all of Sweden's population of 9M persons. Not all of us rely on this money, but every Swede who happens to be eligible for any payments is.

A lot of errors seem to contribute. One of the larger is basing a national insurance system on computers that are defenseless against any external threat, another that those "toy-computers" are exposed to external threats.

Maybe the golf-tours made the difference during the purchasing procedures??

There's never money to do it right, but always money to do it again ... and again ... and again ... and again.

(Det är billigare att göra rätt. Det är dyrt att laga fel.)

⚡ Terror over Internet Protocol?

<"NewsScan" <newsscan@newsscan.com>>

Thu, 17 Jun 2004 08:45:44 -0700

A senior Justice Department official has told a Senate committee that law enforcement faces new threats from Internet-based telephone services, and warned that legislative efforts to deregulate VoIP (Voice over Internet Protocol) services could undermine the ability of law enforcement officials to investigate criminal or terrorist activity. The Justice Department has asked the FCC to require Internet phone companies to design electronic conduits in their networks that would make it easier to tap conversations. James X. Dempsey of the Center for Democracy and Technology says that a better approach would be for investigators to work cooperatively with Internet phone providers. (*The Washington Post*, 16 Jun 2004; NewsScan Daily, 17 Jun 2004]

<http://www.washingtonpost.com/wp-dyn/articles/A47882-2004Jun16.html>

✶ Canada's largest bank has "processing disruption"

<Yves Bellefeuille <yan@storm.ca>>

Sun, 20 Jun 2004 22:46:47 -0400

[Written on 4 June, but only sent now because of a problem with my Usenet server. :-)]

Canada's largest bank, the Royal Bank of Canada, has been unable to process deposits or report balances for the last five days. The bank is

blaming "a processing disruption during a routine programming update to one of our computer systems".

Direct deposit to a bank account is a common way to pay salaries here, especially for large employers, and among those affected are employees of the Government of Ontario, Canada's largest province, which apparently uses the Royal Bank for its payroll.

The Royal Bank has 10 million customers, about a third of Canada's population. It says that it "processes tens of millions of transactions each day". The bank confirms that "the processing disruption was national in scope so we expect a significant number of clients have been affected".

The bank promises that: "We will fully refund any service fees or overdraft interest charged to RBC clients' accounts due to this processing delay. Any other reasonable costs incurred as a result of this delay will be handled on an individual basis". It also says that:

"All the other banks are aware of this situation and we have asked them to be as accommodating as possible". (There are seven major banks in Canada.)

More information at:

http://www.royalbank.ca/client_faq.html

<http://www.globeandmail.ca/servlet/story/RTGAM.20040604.wrbc0604/BNStory/Business/>

PFIR "Preventing the Internet Meltdown" Conference Info Online

<Lauren Weinstein <lauren@vortex.com>>

Sat, 26 Jun 2004 10:01:44 -0700

Peter,

I'm pleased to announce the availability of detailed registration, schedule, program, hotel, and other information relating to our People

For Internet Responsibility (PFIR) "Preventing the Internet Meltdown"

conference here in L.A. from July 26 through 28, 2004. The registration period for the conference commences immediately.

The conference information is all available from the Meltdown official announcement document and related linked pages via:

<http://www.pfir.org/meltdown>

In the time since you, Dave Farber, and I originally suggested this conference, the situation with many issues related to the Internet have become even more complex and controversial. These range from Internet governance and control to Homeland Security issues; from VoIP, WHOIS, DNS, and privacy to spam, viruses, and other attacks on the Internet infrastructure and its users; and much more. The Internet and the global populations who depend upon it are at real risk.

We hope that this gathering will aid in mapping out some specific courses of action that can help us all avoid the many negative impacts that an Internet meltdown would impart.

We're looking forward to a most interesting and productive event. Thank you very much. Be seeing you!

--Lauren--

Lauren Weinstein

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

Tel: +1 (818) 225-2800

<http://www.pfir.org/lauren>

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

Co-Founder, Fact Squad - <http://www.factsquad.org>

Co-Founder, URIICA - Union for Representative International Internet

Cooperation and Analysis - <http://www.uriica.org>

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

Member, ACM Committee on Computers and Public Policy

✶ Attacking the attackers: maybe not a good idea

<"NewsScan" <newsscan@newsscan.com>>

Mon, 21 Jun 2004 09:00:56 -0700

A company called Symbiot Security has created "Intelligent Security

Infrastructure Management Systems" (iSIMS) that not only provide traditional defensive measures against viruses, worms, and other kinds

of network vandalism -- but also offer the victims of vandalism a gradual escalation of retaliation measures. These include the ability

to flood the attacking computers with data. However, some experts say

that retaliatory actions could be a very bad idea. Adrian Vanzyl of

the security firm Seclarity comments: "So you are in effect breaking

into each of those systems as you follow this person back. Are you

legally liable for that? It's a very, very good question." And Dorothy

Denning, professor of defense analysis at the Naval Postgraduate

School, warns: "We've seen worms that have had major impact like causing delays in airline schedules, shutting down ATM machines, 911 systems and so on. Putting any kind of worm out there would be dangerous." (AP/*San Jose Mercury News*, 18 Jun 2004; NewsScan Daily, 21 Jun 2004]

<http://www.siliconvalley.com/mld/siliconvalley/8957335.htm>

✶ Shocking laptop horror stories

<Aahz <aahz@pythoncraft.com>>

Mon, 21 Jun 2004 23:07:05 -0400

Press release dated June 11 (plus other stories found through Google):

<http://www.newsroom.ucla.edu/page.asp?RelNum=5275>

The story says that a laptop was stolen from the University of California, Los Angeles in 11/2003, containing a database of 145,000

blood donors that was password-protected but not encrypted. The database

contained names, birthdates, and social security numbers. The victims

were not notified until a week before the story was filed, roughly six

months after the theft.

The laptop was stolen from a locked van. A second laptop was stolen in

late May from an office, putting another 62,000 people at risk -- UCLA

will notify these people, "...in the next few weeks."

Nothing really new here. Question is, when will these stories stop

getting resurrected from the grave? Of even more interest to me

is that
none of my usual sources have popped up with this story; I
learned about
it during a trip to LA this past weekend, more than a week after
it hit
the news. Are we getting that blase about this?

Aahz (aahz@pythoncraft.com) <http://www.pythoncraft.com/>

⚡ Hacker hits South Korean defense

<"NewsScan" <newsscan@newsscan.com>>

Tue, 22 Jun 2004 10:03:31 -0700

A network vandal has broken into computers at sensitive South Korean research institutes and government agencies, infecting more than 60 PCs with a variation of the Peep Trojan program. The National Cyber Security Center (NCSC) said the hacker had broken into computers at the Agency for Defense Development, which develops weapons, the Korea Atomic Energy Research Institute, the Korea Institute for Defense Analysis and three other government agencies. [*The Australian*, 21 Jun 2004; NewsScan Daily, 22 Jun 2004) Rec'd from John Lamp <http://tinyurl.com/24wyw>

⚡ /Not/ keeping security information up to date

<tfb@cley.com>

Mon, 28 Jun 2004 12:04:21 +0100

Some time ago, in 2003, CERT announced a WAP service, so you could check current CERT alerts and so on from your phone, at <http://wap.cert.org/>. WAP hasn't been wildly successful, of course, but all phoes have it, at least in the UK. Since I'm away from home a lot, and I'm responsible for the security of our machines (and sometimes of clients' machines too), I thought it would be useful: it's nice to be able to check that there is nothing to panic about from a device I carry all the time anyway. This is also potentially a nearly-ideal use of a phone-type interface - the amount of information needed is absolutely tiny ('sendmail issue, patch now!'), and promptness is very important. Push would be better than pull, but you can't have everything.

Fortunately, although I put the URL in my bookmarks, I didn't use it very often, because something completely toxic happened. For whatever reason, CERT obviously lost interest in the WAP interface, and *left a static version of it in place*. If you check that URL (from a phone) now, you'll find some information from November 2003, and *no indication at all* that all the information is hopelessly out of date.

This is the worst possible scenario for a system like this. A system which is meant to be providing alerts of some kind needs to either work, or fail in such a way that its users know it's failed. This is the equivalent of the coolant level meter reading 'full' while coolant pours from some fractured pipe and the core melts. If the

coolant

meter is broken it's way better to have sparks and smoke pouring from it than for it to quietly repeat the last reading...

I'd urge anyone who provides security information over the net to arrange life so that when the system breaks or they lose interest, it fails in a way that is extremely visible to its users.

🔥 Wyoming woman arrested on false federal charges

<Dirk the Daring <dirk@psicorps.org>>

Sat, 19 Jun 2004 18:01:27 -0400 (EDT)

<http://www.billingsgazette.com/index.php?id=1&display=rednews/2004/06/19/build/wyoming/55-arrest.inc>

Summary: A vacationing Wyoming teacher's aide was roused from her cruise ship bed, shackled and dragged into federal court based on information in a federal warrant database that wrongly accused her of failing to pay a fine after she was cited in a US national park last year.

The RISKS: Federal agents apparently blindly relied on the database, even though the court had a copy of the citation showing she had paid.

The US Attorney even continued to ask for the woman to have to appear in court in Wyoming after being told that the citation showed she had paid, and standard procedure for the park is that visitors must pay fines before they can leave.

Clearly, federal law enforcement authorities continue to place too much reliance in computer databases and not enough on the information in front of them. Further, the fine was a matter of US\$50 for failing to properly store her hot chocolate and marshmallows, yet the federal authorities saw fit to drag the woman out of bed, shackle her like a mass-murderer, and haul her into court.

✶ Exploding vending machine emits phosgene gas

<"Cheryl Hoefelmeyer" <hoefelmeyer@hotmail.com>>

Sat, 26 Jun 2004 01:14:51 +0000

A repairman working on a soft drink vending machine in Park Place Medical Center in Port Arthur, Texas apparently triggered an explosion which converted the freon in the machine to phosgene gas, a poisonous gas that was used in WWI as a weapon.

Reference: (*Houston Chronicle*)

<http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/2647290>

✶ Irresponsible traffic announcement

<Steve Friedman <steve@ads-i-m4.com>>

Thu, 3 Jun 2004 13:51:03 -0400 (EDT)

On the way to work this morning, around 9:45 am I heard a

surprising
traffic announcement on the radio (WAMU). On this road, one is
legally allowed to drive on the right shoulder (aka breakdown)
lane
until 10am. To indicate when it is permissible, lights over the
lane
either indicate a red X or a green arrow.

Apparently, today the lights were showing red (thus closing down
one
lane). The announcer indicated that, since it was still legal to
drive on the right shoulder until 10am, motorists should ignore
the
computerized signs and drive on the right lane anyway.

It wasn't clear whether the insight into letting motorists
decide to
ignore the signs was made by the announcer or Virginia state
police;
however, it doesn't seem like a good idea to train motorists
that the
only reason why the lane might be closed is because of computer
malfunction and thus ignore the signs when the motorist "knows"
that
the lane should be open.

Who am I?

<Erann Gat <gat@flownet.com>>

Fri, 18 Jun 2004 11:35:41 -0700 (PDT)

I just completed the process of legally changing my name. I am
no longer
Erann Gat. I am now Ron Garret.

The interesting thing (I have been reading RISKS far too long
for this to
be shocking or even surprising) is that the only time during the
entire

process that I was asked to produce any identification was when I tried to pay the court fees with my credit card. If I had paid in cash I could have gone through the entire process without ever having to produce an ID.

And, of course, so could anybody else.

Ron Garret f.k.a. Erann Gat

✶ Autorun evil? (Re: da Silva, [RISKS-23.42](#))

<Thomas Wicklund <wicklund@eskimo.com>>

Mon, 21 Jun 2004 09:20:05 -0700 (PDT)

Peter da Silva questions who would think autorun a good idea. The answer should be obvious. Most computer users aren't technically sophisticated and want to have "plug and play" devices. A few minutes with market research or support personnel will show that a typical consumer wants to plug a device into a computer and user it. The consumer doesn't want to have to perform a software installation step using a CD which was probably lost months ago, nor answer a bunch of "do you want to enable this device you just plugged in" questions. Anybody with non-technically inclined relatives who's been asked to help setup a system should also see the reasons for plug and play features.

Obviously this opens up security concerns. Autorun is subject to abuse. So is the lack of autorun (just create a CD with a virus named

"setup" and tell the user to install it).

There is a fundamental conflict between security and convenience. Many common system features are security holes such as programmable access to network features, copy/paste clipboards, I/O redirection, and allowing default "other read" file access. Most features which allow one to do useful work can also be abused. Similarly, the feature of the automobile which allows one to travel faster than a walk also allows one to be more easily killed in a collision.

In the same Risks edition, Aahz objects to labeling Verity technology as data mining software. Yet in some sense, any search program is a form of data mining. And as with any search, it can be used (find the best price for product X) and abused (find all information about John Doe).

✶ Risks of testing (Cohen, [RISKS-23.42](#))

<Thomas Wicklund <wicklund@eskimo.com>>

Mon, 21 Jun 2004 09:25:08 -0700 (PDT)

Fred Cohen mentions wanting to be able to prove things like "the green lights will not be on in non-parallel directions at traffic lights".

One thing software professionals must always remember, and may easily forget, is that software is dependent on hardware. No amount of software will protect against a short in the hardware, and even with

fault tolerant techniques one must ultimately ensure that the hardware is properly designed or provides the proper interlocks.

In the traffic light case, while software may be cheaper, hardware interlocks may ultimately be the most reliable solution.

⚡ Re: Whom do I tell? (Jerry James)

<"Chris Brand" <Chris_Brand@spectrumsignal.com>>

Fri, 18 Jun 2004 10:21:11 -0700

> ... when I dial a number I know is good, I get the message that I am calling a disconnected number.

This sounds similar to a problem I have. Here in BC, in November 2001, we switched to 10-digit dialing, where you always have to dial the area code even if your area code is the same. If you get it wrong, you get a polite message telling you that you need to redial with the "604".

The problem is that I occasionally get the same message when I have dialed the 604. Just as Jerry described, I hang up, press "redial" and the call goes through.

I haven't actually bothered trying to report it. In this age of Windows, "try it again", "it worked that time", "well ok, then. Goodbye" seems to have become the norm.

⚡ REVIEW: "Security Warrior", Cyrus Peikari/Anton Chuvakin

<Rob Slade <rslade@sprint.ca>>

Thu, 24 Jun 2004 12:48:24 -0800

BKSECWRR.RVW 20040509

"Security Warrior", Cyrus Peikari/Anton Chuvakin, 2004, 0-596-00545-8,

U\$44.95/C\$65.95

%A Cyrus Peikari

%A Anton Chuvakin

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 2004

%G 0-596-00545-8

%I O'Reilly & Associates, Inc.

%O U\$44.95/C\$65.95 800-998-9938 fax: 707-829-0104 nuts@ora.com

%O <http://www.amazon.com/exec/obidos/ASIN/0596005458/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0596005458/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0596005458/>

[robsladesin03-20](#)

%P 531 p.

%T "Security Warrior"

The preface isn't a really clear piece of writing, but does, eventually, get around to stating that the book focuses on security

from an attack, rather than defence, perspective. I have, in numerous

other reviews, pointed out the errors and limitations in this position.

Part one deals with cracking software, primarily involved with breaking copy protection. Chapter one explains a few concepts about

assembly language quite well, and then ends abruptly. Some Windows

tools for reverse engineering are listed in chapter two, plus a couple

of poorly explained examples. The material on reverse engineering in

Linux is longer and more detailed, but still has very limited tutorial value, and is padded with extensive code listings of dubious worth.

Chapter four is supposed to deal with reverse engineering for Windows CE, but contains an odd mix of CE operating system architecture, a partial list of ARM CPU opcodes, and a description of how to crack the registration code check in a program written solely to allow you to crack the registration code check embedded within it.

Overflow attacks, in chapter five, explains buffer and other overflow conditions, and gives an example of a buffer overflow as a crack in another fake program.

Part two presents information about networks. Chapter six is a rather unstructured overview of TCP/IP and a listing of some sniffing tools.

(TCP is explained before IP itself, and the relationship of the various protocols in the suite is not discussed. A section on "covert channels" emphasizes a strange misuse of header fields, and then drifts into something like session hijacking.) Social engineering can be used in a variety of ways, so it is strange that chapter seven should be here rather than in the "Advanced Defence" of part four.

The random content provided has little organization and a fair number of errors: the authors insist that social engineering attacks can be divided into active and passive types, but, by its nature, social engineering is almost entirely active. (The book does seem to tacitly admit this: there is a list of example "active" attacks, but no corresponding "passive" list.) Chapter eight mentions a few methods of reconnaissance with differing levels of detail. Some more advanced

techniques for identifying the operating systems in chapter nine, but the particulars are similarly inconsistent.

Part three lists attacks against specific platforms. The authors betray their lack of study once again in chapter eleven: UNIX is **not** "reborn from" MULTICS (although it was heavily influenced), and TCSEC (the Trusted Computer System Evaluation Criteria) is definitely **not** the Common Criteria. The various security related aspects, tools, and hardening of UNIX are not bad, but lack definition. The UNIX attacks listed in chapter twelve are good: ironically, because of the generic nature of the descriptions the examples are probably useful as a guide to defensive measures, rather than being outdated tricks. The Windows client attacks listed in chapter thirteen, because they are specific, have limited the material both in scope and utility. Chapter fourteen, listing Windows server attacks, notes some interesting security bugs in Server 2003 and other programs (and one bit on smartcards.) "SOAP XML Web Services Security," in chapter fifteen, is a long title for a short piece on XML digital signatures. "SQL Injection," in chapter sixteen, has some examples of malformed data attacks, and also points out the dangers of adding programming functionality to applications. As with social engineering, the tie to networks is thin, seemingly limited to the PHPNuke program. Some aspects of wireless antennae, sniffing, and a brief review of the weaknesses in WEP (Wired Equivalent Privacy) are in chapter seventeen.

Part four looks at more advanced defence. Miscellaneous thoughts on logging are in chapter eighteen. Chapter nineteen has a confused explanation of intrusion detection systems (IDS). There is no

mention

of rule (or activity monitoring) based engines, signature based engines are said to be restricted to net-based IDS, different terms

are used for anomaly detection engines on hosts versus networks, and

there is a muddled attempt to tie Bayesian analysis to odd mathematical ratios of false positive (false rejection) and false negative (false acceptance) errors. The installation of a simple honeypot is described in chapter twenty (which probably **should** be in

part two). There is a good initial outline of incident response in

chapter twenty one, but it breaks down when getting into specifics.

Forensics and antifoensics, in chapter twenty two, gives some background and tools for data recovery and obfuscation.

It is ironic that the book starts out with a quotation from "The Code

of the Samurai," stating that "[a]ll samurai ought certainly to apply

themselves to the study of military science. But a bad use can be

made of this study to puff oneself up and disparage one's colleagues

by a lot of high-flown but incorrect arguments that only mislead the

young ..." This assessment fits Peikari and Chuvakin's work almost

perfectly. There is a lot of interesting information in this volume:

if you have limited technical background in the fields examined, you

will find that a quick perusal will provide you with some superficial

familiarity with the topics. However, the uneven coverage ensures

that the information is spectacular, rather than tutorial. The disjointed jumps from one subject to the next prove the technical erudition of the authors, but do not help the reader very much.

copyright Robert M. Slade, 2004 BKSECWRR.RVW 20040509

rslade@vcn.bc.ca
niu.edu

slade@victoria.tc.ca

rslade@sun.soci.

[http://victoria.tc.ca/techrev
~rslade](http://victoria.tc.ca/techrev/~rslade)

or

<http://sun.soci.niu.edu/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 44

Saturday 3 July 2004

Contents

- [Acting Now to Prevent the Internet Meltdown](#)
[PGN](#)
- [Court rules e-mail eavesdropping okay](#)
[NewsScan](#)
- [Fed. Court Rules No Privacy For E-Mail Passing Through ISP Servers](#)
[Lauren Weinstein](#)
- [Florida Felon list is wrong, wrong, wrongity wrong](#)
[Danny Burstein](#)
- [Israeli Police losses laptop with critical agents information](#)
[Gadi Evron](#)
- [DC Metro discovers flag-day issues with changeover in payment systems](#)
[Joe Thompson](#)
- [Coca-Cola Cans as Security Threat](#)
[Jack M Dominey](#)
- [Pharmacists worry about drug vending units](#)
[Daniel P. B. Smith](#)
- [RFID could cost 4 million jobs by 2007](#)
[NewsScan](#)
- [Barclays Bank of Zimbabwe suffers data theft](#)
[Bob Heuman](#)

- [French authority forbids "DIDTHEYREADIT?" service](#)
[Bob Heuman from NewsScan](#)
 - [Web service maps tax codes to ID info](#)
[John](#)
 - [Re: Attacking the attackers: maybe not a good idea](#)
[Nick Brown](#) [Curtis Karnow](#)
 - [REVIEW: "Exploiting Software", Greg Hoglund/Gary McGraw](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Acting Now to Prevent the Internet Meltdown

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

Sun, 4 Jul 2004 08:12:11

Both the Internet and its users are under increasingly serious attacks from numerous technical and non-technical threats. If you are seriously interested in helping to avoid an "Internet meltdown" that could negatively and dramatically impact people around the world, please consider joining a group of us who will be meeting in Los Angeles from July 26 - 28 to address these issues under the aegis of People for Internet Responsibility (which I co-founded with Lauren Weinstein).

The expanding program agenda is on the conference main Web page:

<http://www.pfir.org/meltdown>

In contrast to many other meetings, the conference program is oriented toward technology-related *policies* rather than to technical details, and should be of interest to techies and non-techies alike.

Please note that conference registrations need to be received prior to July 18 for the reduced conference rate, and that the hotel is offering discounted room rates through July 11.

I'm looking forward to seeing many of you at the conference.

Peter G. Neumann
Principal Scientist, SRI International Computer Science Lab
Chairman, ACM Committee on Computers and Public Policy

★ Court rules e-mail eavesdropping okay

<"NewsScan" <newsscan@newsscan.com>>

Thu, 01 Jul 2004 08:33:22 -0700

In a surprise decision, a federal appeals court has ruled that it was acceptable for a company that offered e-mail service to peruse messages sent by its subscribers. The case stems from 1998 when it was discovered that Interloc, a now-defunct literary clearinghouse, surreptitiously copied messages sent to its subscribers by rival Amazon in order to "develop a list of books, learn about competitors and attain a commercial advantage." An Interloc executive was later indicted on an illegal wiretapping charge, but yesterday's ruling upheld a federal judge's dismissal of that charge on the grounds that the e-mails were copied while in "electronic storage" (during the process of being routed through a network of servers to recipients). The Wiretap Act prohibits unauthorized eavesdropping on messages that are not stored -- such as a real-time telephone conversation -- but does not afford the same protection to stored messages. In a dissenting opinion, Appeals Court Judge Kermit

Lipez

wrote that the ruling unravels "decades of practice and precedent regarding the scope of the Wiretap Act" and essentially renders the

act "irrelevant to the protection of wire and electronic privacy." In

a concurring statement, the Electronic Frontier Foundation said that

yesterday's ruling "dealt a grave blow to the privacy of Internet communications." [AP 30 Jun 2004; NewsScan Daily, 1 Jul 2004]

<http://apnews.excite.com/article/20040701/D83HMB000.html>

⚡ Fed. Court Rules No Privacy For E-Mail Passing Through ISP Servers

<Lauren Weinstein <lauren@vortex.com>>

Fri, 02 Jul 2004 17:32:20 -0700

PFIR Bulletin

Federal Court Rules No Privacy in E-mail Stored
at ISPs, Even Temporarily in Transit

July 2, 2004

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

[To subscribe or unsubscribe to/from this list, please send the command "subscribe" or "unsubscribe" respectively (without the quotes) in the body of an e-mail to "pfir-request@pfir.org".]

A federal appeals court has ruled that your e-mail passing through ISP servers is virtually without privacy protections. It is

impossible to
overstate the potential significance of this astoundingly poor
decision.

For the news story, please see:

<http://www.washingtonpost.com/wp-dyn/articles/A19211-2004Jun30.html>

The full text of the decision is at:

<http://www.cal.uscourts.gov/pdf.opinions/03-1383-01A.pdf>

If generally upheld, it means that user e-mail stored on ISP
servers
even temporarily or while in transit (Gmail, Hotmail, POP, IMAP,
SMTP,
etc.) is vulnerable to legal monitoring or other abuses by ISPs
and
others, including use for competitive or even prurient purposes,
without notification to the persons whose e-mails are involved.

With many ISPs forcing more users (especially typical dynamic-IP
customers) to route all mail through ISP servers (e.g., via
blocking
of port 25), the implications are staggering.

Though ISPs may claim privacy policies that prohibit snooping,
policies are subject to change, and the legal barriers for
access to
the mail by outside entities is also much lower in such cases.

Regardless of whether or not this decision stands, the underlying
facts should be very clear. The most reliable and trustworthy
path to
secure e-mail is via direct, end-to-end, encrypted connections
that
are not forced to route through ISP mail servers. This is one
of the
goals of the PFIR "Tripoli" project (
<http://www.pfir.org/tripoli-overview>).

The court's ruling will also now be a topic at a legal issues
panel at our PFIR "Internet Meltdown" conference late in July
(<http://www.pfir.org/meltdown>). [See above. PGN]

This is one of the worst and most dangerous court decisions ever to appear relating to the Internet.

Lauren Weinstein

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

Tel: +1 (818) 225-2800

<http://www.pfir.org/lauren>

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

Co-Founder, Fact Squad - <http://www.factsquad.org>

Co-Founder, URIICA - Union for Representative International Internet

Cooperation and Analysis - <http://www.uriica.org>

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

Member, ACM Committee on Computers and Public Policy

✶ Florida Felon list is wrong, wrong, wrongity wrong

<danny burstein <dannyb@panix.com>>

Sat, 3 Jul 2004 01:06:21 -0400 (EDT)

First, after a court battle, some news organizations and the Florida ACLU got a judge to grant them access to the Florida Felon list - the one that keeps people from voting (a very painful topic we all recall from 2000):

> "TALLAHASSEE - In a victory for Florida voters, a Leon circuit court judge

> today struck down a state law that prevents copying a state list with

> names of more than 47,000 registered voters who may be deleted from the

> voter rolls because the state has identified them as possible ex-felons.

http://www.aclufl.org/news_events/index.cfm?action=viewRelease&emailAlertID=289

And to no one's surprise, a couple of days later we got stories like this:

Thousands of eligible voters are on felon list
BY ERIKA BOLSTAD, JASON GROTTO AND DAVID KIDWELL

More than 2,100 Florida voters -- many of them black Democrats -- could be wrongly barred from voting in November because Tallahassee elections officials included them on a list of felons potentially ineligible to vote, a Herald investigation has found.

A Florida Division of Elections database lists more than 47,000 people the department said may be ineligible to vote because of felony records. But a Herald review shows that at least 2,119 of those names -- including 547 in South Florida -- shouldn't be on the list because their rights to vote were formally restored through the state's clemency process...

http://www.miami.com/mld/miamiherald/news/front/9062928.htm?ERIGHTS=-2146699848262413226miami::cypherpunks@toad.com&KRD_RM=4ksloqmmnrqknptkkkkkkkklnk | Nobody | Y

✶ Israeli Police losses laptop with critical agents information

<Gadi Evron <ge@linuxbox.org>>
Sat, 03 Jul 2004 04:39:18 +0200

The Israeli Police psychologist, in-charge of consulting and evaluating police under-cover agents, lost her laptop.

The laptop was stolen in a break-in to her house.

According to Police sources the laptop held no names, rather than just the psych evaluations and information. Police said the loss is not critical, but non-the-less, they invested a lot of resources in locating the thieves and arranging for a buy.

The laptop was bought for only 5K INS (a bit over 1K USD). When bought, the information on the laptop was also deleted. This suggests that maybe the thieves were only after selling the laptop and were completely unaware of the information it held or of its value. When were any of us last that lucky? I figure that's wishful thinking, but that's only my opinion.

Heck, I personally hope they were lucky, but I've seen many such warning signs completely ignored by different organizations until a 9/11 of sorts happens. Maybe this will be enough of a shock for them to bump-up information security enforcement. I am pretty sure they already have a policy and regulations.

The laptop supposedly holding no names is a consolation. At least proper compartmentalization policies were followed.

⚡ DC Metro discovers flag-day issues with changeover in payment systems

<Joe Thompson <joe@orion-com.com>>

Tue, 29 Jun 2004 13:27:05 -0400

Recently the DC Metro discovered two things: 1) it was short on cash,
2) parking revenues weren't what they should be. An audit implicated theft by parking attendants as a contributor to the revenue shortfall.

Accordingly, the decision was apparently made to ax the contract with the company which provided the attendants and change over completely to the existing automated "SmarTrip" smart-card system.

Yesterday was the first day of all-automated parking (with attendants standing by in case of problems) and all failed to go quite according to plan:

<http://www.wtopnews.com/?sid=217505&nid=30>

"New machines selling SmarTrip cards were installed in stations, but many customers trying to use credit cards in those machines found they were unable to. Metro said the volume of sales was too much."

...further annoying commuters already miffed at having to shell out \$5 just to buy yet another card. Apparently to buy a card in cash, the machines would *only* accept a \$10 bill. (Here in DC and the surrounding area, the \$20 has been the bill of choice for some time now. They're known as "yuppie food-stamps" because so many people have them and so few people can make change for them.)

For the time being, commuters can buy a traditional Metro farecard for the exact amount of the parking fee and hand that in to the attendants, but no one has addressed what happens when the attendants

are gone and the SmarTrip machines are all that remains.

Also unaddressed, to my knowledge, are questions about the degree of redundancy and the failure modes in the SmarTrip system. Even before the changeover it was a regular occurrence for SmarTrip card readers in parking-lot exit gates to fail, leaving the gate down and forcing everyone to shift to another exit line. After fully-automated operation commences, will a single failed telephone or network line incapacitate all readers in a station's lot (or more than one station's lot)? Is there a contingency plan in place for that? Will gates be changed to automatically lift if communications with the card-authorization system are lost? Have they been changed to do so already, and if so, has the change been tested?

(The SmarTrip cards appear to store the current value in the chip embedded in the card, but some kind of communication does go on since registered cards' value is protected from the time the card is reported lost or stolen.)

What puzzles me is why the existing paper farecards aren't an option for automated parking payment. The readers for those much predate the SmarTrip system and the farecard vending machines are much more flexible.

RISKS: Making major system changes without sufficient forethought and testing for what are essentially political reasons. -- Joe

★ Coca-Cola Cans as Security Threat

<"Dominey, Jack M, NEO" <dominey@att.com>>

Wed, 30 Jun 2004 08:48:23 -0400

Following message forwarded by my boss. I wonder what they think of this at Coca Cola HQ?

Subject: SCIF Security Advisory

Security Managers:

The Coca Cola Company has a summer game promotion running from 5/17 - 7/12/04 in all 50 states and the District of Columbia that has the capability to compromise classified information. The company has intermixed approximately 120 Coca-Cola cans that actually contain GPS locators equipped with a SIM card, keypad and GPS chip transponder so it functions as a cell phone and GPS locator. The cans are concealed in specially marked 12, 18, 20, or 24 can multi-packs of Coca-Cola Classic, Vanilla Coke, Cherry Coke and Caffeine Free Coke. The hi-tech Coke "Unexpected Summer" promotion can has a button, microphone, and a tiny speaker on the outside of the can. Pressing the larger red button starts the game in process, thus activating the GPS signal and a cell phone used by the customer to call a special hotline. Consumers who find these cans, activate the technology, and call the hot line must agree to allow Coke "search teams" using the GPS tracker (accurate to within 50 feet), to surprise them anyplace, anytime within three weeks to deliver a valuable prize.

In accordance with DIA, no specific policy for this promotion will be

issued. However, DISA employees with access to SCIFs should take a common sense approach and if one of these cans are found inside a SCIF, they should treat it as they would any two-way electronic device in a SCIF and remove it immediately. Until such time as this sales promotion ends and all 120 cans are accounted for, Coca-Cola packages should be opened and inspected before taking them into any area marked as a "Restricted Area" or classified meetings/discussions, etc. are in progress or have the potential to occur at any time.

Scott Addis, Chief, SSO, Defense Information Systems Agency

RISKS submission from Jack Dominey, AT&T Network Disaster Recovery

⚡ "Pharmacists worry about drug vending units"

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

Sat, 3 Jul 2004 06:54:06 -0400

Boston Globe, July 3, 2004. Available (for 48 hours) at http://www.boston.com/news/nation/articles/2004/07/03/drug_vending_units_worry_pharmacists/

"...[The Beth Israel Deaconess network] wants to introduce automatic prescription machines to their clinics in the Boston area. From afar, a pharmacist sends a message from his computer telling the machine which prepackaged bottles of pills to dispense. A staffer at a clinic retrieves the bottle, affixes a label, and gives it to the patient.

...Telepharmacy Solutions Inc., ...pioneered the concept in the 1990s.

The automated dispensers cost about \$60,000 each, and so far a smattering of public health centers, hospitals, and Veterans Administration clinics around the country use them. The VA has 55 machines in different states and is considering wider use."

"...[A machine at the Thundermist Clinic in Warwick, Rhode Island] The

West Warwick machine carries 50 branded and generic drugs in preset

doses and bottle sizes, including antibiotics, blood-pressure medication, Lipitor for cholesterol, and several kinds of antidepressants. 'I liken it to a Coke machine,' said Stephanie McCaffrey, Thundermist's vice president for program development.

'You

put the order in, and plop, it comes out.' To get drugs, a doctor faxes

the patient's prescription to a pharmacist in Woonsocket. The pharmacist reviews it and sends an electronic message via a secure

computer link to the vending machine telling which drug to dispense.

Bar codes on the pills and on the labels ensure the right medicine is

given to the right patient."

"A staffer gives the bottle to the patient with printed information

showing the drug's side effects and warnings. The patient is asked

whether he or she wishes to speak to a pharmacist. If the answer is

yes, the patient is directed to a telephone."

In addition to the obvious RISKS (machines never make a mistake--make a

mistake--make a mistake), we have yet another area where automation is

being used to handle the easy part of a difficult task, one that traditionally involved the personal participation of very highly skilled humans. No doubt the bulk of today's pharmaceutical practice

consists of repeatedly dispensing the "top forty hits" of the drug world on a routine basis. This will now be handled by machines, by remote access, and by relatively lower-skilled persons that "give the bottle to the patient" (at least until someone decides these staffers can be eliminated, too). At clinics with the machines which "plop" out drugs, the functions for which pharmacists train for six years will theoretically still be available. But now it will be the exception rather than the rule, and over time these services may become rarer and harder to access. Today, what happens in those rare occasions when a prescription actually needs to be compounded? What will happen ten years from now?

Daniel P. B. Smith, dpbsmith@verizon.net dpbsmith@alum.mit.edu

RFID could cost 4 million jobs by 2007

<"NewsScan" <newsscan@newsscan.com>>

Fri, 02 Jul 2004 08:32:22 -0700

The Yankee Group, a prominent market research firm, is predicting that RFID tags will cost four million U.S. jobs by 2007, throughout numerous industries. (RFID stands for Radio Frequency Identification, a technology embedded for inventory and tracking purposes into products, materials, and shipments.) However, Yankee Group analyst Adam Zabel thinks that most workers who lose their jobs due to increased efficiencies made possible by RFID technology will be

able

to obtain 'more value-added' positions. [Vnunet 2 Jul 2004;

NewsScan

Daily, 2 Jul 2004]

<http://www.vnunet.com/news/1156369>

✶ Barclays Bank of Zimbabwe suffers data theft

<Bob Heuman <rsh@idirect.com>>

Fri, 02 Jul 2004 10:34:47 -0400

No new risk in the following article, but under the government of Robert Mugabe it is possible that this theft was government sponsored!

Barclays victim of data robbery

GodFrey Marawanyika /Anita Fleming

<http://www.theindependent.co.zw/news/2004/July/Friday2/885.html>

Barclays Bank of Zimbabwe has become the second financial institution

to fall victim to computer data robbery, the Zimbabwe Independent

has established. Barclays lost computer hard drives which contained

classified information on the bank and its clientele. The hard drives

were stolen over the weekend. Barclays has since informed the central

bank of the incident.

The FIRST financial institution was robbed of a hard drive in February, [when] NMB fell victim to hard-drive robbery and up to now

the case is still to be resolved.

🔥 French authority forbids "DIDTHEYREADIT?" service

<Bob Heuman <rsh@idirect.com>>

Fri, 02 Jul 2004 19:59:00 -0400

To me via NewsScan Daily, 2 Jul 2004 ("Above The Fold")

And what is the risk to someone from outside of France who has this type of service and flies into France? Do they too risk a 5 year prison term and a substantial fine? If so, Yankee stay home! This service seems to be offered almost all over North America, after all...

> From: "NewsScan" <newsscan@newsscan.com>:

CNIL, the French data protection authority, has declared Rampell Software's new mail-service 'Did they read it?' to be illegal.

(Subscribers to "DidTheyReadIt?" get a report about the exact time their e-mail was opened, for how long, on what kind of operating system and if the mail was forwarded to other people.)

The CNIL finds the service unacceptable under French privacy Legislation; as a result, any French subscriber to this service risks a prison sentence of 5 years plus a substantial fine.

(EDRIGram 1 Jul 2004) www.edri.org Rec'd from Jim Sterne via Mark Gibbs

🔥 Web service maps tax codes to ID info

<"John" <john@ngi.it>>

Thu, 1 Jul 2004 19:30:23 +0200

The Lombardia Region (Italy) local administration has set up a web service to help citizens obtain a certificate of free entitlement to medical treatment (form E111) for travel to other European Union countries. The web service asks for only your tax code as proof of identity and then proceeds to supply you the following information:

- Forename and Surname
- Health authority district of registration
- Health authority registration number

So, if I have only the tax code of a Lombardia resident I can at least find out their full name and their health district (which is more or less certain to be in the same area of their home address).

The risk is providing a service without user authentication which gives out id information to unknown users if they are in possession of a valid tax code.

When challenged about this, the technical staff replied that they had examined the possibility that someone could make up a valid tax code by trial and error. They believed this to be quite remote (and I agree with them). The risk is that they hadn't considered the circumstances where someone might come into possession of a real tax code and then use it to complete the ID info.

⚡ Re: Attacking the attackers: maybe not a good idea ([RISKS-23.43](#))

<Nick Brown <Nick.BROWN@coe.int>>

Wed, 30 Jun 2004 23:40:16 +0200

It's now common practice for viruses to leverage the expected countermeasures of security software, as part (or all) of their payload.

For example, the authors of the various Netsky (etc) worms know that for every mail their software sends, at least one more of the "you sent us a virus" variety will be sent by a corporate e-mail gateway virus scanner.

Once any type of automated retaliation is in place, exactly the same thing will happen. Indeed, there's plenty of potential for DOS attacks, eg if someone in company X can forge an attack as being "from" their rivals at company Y.

⚡ Re: Attacking the attackers: maybe not a good idea ([RISKS-23.43](#))

<Curtis Karnow <cekarnow@yahoo.com>>

Mon, 28 Jun 2004 11:39:52 -0700 (PDT)

Attacking the attacker may or not be a good idea: there are public relations, and practicalities to consider. In many cases, it's a very bad idea. But if done correctly (accurate, targeted, no or [relatively] little collateral damages) it might be legal. See

my

"Launch On Warning: Aggressive Defense of Computer Systems," 8
Cyberspace Lawyer 4 (March 2003); rewritten and published at
[http://islandia.law.yale.edu/isp/digital%20cops/papers/
karnow_newcops.pdf](http://islandia.law.yale.edu/isp/digital%20cops/papers/karnow_newcops.pdf)

★ **REVIEW: "Exploiting Software", Greg Hoglund/Gary McGraw**

<Rob Slade <rslade@sprint.ca>>

Mon, 28 Jun 2004 08:23:22 -0800

BKEXPLSW.RVW 20040531

"Exploiting Software", Greg Hoglund/Gary McGraw, 2004, 0-201-
78695-8,

U\$49.99/C\$71.99

%A Greg Hoglund

%A Gary McGraw

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

%D 2004

%G 0-201-78695-8

%I Addison-Wesley Publishing Co.

%O U\$49.99/C\$71.99 416-447-5101 fax: 416-443-0948

%O [http://www.amazon.com/exec/obidos/ASIN/0201786958/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0201786958/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0201786958/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0201786958/robsladesinte-21)

[http://www.amazon.ca/exec/obidos/ASIN/0201786958/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0201786958/robsladesin03-20)

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0201786958/robsladesin03-20)

%O [http://www.amazon.ca/exec/obidos/ASIN/0201786958/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0201786958/robsladesin03-20)

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0201786958/robsladesin03-20)

%P 471 p.

%T "Exploiting Software: How to Break Code"

I have learned to beware of books with titles like this, which
generally indicate a hastily compiled set of old vulnerabilities,
benefitting nobody save the author. This work, however, turns
out to
have a lot of value for those interested in security of software.

Although it does not deal with the factors inherent in software that almost ensure problems, chapter one outlines the fact of bugs in software, the relative rate and increasing prevalence, and future developments that may exacerbate the issue. Chapter two provides taxonomies of general types of software problems (distinguishing, for example, between a bug and a flaw), patterns of attack activities (pointing out that most exploits are used in combination), and types of system scanning activities (used to determine specific attacks that might be effective). This material is very useful in structuring the debate about software exploits and attacks in general, but, ironically, the chapter (and book) itself could benefit from better organization. Reverse engineering, both via black box testing and through code analysis, is described in chapter three. The discussion is general, and presents the different activities that can be undertaken, usually at a fairly abstract level. (This is not true in all cases: there is a chunk of twelve pages of code for a plug-in module and eight pages of script for the IDA disassembler, which is of questionable utility, depending on the familiarity the reader may have with that particular program.)

At this point in the book, the issue of the validity of the "learn to exploit in order to learn to protect" philosophy should be addressed. In general, the "hack to protect" books do not provide much that is of value for the defenders. That statement is not necessarily true of this work. Since most of the presentation is at a conceptual level, it is the ideas, and not particular exploits, that are being

reviewed.

The authors are explaining tools and techniques that, yes, can be used by attackers, but can equally be used by those who wish to probe a given system for weaknesses in order to determine vulnerabilities to be patched. (There appears to be only one exception in chapter three:

the authors note that vendor patches tend to act as a roadmap for vulnerabilities, and it is difficult to say how this technique is useful for defence, other than to note that the probability of an exploit increases after a patch has been issued.)

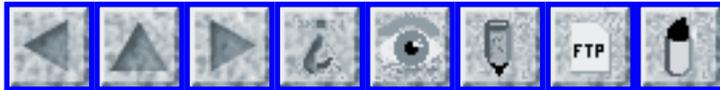
Chapter four lists types of attacks on server software, while five looks at clients, primarily web browsers. Indications pointing to patterns of malformed input that are likely to generate successful exploits are described in chapter six. The classic and ubiquitous buffer overflow gets a detailed explanation (supported with a number of examples) in chapter seven, which has a strangely extensive section on RISC (Reduced Instruction Set Computer) architectures. Chapter eight is rather disappointing in light of the tone of the rest of the book: it is primarily concerned with how to create and program rootkits, and the worth for defence is doubtful.

While ultimately of greatest use to a rather select audience (those specifically concerned with finding and patching loopholes in software), this book does have a lot to say to most security professionals. The security aspects of software development tend to be glossed over too quickly in most general works on security. Specific examples of malformed input are used, in too many security texts, as evidence of the author's superior security erudition,

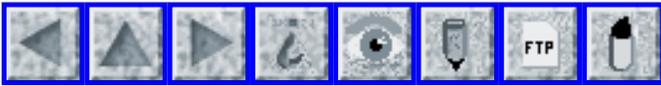
rather

than to explain the underlying concepts. Hوجلund and McGraw have prepared solid tutorials and definitions of these important ideas (although one could wish that they had prepared the arrangement of the book with the same degree of care).

copyright Robert M. Slade, 2004 BKEXPLSW.RVW 20040531
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

Volume 23: Issue 45

Saturday 10 July 2004

Contents

- [\\$500 million and counting](#)
[Tom Gray](#)
- [Keyless remotes to cars suddenly useless](#)
[Paul Saffo](#)
- [Stolen: one-third of the world's software](#)
[NewsScan](#)
- [Obstacles to Net phone service](#)
[NewsScan](#)
- [Zinc whiskers](#)
[Craig S. Bell](#)
- [Friends don't let friends use Microsoft Internet Explorer](#)
[Tom Van Vleck](#)
- [Bev Harris crusades to expose e-voting flaws](#)
[Fredric L. Rice](#)
- [E-voting concerns](#)
[NewsScan](#)
- [Perils of Database Matching, Chapter 47,061](#)
[Paul Wallich](#)
- [Private-sector firm maintains dossiers in U.S.](#)
[David Marston](#)
- [Re: Web ads threat to bank security](#)
[Rich Kulawiec](#)
- [E-mail non-privacy is a good decision!](#)
[Craig DeForest](#)

- [VoIP hacks gut Caller I.D.](#)
[Monty Solomon](#)
 - [Using google against google](#)
[Peter Parker](#)
 - [Re: Coca-Cola Cans as Security Threat](#)
[Nick Brown](#)
 - [REVIEW: "Network Security Jumpstart", Matthew Strebe](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ \$500 million and counting (from Dave Farber's IP list)

<Tom Gray <tom_gray_grc@yahoo.com>>

July 10, 2004 6:00:25 AM EDT

It is not mentioned directly, but this \$500 million dollar computer system owned by the Ontario government is incapable of adjusting the social assistance rates. Recipients will be receiving two lump sum payments, one this summer and one in the fall, to make up the 3% increase that the government has decided on.

How can a computer system cost \$500,000,000? Just how can training by itself consume hundreds of millions of dollars? Why if a program cost \$500,000,000 to produce does it not work?

[I guess you have not followed the IRS and FAA modernization fiascos, each over \$4 Billion, discussed in RISKS... The more money spent, the less likely it seems success will follow. PGN]

http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1089411015907&call_pageid=968332188492&col=968793972154

How costly computer sparked a `nightmare':
Social services system `inflexible from Day 1,' expert says;
Government estimates fixing flaws could top \$10 million
Richard Brennan and Robert Benzie, Queen's Park Bureau

It seemed like a good idea at the time. An ideologically driven, cash-strapped Conservative administration wanted to reduce social assistance costs and increase the role of the private sector in government. In Jan 1997 then-premier Mike Harris contracted with Andersen Consulting to revamp the Ministry of Community and Social Services' outdated computer system. But a two-year independent study of the \$500 million computer system has concluded that it has been seriously flawed from the very beginning and virtually incapable of making timely changes. That became clear when it was learned the system, responsible for distributing welfare and disability benefits to 670,000 Ontarians, is unable to calculate a 3 per cent increase, the first rise in 11 years. It's going to cost at least \$10 million to fix the problem -- \$3 million to correct the computer system and an additional \$7 million to test it.

⚡ Keyless remotes to cars suddenly useless

<Paul Saffo <psaffo@iftf.org>>
Mon, 5 Jul 2004 11:55:26 -0700

Increasingly we hear sagas of entire shopping center parking lots (and less widespread cases) in which keyless remote entry devices for automobiles are inoperative. For those of you with such systems, an article by Joshua Partlow with the above caption may be of particular interest. Waldorf (15 miles from Andrews Air Force Base in Charles County MD), Bremerton Washington, Las Vegas, etc. (The Florida Panhandle garage-door openers jammed from Eglin Air Force is also mentioned, noted previously in RISKS.)
[PGN; county/state correction in archive; mea culpa]

"Keyless entry remotes have become standard in new cars in recent years. Of the more than 14 million cars and light trucks produced in the United States last year, 77 percent came with the remotes, up from 32 percent in 1996." "... unlike other more powerful radio signals, keyless entry remotes are not licensed by the Federal Communications Commission. They are allowed to operate on frequencies used by licensed customers as long as their signals are sufficiently weak and don't interfere with others. But because of this outlaw status, their

own signals can be jeopardized."

[Source: Joshua Partlow, **The Washington Post**, 5 Jul 2004; PGN-ed]
<http://www.washingtonpost.com/wp-dyn/articles/A28217-2004Jul4.html>

⚡ Stolen: one-third of the world's software

<"NewsScan" <newsscan@newsscan.com>>
Wed, 07 Jul 2004 08:26:19 -0700

The Business Software Alliance, a trade group, says that 36% of all the software in the world has been pirated, costing the industry \$29 billion in lost revenue. The five countries with the highest incidence of pirated software are: China (92%), Vietnam (92%) and Indonesia (88%), Ukraine (91%), and Russia (87%). (AP/**San Jose Mercury News**, 7 Jul 2004; NewsScan Daily, 7 Jul 2004]
<http://www.siliconvalley.com/mld/siliconvalley/9097724.htm>

⚡ Obstacles to Net phone service

<"NewsScan" <newsscan@newsscan.com>>
Tue, 06 Jul 2004 08:29:13 -0700

AT&T says it expects to have 1 million customers for its voice-over-Internet-protocol (VoIP) phone service by the end of next year, and cable-TV company Comcast expects to offer VoIP all its customers by the end of 2006; however, Mark Main of the British consulting firm Ovum warns that -- although everyone will be using VoIP 10 or 15 years from now -- the road to that point "will be quite varied, quite torturous [tortuous?] and not at all clean." Some obstacles in the way: only 27% of U.S. online users have even heard of it; a VoIP subscriber needs a broadband connection, and

phone service will be only as good as that broadband connection; prices may go up in the future due to increased regulation and taxes; and VoIP service, which depends on the regular power grid, will fail if grid should fail. [AP/*San Jose Mercury News*, 6 Jul 2004; NewsScan Daily, 6 Jul 2004] <http://www.siliconvalley.com/mld/siliconvalley/9089156.htm>

⚡ Zinc whiskers

<"Craig S. Bell" <craig@runbox.com>>
Thu, 08 Jul 2004 15:37:17 -0700 (PDT)

The zinc coating on the underside of datacenter floors can emit tiny metallic whiskers, which could lead to abnormally high rates of electronic equipment failure:

http://nepp.nasa.gov/whisker/other_whisker/

The State of Colorado recently suffered a non-trivial outage, apparently due to zinc whiskers:

<http://www.denverpost.com/Stories/0,1413,36%257E33%257E2245069,00.html>

⚡ Friends don't let friends use Microsoft Internet Explorer

<Tom Van Vleck <thvv@multicians.org>>
Tue, 6 Jul 2004 08:41:29 -0400

<http://isc.incidents.org/diary.php?date=2004-06-29>

Describes an attack on IE where a file named imglbig.gif installs and runs an IE Browser Helper Object that steals information before SSL transmission and sends copies to <http://www.refestltd.com/cgi-bin/yes.pl>

Visit the wrong website and your IE is invisibly bugged.

⚡ **Bev Harris crusades to expose e-voting flaws**

<"Fredric L. Rice" <damoclese@skeptictank.org>>

Tue, 06 Jul 2004 22:20:59 -0700

Ambushing registrars and tracking down executives at their homes and offices, Harris, 52, has uncovered conflicts of interests and security laws inside the companies that make electronic ballot machines. Searching the Web and poring over newspaper clippings, Harris has unearthed obscure arrest records, ties to conservative political groups and other embarrassing secrets of senior executives at voting companies.

<http://www.cnn.com/2004/TECH/07/05/profile.e.voting.ap/index.html>

Her conclusion: there will be so many problems with the more than 100,000 paperless voting terminals to be used in the November presidential election that the fiasco will dwarf Florida's hanging chad debacle of 2000.

⚡ **E-voting concerns**

<"NewsScan" <newsscan@newsscan.com>>

Thu, 08 Jul 2004 07:57:24 -0700

California's Secretary of State has won a victory in federal court and new agreements from counties with touch-screen machines to make extra security arrangements. U.S. District Judge Florence-Marie Cooper denied requests by disability rights activists and four California counties to overturn the Secretary's conditional April 30 ban on touch screens for the November election. In the suit, disability groups argued that banning electronic voting will deny hundreds of thousands of people the right to vote in private, but the judge ruled the Americans With Disabilities Act requires only that disabled voters be given the opportunity to vote. [Bloomberg News/*San Jose Mercury News* 7 Jul 2004; NewsScan Daily, 8 Jul 2004]

<http://www.siliconvalley.com/mld/siliconvalley/9100600.htm>

⚡ Perils of Database Matching, Chapter 47,061

<Paul Wallich <pw@panix.com>>

Sat, 10 Jul 2004 09:48:37 -0400

(if a bunch of people haven't sent this already)

The New York Times reports this morning

<<http://www.nytimes.com/2004/07/10/national/10florida.html?hp=&pagewanted=print&position=>>

that the reason for the extraordinary paucity of hispanic voters on the latest Florida felon-purge list was the lack of a "hispanic" category in the felon database, so that race-matching against voters who identified themselves as hispanic would automatically fail. (This on top of not having bothered to check whether any of the felons had has their rights restored.)

"The method uses race as one of several factors in determining whether a felon has registered to vote. If a voter's first name, last name and date of birth are the same as those of a convicted felon but the race is different, the name is not put on the list for potential purging.

But the database of felons has only five variables for race: white, black, Asian, Indian and unknown. And a voter registered as Hispanic whose name and birth date matched a felon's would be left off the purge list unless his race was listed as unknown. ...

The paucity of Hispanic voters on the felon list was first reported Wednesday, by The Sarasota Herald-Tribune, but officials said then that the problem was not systematic. After The New York Times examined the data, state officials acknowledged that the method for matching lists of felons to those of voters automatically exempted all felons who identified themselves as Hispanic.

...The exclusion of Hispanics from the purge list explains some of the wide discrepancies in party affiliation of voters on the felon list, which bears the names of 28,025 Democrats and just 9,521 Republicans, with most of the rest unaffiliated."

Pretty much anyone who has ever tried to match items in one database against those in another knows that you have to get the record formats and categories right for the results to mean anything. In this case, even the simplest of properly-prepared test data sets would have

uncovered the screwup. (And now I'm trying to decide whether it's scarier to think that there was malice involved or that a bunch of ostensible paid professionals with more than two years two work on the problem could hand over a list like this with straight faces.)

PS. And these are some of the same folks who are supposedly evaluating the quality of paperless voting machines?

✈ Private-sector firm maintains dossiers in U.S.

<"David Marston" <marston@mv.mv.com>>

4 Jul 2004 22:08:58 -0400

The 28 Jun 2004 issue of Mass. High Tech ("The Journal of New England Technology") has a page 1 story about LocatePlus of Beverly, MA. The news angle is that a unit of the Massachusetts State Police will upgrade their use of LocatePlus from CD-ROMs of vehicle records to wireless access (via Blackberry) to all LocatePlus data.

Checking locateplus.com reveals that they offer some data (public records) to the public and more to licensed private investigators and the like, but law enforcement customers get everything, including non-public information. The website does not say (where I could see it, at least) how to opt out or correct erroneous information about oneself.

The MHT article says that LocatePlus claims to have information on 98% of the U.S. population (note: not just adults), including residence data, "court filings" and "restricted government data." Banks can "verify" Social Security numbers against whatever data LocatePlus has, and can use the service to screen for illegal money laundering or funneling. There are nearly 16000 LocatePlus customers in all.

The RISKS are many. Wireless communication can be intercepted, and what

happens if a cop's Blackberry falls into the wrong hands? Data aggregation

depends on correctly matching the person across databases. If a private company has "restricted government data", how did they get it, and are they obligated to protect it and cleanse it as zealously as the agency from which it came? Are the customers obligated to provide their data to LocatePlus to help it amass information? As we know from credit bureaus, the standard for data accuracy is set by the satisfaction level of the paying customers rather than the data subjects; in the case of credit data,

those paying customers seem to tolerate a 20% error rate year after year.

They believe someone is a law enforcement agency on the strength of a printed letterhead. Add on the standard set of security concerns.

✉ Re: Web ads threat to bank security (From Dave Farber's IP list)

<Rich Kulawiec <rsk@gsp.org>>

July 7, 2004 8:06:10 AM EDT

> Security experts said updating virus software was the best protection.

But it's not. Oh, not that it isn't a good idea for people who are running operating systems which are susceptible to viruses, but like most security problems, a multi-layered approach is more likely to work, especially if one of the layers fails.

For example, in this case:

- use a robust browser, such as Mozilla: never use IE
- use a robust mail client, such as Thunderbird: never use Outlook
- subscribe to the -announce list for that browser and get in the habit of downloading new versions whenever there's a major new release OR a significant security fix
- disable pop-ups
- restrict use of cookies
- run a web proxy (I use Privoxy, www.privoxy.org) that adds another layer of defenses
- run anti-adware software (because it will catch things that AV software won't)
- if you insist on using a web browser to read your mail, then disable Javascript in it

- (better) turn off HTML interpretation in mail
- and so on.

Aside: it's fascinating how many of these articles say "email virus" when the proper term is "Microsoft Outlook virus" and "web threat" when the proper term is "Microsoft Internet Explorer security bug".

⚡ E-mail non-privacy is a good decision!

<zowie@euterpe.boulder.swri.edu (Craig DeForest)>

Mon, 5 Jul 2004 11:39:32 -0600

In the 3 Jul 2004 issue of RISKS, there were several articles about the recent court decision that e-mail is not private. Surprisingly, I must take a contrarian position: this is a good decision. One cannot legislate privacy; one can only give most users a false sense of security.

Consider, for example, the results of another legislated-privacy "solution": analog cellphones use normal, unencrypted broadcast radio to transmit conversations, so it is now illegal (in the U.S.A.) to build or buy a radio scanner that receives on those frequencies. As a result, a black market developed in radio scanners that were capable of receiving that frequency range. Meanwhile, people with analog cellphones continued for many years to hold private conversations on the airwaves, with occasionally hilarious results as scofflaws listened in anyway. The problem of broken privacy would be much less, if the cellphone companies had instead been forced to educate their users that they were essentially bellowing their conversation from a rooftop. (Of course, most people now use some sort of encryption as a side-effect of using digital cellphones.)

Long-time readers may recall that, as a younger and angrier man, I have ranted about similar discrepancies between the law and reality in the satellite-communications market: it is illegal (again, in the U.S.A.) to build a radio receiver that can receive satellite television. This despite the fact that (for many years) the television signals were being beamed directly into your backyard, unencrypted. If the proprietors don't want you to receive their radio signals, they should not be bombarding you with them in the first place -- or should encrypt them.

It's best to call a spade a spade: non-secure communications are non-secure, and people who use them should be aware of what they are getting. After all, truly private solutions (PGP, GPG and the like) do exist, and folks who expect privacy should use them.

⚡ VoIP hacks gut Caller I.D.

<Monty Solomon <monty@roscom.com>>

Wed, 7 Jul 2004 13:27:35 -0400

Implementation quirks in Voice over IP are making it easy for hackers to spoof Caller I.D., and to unmask blocked numbers.

By Kevin Poulsen, SecurityFocus Jul 6 2004 1:54PM

Caller I.D. isn't what it used to be.

Hackers have discovered that the handy feature that tells you who's calling before you answer the phone is easily manipulated through weaknesses in Voice over IP (VoIP) programs and networks. They can make their phone calls appear to be from any number they want, and even pierce the veil of Caller I.D. blocking to unmask an anonymous phoner's unlisted number.

At root, the issue is one of what happens to a nugget of authentication data when it leaves the tightly-regulated realm of traditional telephony, and passes into the unregulated domain of the Internet.

On the old-fashioned phone network, Caller I.D. works this way: your local phone company or cell phone carrier sends your "Calling Party Number" (CPN) with every call, like a return address on an envelope. Transmitted along with your CPN is a privacy flag that tells the telephone switch at the receiving end of the call whether or not to share your number with the recipient: if you have blocking on your line, the phone company you're dialing into knows your number, but won't share it with the person you're calling.

This arrangement relies on telephone equipment at both ends of the call being trusted: the phone switch providing you with dial tone promises not to lie about your number to other switches, and the switch on the receiving end promises not to reveal your number if

you've asked that it be blocked. In the U.S. that trust is backed by FCC regulations that dictate precisely how telephone carriers handle CPNs, Caller I.D. and blocking. Most subscribers have come to take Caller I.D. for granted, and some financial institutions even use Caller I.D. to authenticate customers over the phone. ...

<http://securityfocus.com/news/9061>

⚡ Using google against google.

<"Peter Parker" <peterparker@fastmail.fm>>
Fri, 09 Jul 2004 03:05:30 -0700

Good news for the spammers!!

As most of us are aware that Google provides various options/operators for writing effective queries. One of the operator is the "site:" option, which restricts the search to the website specified with this tag. Just tried googling for some gmail accounts with site:gmail.google.com and the results were a list of urls with the title "Link Already Used". The area of concern is that all these pages are actually error pages with a valid gmail user accounts.... so with a small script its very easy for some one to glean a list of _valid_ gmail accounts.

Do you have a gmail account?check if your name is already harvested ; -)

⚡ Re: Coca-Cola Cans as Security Threat (Dominey, [RISKS-23.44](#))

<BROWN Nick <Nick.BROWN@coe.int>>
Mon, 5 Jul 2004 14:05:41 +0200

The immediate RISKS to US national security are minimal - apart from anything else, the GPS signal won't work inside most office buildings - but taking it on trust that Coke has issued exactly 120 of these cans seems optimistic, and assuming that more than 100 or so will ever be found,

even
more so.

One would hope that either this promotion, or similar ones in the future,
will have some sort of self-limiting features to the technology - for example, limiting the time validity of the SIM cards.

🔥 REVIEW: "Network Security Jumpstart", Matthew Strebe

<Rob Slade <rslade@sprint.ca>>
Tue, 6 Jul 2004 09:25:12 -0800

BKNTSCJS.RVW 20030604

"Network Security Jumpstart", Matthew Strebe, 2002, 0-7821-4120-X,
US\$24.99/C\$39.95/UK#18.99

%A Matthew Strebe mbs+jumpstart@connectic.net

%C 1151 Marina Village Parkway, Alameda, CA 94501

%D 2002

%G 0-7821-4120-X

%I Sybex Computer Books

%O US\$24.99/C\$39.95/UK#18.99 800-227-2346 info@sybex.com

%O <http://www.amazon.com/exec/obidos/ASIN/078214120X/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/078214120X/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/078214120X/robsladesin03-20>

%P 365 p.

%T "Network Security Jumpstart"

The introduction states that this book is suitable for anyone from the home user to the network administrator to the CEO. Which is a pretty tall order.

Chapter one has a decent overview of why computers aren't secure, a scant computer security history, a few security concepts, and a fairly trivial set of "review" questions. There is a media level exposition on "hackers," in chapter two, a rough outline of intrusion procedures, and a list of specific attacks that I'm not sure the author fully understands. (Immediately following "Denial of Service" comes a separate entry for "Floods": flooding being a type of denial of service.) There is a terse introduction to cryptography, and not much more than chapter one gave us about authentication, in chapter three.

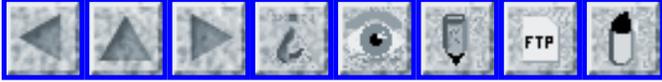
The suggestions for policy creation, in chapter four, aren't bad for simple cases, but seriously understate the difficulty of establishing a full policy, even for home users. Chapter five describes firewalls (and seven tells a little bit more about using them at home). Chapter six makes the common mistake of assuming that all VPNs (Virtual Private Networks) are about confidentiality: some are merely about managing communications configurations.

There is some correct and useful information about viruses in chapter eight, but it is unfortunately mixed in with a lot of garbage. Windows NT and its subsequent versions are **not** immune to viruses, although a rigorous set of file permissions can reduce your risk of file infectors (which are no longer a major category anyway). Signature scanners are **not** the only type of antiviral software. Viruses were **not** invented by accident, BRAIN **never** had an onscreen display and didn't infect program files, and neither Stoned nor Jerusalem (Friday the 13th is one variant) were based on BRAIN. Neither Stoned nor BRAIN relied on program sharing to propagate: data disks were quite sufficient. Viruses that only replicate are **not** benign (anybody ever have problems with Stoned? Melissa? Loveletter?), **will** be discovered, and scanning signatures **are** created.

Fault tolerance, in chapter nine, is not quite business continuity planning (BCP), but does go beyond the usual UPS (Uninterruptible Power Supply) and backup recommendations. Although chapter ten lists a number of security mechanisms in Windows, a practical understanding of their use is not presented. The UNIX tools in eleven are described more usefully--but they only relate to file permissions. The network security tools for UNIX are in twelve--but are only enumerated. Chapter thirteen has good suggestions for Web server security--but doesn't say how to implement them. A random collection of e-mail security tools and threats makes up chapter fourteen. IDS (Intrusion Detection System) concepts are not explained very well in chapter fifteen: Strebe apparently doesn't understand that all forms use audit data of one type or another, and doesn't list the major distinctions between either the engine type or sensor location.

Even given all the faults, one has to admit that Strebe has not done a bad job with his ambitious intent. Certainly home users and CEOs can find better explanations here than in many of the other works aimed at them, however much I might wish that the book as a whole was more accurate. And, yes, even the network administrators might find some helpful points in the more conceptual material at the beginning of the book: most of them could do with a better understanding of the need for policy. This work isn't great, by any means, but it can fulfill a need for a quick guide to network threats, for a variety of audiences.

copyright Robert M. Slade, 2004 BKNTSCJS.RVW 20030604
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

Volume 23: Issue 46

Thursday 29 July 2004

Contents

- [*Chicago Tribune* computer meltdown](#)
[J H Haynes](#)
- [Balloon stuck over Baltimore, risk of automatic shutdowns](#)
[Dave Provine](#)
- [NASA space station software repairs](#)
[James Paul](#)
- [Laptops at the FleetCenter at risk of breaches, attack](#)
[Hiawatha Bray via Monty Solomon](#)
- [Censorware deletes Japanese city](#)
[John S. Karabaic](#)
- [Using Google against Google!](#)
[Peter Parker](#)
- [Court Opens Door To Searches Without Warrants](#)
[Monty Solomon](#)
- [Risks of ordinary GUI "pop-up" windows?](#)
[Daniel P. B. Smith](#)
- [Windows XP SP2 Installation Failures](#)
- [Should we trust them?](#)
[Bruce Sinclair via Dawn Cohen](#)
- [Citibank 'sorry' for current account difficulties](#)

[Patrick O'Beirne](#)

- [Citibank assists scammers](#)

[Keith Gregory](#)

- [Cosmic ray hits Brussels election - really?](#)

[Dirk Fieldhouse](#)

- [Florida faces vote chaos in 2004, Commission hears](#)

[Fredric L. Rice](#)

- [Lost Record '02 Florida Vote Raises '04 Concern](#)

[Joe Shead](#)

- [Counting error on SMS poll evicts wrong contestant from 'Big Brother'](#)

[George Michaelson](#)

- [California Online Privacy Protection Act](#)

[Monty Solomon](#)

- [iPod security](#)

[Paul Wexelblat](#)

- [Re: E-mail nonprivacy](#)

[David Cantrell](#)

- [Re: Keyless remotes to cars suddenly useless](#)

[Chuck Charlton](#)

- [Re: "Stolen:" one-third of the world's software](#)

[Pascal J. Bourguignon](#)

- [Update: DC Metro flag-day issues](#)

[Joe Thompson](#)

- [REVIEW: "The Sundering", Walter Jon Williams](#)

[Rob Slade](#)

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

✶*Chicago Tribune* computer meltdown

<jhhaynes@earthlink.net>

Tue, 20 Jul 2004 11:50:51 -0500 (CDT)

Beginning at 5:30am on Sunday morning 18 Jul 2004, the *Chicago Tribune*

began a planned upgrade of their server systems and their

Newsdesk software
(developed by Denmark-based CCI Europe A/S). By noon,
everything tested out
OK. However, around 4pm, proofing pages for the Monday morning
paper could
not be generated. At 7pm, pages sent to the off-site Freedom
Center
printing facility would not produce plates. A third-party
trouble-shooter
(CCI in Denmark) was called in. At 9:45pm, the disaster-
recovery backup
system was considered, but CCI thought that would not be
necessary. At
1:30am Monday sending scanned pages to Freedom Center was
abandoned as
taking too long, and preparations were made to switch back to
the backup
plan. However, by 2am some pages were correctly processed, and
a hybrid
plan was cobbled together. Finally, at 3am, the paper was
abbreviated to 24
pages and printed -- except for four pages that would not print,
and which
were replaced by advertisements. Production of the paper was
finally begun
at 5:30am, well beyond the normal time. It was reportedly the
first time
since the Great Chicago Fire of 1871 that the *Tribune* failed
to print as
planned. Source: Computer glitch nearly stops Tribune presses;
A story we
never thought we'd print, James Coates, *Chicago Tribune*, 20
Jul 2004;
starkly PGN-ed; also noted by Rich Harrington; PGN-ed]

🚨 Balloon stuck over Baltimore, risk of automatic shutdowns

<Dave Provine <dave@premiermac.com>>

Sun, 18 Jul 2004 08:14:34 -0400

A tourist balloon tethered over downtown Baltimore stalled during a wind squall on 17 Jul 2004, with 17 occupants stranded 200 feet in the air for two hours, amid strong wind gusts that swung the balloon around the tether, resulting in the computer control system losing track of the balloon's position -- which apparently automatically shut down the winch engine. Because the program cannot restart the engine unless the balloon is on the ground, a smaller backup engine was invoked -- although an added complication was involving releasing the brakes that had automatically clamped on the winch. (This was supposed to be a 20-minute excursion.) Four people were hospitalized. [*The Baltimore Sun*, 18 Jul 2004; PGN-ed]

<http://www.baltimoresun.com/news/local/bal-te.md.balloon18jul18,0,4500292.story?coll=bal-home-headlines>

NASA space station software repairs

<"James Paul" <James.Paul@mail.house.gov>>
Thu, 29 Jul 2004 01:17:48 -0400

John Kelly, NASA begins repairing station glitches, 29 Jul 2004

NASA and the Russians are beaming a series of software-upgrade files from

Earth to several International Space Station computers with the goal of

eliminating hundreds of potentially dangerous glitches before year's end.

The carefully scheduled updates are meant to fix about 500 of the more

than 1,000 errors in the computer code that operates everything from the space station's robot arm to critical life-support systems. Most notably, the repairs are expected to fix 35 of 39 software bugs that were deemed "safety critical" in a review done by the space station program in the wake of the shuttle Columbia disaster.

Source:

<http://www.floridatoday.com/news/space/stories/2004b/spacestoryN0729STATIONBUG.htm>

Earlier items:

<http://www.floridatoday.com/news/space/stories/ISS2004/spacestoryONSFTWARE06.htm>

🔥 Laptops at the FleetCenter at risk of breaches, attack (H.Bray)

<Monty Solomon <monty@roscom.com>>

Fri, 23 Jul 2004 17:02:09 -0400

Hiawatha Bray, *The Boston Globe*, 22 Jul 2004

The Democratic National Convention will attract thousands of visitors armed with laptop computers that feature wireless Internet access. And that could be a formula for disaster, according to Michael Maggio, whose Newbury Networks Inc. recently ran a vulnerability test in the area around the FleetCenter: Unless proper precautions are taken, computer vandals will be able to tap into these laptops by using wireless transmitters located outside of the FleetCenter. The attackers could then use the compromised

laptops to gain access to the computer network used to run the convention.

http://www.boston.com/business/technology/articles/2004/07/22/laptops_at_the_fleetcenter_at_risk_of_breaches_attack/

✶ **Censorware deletes Japanese city**

<"John S. Karabaic" <risks@exnext.com>>

Fri, 16 Jul 2004 11:03:14 -0400

Censorware installed either at the LinuxElectrons or IBM press release site has inadvertently deleted part of the name of a Japanese city in a press release from IBM:

<http://www.linuselectrons.com/article.php/20040714101727502>

relevant excerpt:

The trial is expected to be completed by early August and then, if successful, onsite testing will take place at Kureha Environmental Engineering's waste processing site. When the effectiveness of RFID tagging is confirmed the company plans to equip Kureha General Hospital, in *censored*ushima, Japan, with the RFID technology to track their discarded medical waste.

John Karabaic, 3545 Zumstein Ave, Cincinnati OH 45208-1309
513.295.6365

✶ Using Google against Google!

<"Peter Parker" <peterparker@fastmail.fm>>

Fri, 09 Jul 2004 03:05:30 -0700

Good news for the spammers!!

As most of us are aware that Google provides various options/operators for writing effective queries. One of the operator is the "site:" option, which restricts the search to the website specified with this tag. Just tried googling for some gmail accounts with site:gmail.google.com and the results were a list of urls with the title "Link Already Used". The area of concern is that all these pages are actually error pages with a valid gmail user accounts.... so with a small script its very easy for some one to glean a list of `_valid_ gmail` accounts.

Do you have a gmail account?check if your name is already harvested ;-)

✶ Court Opens Door To Searches Without Warrants

<Monty Solomon <monty@roscom.com>>

Tue, 27 Jul 2004 18:08:02 -0400

It's a groundbreaking court decision that legal experts say will affect everyone: Police officers in Louisiana no longer need a search or arrest warrant to conduct a brief search of your home or business.

Leaders in law enforcement say it will keep officers safe, but others argue it's a privilege that could be abused. The decision in United States v. Kelly

Gould, No. 0230629cr0, was made March 24 by the New Orleans-based 5th

Circuit Court of Appeals. ... [29 Mar 2004]

<http://www.theneworleanschannel.com/news/2953483/detail.html>

<http://caselaw.findlaw.com/data2/circs/5th/0230629cr0p.pdf>

<http://caselaw.findlaw.com/data2/circs/5th/0230629cv0p.pdf>

<http://caselaw.lp.findlaw.com/data2/circs/5th/0230629cv0p.pdf>

✶ Risks of ordinary GUI "pop-up" windows?

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

Wed, 28 Jul 2004 11:08:18 -0400

Yesterday, I was annoyed yet again--by Mac OS X, as it happens, but OS X and WinNT/2K/XP are equal-opportunity annoyers in this regard. I was about to hit "return" to accept the default in a dialog box, and another application that was running at the same time popped up its own dialog box just as I was pressing the key. I couldn't stop in time. I intended to OK one dialog box, and I ended up OK-ing a completely different one.

No harm done this time. But this sort of thing happens to me several times a week. Frequently I will type two or three keystrokes into a window that has unexpectedly popped up before I can stop myself. Occasionally I will actually mouse-click on a button in a window that popped up just as I was

starting to press the mouse.

It seems astonishing to me that nobody complains about this, and that in twenty-odd years of GUI use there isn't a well-established solution to this problem. It appears that when it comes to computer usability, any problem that persists for more than a few years is apparently no longer perceived as a problem. Or am I the only person this happens to?

The RISKS when a user who intends to confirm one dialog box accidentally confirms another are obvious. Serious consequences in ordinary daily use are admittedly unlikely; contriving a suitably example will be left as an exercise for the reader.

⚡ Windows XP SP2 Installation Failures

<[identity withheld by request]>

Fri, 23 Jul 2004 20:08:49 PDT

Some choice bits from this site:

<http://www.crn.com/sections/breakingnews/breakingnews.jhtml?articleId=23905071>

"CRN Test Center engineers evaluated a release candidate two (RC2) version of SP2, and upon completion of the install on three out of five systems, the machines blue-screened."

"[Microsoft] provided instructions on how to work around the blue screen and uninstall SP2. After that process finished, some

interesting events

occurred. The rollback process uninstalled every device that existed in

the PC. Network cards, video cards and all system resources were

uninstalled. The rollback also removed SP1; absolutely no remnants of SP1

existed anywhere in the system. "

If they can't get the installation process right, I highly doubt they got the security fixes right either.

✶ Should we trust them? (Bruce Sinclair)

<Dawn Cohen <cohend64@yahoo.com>>

Thu, 29 Jul 2004 07:03:26 -0700 (PDT)

Here's one from the absurd department...

(As reported on <http://www.netfunny.com/rhf/jokes/04/Jul/cia.html>)

Did they really say that ?

bruce.sinclair@NOSPAMagresearch.NOTco.NOTnz (Bruce Sinclair)
TelstraClear

Found recently on a web site as part of a privacy policy statement ...

[<http://www.odci.gov/cia/notices.html#priv>]

Privacy Notice: The Central Intelligence Agency is committed to protecting

your privacy and will collect no personal information about you unless you

choose to provide that information to us.

✂ Citibank 'sorry' for current account difficulties

<"Patrick O'Beirne" <pob2004@sysmod.com>>

Wed, 28 Jul 2004 12:19:45 +0100

<http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1087373456479>

Customers of Citibank, the world's largest bank, are suffering a wave of current account service problems that has forced the company to post a seven-page "service update" explanation on its website.

The bank admitted receiving complaints from customers over direct debit payments which mistakenly defaulted to 999,999.99 pounds and personal identification numbers for automatic teller machines, internet and telephone banking that did not work.

Other problems included current accounts being debited twice, incorrect reference and cheque numbers, changes to statements, canceled cheques and replacement cheque books and cards being sent to old or wrong addresses.

Citibank said that it was "very sorry" about the problems, which were caused by a large systems upgrade in late March that triggered a big increase in the volume of calls from customers.

Patrick O'Beirne, Systems Modelling Ltd. +353 55 22294 www.sysmod.com/blog

✂ Citibank assists scammers

<"Keith Gregory" <kgregory@gestalt-llc.com>>

Thu, 22 Jul 2004 09:30:11 -0400

Today an a phishing scam e-mail got past the spam filters. It had the usual wording about clicking on the link to update my e-mail address with CityBank, which "required" my ATM card and PIN.

The strange thing about the URL was it wasn't the expected "this site @ that site", instead, it began with: <http://www.citi.com/domain/redirect>

... YIPES!

Sure enough, replacing the scammer's URL with Google's took me to Google ... which didn't like the Citibank-specific query string. Being curious, I clicked on the original URL, and was taken to what appeared to be the Citibank site, after bouncing around a while. Needless to say, I exited Mozilla after doing this.

✂ Cosmic ray hits Brussels election - really?

<"Dirk Fieldhouse" <fieldhouse@gmx.net>>

Thu, 29 Jul 2004 13:04:14 +0100

John Miller, Dow Jones Newswires (07/26/04); seen via ACM Tech News:

<http://www.acm.org/technews/articles/2004-6/0728w.html#item1>

"European citizens and governments generally prefer traditional paper-based voting because of unresolved reliability and security issues surrounding electronic voting. ...

[DF comment: what a fair summary, and in the UK issues are also being

raised by the extension of postal paper voting] ... Fueling the arguments of paper ballot supporters are incidents such as a 2003 Belgian election in which almost 4,100 extra votes for Maria

Vindevoghel's Communist Party were recorded in a precinct of Brussels due to a malfunction triggered by a cosmic ray. ..."

I found this jaw-dropping -- not the possibility of a cosmic ray causing a computer malfunction, which is an obvious threat for space-borne systems,

but how such an apparently unrepeatable external event could be accepted as the cause of a terrestrial computer malfunction. The lack of any confirmation through Google seems to support my astonishment.

Can the select RISKS readership confirm whether this actually occurred, or is it an urban legend?

If people are prepared to accept this as an explanation for computer malfunctions, maybe we're wasting our time testing software?

✶ Florida faces vote chaos in 2004, Commission hears

<"Fredric L. Rice" <damoclese@skeptictank.org>>

Fri, 16 Jul 2004 20:02:05 -0700

Alan Elsner, Reuters, 15 Jul 2004

http://story.news.yahoo.com/news?tmpl=story&cid=584&e=3&u=/nm/20040715/pl_nm/campaign_florida_dc

Florida faces another debacle in the upcoming presidential election on Nov. 2, with the possibility that thousands of people will be unjustly denied the right to vote, the U.S. Commission on Civil Rights heard on Thursday.

✶ Lost Record '02 Florida Vote Raises '04 Concern

<"Joe Shead" <Joe@sheadprogramming.com>>
Wed, 28 Jul 2004 12:14:06 -0500

Almost all the electronic records from the first widespread use of touch-screen voting in Miami-Dade County have been lost. [Abby Goodnough, *The New York Times*, 28 Jul 2004]
<http://www.nytimes.com/2004/07/28/politics/campaign/28vote.final.html?ex=1092033819&ei=1&en=5808587bdbefd3a6>

✶ Counting error on SMS poll evicts wrong contestant from 'Big Brother'

<George Michaelson <ggm@apnic.net>>
Mon, 5 Jul 2004 16:36:27 +1000

Big Brother evictee returns after SMS error
<http://www.abc.net.au/news/newsitems/200407/s1147056.htm>

The most recent evictee from the Big Brother reality television household,

Bree, will return to the show tonight after the company which tallies telephone and SMS votes for the show admitted it made an mistake.

Bree was voted out of the show last night but Channel Ten, which airs the show, and Endemol Southern Star, its producers, have released a statement admitting the vote count was wrong.

Apparently this was detected by the phone/SMS company by an internal audit so at one level, 'the system worked' but there are so many questions about HOW they counted SMS votes wrong..

I'm guessing this is not a very integrated process, and somebody either slipped up doing spreadsheet column/field edits, or in parsing data.

With \$AU 1,000,000 up for grabs in a winner-takes-all outcome, I think both the phone company and the TV station felt it was better to head off litigation. Else, why does anybody care? its not like this is a 'real' vote is it...

(obvious comparisons to 'beauty contest' electronic election methods invited)

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

California Online Privacy Protection Act

<Monty Solomon <monty@roscom.com>>
Thu, 8 Jul 2004 08:44:05 -0400

Excerpt from

Piper Rudnick E-Commerce & Privacy Group @lert, 25 Jun 2004,
Vol. 4, No. 5

[http://www.piperrudnick.com/db30/cgi-bin/pubs/E-Commerce%
20Alert062504.pdf](http://www.piperrudnick.com/db30/cgi-bin/pubs/E-Commerce%20Alert062504.pdf)

CALIFORNIA LAW REQUIRING WEB SITES AND ONLINE SERVICES TO POST A
PRIVACY
POLICY GOES INTO EFFECT JULY 1, 2004

Overview and Summary of Requirements

On 1 Jul 2004, the first online privacy law in the country that
applies to
the collection of information from consumers over the age of 13
will take
effect.

The California Online Privacy Protection Act of 2003, CAL. BUS.
& PROF. CODE
22575 et seq., ("Section 22575") is a privacy notice requirement
law. It
contains a generous safe harbor that gives companies 30 days to
come into
compliance if notified of failure to post a policy. The law also
prohibits
"negligently and materially" or "knowingly and willfully"
failing to follow
promises in a posted privacy policy.

The California law will require operators of a commercial Web
site or online
service that collect through their Web site or online service
personally
identifiable information(1) from consumers(2) residing in
California to
conspicuously post their privacy policy on their Web site (or,
in the case
of an online service, to use any other "reasonably accessible
means of
making the privacy policy available to consumers"). The law

exempts Internet service providers and similar entities that transmit or store personally identifiable information at the request of third parties. Because many Web sites and online services do not collect physical address information, and for that reason may be unaware that they are collecting personally identifiable information from California consumers, sites and services may be well advised to conform their privacy policies to the requirements of this new law. ...

<http://www.piperrudnick.com/db30/cgi-bin/pubs/E-Commerce%20Alert062504.pdf>

⚡ iPod security

<Paul Wexelblat>

Tue, 13 Jul 2004 14:06:56 -0400

It appears that it has occurred to folks that the iPod is a security risk

<http://www.cnn.com/2004/TECH/internet/07/13/britain.mod.reut/index.html>

If someone who had access to that dangerous USB port were going to down/upload some data, wouldn't a thumb drive be easier and smaller?

If someone was serious, how hard would it be for a real baddie to give a CD player or Walkman (r) write capability.

Gee, why not just plug a WI-FI device into some obscure RJ45 and

get the
stuff in the parking lot? or a Zip disk, or a floppy, or a
laptop, or one of
those non-spec 10Xpower bluetooth thingies

Isn't it much more likely that this poor soul with the iPod is
just
trying to listen to music?

Paul Wexelblat, Dept. of Computer Science, University of
Massachusetts Lowell
One University Ave, Lowell, MA 01854

✶ Re: E-mail nonprivacy (DeForest, [RISKS-23.45](#))

<David Cantrell <d.cantrell@outcometechnologies.com>>

Mon, 12 Jul 2004 09:59:49 +0100

I read with interest Craig DeForest's recent message about
legislating for
privacy. His argument - which is far from new - is that because
legally
protecting email privacy wouldn't be 100% effective, legal
protection is
foolish. You could equally well say that because legislating to
outlaw
burglary is not 100% effective, you may as well not legislate
against
burglary. A foolish notion!

Laws won't stop determined evil-doers from doing bad things.
However, they
can be used to punish them after the fact, and do have a
deterrent effect on
evil-doers who are less brave. Just look at the effort
companies go to to
make sure they don't break (many) laws. Add privacy to that
list of laws

that they at least try not to break, and I for one will be a little happier.

⚡ Re: Keyless remotes to cars suddenly useless ([RISKS-23.45](#))

<Chuck Charlton <charlton@gmail.com>>

Mon, 12 Jul 2004 01:14:14 GMT

This isn't news and isn't sudden to those of us in San Francisco who shop at Tower Market. Keyless remotes to cars have never functioned in much of Twin Peaks area. The seven television stations and numerous FM radio stations that broadcast from Sutro Tower appear to overwhelm the low-power keyless systems used in nearby cars.

⚡ Re: "Stolen:" one-third of the world's software (NewsScan, [R-23.45](#))

<"Pascal J. Bourguignon" <pjb@informatimago.com>>

Sat, 10 Jul 2004 23:06:40 +0200

I won't comment on the risks of accepting the novlang, but wondering why all these people don't use free software instead, what are the risks they take in using non-free software, in their countries?

Assuming there's no legal risk for them, given the political and technical

risks of using non-free software, why don't they switch to free software?

✶ Update: DC Metro flag-day issues ([RISKS-23.44](#))

<Joe Thompson <kensey@gmail.com>>

Tue, 27 Jul 2004 17:09:09 -0400

Metro has now reversed their decision and declared they will continue to sell SmarTrip cards until the current inventory runs out, by which point they hope new shipments will have come in:

<http://www.wtopnews.com/index.php?nid=25&sid=234093>

"Taubenkibel says the agency decided to reverse course because it hopes to receive a new shipment of about 10,000 SmarTrip cards by the end of the month, and another 62,000 cards sometime in August."

✶ REVIEW: "The Sundering", Walter Jon Williams

<Rob Slade <rslade@sprint.ca>>

Wed, 28 Jul 2004 08:34:36 -0800

BKSNDRNG.RVW 20040629

"The Sundering", Walter Jon Williams, 2004, 0-380-82021-8

%A Walter Jon Williams

%C 10 East 53rd Street, New York, NY 10022-5299

%D 2004

%G 0-380-82021-8

%I HarperCollins/Basic Books/Torch

%O 800-242-7737 fax: 212-207-7433 information@harpercollins.com

%O <http://www.amazon.com/exec/obidos/ASIN/0380820218/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0380820218/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0380820218/robsladesin03-20>

%P 436 p.

%T "The Sundering"

Once upon a time, a long, long time from now (and far away) there was a great space war.

Given that it's a long time from now, it's rather bemusing that technology hasn't advanced very far, aside from discovering traversable wormholes and producing antimatter in commercial quantities. This isn't entirely the fault of human beings, since a mysterious and powerful race has come along and generally interfered with social and technological development, although they now seem to have stepped out for an extinction.

But you can forgive a lot to a book that understands that space battles, even those confined to a mere solar system, take place over days, and that the ability to withstand crushing accelerations for long periods of time is what makes the difference.

Faster than light communications would certainly help, but that may be too much to ask from the universe. Smarter computers would *definitely* help, and should have been possible.

The use and operation of computers in this brave new world is not clearly

spelled out, but they seem to run on scripts, rather than machine code. The mysterious and powerful race have ensured that all computers are registered and known, thus fulfilling Microsoft's dreams for Palladium. (Apparently no Linux hackers, or other amateur computer enthusiasts, have survived.) Serious cryptography seems to have been forgotten: there is one reference to the fact that nobody can use cryptography since everyone has powerful computers and can therefore break any ciphers. This indicates that everyone has forgotten that, when computer power increases, you can just increase the key length.

The fact that computers are known and registered is used to prove the need for low-tech communications solutions when the bad guys move in and take over the seats of power. However, a few pages later, our merry band of counter-revolutionaries is happily using communications devices that seem to have a lot of computer-related functions (even real-time broadcasts seem to be "store and forward").

Our underground heroine manages to become a fully-fledged intruder in the space of twenty-four hours. Along the way she does learn something that I wish every security professional knew: when you have functional security, you'd better have an assurance activity as well.

(Of course, if anyone had put "defence in depth" in place, she'd have been sunk.)

rslade@vcn.bc.ca
niu.edu

slade@victoria.tc.ca

rslade@sun.soci.

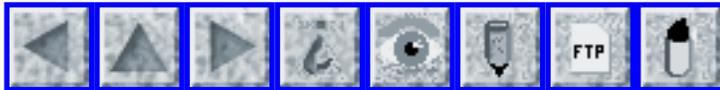
[http://victoria.tc.ca/techrev
~rslade](http://victoria.tc.ca/techrev/~rslade)

or

<http://sun.soci.niu.edu/>

[Rob, It's typically Weakness in Depth rather than Defense in Depth.

But I suppose things will not have changed much by then anyway. PGN]



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 47

Monday 2 August 2004

Contents

- [Computer Failure Grounds and Delays Flights on 2 Airlines](#)
[Monty Solomon](#)
- [E-voting critic issues challenge to hackers](#)
[PGN](#)
- [VoIP -- Voyeurism over Internet Protocol?](#)
[NewsScan](#)
- [Russian extortionists: each did his bit of work](#)
[NewsScan](#)
- [The Mr Micawber Syndrome](#)
[Michael Bacon](#)
- [Implementing Information Security: Risks vs. Cost](#)
[Gideon T. Rasmussen](#)
- [Re: Cosmic ray hits Brussels election -- really?](#)
[Peter B. Ladkin](#) [Dirk Fieldhouse](#) [Sergio Gelato](#)
- [REVIEW: "Official \[ISC\]² Guide to the CISSP Exam", Hansche et al.](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

Computer Failure Grounds and Delays Flights on 2 Airlines

<Monty Solomon <monty@roscom.com>>

Sun, 1 Aug 2004 23:39:46 -0400

A computer problem grounded American Airlines and US Airways flights from coast to coast on Sunday morning, causing delays that lasted all day. A computer company official said human error was the likely cause. American had its planes back up after two hours, while US Airways flights resumed after about three. [Source: Associated Press, 2 Aug 2004]
<http://nytimes.com/2004/08/02/national/02delay.html>

✶ E-voting critic issues challenge to hackers

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

Sun, 1 Aug 2004 13:44:40 PDT

At the annual Black Hat convention in Las Vegas last week, Rebecca Mercuri [who will be a Radcliffe Fellow at Harvard in the coming academic year] challenged computer hackers to test whether it is possible to rig an election held using the unauditable paperless electronic voting machines that have been a frequent subject of discussion in RISKS. She suggested the VoteHere software would be a good system to consider. She also urged other voting system companies to make their software available for scrutiny. ``I'm tired of hearing members of the election community say that no problems have occurred with electronic voting systems when every

election

there's plenty of newspaper reports of `glitches.' '' (Vendors have made such analyses difficult by keeping their software proprietary.)

[*San Jose

Mercury News*, 30 Jul 2004; PGN-ed]

<http://www.siliconvalley.com/mld/siliconvalley/9278952.htm>

✶ VoIP -- Voyeurism over Internet Protocol?

<"NewsScan" <newsscan@newsscan.com>>

Mon, 02 Aug 2004 10:03:45 -0700

With businesses and individuals flocking to Internet telephony as a cheap alternative to pricey landline phones, hackers are discovering new opportunities for eavesdropping and making mischief. Tapping phones by hacking into servers and hard drives is much easier than conventional wiretapping and analysts say even though very few incidents have been reported to date, it's just a matter of time. "Once you are running an Internet phone network, all those threats you worry about in the data world will be transferred to the voice world," says one security consultant. "Voice over Internet phones are not in the spotlight of hackers yet, but in this voyeuristic world, if someone can listen in on people's conversations and get a thrill, they will." In addition, voice packets offer new opportunities for disguising and distributing malignant code. "You can spoof a packet and insert myself into a communications flow," says a

systems

engineer for Mirage Networks. "This kind of threat has been around for a while for data, but now it will move into voice. As you see a broader

acceptance of voice over Internet, you'll see more spoofs." [*The New York

Times*, 2 Aug 2004; NewsScan Daily, 2 Aug 2004]

<http://www.nytimes.com/2004/08/02/technology/02virus.html>

✶ Russian extortionists: each did his bit of work

<"NewsScan" <newsscan@newsscan.com>>

Thu, 29 Jul 2004 08:56:38 -0700

Police authorities in Russia have broken up a hacker ring that extorted money from British bookmakers by flooding online betting sites with false requests for information in "denial-of-service" attacks and then sending e-mail demanding money for stopping the attacks. Investigators said that bookmaker companies were the most convenient prey because the attacks could be timed to major sport events. The ring consisted of well-educated people in their early 20s who had found each other on the Internet and agreed to work together in the extortion. A Russian police official said: "There was no chief organizer in plain terms, each of them did his bit of work. And they didn't consider themselves criminals." [AP 29 Jul 2004; NewsScan Daily, 29 Jul 2004]

<http://apnews.excite.com/article/20040728/D843R7EG1.html>

✶ The Mr Micawber Syndrome

<michael_bacon@synigystic.com>

Fri, 30 Jul 2004 07:22:49 +0100

Once again (in [RISKS-23.46](#)), we have examples of what I call the, "Mr Micawber Syndrome". This syndrome was exhibited very strongly in the stories about the problems of the *Chicago Tribune* and the DC Metro, and also to a certain extent in those about the tethered balloon operator in Baltimore, NASA, Microsoft, and the operators, regulators and promoters of electronic voting systems.

For the "bibliophilically-challenged", Charles Dickens' Mr Micawber was a man living on the bread-line for whom, always, "Something will turn up."

It appears that this mantra has become the de facto standard when things go wrong with technology today. My experience suggests that this very phrase (or one conceptually synonymous) is often contemporary with the "incident" becoming a "disaster" and, indeed, is probably the trigger for that disaster though its reinforcement of a belief-system.

However, the belief that the causation will be resolved in some short, and often very tightly stated, time-frame is seldom, if ever, factored into risk calculations, either beforehand or at the time. I have lost count of the number of times I have seen this behaviour -- and readers of

these pages
will have many more stories of a similar ilk.

The RISKS stem from: (1) not considering every "incident" as a potential "disaster"; (2) not pre-establishing a definite time following the recognition of an incident at which its severity will be escalated to that of a "disaster"; (3) not having a Regression Plan that has been tested and can be trusted; (4) not having a pre-set time at which the "Disaster Recovery" or "Business Continuity" plan is put into operation -- regardless of what else is happening; (5) not having senior managers who have been properly informed of the RISKS (both of doing something and of doing nothing); (6) having a belief in one's own abilities and those of one's suppliers that transcends the reality of past experience; (7) continually demonstrating an inability to learn from one's and others' mistakes; and (8) too boldly going where everyone has gone before ... and met the same fate!

Michael (Streaky) Bacon, Principal, Synigystic Ltd.

✶ Implementing Information Security: Risks vs. Cost

<"Gideon T. Rasmussen" <lists@infostruct.net>>

Thu, 29 Jul 2004 18:26:14 -0400

http://www.cyberguard.com/news_room/news_newsletter_040628security.cfm

Implementing Information Security: Risks vs. Cost

Gideon T. Rasmussen - CISSP, CISM, CFSO, SCSA

As a security professional who understands how the business world works, I wrote this article to convey the imperative need for security professionals and senior management to see eye-to-eye. Being motivated by business, senior management focuses on productivity and the bottom line. It is sometimes difficult to calculate a return on investment for security, but the damage caused by the absence of efficient controls is far greater than the cost of implementing them.

Over the past few years, there have been several highly publicized security incidents ranging from fraud to terrorism. These events demonstrated the need for disaster recovery plans and checks and balances within accounting systems. Many threats present themselves internally in the form of disgruntled or dishonest employees or as the result of social engineering. Human error and neglect are also examples of internal threats. New threats emerge daily. For more information, refer to the CSI/FBI Computer Crime and Security Survey (<http://www.gocsi.com/forms/fbi/pdf.jhtml>).

The U.S. is beginning to mandate information security based on the concepts of due diligence and the prudent man principle. The most recent examples are the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA). Compliance with government regulations represents a threat of a sort. Under SOX, senior

management is responsible for the accuracy of financial statements. Criminal penalties include fines of \$1-5 million and prison terms of 10-20 years. A popular international standard is the Code of Practice for Information Security Management (ISO 17799).

A variety of control frameworks have been developed to meet financial and IT security concerns. Two of the leading standards are the Internal Control - Integrated Framework - Committee of Sponsoring Organizations of the Treadway Commission (COSO) and Control Objectives for Information and related Technology (CobiT).

IT governance and compliance must be addressed with a formal information security program. Basic elements include security policies, an annual audit and internal controls to mitigate threats and vulnerabilities. Nothing can take the place of an information security audit (http://www.sans.org/score/ISO_17799checklist.php). It is critical to take a snapshot of each site's security posture and work against the findings.

Senior management should be aware of the state of the information security program. Usually this is facilitated through an annual security audit report and monthly security status reports.

In the absence of current information, it is a good exercise to ask the following questions of information security management:

* Are employees required to sign off on the general security policy and specific policies in their functional area as well?

- * How have applicable security standards been met (e.g. SOX, GLBA and HIPAA)?
- * Which control frameworks are in use (e.g. COSO, CobiT and/or ISO 17799)?
- * How are logical and physical perimeters defined? Please provide rationale and diagrams.
- * Is security built into custom applications from the design phase?
- * Are all systems routinely patched and hardened?
- * Are strictly controlled development environments in place (e.g., development, quality & user acceptance)?
- * What is the maturity level of business continuity and disaster recovery planning?
- * Are accesses systematically rescinded when an employee leaves or their role changes?
- * In general, are internal controls layered (i.e., defense-in-depth measures)?
- * How are the concepts of least privilege and separation of duties addressed?
- * Is a tactical incident response program in place?
- * What are the details of the security awareness program?
(http://www.cyberguard.com/news_room/news_newsletter_030926threatwithin.cfm)

* How recently have each of these topics been addressed? Are they truly maintained?

Establishing a culture of security is critical. Information security managers must be well versed in the breadth of the IT career field and other disciplines as well (e.g. physical security, accounting and human resources management). In addition, a security manager must be a passionate advocate and an effective communicator. Interpersonal skills should include the ability to communicate in non-technical terms.

Many small organizations lack a dedicated information security professional. This practice should be avoided. As you can see, an effective security program requires constant care and feeding. A dedicated information security professional will reduce the high cost associated with unmanaged risk.

Consider the impact on an organization if it does not adequately mitigate risks. In the end, how an organization approaches security depends on its appetite for risk. A healthy dose of paranoia is warranted here. After all, the stakes are extremely high.

⚡ Re: Cosmic ray hits Brussels election -- really? ([RISKS-23.46](#))

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

Fri, 30 Jul 2004 09:19:49 +0200

Dirk Fieldhouse ([RISKS-23.46](#)) asks whether it has ever been confirmed that a cosmic ray has caused a terrestrial computer malfunction.

I looked at the issue of what are called Single Event Effects (SEEs) in 2000-2001. Basically, cosmic rays are particles, gamma rays (which are also particles -- everything is a particle) and so on which come from outside the earth's atmosphere (primary) or which are generated from primary rays by atmospheric reactions (secondary). Cosmic radiation also keeps us alive - thanks to all those photons which make it through from the sun.

Cosmic rays can cause bits to flip, latch up, or burn out in computer memories. As far as I could tell, no one had recorded a processor fault due to radiation by 2001. The problems were first noticed with the advent of SRAMS in 1978 when the bits got small enough to be affected by alpha particles (helium nuclei) of around 5-10 MeV (Mega-electron-Volts. Mass and energy are identical, measured in electron-Volts). Alpha particles with these energies can produce up to 3 million electron-hole pairs in silicon, and 1978 was apparently when SRAMs became sensitive to noise bursts of about that size. These alpha particles were caused by the decay of thorium, a trace element in the silicon substrate. Refine it out, and the noise bursts disappear. Alpha particles of these energies could also come from uranium decay. Classic references are Ziegler and Lanford, Science 206 (16):776-88, 16 November 1979, and Journal of Applied Physics 52(6): 4305-12, June 1981.

These so-called Single Event Effects (SEEs) in computer memory are a whole branch of avionics research. Satellites and other spacecraft have to worry significantly about them and their processors and memories are designed to tolerate faults so caused. SEEs have been observed and measured in aircraft avionics. Current estimates of the rate of SEEs in aviation at 30-50,000 ft altitude are around $O(10^{-9})$ to $O(10^{-8})$ per bit per hour. That is a single bit per 1M of memory per one hundred to one thousand hours exposure. Radiation intensity of the same energy levels on the ground are some two orders of magnitude lower. See Eugene Normand, Single Event Effects in Avionics, IEEE Transactions on Nuclear Science 43, 1996, also available from the Boeing Radiation Lab WWW site. So we are talking $O(10^{-11})$ to $O(10^{-10})$ events per bit per hour, which is a rate of one bit per Gigabyte (1 Byte = 8 bits) per hour to ten hours.

Of course, it is theoretically possible that a hugely energetic particle could come blasting through your memory and take out multiple bits. All sorts of things are theoretically possible, but the question is whether people have ever seen them occurring.

There was some worry in the 1990's about SEEs in power MOSFETs (semiconductors that operate at thousands of volts, such as used in engine control for electric railway locomotives).

Now, it is extremely difficult to determine what the causes of these SEEs are. The SEE-and-avionics people seem convinced that the effects at altitude are primarily due to neutrons. My particle physicist colleagues

at Bielefeld
were somewhat sceptical. So I researched the literature and
found only some
very indirect and questionable evidence for this oft-repeated
claim. I am
inclined to be sceptical also. But this is an aside. That SEEs
occur is
clear, as is the phenomenon that they are single-bit problems.

So how does one know that a particular SEE is caused by a cosmic
ray?

Basically, one doesn't. It took until 1992 for people to find
what they
believed to be incontrovertible evidence of an SEE in a
spacecraft caused by
a cosmic-ray proton, for example. It was a publishable discovery.

Fieldhouse finds "... the possibility of a cosmic ray causing a
computer
malfunction [to be] an obvious threat for space-borne systems".

My
impression is that it isn't so much of a threat because people
spend a lot
of time on SEE-tolerant architectures for spacecraft. You don't
want to
spend large amounts of money launching a spacecraft only to get
bits
predictably fried and lose data. So you use standard bit-error
correction
coding techniques implemented in silicon, and put up with the
extra resource
consumption of all those extra bits. These are not mass-
production chips,
after all.

I find many reasons to question a claim that a cosmic ray
trashed the
results of a computer vote-counting program. First, I find it
implausible
that anyone knows that flipping or latching one bit caused a
miscount of
4,100 votes. I doubt whether anyone analysed the program or the
hardware

architecture thoroughly enough to determine that. Show me the chip and the latched bit. And show me the causal chain between that flipped bit and the 4,100 miscounted votes. Anything other than an SEE is a purely theoretical possibility that one can ignore. Second, I presume no one has determined whether the SEE in question was caused by a cosmic ray or by a noise burst in the silicon, or by a thermal problem in the computer, or by the results of a manufacturing error. We have had memory and processors go wrong on us, and nobody ever knows the reasons why. The chip or board just gets swapped and life continues. You need large numbers of SEE events to trace their cause, and you need large numbers of particles to correlate with the large numbers of SEE events and a not insignificant number of competent particle physicists and nuclear engineers to analyse the evidence to conclude that it was a radiation event.

I wouldn't call it an urban legend, for that means a tall tale that did not come to pass, and terrestrial SEEs caused by cosmic rays can come to pass. But I would suspect that someone is shooting their mouth off on evidence that is so meagre as not to come close to supporting any assertion of this type.

I would question any results generated by a program which is claimed to be sensitive to one SEE. Whoever determined that a cosmic ray might have caused the problem should also have concluded that the program was so obviously untrustworthy that none of its results should ever be believed.

Peter B. Ladkin, University of Bielefeld, Germany
<http://www.rvs.uni-bielefeld.de>

✶ Re: Cosmic ray hits Brussels election -- really? ([RISKS-23.46](#))

<"Dirk Fieldhouse" <fieldhouse@gmx.net>>
Fri, 30 Jul 2004 20:27:55 +0100

To summarise the responses to this item, I have now been able to confirm the story [4100 votes given to candidate in local Brussels election by computer error due to cosmic ray]. It was of course actually $4096 = 2^{12}$ votes, as correspondent Robson and I expected.

Correspondents Coggins, Leavitt and Ladkin (see also his RISKS post 'Cosmic Rays and Computers') confirmed that, as expected, such a malfunction could be experienced by a terrestrial computer. The primary known effect is on RAM and the likelihood of a 'soft error' increases with the amount of RAM and the density of components on the chip. Even PCs nowadays, having 1Gb or more RAM, could be noticeably (say, weekly) affected if ECC memory is not used -- unless they are located in tunnels! Presumably this would only be noticed if users expected the running software itself to be stable.

Correspondent Cole recalled a mini-supercomputer system in the mid-80s that had frequent parity errors in the instruction cache because "the memory manufacturer had omitted a mask in the memory chip packaging

that protected
the memory circuits from low-level radiation due to radioactive
heavy-metal
elements in the ceramic outer packaging layer".

Correspondent Baeck (special thanks) provided the election's
exact location,

Schaerbeek, in his post to RISKS, and that led me to

<http://wiki.ael.be/index.php/>

[ElectronicVotingRandomSpontaneousBitInversion](#)

and finally to

http://www.poueva.be/article.php3?id_article=32 (en Francais)

The event occurred in the election held on 18 May 2003. An
expert review

determined that as no software defects had been found on
inspecting the

source code and no test had been able to reproduce the error, it
was

probably attributable to a spontaneous inversion of a bit in the
RAM of the

PC (no explicit mention of cosmic rays). However the report
concluded that

even if the voting system under review was not perfect the
totality of

controls was sufficient to be confident in the overall result. I
wonder.

To a colleague's fundamental question -- how was it known that
the result

was wrong -- the answer is that the count was not consistent
with the

proportional representation rules in the election.

So it looks like I'll have to carry on testing my software.

Thanks to all.

Dirk Fieldhouse, London, UK

✶ Re: Cosmic ray hits Brussels election -- really? ([RISKS-23.46](#))

<Sergio.Gelato@astro.su.se>

Sun, 1 Aug 2004 16:16:50 +0200

An English-language Google search may have failed to confirm the story of a cosmic ray being blamed for a 4096-vote error in Schaerbeek during the 2003-05-18 Belgian parliament election, but a French-language search was more successful, and led me to the following very informative link:

http://www.poueva.be/article.php3?id_article=36

from which one learns that the investigation, having failed to find a software bug, and considering the internal structure of the program, concluded that the error was "very likely" due to a spontaneous, random bit flip--for which cosmic rays are a possible cause. They provide a link to

<http://www.research.ibm.com/journal/rd/401/tocpdf.html>

on "Terrestrial cosmic rays and soft errors" (in English).

The problem, as I (and others) see it, is not that cosmic rays are blamed (that may be correct) but that insufficient safeguards appear to be in place to reliably detect such errors. (Cheap hardware without ECC memory? No other checksums to protect the integrity of the data?) From that same web page, translation mine:

"The experts' report underlines that the problem is known, that solutions do exist, but that nothing has been done to protect oneself or to detect, other than by chance or from the absurdity of the results, that such a

phenomenon has taken place."

★ REVIEW: "Official [ISC]^2 Guide to the CISSP Exam", Hansche et al.

<Rob Slade <rslade@sprint.ca>>

Fri, 30 Jul 2004 07:54:11 -0800

BKOIGTCE.RVW 20040618

"Official (ISC)^2 Guide to the CISSP Exam", Susan Hansche/John Berti/Chris Hare, 2004, 0-8493-1707-X, U\$69.95/C\$101.50

%A Susan Hansche susan.hansche@pec.com

%A John Berti jberti@deloitte.ca

%A Chris Hare chare@chris-hare.com, chare@nortelnetworks.com

%C 920 Mercer Street, Windsor, ON N9A 7C2

%D 2004

%G 0-8493-1707-X

%I Auerbach Publications

%O U\$69.95/C\$101.50 800-950-1216 orders@crcpress.com

%O <http://www.amazon.com/exec/obidos/ASIN/084931707X/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/084931707X/robsladesinte-21>

<http://www.amazon.ca/exec/obidos/ASIN/084931707X/robsladesin03-20>

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/084931707X/robsladesin03-20)

%O <http://www.amazon.ca/exec/obidos/ASIN/084931707X/robsladesin03-20>

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/084931707X/robsladesin03-20)

%P 910 p. + CD-ROM

%T "Official (ISC)^2 Guide to the CISSP Exam"

Once again I have to state a bias in regard to this book. I've known about

this book since its inception, I've known and advised the authors, I

provided bits of the material, and even contributed one appendix. (The

annotated bibliography and references--surprise, surprise.)

I was asked to review the chapters while the book was in

production. The reason was, of course, that I had reviewed all the other CISSP (Certified Information Systems Security Professional) guides. Specifically, the intent was to ensure that this manual, prepared and supported by (ISC)² (International Information Systems Security Certification Consortium) was "head and shoulders" above all the other published works. This volume is not perfect, by any means, but it is the best of the current bunch.

Taking material from one source is copying, taking material from two sources is plagiarism, and taking material from many sources is research. This volume has not only research but direct input from a great many sources. Some are mentioned in the acknowledgements, a number of others are to be found on the title page, since sections of major articles from the venerable "Information Security Management Handbook" (cf. BKINSCMH.RVW) were included or used as the basis for parts of the guide. Even this doesn't exhaust the contributions, since much of the work is informed by the material in the (ISC)² CBK (Common Body of Knowledge) Review Seminar, and over a hundred individuals have had the chance to augment that content. The result is a breadth and currency of information that exceeds any other guide on the market.

Sample questions and exams are eagerly sought by candidates for the CISSP exam. This guide has a significant advantage in this regard: not only do a number of the contributors produce questions for the exam itself (therefore

being more than passingly familiar with the style and level of difficulty required), but the CISSP exam committee was also approached for advice and input. No source is able to provide "actual" CISSP exam questions, but the examples provided in this volume are very close in form, mix, degree of difficulty, and concept.

The book is not without its faults. The sheer volume of the contributors ensured that topics were covered multiple times, and not all duplicated areas have been amalgamated. In addition, the variety of writing styles can make the text disjointed in places, as it moves from section to section and subject to subject. These factors can make the work difficult and demanding to read and follow.

The CISSP exam, as the security field itself, is a changing target, and no book can expect to provide the "best" coverage of the topic indefinitely. As well, security is an immense discipline, and touches on an inordinate number of other areas. This work, however, has come closest to spanning the range of subject matter necessary to challenge the CISSP exam, and is currently the best of the guides.

copyright Robert M. Slade, 2004 BKOIGTCE.RVW 20040618
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

Volume 23: Issue 48

Monday 9 August 2004

Contents

- [Kolwicz kicked out for submitting real election tests](#)
[via Susan Marie Weber](#)
- [Image flaw pierces PC security](#)
[Keith A Rhodes](#)
- [Windows Buffer Overflow Protection Programs: Not Much](#)
[Paul Robinson](#)
- [Security Cavities Ail Bluetooth](#)
[Kim Zetter via Monty Solomon](#)
- [Emoticon-interpreters create risks in instant messaging services](#)
[Dale Hawkins](#)
- [First malicious program aims for handhelds](#)
[Keith A Rhodes](#)
- [Two more Canadian Banks with computer software screwups](#)
[Bob Heuman](#)
- [Top Australian banking sites vulnerable](#)
[NewsScan](#)
- [Cable giants seek to dominate VoIP](#)
[NewsScan](#)
- [Another airline outage](#)
[Jeremy Epstein](#)

- [Two Million Scans Uncover 55 Million Instances of Spyware](#)
[Monty Solomon](#)
 - [Memory error paper](#)
[Laurent Guerby](#)
 - [Risks of automated calling systems](#)
[Jeremy Epstein](#)
 - [Internet voting in The Netherlands update](#)
[Joseph Kiniry](#)
 - [Re: The Mr Micawber Syndrome](#)
[Fernando Pereira](#)
 - [Re: Stolen: one-third of the world's software](#)
[Jurek Kirakowski](#)
 - [REVIEW: "Software Forensics", Robert M. Slade](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Kolwicz evicted for submitting real tests (via Susan Marie Weber)

<alkolwicz@qwest.net>

Thursday, August 05, 2004 11:27 AM

```
> Date: Thu, 5 Aug 2004 14:30:13 -0700
> From: "SusanMarieWeber" <susanmarieweber@earthlink.net>
> Subject: Kolwicz kicked out for submitting real election tests

> This is message from Al Kolwicz. I suspect that we are all
going to face
> these problems during the next accuracy and logic testing of
the voting
> machines before the November 2004 election. Imagine having
cops around to
> tell people to leave. We must stop questioning authority? I
don't think
> so, NOW more than ever we need to keep asking these questions.

> Susan Marie Weber
```

Kolwicz kicked out for submitting real election tests

Al Kolwicz, official representative to Boulder County's test of its new vote counting system, was asked by County Clerk, Linda Salas, to leave the test.

When asked what happened, Kolwicz said, "we submitted sample ballots to test the security and accuracy of the county's new vote counting system."

The sample ballots included tests such as - (a) what happens if a voter circles the box rather than filling in the entire box with a black pen, and (2) what happens if a voter marks over the ballot serial number in hopes that this will make the ballot secret. (Boulder County's new ballots are not secret.)

Salas consulted with the Secretary of State, Donetta Davidson's office, by phone. Following their private conversation, Salas asked Kolwicz to leave. Kolwicz left immediately and went outside of the building to record some notes. Deputy P. Dunphy, who was in the room where the testing was being conducted, came out to find Kolwicz on a bench. He told Kolwicz that he was not to return to the building. "It looks like a sham is being foist upon the public", said Kolwicz. The tests prepared by Kolwicz are limited to things that can happen in this year's primary election.

Al Kolwicz, CAMBER - Citizens for Accurate Mail Ballot Election Results
2867 Tincup Circle, Boulder, CO 80305, 303-494-1540
AlKolwicz@qwest.net
www.users.qwest.net/~alkolwicz <http://coloradovoter.blogspot.com>

Image flaw pierces PC security

<"Keith A Rhodes" <RhodesK@GAO.GOV>>

Fri, 06 Aug 2004 07:31:51 -0400

Robert Lemos, CNET News.com, 5 Aug 2004

<http://zdnet.com.com/2100-1105-5298999.html>

Six vulnerabilities in a common code that handles an open-source image format could allow intruders to compromise computers running Linux and may allow attacks against Windows PCs as well as Macs running OS X. The security issues appear in a library supporting the portable network graphics (PNG) format, used widely by programs such as the Mozilla and Opera browsers and various e-mail clients. The most critical issue, a memory problem known as a buffer overflow, could allow specially created PNG graphics to execute a malicious program when the application loads the image.

Among the programs that use libPNG and are likely to be affected by the flaws are the Mail application on Apple Computer's Mac OS X, the Opera and Internet Explorer browsers on Windows, and the Mozilla and Netscape browsers on Solaris, according to independent security researcher Chris Evans, who discovered the issues. Apple and Microsoft could not immediately be reached for comment. Evans did not test every platform to check which vulnerabilities work, he said.

🔥 Windows Buffer Overflow Protection Programs: Not Much

<"Paul Robinson" <postmaster@paul.washington.dc.us>>

Mon, 09 Aug 2004 17:24:00 GMT

I happened to stumble upon the most recent issue of the hacker e-zine Phrack, Issue #62, of July 10, 2004, and looking over the table of contents I found article #5, "Bypassing 3rd Party Windows Buffer Overflow Protection" which can be read at the following url:
<http://www.phrack.org/show.php?p=62&a=5>

I found the article fascinating in that it shows exactly why several major commercial anti-buffer overflow exploit programs are inadequate for their advertised purposes. The article even points out what you are going to end up with: a false sense of security.

For those who are not so technically inclined, a buffer overflow exploit is one in which someone sends too much data to a program (such as a web server application), sending far more data than the program would expect, in order to force arbitrary data into a storage area (a "buffer") so the amount of data forced into the buffer goes beyond the expected limits, causing the data to overflow the buffer and makes it possible for that data to be executed as arbitrary program code. Since the attacker forces code of his choosing into the execution stream, he now owns your box, because as the saying goes, if I can run code on your machine - especially if

it's a
Windows machine where there is not much protection - I can
pretty much do
anything I please there.

These anti-buffer overflow exploit protection programs then try
to prevent
this by watching for attempts to execute calls to the operating
system, in
places where only data should occur as opposed to program code.
The article
shows why these programs are inadequate both from a standpoint
of how they
fail to provide full protection, and how to get around the
limited
protection they do provide.

This sort of article is an excellent example of why full
disclosure of a
serious problem is necessary in order to solve it. The type of
response to
an anti-buffer overflow exploit protection program by an
attacker would, as
a matter of necessity, be somewhat complicated and technical in
nature, and
the only way one could explain why there is a problem, what the
problem is,
and then allow someone to be able to solve it, is to describe
how to
exploit the flaw. Nothing less will do because nothing less
will explain
how the flaw is exploited.

It is reports such as these that are important even to those
that are not
interested in breaking into a place, and in fact are probably of
crucial
interest to security people in order that (1) they not be given
a false
sense of security by these products that only solve part of the
problem; (2)
explain exactly why the products are ineffective; and (3)
explain exactly

what the issues are.

An explanation such as the one given shows why these products are ineffective, shows what those who have to defend themselves need to look for, and can show those trying to build safety systems in the future how to better secure them.

Does this mean someone can create an attack using the information shown?
Absolutely.

This does not make the exposure of such information any less valid. Telling someone that it is still possible to trigger a buffer overflow exploit even if a buffer overflow exploit security program is in place is probably not going to convince them without some proof. Explaining that these systems don't block everything and mentioning why will not give someone enough information to reliably check what is happening or understand how the problem affects them. Only a clear explanation of how the process is done is going to show someone how to guard against it.

Digging one's head in the sand does not hide a danger, nor does making it illegal to publicize such information help, as those who will use such information for criminal purposes, since they are already breaking the law, any penalties for selling such information to other crackers (or trading it for other information) simply keeps it out of the hands of the good guys who would need it to figure out how to work around it.

Additionally, by making such information available, third parties, who are

neither selling security software, nor trying to crack other people's boxes in order to own them, can read this information and give an objective validation as to whether they are valid or not, and perhaps can supply solutions not requiring multi-thousand-dollar support contracts from some vendor who is more interested in what they can sell than in security, who just happen to sell this particular type of product because there is a market for it and who might not be interested in giving away information that they can sell to others. There's nothing particularly wrong with charging whatever the traffic will bear for what you know, but it creates a strong disadvantage for those kept in the dark.

Which is the only thing that security by obscurity - trying to hide problems in the hope someone doesn't discover them - does, it keeps the people who most need to know how to solve the problem in the dark.

✶ Security Cavities Ail Bluetooth

<Monty Solomon <monty@roscom.com>>

Sat, 7 Aug 2004 16:20:31 -0400

Kim Zetter, Wired.com, 6 Aug 2004

Serious flaws discovered in Bluetooth technology used in mobile phones can let an attacker remotely download contact information from victims' address books, read their calendar appointments or peruse text messages on their

phones to conduct corporate espionage.

An attacker could even plant phony text messages in a phone's memory, or turn the phone sitting in a victim's pocket or on a restaurant table top into a listening device to pick up private conversations in the phone's vicinity. Most types of attacks could be conducted without leaving a trace.

Security professionals Adam Laurie and Martin Herfurt demonstrated the attacks last week at the Black Hat and DefCon security and hacker conferences in Las Vegas. Phone companies say the risk of this kind of attack is small, since the amount of time a victim would be vulnerable is minimal, and the attacker would have to be in proximity to the victim. But experiments, one using a common laptop and another using a Bluetooth "rifle" that captured data from a mobile phone a mile away, have demonstrated that such attacks aren't so far-fetched.

Laurie, chief security officer of London-based security and networking firm ALD , discovered the vulnerability last November. Using a program called Bluesnarf that he designed but hasn't released, Laurie modified the Bluetooth settings on a standard Bluetooth-enabled laptop to conduct the data-collection attacks.

Then, German researcher Herfurt developed a program called Bluebug that could turn certain mobile phones into a bug to transmit conversations in the vicinity of the device to an attacker's phone. ...

<http://www.wired.com/news/privacy/0,1848,64463,00.html>

✶ Emoticon-interpreters create risks in instant messaging services

<"Hawkins Dale" <hawkins@pobox.com>>

Fri, 30 Jul 2004 09:36:39 -0400

Many popular instant-messaging tools interpret text "emoticons" and replace them with graphical icons. For example, if you send your buddy a colon-right-parenthesis, your correspondent's messaging client may replace the :) with a yellow smiley-face icon.

This is very nice, but the sender has no control. And it's hard to know in advance what character-strings will be parsed into what kind of unintended image.

A colleague was discussing his 401(k) plan with his boss, who happens to be female, via instant messaging. He discovered, to his horror, that the boss' instant-messaging client was rendering the "(k)" as a big pair of red smoochy lips. :(

✶ First malicious program aims for handhelds

<"Keith A Rhodes" <RhodesK@GAO.GOV>>

Fri, 06 Aug 2004 07:29:27 -0400

[The "first" as far as we know.]

Ina Fried, Malicious program aims for Pocket PCs, CNET News.com,
5 Aug 2004

<http://zdnet.com.com/2100-1105-5298781.html>

A malicious Trojan horse program has emerged for Pocket PCs, antivirus companies, but they characterized the threat as relatively low. The program, known alternately as Backdoor.Bardor.A and WinCE.Brador.a, lets an attacker gain full control of the handheld and is the first such "backdoor Trojan" program to emerge for Pocket PCs. However, such backdoor programs are not capable of propagating on their own and instead must be sent as e-mail attachments or through similar means, making them less dangerous.

✶ Two more Canadian Banks with computer software screwups

<Bob Heuman <rsh@idirect.com>>

Fri, 30 Jul 2004 21:17:30 -0400

TD, CIBC glitches bring down key banking systems, ITBusiness, 29 Jul 2004

<http://www.itbusiness.ca/userredirect.asp?linkid=37706&userid=5>

Two of Canada's best-known financial institutions join RBC in the annals of IT horror stories. Find out what went wrong, and to what extent customers' loyalty will be tested.

* The CIBC error was definitely a program change that made it through testing and was put into production with an uncaught error in the code.

* The TD error was still being investigated at the time of the article I reference above. Basically, more of the same, and impacting a lot of customers in Canada and elsewhere.

Proof that as many times as it gets pointed out to them, it still happens, and will continue to happen.

⚡ Top Australian banking sites vulnerable

<"NewsScan" <newsscan@newsscan.com>>

Tue, 03 Aug 2004 09:16:48 -0700

The Web sites of three of Australia's four big banks are susceptible to cross-site scripting attacks, according to a British tech professional who gained prominence last year when he discovered a URL spoofing flaw in Microsoft's Internet Explorer browser. Sam Greenhalgh, who recently tested the Web sites of several British financial services companies and found many of them susceptible to the same kind of attacks, said the flaw resulted from sites not "sanitizing" information the user submits before displaying the information on the page: "If the information contains HTML, those HTML tags will be included on the site. Among other things this allows an attacker to include a tag that instructs the page to load a JavaScript file from another Web site." Greenhalgh provided demonstrations of injecting HTML on the sites using scripts he wrote himself. [**The Age**, 2 Aug 2004; Rec'd from John Lamp,

Deakin U.; NewsScan Daily, 3 Aug 2004]

[<http://theage.com.au/articles/2004/08/02/1091412044139.html>]

🔥 Cable giants seek to dominate VoIP

<"NewsScan" <newsscan@newsscan.com>>

Wed, 04 Aug 2004 08:05:40 -0700

Time Warner Cable, Cablevision and other cable giants have begun setting up their own Voice over Internet Protocol (VoIP) services for American consumers, says a new Yankee Group report, aimed at quickly gaining the lead over alternative Internet telephony providers in 2004. "After many years of testing, the VoIP technology is finally available and ready for prime time. The U.S. market, which represents almost all the cable VoIP market today, also will drive the global MSOs (multiservice operators) to move forward," says a Yankee Group analyst. Already, some alternative providers such as Vonage and Net2Phone are collaborating with cable and other broadband partners to offer their services, but in the long run, consumers likely will opt for VoIP service straight from their local cable or phone company. In a separate report on the U.S. broadband market, Yankee predicts that subscriptions to high-speed services will overtake narrowband signups by 2006. That study listed Comcast as the leader in cable modem subscribers and SBC as the dominant DSL provider. [CNet 3 Aug 2004; NewsScan Daily, 4

Aug 2004]

<http://news.com.com/2100-7352-5295023.html>

✈ Another airline outage

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Tue, 3 Aug 2004 08:49:51 -0700

Independence Air (www.flyi.com), a newly formed airline, suffered from a rather severe computer outage yesterday from about 3pm-9pm (not sure exactly). The result was that they couldn't check passengers in, couldn't track baggage, etc. The front-side people had no way of knowing which flights were in the air or who was on them.

This may have been related to a severe round of thunderstorms that went through the Washington DC area at about the same time. One would hope they had backup computer systems (or power supplies, or network connectivity), but that's just a guess.

What made this particularly nasty as an outage is that they didn't have backup procedures - no one had phone numbers, as they rely on getting those from the computer system. It made for a particularly long evening waiting 7 hours to pick my daughter up, since no one could tell us what the status was of any flight, or even what flight she was on. So when she walked out from the security area, it was something of a surprise....

⚡ Two Million Scans Uncover 55 Million Instances of Spyware

<Monty Solomon <monty@roscom.com>>

Wed, 4 Aug 2004 09:00:46 -0400

EarthLink and Webroot Release Six-Month SpyAudit Report;
CoolWebSearch Identified as the Most Virulent Adware Program
(PR Newswire, 4 Aug 2004)

<http://finance.lycos.com/home/news/story.asp?story=42899777>

EarthLink and Webroot Software (a producer of award-winning privacy, protection and performance software) released their third SpyAudit Report, which has tracked the growth of spyware on consumer PCs for the first half of 2004. Since the SpyAudit report's inception on 1 Jan 2004, more than two million scans have been performed. The scans discovered approximately 54.8 million instances of spyware, for an average of 26.5 traces per SpyAudit scan. Scans nearly doubled from the first to the second quarter. For each category, the instances of adware increased month-over-month, while adware cookies, system monitors and Trojans decreased slightly overall. The complete report is available at <http://www.earthlink.net/spyaudit/press>.

⚡ Memory error paper

<Laurent GUERBY <laurent@guerby.net>>

Wed, 04 Aug 2004 00:19:11 +0200

Since we're talking about memory errors, there's a nice paper on memory vs a light bulb:

A. Appel and S. Govindavajhala. "Using Memory Errors to Attack a Virtual Machine" in IEEE Symposium on Security and Privacy, 2003.

<http://www.cs.princeton.edu/~sudhakar/papers/abstracts/memerr.html>

<http://www.cs.princeton.edu/~sudhakar/papers/memerr-slashdot-commentary.html>

I guess people designing voting machines without using some kind of heat sensor with alert procedure, using properly shielded case, ECC memory, etc... are not doing their engineering job. Not adding a paper trail at all is also a real bad idea, but that's just me :).

⚡ Risks of automated calling systems

<Jeremy Epstein <jeremy.epstein@webmethods.com>>
Tue, 3 Aug 2004 17:48:37 -0400

I got this a few weeks ago, and just noticed it. As with so many risks, the problem isn't the technology, but rather the unexpected combinations of technologies (i.e., cell phones left on all night along with automated calling systems).

>I wanted to open this month's newsletter by sincerely apologizing to the
>almost 60 people in our database who mistakenly received a call in the

>middle of the night to remind them of our upcoming webinar held on [date].
>[Vendor] does not usually "telemarket" to our database - in fact, we
>had never done so before. But when the webinar company offered us a chance
>to broadcast a pre-recorded VM reminder at no charge, we fell for the lure
>of the "free" opportunity against our better judgment. The theory was
>that if it was sent after hours, it would not disturb anyone during their
>work day. It sounded good in theory...
>
>The result? Four complaints the next morning from people notifying us that
>we had woken them up by calling their home offices or cell phones that had
>not been turned off that night. I asked the webinar company to run a call
>report afterward and although we only received a few actual complaints,
>the data showed that up to as many as 60 of you may have received these
>disturbing calls. All I can say is that I am extremely sorry for the
>inconvenience and I assure everyone that we will never mass call to our
>database again. I do hope you accept my sincere apology for the mistake.

⚡ Internet voting in The Netherlands update

<Joseph Kiniry <kiniry@acm.org>>

Wed, 4 Aug 2004 09:58:09 +0200

Major events in Internet Voting are taking place in The Netherlands.

The Dutch government tested an Internet voting system called "KOA" in the European Elections last month. A portion of that system was written by the Security of Systems (SoS) Group using formal methods. Additionally, partially based upon my group's work and influence, the entire KOA system has been Open Sourced under the GPL license.

I have written a short article "Electronic and Internet Voting in The Netherlands" on what has been happening here over the past few months.

See <http://www.cs.kun.nl/sos/> and http://kind.cs.kun.nl/~kiniry/papers/NL_Voting.html for more information.

⚡ Re: The Mr Micawber Syndrome

<Fernando Pereira <pereira@cis.upenn.edu>>

Mon, 2 Aug 2004 22:01:59 -0400

I was struck by the parallels between the risks discussed by Michael Bacon and those arising in backcountry skiing and mountaineering. For example, his risk (4) pretty much corresponds to the failure to set a firm turn-around time that allows for a safe return. See Chapter 18 of "Mountaineering: the Freedom of the Hills" (6th edition, Graydon & Hanson, 1997) for additional interesting parallels. Articles like Ian McCammon's "Evidence of Heuristic Traps in Recreational Avalanche Accidents" <http://www.snowpit.com/articles/traps%20reprint.pdf>

give independent evidence of decision-making bugs that are quite familiar to us in the computing realm: "Even though people are capable of making decisions in a thorough and methodical way, it appears that most of the time they don't. A growing body of research suggests that people unconsciously use simple rules of thumb, or heuristics, to navigate the routine complexities of modern life. In this paper, I examine evidence that four of these heuristics -- familiarity, social proof, commitment and scarcity -- have influenced the decisions of avalanche victims."

Fernando Pereira, Dept. of Computer and Information Science U. of Pennsylvania

⚡ **Re: Stolen: one-third of the world's software ([RISKS-23.45-46](#))**

<"Jurek Kirakowski" <jzk@ucc.ie>>

Mon, 12 Jul 2004 14:02:41 +0100

A while ago, I tried to find out the empirical basis for claims such as these made by the Business Software Alliance. After all, they can't actually be going round and physically inspecting the software being run on people's computers, can they? Nor, presumably, are they relying on conviction rates!

After some digging, I found that in 2002 their basic methodology was to count up the number of computers sold per year, and then check against the revenue from licensed software sold. They make the assumption that each

computer should be loaded with X amount of licensed software. There is of course an imbalance between predicted and actuals and this is the inferential support for the detailed lists of amounts of software fraud per country they publish.

The hazards of this methodology are (1) you don't check with enough software vendors, only, say the top 1,000 big ones; and (2) you don't consider that especially in economically poor countries, users may be using free-ware and open-source software. Much of the latter may simply be downloaded anonymously and you don't need to register.

Even in more affluent countries the use of open source software is spreading - not only because of price, but because it is usually better written and subject to less invasive user agreements than software created by many members of the Business Software Alliance.

REVIEW: "Software Forensics", Robert M. Slade

<Rob Slade <rslade@sprint.ca>>

Fri, 6 Aug 2004 08:21:33 -0800

BKSFWRFR.RVW 20040706

"Software Forensics", Robert M. Slade, 2004, 0-07-142804-6, U\$39.95/C\$3.95/UK#29.99

%A Robert M. Slade rslade@vcn.bc.ca rslade@computercrime.org

%C 300 Water Street, Whitby, Ontario L1N 9B6

%D 2004

%G 0-07-142804-6

%I McGraw-Hill Ryerson/Osborne

%O U\$39.95/C\$3.95/UK#29.99 800-565-5758 fax: 905-430-5020

%O <http://www.amazon.com/exec/obidos/ASIN/0071428046/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0071428046/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0071428046/robsladesin03-20>

%P 215 p.

%T "Software Forensics"

As long as I'm reviewing books about which I can't be objective, I might as well review my own.

This book is about software forensics. Nobody seems to know what that is.

"Oh, you look for child porno and drug dealer addresses on seized computers, right?" Umm, no. That's computer forensics which, although it should be broader, has become limited to the basic data recovery aspect of the wider field of digital forensics.

Software forensics delves into what evidence you can glean from software itself. This is useful in malware and virus research (where it has long been known as forensic programming), as well as in cases involving intellectual property and plagiarism. The study and tools utilized in software forensics can assist with determining the intent and authorship of a piece of software. At times it can even help with tasks such as recovering source code with legacy programs, or porting to new systems.

In the book there is an overview of software forensics itself. One chapter looks at blackhat sociology and culture, since those

characteristics can be evident in the programming style. There is material on the various tools, and properties of malicious software. Presentation of this type of evidence in court is difficult, so chapter five reviews expert witness restrictions and other legal issues. Content is included on programming cultures, stylistic analysis, and authorship analysis.

I can say, without any bias whatever, that this is the finest work on this topic available today. I can say that, because it's the *only* book that is dedicated to the subject.

copyright Robert M. Slade, 2004 BKSFWRF.R.VW 20040706
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>

[Incidentally, Tim Grance at NIST noted out of band that a draft of a new guide on PDA Forensics is soon to be released by NIST. Stay tuned. PGN]



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 49

Friday 13 August 2004

Contents

- [U.K.: Don't smile for your passport picture!](#)
[PGN](#)
- [Gloria Estefan performance in Dallas canceled due to computer crash](#)
[Ben Moore](#)
- [Airport Express crypto broken by DVD Jon](#)
[Cory Doctorow via Monty Solomon](#)
- [Buffer Overflow in "I'm Away" feature of AOL Instant Messenger](#)
[Paul Robinson](#)
- [Windows Buffer Overflow Protection Programs: Not Much](#)
[Paul Robinson](#)
- [Obion County Tennessee vote counting problems](#)
[Jeremy Epstein](#)
- [Drivers let Big Brother in to get a break](#)
[Kevin Maney via Monty Solomon](#)
- [DidTheyReadIt operations and security concerns](#)
[Rob Slade](#)
- [Risks of ordinary GUI "pop-up" windows?](#)
[Cody Boisclair](#)
- [REVIEW: "Stealing the Network: How to Own a Continent", Ryan Russell](#)
[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✂ U.K.: Don't smile for your passport picture!

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

Fri, 6 Aug 2004 22:44:39 PDT

The U.K. Home Office ruled that all new passport photos must show an unsmiling face with closed mouth because open mouths can confuse facial recognition systems. The new guidelines require good contrast between the face and background; the full face looking straight at the camera; no shadows; and a neutral facial expression. The rules will apply immediately to new and replacement passports. U.K. prohibits smiling faces on passports,

The Register, 6 Aug 2004

http://www.theregister.co.uk/2004/08/06/passport_scanners/

[When Lauren Weinstein saw this, he commented:

"But what if people keep smiling at the airport?" PGN]

✂ Gloria Estefan performance in Dallas canceled due to computer crash

<"Ben Moore" <ben.moore@juno.com>>

Thu, 12 Aug 2004 15:09:02 GMT

Estefan Enterprises and Clear Channel Entertainment announced (on 9 Aug 2004) that Gloria Estefan's 9 Aug performance at the American

Airlines

Center in Dallas, Texas has been canceled. After performing to a packed house in Houston, the touring company experienced a computer crash that affected the production and its special effects, forcing the cancellation of the performance. Engineers guarantee that the system will be repaired by in time for the next performance in Phoenix, Arizona on 12 Aug. [PGN-ed]

<http://www.gloriaestefan.com/news/press.php?id=20040810>

✶ Airport Express crypto broken by DVD Jon (via Monty Solomon)

<Cory Doctorow <doctorow@craphound.com>>

Thu, 12 Aug 2004 03:28:43 -0400

Jon "DVD Jon" Johansen has cracked the Apple Lossless encryption used by the Airport Express to communicate with iTunes, so that programmers can write tools that use any application and any operating system to send audio to an Airport Express. I've released JustePort, a tool which lets you stream MPEG4 Apple Lossless files to your AirPort Express.

The stream is encrypted with AES and the AES key is encrypted with RSA. ...

http://www.boingboing.net/2004/08/12/airport_express_cryp.html

<http://nanocrew.net/blog/apple/revairtunes.html>

✶ Buffer Overflow in "I'm Away" feature of AOL Instant Messenger

<"Paul Robinson" <postmaster@paul.washington.dc.us>>

Tue, 10 Aug 2004 15:26:44 GMT

An 9 Aug 2004 *Infoworld* article

href=http://www.infoworld.com/article/04/08/09/HNaolimflaw_1.html

notes that there is a bug in AOL Instant Messenger allowing an attacker to send a message that can cause a buffer overflow and possibly execute code on the attacked machine. Apparently this will only occur if the attacker sends a url - like the one in this message - as a hyperlink and the victim clicks on it, which makes the probability of attack much lower than a "standard buffer overflow attack" upon a program.

⚡ Windows Buffer Overflow Protection Programs: Not Much

<"Paul Robinson" <postmaster@paul.washington.dc.us>>

Mon, 09 Aug 2004 17:24:19 GMT

I happened to stumble upon the most recent issue of the hacker e-zine

Phrack, Issue #62, of July 10, 2004, and looking over the table of contents

I found article #5, "Bypassing 3rd Party Windows Buffer Overflow Protection"

which can be read at the following url:

<http://www.phrack.org/show.php?p=62&a=5>

I found the article fascinating in that it shows exactly why several major

commercial anti-buffer overflow exploit programs are inadequate for their

advertised purposes. The article even points out what you are going to end up with: a false sense of security.

For those who are not so technically inclined, a buffer overflow exploit is one in which someone sends too much data to a program (such as a web server application), sending far more data than the program would expect, in order to force arbitrary data into a storage area (a "buffer") so the amount of data forced into the buffer goes beyond the expected limits, causing the data to overflow the buffer and makes it possible for that data to be executed as arbitrary program code. Since the attacker forces code of his choosing into the execution stream, he now owns your box, because as the saying goes, if I can run code on your machine - especially if it's a Windows machine where there is not much protection - I can pretty much do anything I please there.

These anti-buffer overflow exploit protection programs then try to prevent this by watching for attempts to execute calls to the operating system, in places where only data should occur as opposed to program code. The article shows why these programs are inadequate both from a standpoint of how they fail to provide full protection, and how to get around the limited protection they do provide.

This sort of article is an excellent example of why full disclosure of a serious problem is necessary in order to solve it. The type of response to an anti-buffer overflow exploit protection program by an

attacker would, as a matter of necessity, be somewhat complicated and technical in nature, and the only way one could explain why there is a problem, what the problem is, and then allow someone to be able to solve it, is to describe how to exploit the flaw. Nothing less will do because nothing less will explain how the flaw is exploited.

It is reports such as these that are important even to those that are not interested in breaking into a place, and in fact are probably of crucial interest to security people in order that (1) they not be given a false sense of security by these products that only solve part of the problem; (2) explain exactly why the products are ineffective; and (3) explain exactly what the issues are.

An explanation such as the one given shows why these products are ineffective, shows what those who have to defend themselves need to look for, and can show those trying to build safety systems in the future how to better secure them.

Does this mean someone can create an attack using the information shown?
Absolutely.

This does not make the exposure of such information any less valid. Telling someone that it is still possible to trigger a buffer overflow exploit even if a buffer overflow exploit security program is in place is probably not going to convince them without some proof. Explaining that these systems don't block everything and mentioning why will not give someone

enough
information to reliably check what is happening or understand
how the
problem affects them. Only a clear explanation of how the
process is done
is going to show someone how to guard against it.

Digging one's head in the sand does not hide a danger, nor does
making it
illegal to publicize such information help, as those who will
use such
information for criminal purposes, since they are already
breaking the law,
any penalties for selling such information to other crackers (or
trading it
for other information) simply keeps it out of the hands of the
good guys who
would need it to figure out how to work around it.

Additionally, by making such information available, third
parties, who are
neither selling security software, nor trying to crack other
people's boxes
in order to own them, can read this information and give an
objective
validation as to whether they are valid or not, and perhaps can
supply
solutions not requiring multi-thousand-dollar support contracts
from some
vendor who is more interested in what they can sell than in
security, who
just happen to sell this particular type of product because
there is a
market for it and who might not be interested in giving away
information
that they can sell to others. There's nothing particularly
wrong with
charging whatever the traffic will bear for what you know, but
it creates a
strong disadvantage for those kept in the dark.

Which is the only thing that security by obscurity - trying to
hide problems

in the hope someone doesn't discover them - does, it keeps the people who most need to know how to solve the problem in the dark.

🔥 Obion County Tennessee vote counting problems

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

Wed, 11 Aug 2004 13:21:29 -0400

Obion County in Tennessee had to revise its preliminary election results after they discovered that early votes weren't counted. Seems that the DRE vendor changed how the system counted the early votes, which wasn't initially noted. They're now confident they got it right. One preliminary victor will now be defeated.

Note that the problem here wasn't in the voting machines themselves (which is where most of the historical problems have been), but rather in how the results are tallied at the end of the election.

[http://www.ucmessenger.com/cgi-bin/LiveIQue.acgi\\$rec=29188?frontnews](http://www.ucmessenger.com/cgi-bin/LiveIQue.acgi$rec=29188?frontnews)

🔥 Drivers let Big Brother in to get a break (Kevin Maney)

<Monty Solomon <monty@roscom.com>>

Wed, 11 Aug 2004 01:33:12 -0400

In two new tests, car owners will be able to let insurance companies monitor

their driving via new technology in exchange for lower rates. The technology will track some combination of when, where, how far and how fast they drive, giving insurers a way to reward low-risk driving. Now just experiments, the technology might be a glimpse of the future of car insurance. The trials will begin this year. [Source: Kevin Maney, *USA TODAY*, 9 Aug 2004]
http://www.usatoday.com/tech/news/surveillance/2004-08-08-insure_x.htm

⚡ DidTheyReadIt operations and security concerns

<Rob Slade <rslade@sprint.ca>>
Mon, 9 Aug 2004 14:34:39 -0800

DidTheyReadIt is a new service on the Net. It has garnered some attention from the privacy community already: I will deal with some of that later. I would like to examine the actual operations of the service. The discussion surrounding it has been marked by assumptions and lack of knowledge. Some assertions have been made that are at odds with the actual operations. DidTheyReadIt is both less, and more, dangerous than has been made out.

As the name implies, it provides a kind of "return receipt" for e-mail. It does this, of course, using Web bugs. A "single pixel" image file is called from the central host, using a hash that presumably corresponds to the

sender, subject, and receiver, looking like the following:

```
img  
src="http://didtheyreadit.com/  
b906148b2edfdab9e7de03a23f59687eworker.jpg"  
width="1" height="1" /
```

(I have removed the surrounding angle brackets: hopefully this will prevent any mailers from trying to render the HTML.)

Having obtained an account from DidTheyReadIt (and paid for the privilege), there are two ways to use the service.

RISK 1

If you have WinXP or W2K (and a "standard" mailer) you can run a background program on your computer. I have downloaded the installation program and made a cursory examination of it, but I have strong reservations about actually running it on my system. One can assume that the process runs in the background, adds the Web bugs to outgoing e-mail traffic, and sends information to the central computer. However, even a brief analysis of the code indicates it can do more than that. Among other things it calls the kernel, uses the Registry, and obtains information on privileges within your system. These may be valid activities within the context of the operation of the program, but, given what the program must be doing, what else is it doing? There is a significant possibility for information leakage here.

RISK 2

You can use the program without running the background process.

To do this,
you append "didtheyreadit.com" to the e-mail address. If I
wanted to send a
message to my rslade@isc2.org address, I would send it to
rslade@isc2.org.didtheyreadit.com. The central computer then
reformats the
e-mail in HTML and adds the Web bug. In this way, obviously,
DidTheyReadIt
gets to read all the e-mail I send.

When e-mail is opened using a mailer that automatically calls for
information from the Web, the URL is requested, and the central
computer has
confirmation that the individual actually read the e-mail.
DidTheyReadIt
promises that they can tell you how long the e-mail remained
open. (In the
tests that I've done so far this information has been available
in slightly
under half of the cases.)

(When the URL is requested, a series of packets each containing
a single
byte is sent. Lauren Weinstein [see below] has noted that this
may be the
way the Rampell measures how long the message remains open. In
tests the
file transfer time seems to vary, but has always been shorter
than the
longest time that I've been "informed" a message has remained
open. Others
have theorized that the material transferred may be scripting
that remains
active as long as the message is open, passing information back
to Rampell.
This does not seem to be the case. When downloaded manually,
the file is
302 bytes, has the internal structure of a JPEG file, and
displays as a one
[or possibly two] pixel black dot. A refresh tag could be used,
but this
has been observed neither in the coding seen nor the activity of
browsers.

At this point I don't know what the basis of the "read duration" is.)

RISK 3

The central computer actually has rather a lot of information from that URL request. There is information about the time it was opened. There is purported information about the location and organization, but this is obviously obtained from a whois lookup from the IP address. There is information about the browser application, and the language used. In the case of Windows software running under emulation on a non-Windows system, there was enough information to indicate that this was so.

RISK 4

The amount of information that DidTheyReadIt could build up is quite staggering. As well as simple lists of valid e-mail addresses, they can tie address information to browsers and other applications, and the language of the user. They can, of course, build maps of connections between correspondents. The hash seems to also be linked to the subject line, so that even if e-mail is not being sent through the central computer itself a database of topics and interests can be built. I'm rather surprised that Rampell Software (the company behind DidTheyReadIt) is even trying to sell their service: make it free, get the masses on board, and they have a gold mine of marketing information.

Rampell is presumably well aware of the marketing possibilities. Each and every confirmation message from them carries at least two

marketing

messages: one pushing you to buy an upgrade to the version you have, and another promoting some other Rampell product.

The system is not perfect, of course: send a message to me and you will probably not get acknowledgement that I read it, since my mailer does not (automatically) render HTML and go to the Web. However, prevailing upon some friends with more "standard" mailers, such as Outlook and Eudora, the system does seem to work (at least partially) with a wide variety of systems, including Macs, and Macs running Outlook under PC emulation. Cookie filters that prevent you from going to an "outside" site might limit the susceptibility of Web based mail systems, but otherwise these should all return the tracking URL.

The system has interesting limitations with regard to mailing lists, and copies. When sent to a mailing list, and even to a number of people copied on the "To:" and "Cc:" lines, only one hash is generated. Although the confirmation message from Rampell mentions the possibility of further confirmations whenever someone subsequently reads the message, in testing that does not appear to happen. Each hash appears to be good for one use, and one use only. Sending a message to a mailing list gets you a response from the first person (or the first *susceptible* person) to read it.

As noted at the beginning, there has already been some interest in the system and the privacy considerations. There have been two

mentions of the system in the RISKS-FORUM Digest, beginning with <http://catless.ncl.ac.uk/Risks/23.41.html#subj2>

In the first, Lauren Weinstein gave a reasonable account of the system and the potential problems, noting the possible solutions. The use of text-only e-mail is the best solution, and blocking the Rampell server would work as well. Turning off image display may alleviate privacy problems, but that does depend upon how different applications handle that option. Some may submit the URL to the Rampell server, and simply not display the image.

<http://catless.ncl.ac.uk/Risks/23.44.html#subj11>

A second posting noted that DidTheyReadIt is illegal in France, and speculated that travelers to France might find themselves in legal trouble if they were subscribers. In practical terms, having the Rampell software installed on your system could be evidence against you. In which case, using the modified e-mail addresses would leave you free and clear, so long as you didn't send any modified mail while in France. France might, of course, want to block Rampell's IP addresses.

A marketing consultant did an article on the errors that Rampell made in promoting the service. He suggested that an opt-out approach or option would have avoided the bad press. Unfortunately, this demonstrates that he doesn't understand how the system or the technology works. As Weinstein's analysis indicated, you have to change your software, or have some backend support, in order to prevent detection.

It is, of course, quite possible that Rampell has only the purest of motives in providing the service, and would never consider using the information obtained by providing it. I would not dare to impugn the integrity of the company or its principles and principals. However, I would note that historically:

- A certain delivery company stated that it would never sell the database of digitized signatures collected when it started using electronic pads--and then, some years later, did exactly that.

- Companies with very rigorous privacy policies, having collected significant amounts of personal customer data, have gone bankrupt, and the files have been offered for sale.

- It has, sadly, been known to happen that evil intruders have broken into companies and stolen personal information from computerized files--or even planted backdoors and logging/reporting software in their systems.

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>

⚡ Risks of ordinary GUI "pop-up" windows?

<"Cody B." <cody@zone38.net>>
Fri, 30 Jul 2004 15:40:12 -0400

Ah, yes. I don't know how many times I could potentially have sent private or even confidential information to someone inadvertently because that person decided to send me an instant message, which of course would preemptively pop up directly in front of whatever I happened to be working on at the time. The good news is that I've managed to catch myself before ever sending anything potentially risky... still, I *have* confused people with a few stray words or even a snippet of computer code that I just happened to have been in the midst of typing when they sent me an IM.

For that matter, there's already an exploit for Mozilla's XPInstall that takes advantage of this particular race condition, as demonstrated by Jesse Ruderman of squarefree.com:

<http://www.squarefree.com/archives/000487.html>

Basically, Ruderman came up with a deceptive page that causes the installer dialog to appear at just the right moment to trap your keystroke of 'Y', which of course it then interprets as 'Yes'. If you've wondered why Mozilla grays out the buttons in its install dialog for five seconds after you choose to install an extension, this is why-- it's to prevent an inadvertent installation through a stray keystroke or mouse click!

Cody "codeman38" Boisclair cody@zone38.net <http://www.zone38.net/>

REVIEW: "Stealing the Network: How to Own a Continent", Ryan Russell

<Rob Slade <rslade@sprint.ca>>

Mon, 9 Aug 2004 08:06:39 -0800

BKSTNHOC.RVW 20040721

"Stealing the Network: How to Own a Continent", Ryan Russell,
2004,

1-931836-05-1, U\$49.95/C\$69.95

%E Ryan Russell BlueBoar@thievco.com

%C 800 Hingham Street, Rockland, MA 02370

%D 2004

%G 1-931836-05-1

%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/1931836051/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1931836051/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/1931836051/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1931836051/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1931836051/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1931836051/robsladesin03-20)

%P 402 p.

%T "Stealing the Network: How to Own a Continent"

This book is fiction (more a series of short stories or scenarios than a novel), but, like Winn Schwartau's "Pearl Harbor Dot Com" (cf. BKPRHRDC.RVW, and "Terminal Compromise" before it, BKTRMCMP.RVW), the authors intend the book to be taken as a serious addition to security literature.

Chapter one is basically about hiding and paranoia. The central character seems to be using a considerable amount of money to hide while setting up some kind of crime, and then abandons everything.

The points in regard to ensuring computers and data are unrecoverable are interesting, and probably workable. The more important aspects of the plot which involve creating a team, employing cutouts, and disappearing are left almost completely undetailed. If, therefore, we are supposed to learn anything either about crime, or how to detect or prevent it, the content and information simply aren't there. The claim that the "technology" is real, and would work, is unverifiable because we haven't had any technology yet. (The writing is edgy, interesting, and mostly readable. However, it's also difficult and confused in places.)

The story continues, via another character (two, actually) in chapter two. This time the technical aspects are more detailed (and fairly realistic) although the community factors are questionable (and the story has some important gaps). (I can personally vouch for the fact that the description of the physical attributes of that specific hotel are bang on, although the ... umm ... social amenities are not.) An "Aftermath" section is at the end of every chapter. In some instances the segment provides a little advice on detecting the attacks described in the story, but this is by no means true in all cases. Nothing much is added in chapter three: a wireless network is penetrated for a second time. Man-in-the-middle attacks, some IP, and UNIX cracking are added in chapter four, phone phreaking in five, and sniffing and rootkits in six. Chapters seven and eight describe software analysis and exploits. Malware is used in chapter nine, although there are the usual unresolved problems with directing attacks and limiting spread. The lack of particulars on the

intent of
the attack makes the chapter quite perplexing.

As with any volume where multiple authors work on separate chapters,
the quality of the writing varies. (That the authors did strive together on the overall plot is evident from a few subtle ties between
different stories. An appendix lists some of the discussion in this
regard: for those interested in the process of writing and collaboration it is an interesting piece in its own right.) One specific point is that a few sections have very stilted dialogue. Overall, most of the book is readable as fiction, although it is hardly thriller level plotting.

Since it is fiction, the story has to be a story, and interesting, and therefore contain elements that are not related to the technology under examination. It is difficult to draw the line between not enough and too much, but the authors do seem to have included an awful
lot of material that is unimportant either to the security functions
or to the plot. A number of these digressions are simply confusing.

The characters used in the stories are frequently stereotypes, although not always of the same type. (I was very amused by the note
that the book attempted to remain true to geek culture, including "swearing, boorishness, and allusions to sex without there being any
actual sex.") If you watch a lot of movies with somewhat technical
themes you can recognize where quite a number of personae come from.

Basic editing is the province of the publisher rather than the author(s), but it must be noted that spelling, grammatical, and typographical errors are surprisingly common. Not enough to be a real
annoyance, but a proper copy edit would have improved the book

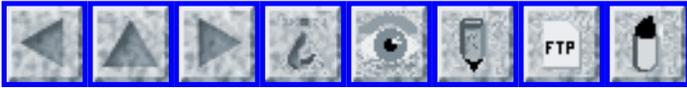
quite a
bit.

This book is certainly interesting enough (albeit rather disjointed) as fiction, and technical enough for everyone tired of the usual Hollywood view of computers. The security risks noted are real, and therefore a read through the book could be used to alert non-specialists to a number of security issues and vulnerabilities (although you'd hardly want to use it for training). I enjoyed it and I think it's got a place, although I'm having difficulty in defining where that place is.

copyright Robert M. Slade, 2004 BKSTNHOC.RVW 20040721
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

Volume 23: Issue 50

Thursday 26 August 2004

Contents

- [Sequoia's new paper audit trail voting systems](#)
[PGN](#)
- [New Mexico votes lost in 2000](#)
[Jeremy Epstein](#)
- [Mac Year 2004 bug](#)
[Tom Van Vleck](#)
- [Ford dumps Oracle system after four years of trouble](#)
[Lindsay Marshall](#)
- [Don't get stuck in the dark: a year later](#)
[Jeff Jonas](#)
- [U.S. air travel without government identification](#)
[Dan Wallach](#)
- [U.S. military sites offer a quarter million Microsoft Word documents](#)
[Diomidis Spinellis](#)
- [The GTS Katie - A risk of privatization or outsourcing](#)
[Joshua Newman](#)
- [Fire engine startup risks](#)
[J.D. Baldwin via Gary G. Taylor](#)
- [Google as back door for pay-per-view information](#)
[Sergei Lewis](#)
- [Network vandals face prison sentences](#)
[NewsScan](#)

- ["EXIT" signs too high](#)
[Henry Baker](#)
 - [Re: U.K.: Don't smile for your passport picture!](#)
[James Moyer](#) [Michael Bednarek](#)
 - [Re: Airport Express crypto broken by DVD Jon](#)
[Marshall Clow](#)
 - [REVIEW: "Computer Security for the Home and Small Office", Thomas C. Greene](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🔥 Sequoia's new paper audit trail voting systems

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

Wed, 18 Aug 2004 14:28:09 PDT

Sequoia Voting Systems has developed a voter-verified paper audit trail for their touch-screen voting system, which will be used in Nevada's state primary election. When it was demonstrated for California Senata staffers earlier in August, the audit trail failed to record votes that testers had cast. Sequoia advertises that its touch-screen machines provide "nothing less than 100 percent accuracy." [Source: Kim Zetter, Wrong Time for an E-Vote Glitch, Wired News, 12 Aug 2004; PGN-ed] [Kim did not report whether the *electronic* version was correct, although in that the paper version is supposed to be IDENTICAL in the end-results, that is itself suspect. By the way, for those of you wondering about ownership, Sequoia is not a US-owned company. PGN]

<http://www.wired.com/news/feedback/mail/1,2330,0-1246-64569,00.html>

✂ New Mexico votes lost in 2000

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

Mon, 23 Aug 2004 07:26:56 -0400

According to a WashPost article, at least 678 votes were entirely lost in one county in New Mexico in the 2000 election. In one of Rio Arriba county's voting districts, not a single vote was recorded for either Bush or Gore, and in another district not a single vote was recorded for any candidate for any office. The problem occurred with "early voters". Because it's all electronic (no paper audit trail), there's absolutely no record of what the votes should have been.

The problem wasn't a bug in the software per se, or an attack on the voting machines, but rather an error in how the county election officials entered the information about the races. The error was discovered after the election that only affected early voters, but by that time the votes were lost.

For all those election officials who say "it can't happen here", let this be a warning!

<http://www.washingtonpost.com/wp-dyn/articles/A22536-2004Aug21.html>

And BTW, the number of lost votes in that one county is greater than Gore's victory margin in New Mexico. Lest anyone think accurate voting is a partisan issue, this is one where it could have swung the state to Bush.

Had Gore won Florida, New Mexico's five electoral votes would have decided the election.

Mac Year 2004 bug

<Tom Van Vleck <thvv@multicians.org>>

Thu, 26 Aug 2004 11:47:13 -0400

From www.macintouch.com

[Jo Lejeune] Following John Delderfield's report on sudden expiry date

message in Canvas 3.5.5, we've also faced this issue last week.

After

contacting Deneba.com (now owned by ACD Systems), we've received detailed

info about this Canvas 3.5 Mac "Year 2004" bug :

To make a long story short, Canvas maintains a counter for date/time settings. In the Mac architecture, the theoretical start date for all clocks

is 1904. All times from there forward are measured after 1904. As this value

increases in size, it reached the limit in terms of the allotted length for

that string in the Canvas 3.5 Mac code. Once it hits that limit, it begins

to count in negative numbers, thus triggering a Canvas expiration.

The existence of the dialog box regarding an expiration is because the

installation code for Canvas 3.5 was the same code used for trial, NFR, and

Beta versions. So when the date count flips to negative because of this bug,

Canvas is considering that negative date to reflect that it's a trial/NFR/beta copy and is expiring it.

Interestingly, we believe this same thing could happen on Windows, but

because Windows has a clock start date of 1970, the problem wouldn't manifest till 2070.

Unfortunately, according to the same source, since "the source code and

compilers for 3.5 are not accessible at this time to allow any patches" the

only workarounds are :

- * use the mechanism for exporting files out into other formats (the EPSF format is really effective while exporting to Illustrator)
- * rolling the Mac clock settings back (only a temporary workaround)

As a more long-term solution Deneba can only recommend an upgrade to Canvas 9 (which will open all Canvas 3.5.4 or higher files directly).

✂ Ford dumps Oracle system after four years of trouble

<"Lindsay Marshall" <Lindsay.Marshall@newcastle.ac.uk>>
Wed, 18 Aug 2004 09:04:28 +0100

After four years of trying to integrate Oracle's eVEREST Internet-based purchasing software with its own existing systems, and having spent in excess of US\$200 million, Ford is reverting to legacy systems (which fortunately are still operative). Many factors were reportedly involved, although they were not specified other than supplier complaints. [Source:

Reuters, 18 Aug 2004; PGN-ed]

http://www.nzherald.co.nz/business/businessstorydisplay.cfm?storyID=3584_995&thesection=business&thesubsection=world&thesecondsubsection=usa

✂ Don't get stuck in the dark: a year later

<"Jeff Jonas" <jeffj@panix.com>>
Sat, 21 Aug 2004 05:16:01 -0400 (EDT)

For the one year anniversary of the power failure, folders were handed out at the train station "Don't Get Stuck In The Dark": trans-hudson transportation options. It lists the trains, busses and ferries and their terminals to consider options if any are closed (due to power fail, too many Republicans, etc.).

Just like the recent IEEE Spectrum article says, a year later and we're not any more prepared than before, and only resigned to accepting that more power fails are possible and even likely. I'd assert this is yet another indication that the Patriot Act ought to be repealed and the Homeland Security program de-funded. After 2 years our vital infrastructures are NOT secured!

✈ U.S. air travel without government identification

<Dan Wallach <dwallach@cs.rice.edu>>

Thu, 19 Aug 2004 19:41:02 -0500

Recently, John Gilmore has been publicly decrying the unstated Federal requirement that one must present government-issued identification (e.g., a driver's license) in order to travel via air within the U.S. Unfortunately for me, I got to test this requirement on a recent trip to give a talk at Fermilab when I managed to leave my driver's license at home. Here's what happened.

For what it's worth, I've recently taken to carrying two wallets. The large one has my money, credit cards, receipts, and other assorted junk. The

small one has my business cards and the two ID cards I most often need: my driver's license and my university ID card (a magstripe card that I need to get into my building after hours). In order to make my flight at the ungodly hour of 7:35am, I had to get up quite early. In the confusion of the morning, I managed to leave the little wallet at home. I didn't notice this oversight until I was standing in front of the ticket counter at 7:00am. In order to have gotten my driver's license, I would have had to miss my flight. Instead, I decided to see how the system would work without it.

== Intercontinental Airport: Houston, Texas

I pleaded my case to the Continental ticket agent. "Do you have any picture ID on you at all?" Nope. I showed her my Continental frequent flyer card, my credit card, and my social security card (which I probably shouldn't have had in my wallet, but that's a story for another day) as well as my boarding pass, printed that morning on my home computer. She escorted me to the security guard, with all my cards in her hand, and briefly described the situation. The guards expressed some confusion, but decided to let me through. After that, everything proceeded normally.

== Fermilab: Suburban Chicago, Illinois

My hosts at Fermilab had helpfully arranged a rental car for me. It dawned on me that I'd never get out of the rental car lot without a driver's license. I called Fermilab's travel agent and explained my predicament. As it turns out, Fermilab has a limo service that they regularly use. The travel agent made a reservation for me with the limo service, who happily

picked me up at the airport and delivered me to Fermilab.

If you're into high-energy physics, you know all about Fermilab. For the rest of us, they have a ring, about 1km in radius, around which they fling protons and anti-protons at very high energies, arranging for them to collide inside a massive detector. Those high-energy collisions cause all sorts of interesting subatomic particles to come flying out, hopefully to be detected by a variety of impressive devices. (My high school physics teacher quipped that it's like trying to learn how cars work by smashing them together and seeing what falls out.) Before September 11, the Fermilab campus was wide open, and the locals could go fishing in the lake, jogging around the ring, and so forth. These days, you have to go to a guard shack.

Visitors get a limited pass and are instructed to only go to specific places where they're allowed (e.g., the education center). I'd been told that a badge would be waiting for me. The guard asked for my ID. "Let me tell you a story," I began. Ultimately, the guard had to telephone my hosts who drove down to the guard shack to pick me up. After that, it was smooth sailing.

== O'Hare Airport: Chicago, Illinois

Everybody to whom I'd told this story was amazed that I'd gotten as far as I did, and I was repeatedly warned that O'Hare security was quite stringent. Just to make sure, I had the limo get me to the airport a full two hours before my 11:00am flight. I printed out my boarding pass using the Continental kiosk, using my credit card to authenticate myself to the system, and then explained my story to the ticket agent. "Do you have any

government issued ID?" Sorry, no. She wrote "SSSS" in big letters on my boarding pass, highlighted it in pink, and pointed me at the security checkpoint: the special security checkpoint without a line in front of it. I walked up and presented my boarding pass to the guard. "ID?" I began my story, but the only phrase that seemed to matter was "No ID", which she wrote onto my boarding pass. She then wrote "SSSS" again and circled it, also circling the original pink-highlighted copy. On I went. First the normal X-ray machine, take your laptop out, etc. Then, on the other side, they gave me the extended treatment, which normally occurs when I've been "randomly" selected. They X-rayed my shoes, swabbed my laptop for explosives, and unzipped every compartment of my luggage. After I passed all of those tests, they let me through, never once examining any of the cards I had in my wallet.

Moral of the story

While my story is hardly the same thing as a conclusive examination of the policies of all major U.S. airports, my experience shows that it is, indeed, possible to do interstate air travel without a driver's license. You're no longer using the "fast path" of the airport security apparatus, and there is clearly some variation in how the rules govern your slow path through the system. However, if you're willing to put up with the "SSSS" treatment, then it appears that you can legally travel by air within the U.S. without a government-issued ID. (Gilmore acknowledges this in his lawsuit, which is focused on finding out where the requirement for presenting ID came from, in the first place.)

Postscript

As a Continental frequent flyer, I was invited to show up at the airport to be measured for a new biometric-based system that they've installed in Houston. (I think it measures fingerprints, but I'm not entirely sure.) I was out of town, and thus unable to give that system a shot. They do require several forms of ID to get yourself registered, so it will have to wait for another day. Maybe I'll give it a try and write something about it later for RISKS. For all the known issues with biometric authentication, it's quite difficult to leave your fingerprints at home in the wrong trousers.

✈ U.S. military sites offer a quarter million Microsoft Word documents

<Diomidis Spinellis <dds@aueb.gr>>

Wed, 25 Aug 2004 23:33:02 +0300

I was Google-searching for the Air Force Operational Test & Evaluation Center publication "Software Maintainability - Evaluation Guide". To make my search more efficient I restricted it to military (.mil) sites, using the Google keyword "site:.mil".

I was not able to find the publication I was looking for, but was surprised to see a number of Microsoft Word documents in the search results. Most comp.risks readers are surely aware that earlier versions of Word, running on earlier versions of Windows would include in unused portions of the document file anything that was previously in the memory space where Word

was executing. A number of past comp.risks articles have documented embarrassing incidents of confidential data leaking through Microsoft Word documents; see for example [RISKS-17.76](#), Thomas Gebe, "Risks of using Microsoft Word", and [RISKS-21.40](#), Clive Page, "Word file turns into two disjoint texts".

I then modified my search to look for Microsoft Word documents made available on the web by US military sites:

<http://www.google.com/search?q=+site%3A.mil+filetype%3Adoc>

The search reports about 266,000 results. I am aware that the US military implements a strict separation policy between operational computers and machines connected to the Internet, and that truly confidential data is probably stored in multilevel secure systems protected by mandatory access controls.[*] However, I doubt that no gems are to be found in such a large volume of inherently leaky data.

Diomidis Spinellis - <http://www.dmst.aueb.gr/dds>

Athens University of Economics and Business

[* Probably not multilevel secure. More likely "system high" all aggregated together at a particular level such as Top Secret. PGN]

✶ The GTS Katie - A risk of privatization or outsourcing

<Joshua Newman <katzenpigs@fastemail.us>>

Tue, 24 Aug 2004 14:00:55 -0700

<http://www.kathryncramer.com/wblog/archives/000515.html>
http://cbc.ca/cgi-bin/templates/view.cgi?/news/2000/08/03/katie_confront000803

To summarize this rather odd story in a single sentence: For almost

two weeks in July 2000, about 10% of the Canadian Army's equipment and a number of Canadian soldiers were made unavailable because the GTS Katie, a privately-owned American vessel carrying them home to Canada under a contract with the Canadian Government, became embroiled in a financial dispute between subcontractors; its owners, Third Ocean Marine Navigation, refused to deliver the troops and materiel until the dispute was resolved. Finally the ship was boarded and taken over by Canadian military personnel and escorted by Canadian warships to port.

✶ Fire engine startup risks (J.D. Baldwin)

<"Gary G. Taylor" <gary@donavan.org>>

Wed, 18 Aug 2004 14:59:14 -0700

>From a discussion on scarydevilmonastery. Here's the original post, pasted

>from google groups; the thread continues:

From: J.D. Baldwin (INVALID_SEE_SIG@example.com.invalid)

Subject: This is why people hate computers

View this article only

Newsgroups: alt.sysadmin.recovery

Date: 2004-08-15 11:58:00 PST

I've been ranting and raving, with monotonically increasing intensity (both here and IRL), about how much more computers in general are sucking now than they did a few short years ago -- and about how the trend shows no sign of changing. But this is real Next Level stuff.

A warning note from one of the deputy fire chiefs in the city department in which I am a part-time firefighter:

With [certain trucks], there are computers that activate when the ignition is turned on. The computer diagnoses several system checks on the engine prior to it starting. If you do

not allow the computer to complete its system check prior to starting the engine, the engine will start, but then immediately shut down. You then have to wait several minutes to allow the computer to reset before the engine will start. I would recommend the following procedure to be followed to prevent this from occurring.

1. Turn the ignition switch on.
2. Watch your instrument panel at the top of the dash and it will show all the checks that are occurring.
3. All the indicator needles on the gauges will move almost completely on the dials and then return to their normal positions.
4. When the gauge indicators return to their normal position, you can then start the engine.

Okay, let me get this straight: you have taken the simplest technical procedure known to man -- starting a vehicle -- and turned it into a ... well, not a **complex** operation, exactly, but what the hell kind of "computer" can't handle a quick reset? Some driver gets just a little overexcited, and turns the switch in one smooth motion to "start" (you know, the way everyone starts every other car in the world?), and now the apparatus is out of commission for "several minutes"? So a fucking COMPUTER can pull its head out of its ass?

Meanwhile, of course, someone is having a heart attack, or perhaps his house is burning down with a kid inside, or ... you get the idea.

🔥 Google as back door for pay-per-view information

<Sergei Lewis <moonshadow@toothycat.net>>
Mon, 23 Aug 2004 13:08:07 +0100 (BST)

Google's bot is often allowed to crawl areas of sites normally restricted to subscription-only or pay-per-visit customers. This practice risks

rendering

the site content vulnerable to automated retrieval from the Google cache.

More here: <http://www.toothycat.net/wiki/wiki.pl?ScriptWritingPeople>

✦ Network vandals face prison sentences

<"NewsScan" <newsscan@newsscan.com>>

Thu, 05 Aug 2004 08:06:50 -0700

Pleading guilty to attempts to hack into the national computer system of the Lowe's home improvement chain and steal credit card information, three Michigan men now face sentences of up to 25 years in prison. In the indictment, federal prosecutors had said that the men accessed the wireless network of a Lowe's store and used that connection to enter the chain's central computer system and eventually to reach computer systems in Lowe's stores across the country. Lowe's executives say the men did not gain access to the company's national database and that all customers' credit card information are secure. [*San Jose Mercury News*, 5 Aug 2004; NewsScan Daily, 5 August 2004]
<http://www.siliconvalley.com/mld/siliconvalley/9320081.htm>

✦ "EXIT" signs too high

<Henry Baker <hbaker1@pipeline.com>>

Fri, 13 Aug 2004 13:39:44 -0700

This is not a new risk, nor is it even computer-related. However, many reading this list travel a lot, so I thought it might be informative.

I've noticed that all hotels provide "EXIT" signs, but they are all up near the ceiling. Unfortunately, in the case of a fire, there will also be smoke up near the ceiling, so you'll never see these EXIT signs.

This is why airplanes have installed light systems on or near the floor, so you can crawl your way to an exit if necessary.

What will it take for hotels and other public facilities to move their exit signs down to locations where they might actually be useful in the case of a real fire?

[Although out of the RISKS mainstreams, this item has some relevance because of the lack of emergency environmental foresight, which also arises in some computer-based systems. PGN]

✈️ **Re: U.K.: Don't smile for your passport picture! ([RISKS-23.49](#))**

<james@moyer.com>

Thu, 19 Aug 2004 21:37:00 -0700 (PDT)

The non-smile requirement for UK passport pictures has also been adopted by Canada:

http://www.ppt.gc.ca/passports/get_photo_specs_e.asp

Interestingly, biometric systems probably work best with non-color photos. After all, humans work best with non-color photos (the definition of the face comes out strongest in black and white. Even today,

headshots used
by actors are black and white for this reason.)

Given this, photo ID cards should have always been in black and white, why they are in color remains a bit of a mystery to me.

✶ Re: U.K.: Don't smile for your passport picture! ([RISKS-23.49](#))

<Michael Bednarek <mb@tgm.com.au>>

Mon, 16 Aug 2004 13:05:06 +1000

This contrasts with the position of passport officials in Germany who, reluctantly, allowed a man to stick out his tongue on a passport photo.

[www.iol.co.za/index.php?
set_id=1&click_id=79&art_id=iol1091505398579T520](http://www.iol.co.za/index.php?set_id=1&click_id=79&art_id=iol1091505398579T520)

He had to sign a statement exculpating the officials of any consequences of the risks of such a photo at foreign border patrols.

Michael Bednarek, IT Manager, Tactical Global Management
Waterfront Pl, Brisbane 4000, Australia. <http://mcmbednarek.tripod.com/>

✶ Re: Airport Express crypto broken by DVD Jon ([RISKS-23.49](#))

<Marshall Clow <marshall@idio.com>>

Sun, 15 Aug 2004 07:19:02 -0700

>Jon "DVD Jon" Johansen has cracked the Apple Lossless encryption ...

This seems unlikely to me.

In the first place, there is no such thing as "Apple Lossless Encryption", but rather "Apple Lossless Compression". What appears to have happened is that Mr. Johansen has found the RSA key used to communicate with the Airport Express - a completely different accomplishment.

[Note that he doesn't claim to be able to create "Apple lossless" files, but rather to send them to the Airport Express base station.]

Marshall Clow Idio Software <mailto:marshall@idio.com>

★REVIEW: "Computer Security for the Home and Small Office", Greene

<Rob Slade <rslade@sprint.ca>>
Tue, 17 Aug 2004 08:46:31 -0800

BKCMSCHO.RVW 20040727

"Computer Security for the Home and Small Office", Thomas C. Greene, 2004, 1-59059-316-2, U\$39.99/C\$57.95

%A Thomas C. Greene <http://basicsec.org> tcgreene@verizon.net

%C 2560 Ninth Street, Suite 219, Berkeley, CA 94710

%D 2004

%G 1-59059-316-2

%I Apress

%O U\$39.99/C\$57.95 510-549-5930 fax 510-549-5939 info@apress.com

%O <http://www.amazon.com/exec/obidos/ASIN/1590593162/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1590593162/robsladesinterne)

<http://www.amazon.co.uk/exec/obidos/ASIN/1590593162/robsladesinterne>

<http://www.amazon.ca/exec/obidos/ASIN/1590593162/robsladesinterne>

%P 405 p.

%T "Computer Security for the Home and Small Office"

Thomas Greene asked me to do the technical review for this book, which

speaks to his bravery, regardless of what it says about his wisdom.
So
there's no point in pretending that I'm unbiased here. However, I
must say
that I was bracing myself for yet another security book by a writer
rather
than a techie--and was delightfully surprised, right from the
beginning, at
how useful Greene's material was.

The "Introduction" is a bit unusual: it doesn't lay out the theme or
structure of the book, but jumps right into dispelling myths and
making
suggestions. You will be introduced to the fact that Greene is an
Open
Source/Linux ... well, fanatic might be too mild a term, extremist
might be
closer to reality. There is also a section on how to get, and
configure,
the Mozilla Web browser for safer surfing.

Chapter one deals with the dark side of computing, and a variety of
attendant risks. The descriptions sometimes gloss over technical
niceties,
but the assessment of threat levels is more reasonable than in most
similar
works. Vulnerabilities and means of attack are presented in chapter
two.
An excellent and helpful list of Windows services that most users
can turn
off at no cost to function (and considerable addition in safety) is
provided, as is a similar list for Linux. A sensible review of
social
engineering is presented in chapter three. More advanced tools are
introduced in chapter four, but, in contrast to many similar works,
the text
goes on to provide explanations and suggestions on use.

Chapter five explains many places where information may be stored on
your
computer (and network) in the course of normal operations, and how
to clean
up after yourself. Greene really lets himself go in his promotion
of Linux
and Open Source software in chapter six, presenting sanguine

arguments. In chapter seven, a number of anecdotes are used to support the idea that you can learn about the computer and take control of your own safety, without having to live in fear of the unknown, or be dependent upon consultants of unknown competence.

This book presents material for the intelligent but non-specialist computer user. The text is readable, and the content useful. It does not cover the entire range of computer security, but it does provide valuable information for those who rely on computers for their work, and would like to achieve a level of security that is significantly higher than that available by default, without having to spend a great deal of time and money on it. Particularly for the Windows XP user, this is my primary endorsement for a computer security book. I would also recommend the work to security professionals, at least as a reference, since it contains Windows configuration that system administrators should know, and the vast majority don't.

copyright Robert M. Slade, 2004 BKCMSCHO.RVW 20040727
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

Volume 23: Issue 51

Tuesday 31 August 2004

Contents

- [NASA Spirit nearly done in by DOS](#)
[Hank Nussbacher](#)
- [Sum of a Glitch](#)
[Bev Harris via David Chessler and Dave Farber's IP](#)
- [The case of the screaming telephone](#)
[Debora Weber-Wulff](#)
- [The toll collection hassle in Germany](#)
[Debora Weber-Wulff](#)
- [Website offers CNID falsification service](#)
[Kevin Poulsen via Monty Solomon](#)
- [Rick Broadhead's Dear Valued Customer](#)
[Amit Asaravala via Monty Solomon](#)
- [Canvas expiration 'bug': *not* a Mac OS issue](#)
[Matt Gough via Bob Grant](#)
- [Accounting software number issues](#)
[Darryl Smith](#)
- [Another animal-caused power interruption](#)
[Geoffrey Brent](#)
- [Privacy concern over Australian e-mail law](#)
[NewsScan](#)

- [Lack of sanity checking in Web shopping cart software](#)
[Richard Kaszeta](#)
 - [Correction to New Mexico, Florida, Bush & Gore](#)
[Jeremy Epstein](#)
 - [REVIEW: "Know Your Enemy", Honeynet Project](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ NASA Spirit nearly done in by DOS

<Hank Nussbacher <hank@mail.iucc.ac.il>>

Mon, 30 Aug 2004 11:44:22 +0300

From Wired -
[http://www.wired.com/news/space/0,2697,64752,00.html?
tw=wn_tophead_3](http://www.wired.com/news/space/0,2697,64752,00.html?tw=wn_tophead_3)

Ctrl-alt-del: The communications failure that nearly brought NASA's Spirit mission to Mars to an early end in January was caused by an unforeseen aspect of the DOS file system, a Jet Propulsion Laboratory scientist said Monday. During a presentation at Stanford University's Hot Chips conference, JPL software developer Robert Denise said his team did not anticipate that a DOS file system containing directory information would continue to grow after other files had been deleted from the Spirit rover's flash memory. This oversight, coupled with an instruction to copy the contents of Spirit's flash memory into its limited random access memory launched the rover into a nearly disastrous cycle of errors and reboots. Fortunately for NASA, the JPL team was able to upload a software upgrade

and disable the copy instruction before the rebooting completely drained the rover's batteries.

Spirit has performed well ever since, according to NASA. In April, the agency extended the rover's mission -- along with that of its twin, opportunity -- for an additional five months. Both rovers have already detected evidence of the water that is thought to have once existed on Mars.

✶ FWD: Sum of a Glitch (Bev Harris via Dave Farber's IP)

<David Chessler <chessler@usa.net>>

August 27, 2004 11:54:39 PM EDT

Sum of a Glitch, by Bev Harris

In the Alabama 2002 general election, machines made by Election Systems and Software (ES&S) flipped the governor's race. Six thousand three hundred Baldwin County electronic votes mysteriously disappeared after the polls had closed and everyone had gone home. Democrat Don Siegelman's victory was handed to Republican Bob Riley, and the recount Siegelman requested was denied. Three months after the election, the vendor shrugged. "Something happened. I don't have enough intelligence to say exactly what," said Mark Kelley of ES&S.

When I began researching this story in October 2002, the media was reporting that electronic voting machines are fun and speedy, but I looked

in vain for articles reporting that they are accurate. I discovered four magic words, "voting machines and glitch," which, when entered into a search engine, yielded a shocking result: A staggering pile of miscounts was accumulating. These were reported locally but had never been compiled in a single place, so reporters were missing a disturbing pattern.

I published a compendium of 56 documented cases in which voting machines got it wrong.

How do voting-machine makers respond to these reports? With shrugs. They indicate that their miscounts are nothing to be concerned about. One of their favorite phrases is: "It didn't change the result."

Except, of course, when it did:

In the 2002 general election, a computer miscount overturned the House District 11 result in Wayne County, North Carolina. Incorrect programming caused machines to skip several thousand party-line votes, both Republican and Democratic. Fixing the error turned up 5,500 more votes and reversed the election for state representative.

This crushing defeat never happened: Voting machines failed to tally "yes" votes on the 2002 school bond issue in Gretna, Nebraska. This error gave the false impression that the measure had failed miserably, but it actually passed by a 2-to-1 margin. Responsibility for the errors was attributed to ES&S, the Omaha company that had provided the ballots and the machines.

According to the Chicago Tribune, "It was like being queen for a day--but only for 12 hours," said Richard Miholic, a losing Republican candidate for alderman in 2003 who was told that he had won a Lake County, Illinois, primary election. He was among 15 people in four races affected by an ES&S vote-counting foul-up.

An Orange County, California, election computer made a 100 percent error during the April 1998 school bond referendum. The Registrar of Voters Office initially announced that the bond issue had lost by a wide margin; in fact, it was supported by a majority of the ballots cast. The error was attributed to a programmer's reversing the "yes" and "no" answers in the software used to count the votes.

A computer program that was specially enhanced to speed the November 1993 Kane County, Illinois, election results to a waiting public did just that--unfortunately, it sped the wrong data. Voting totals for a dozen Illinois races were incomplete, and in one case they suggested that a local referendum proposal had lost when it actually had been approved. For some reason, software that had worked earlier without a hitch had waited until election night to omit eight precincts in the tally.

A squeaker -- no, a landslide--oops, we reversed the totals -- and about those absentee votes, make that 72-19, not 44-47. Software programming errors, sorry. Oh, and reverse that election, we announced the wrong winner. In the 2002 Clay County, Kansas, commissioner primary,

voting machines said Jerry Mayo ran a close race but lost, garnering 48 percent of the vote, but a hand recount revealed Mayo had won by a landslide, receiving 76 percent of the vote.

<http://www.progressivetrail.org/articles/040825Harris.shtml>

IP Archives at: <http://www.interesting-people.org/archives/interesting-people/>

✶ The case of the screaming telephone

<Debra Weber-Wulff <weberwu@fhtw-berlin.de>>

Sat, 28 Aug 2004 21:27:47 +0200

The German IT giant, Siemens, has had to recall the entire production of its fancy new x65 mobile phone family because of a software error. This phone, which was filled to the brim with fancy stuff and on offer from most of the mobile operators, has an unfortunate mis-feature. The telephone has a default melody that it plays just before it dies on account of the battery being too low, sort of a swan song.

The problem is that this melody is turned on by default and when it plays, it plays at an ear-splitting noise level that is loud enough to possibly cause hearing damage. Of course this only would happen in the case of someone having it in their ear when it plays, which Siemens says is rare [but has happened to me with my hands-free a few times in the

past years -
dww]

No one had been reported hurt by the phone yet, but Siemens was able to reproduce this in the lab, so the company decided to withdraw the phone and caution customers to turn the feature off until they can get a software update. They do get extra points for being proactive about the problem [1]

This will surely wreak havoc in the balance sheet, and as my newspaper (the Berliner Zeitung [2]) nastily notes, it chalks up one more disaster for Siemens in the area of quality management. Just to mention three recent problems, the Combino street car had to be recalled from all over the world because the body was wrongly constructed, the diesel ICE trains have many problems and the airport Skytrain in Düsseldorf has an annoying tendency to stop for a reboot between stations. Risks readers will remember tales of software controlled rail switches ...

Oh yes, glad you asked, many Siemens divisions seem to be ISO 900x certified...

[1] Siemens press release
http://www.siemens.com/index.jsp?sdc_sectionid=4&sdc_langid=0&sdc_contentid=1207000

[2] <http://www.berlinonline.de/berliner-zeitung/wirtschaft/371491.html>

(but will probably get a new address in the archive, this is called "Qualitätsproblem Siemens" and is written by Thomas H. Wendel.

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Internationale

Medieninformatik Treskowallee 8, 10313 Berlin Tel: +49-30-5019-2320

✶ The toll collection hassle in Germany

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

Sat, 28 Aug 2004 21:30:17 +0200

The Berlin newspaper "Tagesspiegel" reports [1] that there is a real danger of the new attempt to get the toll collection scheme up and running by the beginning of the year failing. Only 37 000 updated so-called "on-board units" have been built into trucks, there need to be at least 400 000 by January 1 in order for the system to work. The truck owners are being offered 50 € if they have one of the first 200.000 new OBUs built in by the end of the year. Of course, many already paid to have a previous version of the OBU installed, so they are understandably reluctant to run out and have this radio-sized box installed in their cabs.

This is the third attempt to get it to work, the system was originally supposed to begin in the summer of 2003 so that the German government can reap in money to pay for roads projects for the world soccer championships in 2006.

A speaker for Toll Collect, the consortium responsible for the mess, says that they can actually start with less OBUs, although this will make long

lines at rest stops and gas stations as drivers purchase tickets. A government spokesperson is quoted as being unaware of any problems that might delay the third start.

Toll Collect is run by DaimlerChrysler Services AG (45%), Deutschen Telekom AG (45%) and the French company Cofiroute S.A. (10%).

[1] <http://archiv.tagesspiegel.de/archiv/27.08.2004/1324184.asp>

[I played with one of the terminals at a rest stop and actually managed to print a toll ticket for myself. I was able to enter a completely stupid route, the system had no problems with this. The usability of the menu system leaves a bit to be desired, this will surely contribute to nice long lines if they ever get this going -dww]

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Treskowallee 8, 10313 Berlin
Tel: +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

🔥 Website offers CNID falsification service (Kevin Poulsen)

<Monty Solomon <monty@roscom.com>>
Tue, 31 Aug 2004 08:50:55 -0400

By Kevin Poulsen, SecurityFocus, 27 Aug 2004

Overdue debtors beware: You may not be able to rely on CNID [Calling Number Identification] to screen out those annoying bill collectors much longer. A

California entrepreneur has a plan to bring the hacker technique of CNID spoofing to the business world, beginning with collection agencies and private investigators. Slated for launch next week, Star38.com would offer subscribers a simple Web interface to a CNID spoofing system that lets them appear to be calling from any number they choose. "It creates an extra avenue for them to have someone pick up the phone," says founder Jason Jepson.

CNID spoofing has for years been within the reach of businesses with certain types of digital connections to their local phone company, and more recently has become the plaything of hackers and pranksters exploiting permissive voice over IP systems. But Star38.com appears to be the first stab at turning CNID spoofing into a commercial venture. Jepson claims the service will charge a twenty-five cent connection fee for each call, and seven to fourteen cents per minute. ...

<http://securityfocus.com/news/9419>

[Lightly PGN-ed for RISKS]

✶ Rick Broadhead's Dear Valued Customer (Amit Asaravala)

<Monty Solomon <monty@roscom.com>>

Fri, 27 Aug 2004 14:40:55 -0400

Amit Asaravala, Loser Delivers Laughs, Wired.com, 27 Aug 2004

In the struggle between humanity and technology, humanity is

clearly getting
its ass kicked. That is the conclusion one comes to after
reading Rick
Broadhead's Dear Valued Customer, You Are a Loser (\$10, Andrews
McMeel
Publishing), a hilarious look at the maddening tendency for
technology to
create as many problems as it solves. Published in May with
little fanfare,
the 315-page paperback is a compilation of more than 100 true
stories of
technological blunder and misfortune. Some of the stories are
bizarre, some
are pathetic -- but all are highly entertaining.

Take, for instance, the case of the Ukrainian businessman who
put 50 new
pagers -- a gift for his employees -- in the back seat of his
car and then
promptly crashed into a lamppost when they all began beeping at
the same
time. The culprit? A welcome message sent by the pager company
to each of
the pagers.

Then there's the story of the German couple who carefully
followed the
driving directions given by their car's satellite navigation
system -- right
up until it guided them into a river. ...

<http://www.wired.com/news/culture/0,1284,64734,00.html>

✶ Canvas expiration 'bug': *not* a Mac OS issue (Matt Gough)

<Bob Grant>

Fri, 27 Aug 2004 18:35:29 -0500

Please see the recently expanded thread at Macintouch which

reveals that the problem stems from a deliberate decision by Deneba to have Canvas disabled at a time of their choosing. It has nothing to do with the normal and correct functioning of the Macintosh system clock.

<http://www.macintouch.com/canvas.html>

Relevant excerpt by Matt Gough

With reference to the problem with Canvas expiring soon, the response from Deneba (now ACD Systems) is utter nonsense.

The System clock on the Mac flipped over to a 'negative' value on Wednesday, January 19, 1972 at 3:14:08 am, and so has been negative since long before the Mac existed.

I have been debugging Canvas here using the venerable Macsbug and have determined that it will deliberately expire at 12:30pm on 31st August 2004.

Thankfully this expiry date is stored in a resource within Canvas, and so anyone with a copy of ResEdit can fix their Canvas to alter this expiry date.

= = = = =

There follows (at the above link) a ResEdit patching technique, provided by Mr. Gough, to restore functionality until 31 August 2039. Bob

Accounting software number issues

<"Darryl Smith" <Darryl@radio-active.net.au>>

Thu, 26 Aug 2004 11:51:00 +1000

Here in Australia, the MYOB (www.myob.com.au) Accounting software is very popular. Like many other vendors they are also bundling services like credit card merchant services, superannuation and the like.

When someone makes a payment you will be notified the next day by email with a file that automatically updates your accounting file. For services like paying my superannuation account (like a 401K), I need to send a message authorizing the transaction from the accounting software connecting to their server.

Today I got a notification informing me that this service will be our for four hours on Saturday. Nothing wrong with that. Just that the footer of the email had some of my data on in.

Company: Radioactive Networks Pty Ltd
Serial Number: 6.16054E+11

The serial number used to be a seven digit number until the beginning of this year. They have now updated all numbers, increasing the number of digits. As you can see they forgot to update their email system to handle the long numbers correctly.

Not only have they converted to Scientific Notation, but they have also rounded. I am just wondering where else they round their numbers.

Darryl Smith, VK2TDS POBox 169 Ingleburn NSW 2565 Australia
Mobile 0412 929 634 [+61 4 12 929 634 Intl] www.radio-active.net.au/blog/

⚡ Another animal-caused power interruption

<Geoffrey Brent <g.brent@student.unsw.edu.au>>

Thu, 26 Aug 2004 08:59:33 +1000

This may be a new size record:

"A hydroelectric plant in Nova Scotia remained closed Tuesday after a wayward humpback whale swam through the underwater gates connecting the facility with the Atlantic Ocean... The plant was shut down because officials were concerned the whale could get trapped in its turbine. Canada's Fisheries Department spokesman Jerry Conway said the whale did not appear to be in immediate danger."

http://story.news.yahoo.com/news?tmpl=story&cid=517&ncid=753&e=3&u=/ap/20040825/ap_on_re_ca/canada_whale_trapped

⚡ Privacy concern over Australian e-mail law

<"NewsScan" <newsscan@newsscan.com>>

Tue, 31 Aug 2004 07:25:20 -0700

Civil libertarians say that a proposed Australian law could allow authorities easy access to private, stored e-mails without a warrant, giving many new government bodies to access private e-mails, voicemail messages and SMS messages. Under current laws, unopened e-mails can only be

accessed if
they involve serious crime and only with a telecommunications
intercept
warrant. If the bill is passed authorities would need only a
search warrant,
or in some cases no warrant at all, according to online civil
liberties
group Electronic Frontiers Australia (EFA). [*The Australian*
30 Aug 2004;
NewsScan Daily, 31 Aug 2004, Rec'd from J. Lamp]

<http://australianit.news.com.au/articles/0,7204,10613440%5E15306%5E%5Enbv%5E,00.html>

⚡ Lack of sanity checking in Web shopping cart software

<Richard Kaszeta <rich@kaszeta.org>>

Fri, 27 Aug 2004 14:25:19 -0500

The Lack of Sanity Checking in Web Shopping Cart Software
or "The Story of the 1.1 Cocktail Shakers"

Recently, I was browsing the web site of a large Burlington, NJ-
based
retailer, and decided to add a cocktail shaker to my shopping
cart.

Due to some slightly twitchy fingers resulting from my morning
coffee, I
accidentally entered the number 1.1 (instead of 1) to the the
"quantity
desired" box, and found myself with a shopping cart containing
1.1 cocktail
shakers at \$9.99/each, for a grand total of \$10.99 plus shipping
of \$5
(shipping is \$5/item, for a total of \$5.50 for 1.1 items). At
this point
curiosity got the best of me, and I decided to check out. To my

surprise,
the site's shopping cart software never did a sanity check on
the data, and
simply confirmed my order for 1.1 cocktail shakers, and I also
received an
email confirmation for "Qty: 1.1." My credit card was charged
for \$16.49.

Due to the atomic nature of cocktail shakers, it's obvious that
at some
point something was going to have to give, and this apparently
happened in
the shipping department: my "Shipping Confirmation Notice"
listed the
quantity shipped as "1", but confirmed that the total charges
were still
those for 1.1 shakers (\$16.49) instead of the appropriate
charges for a
single shaker (\$14.99). Indeed, as expected, I received a
single cocktail
shaker in the mail, with a receipt for "Cocktail Shaker, Qty 1",
also
listing the inappropriate price.

It was relatively easy to square the charges away, but the
company's
customer service representative had to get a supervisor
involved, as they
apparently hadn't seen this before.

The RISK is obvious: a lack of sanity checking on input data
resulted in a
spurious order being sent through the system, with additional
lack of
double-checking resulting in a discrepancy between what was
shipped and what
was billed. Months later, the error remains uncorrected, and
you can still
order fractional items, with the additional risk that a
dishonest customer
may be able to able to get a discount by ordering slightly less
than a
single item and hope for a "roundup" when it gets shipped.

Really, it's too bad, because I was really thinking that my cocktail shaker is a bit small, and could use another 10% of volume. :) That, or perhaps I should buy 0.9 shakers to go with my 1.1 shakers to make a matched pair.

Richard W Kaszeta <rich@kaszeta.org> <http://www.kaszeta.org/rich>

[On the other hand, a round-down would be more consistent: Suppose you had ordered .99 shakers. You probably would have been billed for .99 shakers and received none. Shake-ri-la. PGN]

✂ Correction to New Mexico, Florida, Bush & Gore

<Jeremy Epstein <jeremy.epstein@cox.net>>
Mon, 30 Aug 2004 8:15:00 -0400

At the conclusion of my note in [RISKS 23.50](#), I wrote "Had Gore won Florida, New Mexico's five electoral votes...".

Steve Klein pointed out that regardless of the result in New Mexico, it wouldn't have impacted the result, and whoever carried Florida won the election. Specifically:

> Bush won the electoral vote by 271-266; 270 votes are needed to win.
> (There are a total of 538 electors; one abstained.)
>
> In 2000, Florida had 25 electoral votes, and New Mexico had 5.
> (Due to apportionment, Florida will have 27 electoral votes in 2004.)

>
> If Gore won Florida and New Mexico, he'd have 291 electoral
votes.
> If Gore won Florida but lost New Mexico, he'd have 286
electoral
> votes.
>
> Either way, Gore would have won, and New Mexico would not have
made a
> difference.

Obviously losing votes is a very bad thing, but my conclusion
was incorrect.

Thanks to Steve for pointing this out.

🔥 REVIEW: "Know Your Enemy", Honeynet Project

<Rob Slade <rslade@sprint.ca>>

Tue, 3 Aug 2004 07:59:29 -0800

BKKNYREN.RVW 20040618

"Know Your Enemy", Honeynet Project, 2004, 0-321-16646-9,
U\$49.99/C\$71.99

%A Honeynet Project project@honeynet.org www.honeynet.org/book/

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

%D 2002

%G 0-321-16646-9

%I Addison-Wesley Publishing Co.

%O U\$49.99/C\$71.99 416-447-5101 fax: 416-443-0948

%O [http://www.amazon.com/exec/obidos/ASIN/0321166469/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0321166469/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0321166469/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0321166469/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0321166469/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0321166469/robsladesin03-20)

%P 768 p. + CD-ROM

%T "Know Your Enemy, Second Edition: Learning About Security Threats"

The first edition of "Know Your Enemy" was a lot of fun, and it also contained some valuable advice if you were brand new to the idea of a honeypot, and wanted to get started quickly. This second edition has taken advantage of another couple of years in the development of honeypots and honeynets, and provides guidance on a new generation of the technology. More than that, it promises, and mostly provides, more detailed information on the analytical aspects of honeynet operation, including the all-too-often neglected topic of network forensics. The page count has more than doubled.

I have frequently said that any book with "hack," or any variant thereof, in the title is automatically suspect. This work helps prove my point, first, because the Honeynet Project members have not used the term (they refer to attackers as blackhats), and the text also notes the problems with "exploit" type books: they list old and known attacks, most of which are protected against, and say nothing about the attackers and how they work.

Part one describes the honeynet. Chapter one points out the value of "knowing the enemy" and the history of the Honeynet Project. Chapter two explains what a honeypot is, leading to details on how a honeynet works, in terms of architecture, policies, and the risks and responsibilities of operating one, in chapter three. Building a first generation honeynet, in chapter four, presents specific details, although a number of

concepts have already been given. The lessons from the early years of the project have led to a second generation of design, which is outlined in chapter five. Using a single machine to create a virtual network of simulated machines is described in chapter six. Chapter seven extends all of this into distributed networks of machines. A number of legal issues are discussed in chapter eight: specific citations are primarily from US laws, but general concepts are also examined.

Part two concerns the analysis of data collected from the Honeynet. Chapter nine looks at the various sources of evidence. Network forensic ideas and tools are reviewed in chapter ten, although the material does tend to jump abruptly from Networking 101 to an assumption that the reader can parse Snort captures. Fundamentals of the data recovery aspects of computer forensics are given in chapter eleven, leading to the specifics of UNIX recovery in chapter twelve, and Windows in thirteen. (These chapters contain details of up to date tools not available in most of the standard computer forensic texts.) I was delighted to see that chapter fourteen addresses reverse engineering, although only in a limited subset of the full range of software forensics. Chapter fifteen reiterates the sources from chapter nine, and suggests centralized collection and management of data.

Part three explains what the project has determined about "the enemy" by the types of attacks that have been launched and detected. Chapter sixteen

takes a random crack at several topics related to the blackhat community: a number of points are interesting, but few are very helpful. A general overview of attacks is given in chapter seventeen. Specific attacks, and analyses, on Windows, Linux, and Solaris are detailed in chapters eighteen to twenty. Future trends are projected in chapter twenty one.

The repetition of material that plagued the first edition has been cleaned up to a great extent, although the text would still benefit from a tightening up of the material in some chapters. In addition, the early examples are not thoroughly explained, making the reader initially feel that only a firewall audit log specialist would be able to understand what is being said. However, as with the first edition, most of the book is written clearly and well, and it is certainly worth reading. In addition, the new material definitely makes this not merely an interesting read, but something that has the potential to be a serious reference in the forensic field.

copyright Robert M. Slade, 2004 BKKNYREN.RVW 20040618
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

Volume 23: Issue 52

Thurs 9 September 2004

Contents

- [Shutting the train door before the commuter has bolted?](#)
[Michael Bacon](#)
- [Illinois Secretary of State computer outage](#)
[J H Haynes](#)
- [Overcomputerization enlightenment](#)
[Joseph A. Dellinger](#)
- [More ID theft, via laptop](#)
[David Lesher](#)
- [Missouri vote-by-fax](#)
[PGN](#)
- [E-voting in Nevada](#)
[NewsScan](#)
- [Diebold GEMS central tabulator contains a stunning security hole](#)
[Bev Harris via EEkid](#)
- [Using a paper trail to verify electronic voting machine results](#)
[Diomidis Spinellis](#)
- [Election verification in Venezuela](#)
[Peter B. Ladkin](#)
- [ATMs offer too much information](#)
[Brendan Kehoe](#)

- [Risk of using open forums for disaster recovery](#)
[Espen Andersen](#)
 - [Re: NASA Spirit nearly done in by DOS](#)
[Gene S. Berkowitz](#)
 - [REVIEW: "Security Assessment", Greg Miles et al.](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Shutting the train door before the commuter has bolted?

<"Michael \ (Streaky\) Bacon" <himself@streaky-bacon.co.uk>>
Sun, 5 Sep 2004 12:16:15 +0100

There are reports in today's UK press (echoing previous reports) that "Southern" (New Southern Railway Ltd - a railway operator around London, England) is having problems with the doors in its new, multi-million (Pounds Sterling), trains. In some cases these will not open even when the train is stopped at a platform. One train is reported to have trapped its passengers inside for 45 minutes.

It appears that the new trains are equipped with a GPS-based system to determine whether the train is stopped at a platform or not and whether the platform is long enough to allow (all) the doors to be opened. If the system does not determine this, the doors will not open. There have been a number of accounts of the system failing to detect the GPS signal and reports too that the received signal has overloaded the system. The problem has been compounded by some drivers' inexperience of the new

trains leading
to their inability to determine promptly how to open the doors
manually.

Quoting a spokesperson for Southern, "[The trains] have a
selective door
opening system on board which takes a combination of GPS
satellite signals
to tell the train exactly which station it is located at and
then ensure
only the number of doors that are accommodated on the platform
are opened.

[...] Sometimes we have had problems with the train not
locating itself
and thus not opening the doors at all."

Apparently, in addition, the system sometimes does not recognise
that the
train has stopped at a longer platform (than originally
scheduled) and the
system has to be "reprogrammed" by the driver before the train
can proceed.

Well, I never! The train has a driver, but a complex technology-
based
system is installed to open the doors. The driver can override
the system,
but doesn't know how to - but has been instructed how to
reprogram certain
parameters into the computer.

The RISKS are too obvious and too numerous to mention, but isn't
this so
typical of many designs today? Throw out the simple, well-tried
and working
system and introduce a complex, untried and liable-to-failure
system. One
can assume that someone thought this was a safety feature, but
is this a
"fail-safe" system?

One would have assumed that the designers would have taken
cognisance of the

fiasco on the (London's) Docklands Light Railway when the inaugural train carrying Her Majesty the Queen failed to align properly (by a few inches, IIRC) at one station and the system locked her inside the carriage ... but that's clearly a naive assumption!

✶ Illinois Secretary of State computer outage

<jhhaynes@earthlink.net>

Fri, 3 Sep 2004 12:13:58 -0500 (CDT)

A computer glitch shut down computers for more than an hour at all 136 secretary of state offices in Illinois beginning at 9:30am on 2 Sep 2004. This delayed people who were trying to obtain driver's licenses, renew registrations, or conduct other business -- although those with preprinted renewal forms were able to be helped. [Source: *Chicago Tribune*, 3 Sep 2004; PGN-ed]

✶ Overcomputerization enlightenment

<"Joseph A. Dellinger" <geojoe@freeusp.org>>

Tue, 31 Aug 2004 22:56:47 -0500

I just went to set up our conference room for a meeting tomorrow morning. I had to blunder around in the dark, at first. The light switches have been

replaced by a computerized lighting control. Turning on the lights requires finding the control, selecting the appropriate menu, and then selecting the appropriate item to turn on the room lights. Once I'd done that, I was able to see that the computer that turns the room projectors on and off needed urgent virus updates run on it. Thankfully, nobody has thought to computerize the toilets yet. :-)

[Nobody? See [RISKS-21.35](#), 22.73, and 23.20, for example. It may be a slippery slope, but it's happening! PGN]

✶ More ID theft, via laptop

<David Lesher <wb8foz@nrk.com>>
Fri, 3 Sep 2004 11:41:43 -0400 (EDT)

Calif. Schools Warned of Identity Theft, Associated Press, 2 Sep 2004

<http://www.washingtonpost.com/ac2/wp-dyn/A57539-2004Sep2?language=printer>

California university officials have warned nearly 600,000 students and faculty that they might be exposed to identity theft following incidents where computer hard drives loaded with their private information were lost or hacked into.

Since January, at least 580,000 people who had personal information about them stored in university computers received warnings they might be at risk.

The latest instance of missing equipment occurred in June at California State University, San Marcos. An auditor lost a small external

hard drive
for a laptop computer. Personal data, including names,
addresses, Social
Security numbers and other identifiers for 23,500 students,
faculty and
staff in the California State University system were contained
on the
missing hard drive.

At the University of California, San Diego, and San Diego State
University,
hackers broke into computers and obtained access to files of
personal data
for more than 500,000 current or former students, applicants,
staff, faculty
and alumni. Officials from the Cal State system and UC San
Diego said they
have no evidence any personal data were stolen. At the
University of
California, Los Angeles, a stolen laptop in June led officials
to notify as
many as 145,000 blood donors that their data might be in the
open.

A California law requiring people be notified when they might be
exposed to
identity theft took effect in July 2003. Officials say that
might explain
the rash of notices. "There's no reason to assume that suddenly
in July
2003 all these computer security breaches started occurring,"
said Joanne
McNabb of the Office of Privacy Protection in the California
Department of
Consumer Affairs. "It's just that we know about them now, when
we didn't
hear before."

= =====

And yet, most schools still try and require students to furnish
SSN's to register. I've never once seen a good reason for it,
and in fact, they regularly furnish "shadow numbers" for foreign

students, and upon request, others.

And why is this "auditor" carrying the data around at all?

As for blood donations; the Red Cross is regularly crying for more donors. Wonder how many others, like me, refuse because they started demanding SSN's?

✶ Missouri vote-by-fax

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

Tue, 31 Aug 2004 11:10:33 PDT

Missouri's Secretary of State Matt Blunt (who also happens to be a candidate for the Governor of Missouri in the November election) has announced plans to allow Missouri voters in the military to send in their ballots by unencrypted e-mail. A supposedly trusted third party (Omega Technologies) will handle the unencrypted ballots and redistribute them to the appropriate ballot counters. Apparently North Dakota is also contemplating a similar scheme. Those voters will have to sign a waiver acknowledging that their votes need not be kept secret. I suspect regular RISKS readers will be (1) astounded, (2) horrified, and (3) concerned that certain e-mail messages could be altered or "accidentally" lost, (4) concerned that the acknowledged loss of privacy might be used to coerce votes or prompt vote selling, (5) etc. There are reportedly at least six million eligible overseas voters who

might wish to have the instant satisfaction in believing that their votes might be counted, but there are also at least six million votes that might thereby be subject to compromise.

[This story may have even more legs than the many on electronic voting systems. For example, see *The New York Times* editorial, The Pentagon's Troubling Role, 31 Aug 2004.]

E-voting in Nevada

<"NewsScan" <newsscan@newsscan.com>>
Wed, 08 Sep 2004 07:36:55 -0700

Nevada voters have become the first in the nation to cast ballots in a statewide election using computers that produced printed paper records of electronic ballots. "Knock on wood, so far things have been working flawlessly," said Secretary of State Dean Heller. Nevada's \$9.3 million voting system includes more than 2,600 computers and printers deployed in every county. The system, developed by California-based Sequoia Voting Systems, aims to address concerns that paperless touchscreen votes cannot be properly audited or recounted. "From what I've seen, voters seem to enjoy the experience," says DeForest B. Soaries Jr., chairman of the U. S. Election Assistance Commission. "There hasn't been frustration or confusion."

[AP/*USA Today*, 8 Sep 2004; NewsScan Daily, 8 Sep 2004]

<<http://www.usatoday.com/tech/news/techpolicy/evoting/2004-09-08->

[nv-evote-system_x.htm](#)

<EEkid@aol.com>

Tue, 31 Aug 2004 17:48:10 -0400 (EDT)

[From Dave Farber's IP distribution, excerpted for RISKS by PGN]

<http://www.blackboxvoting.org/?q=node/view/78>

Consumer Report Part 1: Look at this -- the Diebold GEMS central tabulator contains a stunning security hole

Submitted by Bev Harris on Thu, 08/26/2004 - 11:43.

Investigations

Issue: Manipulation technique found in the Diebold central tabulator --

1,000 of these systems are in place, and they count up to two million votes at a time.

By entering a 2-digit code in a hidden location, a second set of votes is created. This set of votes can be changed, so that it no longer matches the correct votes. The voting system will then read the totals from the bogus vote set. It takes only seconds to change the votes, and to date not a single location in the U.S. has implemented security measures to fully mitigate the risks.

This program is not "stupidity" or sloppiness. It was designed and tested over a series of a dozen version adjustments.

Public officials: If you are in a county that uses GEMS 1.18.18, GEMS 1.18.19, or GEMS 1.18.23, your secretary or state may not have told you about this. You're the one who'll be blamed if your election is tampered with. Find out for yourself if you have this problem: Black Box Voting will be happy to walk you through a diagnostic procedure over the phone. E-mail Bev Harris or Andy Stephenson to set up a time to do this. [...]

Full item archived at

<http://www.interesting-people.org/archives/interesting-people/>

✶ Using a paper trail to verify electronic voting machine results

<Diomidis Spinellis <dds@aueb.gr>>

Thu, 09 Sep 2004 11:49:30 +0300

The Economist (4-10 Sep 2004) has an interesting article covering the verification of Venezuela's referendum on the recall of President Hugo Chavez ("What really happened in Venezuela?", pp. 52-54). The article is written by Jennifer McCoy who directed the Carter Center's observer mission in Venezuela.

Two separate tests were used to verify the transmission of the results from the polling stations to the Venezuela National Election Council (CNE) headquarters and the tabulation of the results by the CNE's computers. Note that these tests have nothing to do with the electronic voting

machines,
they cover other elements of the election system that could also
be
manipulated.

The verification of the electronic voting machine results was
performed
using paper ballots that the machines printed and the voters
inspected
before depositing in a ballot box. According to McCoy, the
existence of
this paper trail allowed the observers to verify what happened
"within the
black box of the voting machines". Two audits were performed on
these paper
ballots: a half-completed immediate "hot audit", and a second
audit three
days after the election. Interestingly, the observers also
covered the
possibility of someone having the machines reprogrammed to
produce new paper
ballots matching the results and inserting them into the ballot
boxes.
Specifically, observers were placed in the military garrisons
where the
ballot boxes were kept, before drawing the random sample of the
voting
machines to be audited.

I can see two aspects of this story that will interest RISKS
readers. First
of all, the successful use of the electronic voting machine
paper trail to
verify a crucial element of the election process. Secondly, the
fact that
the mere existence of a paper trail does not in itself guarantee
fair, or
even verifiable, election results. The election process is a
complex
system; its auditing must take into consideration all elements
of the
system. In this case the Carter Center had been mediating in
Venezuela for

two years, and all tests and observer accessibility requirements were planned in advance.

The complete article is available on-line

http://www.economist.com/opinion/displaystory.cfm?story_id=3157671

More information, including the audit of the results, can be found on

the Carter Center's Web site <http://www.cartercenter.org/doc1690.htm>

Diomidis Spinellis - <http://www.dmst.aueb.gr/dds>

Athens University of Economics and Business

✶ Election verification in Venezuela

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

Thu, 09 Sep 2004 10:04:36 +0200

[A second report on the same article, different enough for inclusion. PGN]

The Economist, 4-10 Sep 2004, contains an article by Jennifer McCoy, who directed the Carter Center's observer mission during the Venezuelan election.

According to Ms. McCoy, the opposition, who lost the election, contested the results based on three phenomena. The second was that "there was a pattern of polling stations where several electronic voting machines returned an identical result, in what looked like a pre-programmed "cap" on the number of opposition votes."

The Carter Center planned three tests of the electronic voting system.

First, their observers at a random sample of polling stations called in results to mission headquarters, so they could be checked against the official results transmitted from the machines to the National Election Council (CNE). Second, they drew a larger sample of poll results from those received at CNE headquarters, to test the accuracy of tabulation by CNE computers. But as McCoy says, "missing from those tests was what happened within the black box of the voting machines." They approached that issue as follows.

The voting machines had a paper trail. The machines printed a record for the voter of hisher vote, and after inspection were deposited by himher in a cardboard ballot box. The Carter Center was able to perform a "hot audit" of about 1% of the machines, but only managed halfway to complete it. They proposed and completed a second audit three days after the vote. The audit was suitably blind and insulated from manipulation (McCoy gives the details), and verified in a practical manner that the machines had accurately reported results. The identical results from some machines fell within the range of probability, as shown by Stanford University statistician Jonathan Taylor.

McCoy suggests that cooperation from the CNE was less than perfect, but largely harmed itself: "the vote itself was secret and free, but the CNE's lack of openness, last-minute changes and internal divisions

harmed public confidence in that vital institution both before and after the vote." She suggests that in general Venezuelans have become more cynical towards elections and that it will take a "huge effort by both sides to restore trust in this fundamental democratic right before next month's election for governors and mayors."

It appears to have been essential to the efforts to verify the accuracy of the election that the voting machines generated a paper trail in a specific manner. One imagines from McCoy's comments that without the successful effort to verify the results of the machine voting through that trail, any faith in the democratic process could well have been irretrievably lost during this election. I worry that North America and Europe might suffer a similar loss of faith, over a longer time period, unless similar effective backups, and verifications, are required for electronic voting methods in our supposedly more mature democracies. For motives for manipulation are just as strong no matter where one lives, and no country anywhere lacks people who rate voting accuracy less important than obtaining their favored result.

Peter B. Ladkin, University of Bielefeld, Germany
<http://www.rvs.uni-bielefeld.de>

⚡ ATMs offer too much information

<Brendan Kehoe <brendan@zen.org>>

Wed, 1 Sep 2004 09:18:03 +0100

At a bank recently I watched someone use the ATM to pay their Mastercard bill. Since they weren't making an effort to be very close to the screen, I was able to watch as they went through the menu choices. Then onto the screen popped their credit card number: all 16 digits of it, large and readable from a few feet away.

The customer went on to continue the transaction, but it mystified me that the bank saw it necessary to display the entire number. Even if you've got multiple cards, it would seem to me that only the last four digits, perhaps, are what a customer would need to make sure they're paying off the card they intended.

Right now, the design lets anyone who can see the screen a brief view of the number---in my case approximately 5 seconds. The biggest risk was possibly the most threatening: the number was certainly there long enough for someone talented in number memorization to walk away with it.

Brendan Kehoe <brendan@zen.org> <http://www.zen.org/~brendan/>

[Don't forget the ease of digital cameras, long lenses, etc. PGN]

✶ Risk of using open forums for disaster recovery

<Espen Andersen <self@espen.com>>

Thu, 09 Sep 2004 16:28:21 +0200

Dan Bricklin's elegant essay on the lessons for system design and use of on-line and other information sources

<http://www.bricklin.com/learningfromaccidents.htm>

is very informative and makes some excellent points around the ability and availability of the general public as a participant in disaster recovery.

It nicely validates what every IT prophet has been saying, in one form or another, since the early 90s: Increases in communications and information processing capability will lead to more consumption of that resource, enabling organizations to quickly respond to outside changes -- indeed of "spontaneous" organizations to quickly form to address issues. Dan makes some great points around what this means for systems and component design.

However, there is one problem with using open tools, such as RSS feeds, blogs, wikis and open conference calls: Their very openness makes them a path for a future terrorist. A group of terrorists wanting to do something akin to the 9/11 action could now learn from what happened then, and include a number of on-line participants with a role in spreading misinformation, increasing fear and diverting resources. There were instances of misinformation during 9/11 -- I remember news items about a carful of bombs being stopped on some bridge in New York for instance -- and the news channels normally apply some form of fact-checking. While the Wikipedia model works great when there is time -- and people check changes

against a contributor's past behavior, I think we should be careful with too much openness in a time-pressured situation. Some form of validation needs to be in place.

Espen Andersen (self@espen.com), Norwegian School of Management (www.bi.no)
www.espen.com, +47 6755 7177; The Concours Group www.concoursgroup.com

✶ Re: NASA Spirit nearly done in by DOS ([RISKS-23.51](#))

<"Gene S. Berkowitz" <gene.berkowitz@comcast.net>>
Wed, 01 Sep 2004 22:54:06 -0400

..and as usual, Wired gets the story sideways.

The file system used is a FAT (File Allocation Table) system that was popularized by MS-DOS. The rovers use VxWorks as their operating system; a FAT-compatible file system is provided with VxWorks, but is not the only option. The FAT system is a notoriously bad choice for use with Flash memory devices, because any changes to the files requires an update to the table. This would quickly wear out the flash sectors where the FAT is stored. For this reason, the FAT and directory structure is copied to RAM, changes are made there, and at some point the updated FAT and directory are written back to Flash. The fact is, the rover filesystems contained hundreds of files from the flight portion of the mission; these

files were not deleted, resulting in a directory that grew too large for available RAM. Regardless, the directory never shrinks; the directory entry for a deleted file is simply marked with a special character, and its chain of FAT entries are marked as available.

This was common knowledge circa 1985, and made Peter Norton a rich man, for his "discovery" that the file was never truly deleted at all...

★ REVIEW: "Security Assessment", Greg Miles et al.

<Rob Slade <rslade@sprint.ca>>
Thu, 12 Aug 2004 08:22:47 -0800

BKSACSNI.RVW 20040721

"Security Assessment", Greg Miles et al., 2004, 1-932266-96-8,
US\$69.95/C\$89.95

%A Greg Miles gmiles@securityhorizon.com
%A Russ Rogers rrogers@securityhorizon.com
%A Ed Fuller
%A Matthew Paul Hoagberg
%A Ted Dykstra
%C 800 Hingham Street, Rockland, MA 02370
%D 2004
%G 1-932266-96-8
%I Syngress Media, Inc.
%O US\$69.95/C\$89.95 781-681-5151 fax: 781-681-3585 www.syngress.com
%O <http://www.amazon.com/exec/obidos/ASIN/1932266968/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/1932266968/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/1932266968/>

[robsladesin03-20](#)

%P 429 p.

%T "Security Assessment: Case Studies for Implementing the NSA IAM"

The introduction tries to explain the NSA (National Security Agency) IAM (Information Assurance Methodology), but is so heavily larded with (management) buzzwords that no clear concept emerges. The indications are that the book is primarily aimed at those who have taken one of the IAM courses, although there is an explicit statement that the material can be used by untrained professionals and also by the "customers" who are undergoing an assessment.

Chapter one describes IAM in words that make it seem very similar to such tools as CoBIT (ISACA's Control Objectives for Information Technology tool), ISO 17799, and the NIST (the US National Institute of Standards and Technology) self-assessment guide. However, almost all of the chapter is devoted to a promotion of sharp negotiation of the scope of an IAM contract, from the vendor perspective. Chapter two reiterates the need to control customer expectations and define contract objectives. (There is more jargon, and also the use of idiosyncratic and undefined acronyms like PASV [Pre-Assessment Site Visit].) The Organizational Information Criticality Matrix (OICM) described in chapter three is a kind of simplistic business impact analysis. In chapter four, system information criticality and the System Criticality Matrix (SCM) are said to be more detailed than the OICM.

Defining system boundaries is acknowledged to be difficult, but neither the explanation nor the examples used are of any help in clarifying the issue.

Both the text and the tables used in the "case study" are extremely confusing in regard to the relation between entries in the OICM and the SCM.

The system security environment, described in chapter five, is what most people would know as corporate culture: the general attitudes and behaviours common to an institution. The book suggests finding and using the CONOPS (concept of operations) documentation while admitting that it may not be found in most commercial enterprises. (The authors don't explain that this is basically identical to the common policy and procedures manuals, although they do eventually get around to mentioning these texts.) The TAP (Technical Assessment Plan) is actually just a specific format for a detailed contract, so we have to go through all of that type of editorial comment again, without really getting much information about the recommended TAP structure. Chapter seven involves the assessment itself, and generally deals with administrative details--and making sure that the customer does not modify the scope of the contract. The eighteen basic information security models get listed, although this seems to be almost an afterthought, rather than the core of the IAM itself. Findings, the report of the assessment results, are described in chapter eight. A sixteen page example does little more than provide a format. The close out report, in chapter nine, is a final sales meeting with the customer. The

final report

is given in a different, and more general, format in chapter ten. Cleanup

work and followup sales of consulting are discussed in chapter eleven.

The constant repetition of very basic ideas and the turgid and buzzword-laden text make this work far longer than is justified by the

information provided. In addition, the extreme emphasis on the viewpoint of

a vendor trying to sell a contract (and protect himself from doing any

unbillable work) is a severe limitation on the audience for this tome.

Essential components of the IAM model and process do not seem to hold any

central place in the book, and the reader discovers them almost by accident,

and despite of the writing rather than because of it.

copyright Robert M. Slade, 2004 BKSACSNI.RVW 20040721
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

Volume 23: Issue 53

Thurs 16 September 2004

Contents

- [Two human errors silenced Los Angeles area airports](#)
[Ben Moore](#) [Keith Price](#) [Kent Borg](#)
- [Korean Airport subject to hackers, viruses, worms, etc.](#)
[Bob Heuman](#)
- [Homeland Security Science&Technology BAA and Industry Day](#)
[Douglas Maughan](#)
- [Registration 'nightmare' at UMass](#)
[Monty Solomon](#)
- [Robert Heinlein Does it Again! Re: e-voting](#)
[Paul Robinson](#)
- [E-Voting in Nevada](#)
[NewsScan](#)
- [Electronic voting in Canada](#)
[Richard Akerman](#)
- [Maryland rules against opponents of e-voting machines](#)
[NewsScan](#)
- [Washington State primary and voting machines](#)
[Paul A Below](#)
- [Order of names on electronic ballot](#)
[James Meade](#)

- [Re: Shutting the train door before the commuter has bolted](#)
[Nick Brown](#)
 - [Wired: Pentagon revives memory project](#)
[Joe Shead](#)
 - [Re: More ID theft, via laptop](#)
[F. Barry Mulligan](#)
 - [Updating the Screaming Telephone](#)
[Debora Weber-Wulff](#)
 - [Re: German TollCollect System](#)
[Debora Weber-Wulff](#)
 - [Re: German unemployment system](#)
[Debora Weber-Wulff](#)
 - [Re: U.S. air travel without government identification](#)
[Kathy Gill](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Two human errors silenced Los Angeles area airports

<"Ben Moore" <ben.moore@juno.com>>

Thu, 16 Sep 2004 14:18:11 GMT

[Source: *LA Times* article, 16 Sept 2004, by Ricardo Alonso-Zaldivar, Eric

Malnic and Jennifer Oldham, PGN-ed]

<http://www.latimes.com/news/local/la-me-faa16sep16,1,5928253,print.story>

?coll=la-home-headlines

Two separate human errors caused a breakdown in radio communications around 4:30 pm on 14 Sep 2004 that lasted for three hours and brought Southern California's major airports to a near-stop. There were at least five instances in which planes came too close during the first 15 minutes of the communications breakdown.

The FAA's radio system in Palmdale shut itself down because a technician failed to reset an internal clock -- a routine maintenance procedure required every 30 days by the FAA. Then a backup system failed, also as a result of technician error, officials said. (The Palmdale radar system did not shut down.)

FAA officials said they had known for more than a year that a software glitch could shut down radio communications and were in the process of fixing it. In the meantime, they required manual resetting of the communications system -- a process they described as similar to rebooting a personal computer. The problem so far has been corrected only in Seattle, one of 21 FAA regional air-traffic control centers that have used the system since the mid-1990s. [This is the same problem that was discovered over a year ago in the Atlanta ATC facility.]

About 30,000 passengers were affected, with 500 or 600 spending the night in the terminals. The backlog of incoming flights was not cleared until 3 a.m. Wednesday. At LAX, 450 flights were diverted or canceled and another 150 were delayed. An additional 32 were canceled Wednesday morning because the aircraft did not arrive Tuesday night. Neighboring airports also experienced significant delays.

Two human errors silenced Los Angeles area airports

<Keith Price <price@usc.edu>>

Thu, 16 Sep 2004 09:54:55 -0700 (PDT)

I was struck by the details at the end of the *Los Angeles Times* article

[PGN-ed herewith]:

<http://www.latimes.com/news/local/la-me-faa16sep16,1,3729661.story>

?coll=la-home-headlines

... As originally designed, the VSCS system used computers that ran on Unix.

The VSCS system was built for the FAA by Harris Corp. of Melbourne, Fla., at a cost of more than \$1.5 billion. When the system was upgraded about a year ago, the original computers were replaced by Dell computers using Microsoft software. Baggett said the Microsoft software contained an internal clock designed to shut the system down after 49.7 days to prevent it from becoming overloaded with data. Software analysts say a shutdown mechanism is preferable to allowing an overloaded system to keep running and potentially give controllers wrong information about flights.

Richard Riggs, an advisor to the technicians union, said the FAA had been planning to fix the program for some time. "They should have done it before they fielded the system," he said.

To prevent a reoccurrence of the problem before the software glitch is fixed, Laura Brown, an FAA spokeswoman, said the agency plans to install a system that would issue a warning well before shutdown.

Greg Martin, the chief FAA spokesman in Washington, said the failure was not

an indication of the reliability of the radio communications system itself, which he described as "nearly perfect."

✈️ Two human errors silenced Los Angeles area airports

<Kent Borg <kentborg@borg.org>>

Thu, 16 Sep 2004 10:01:54 -0400

According to a report I heard this morning on KCRW, the system shut itself down on purpose because it had not received its regular 30-day preventive maintenance!

At first glance this seems crazy: a nicely functioning system comes to a halt because some calendar flipped over. There were several close calls on Tuesday because a 30-day timer expired.

However, a coworker of mine made a good point on the likely reason the system designers took the 30-day time period so seriously: Records. These systems record radar data and radio transmissions. After 30-days the tapes (or whatever they use) are probably full. That's pretty serious. It *is* a safety concern, but probably not something worth halting over.

It is instead a situation to be avoided. I suggest that several days before the clock is up the system should complain loudly, and probably complain to the air traffic controllers who are in a position to notice and to do something about it.

Were this a modern system (doesn't the FAA periodically try to build a replacement and fail?) I would suggest that there also be e-mailed warnings, and that if the limit is reached, the system start overwriting old data instead of shutting down. As it is, the system might not be capable of either.

However, be wary of systems that degrade gracefully, for unless they inflict some pain in an attempt to right their hurt, they will tend to always operate in a degraded state.

✶ Korean Airport subject to hackers, viruses, worms, etc.

<"R.S. (Bob) Heuman" <rsh@idirect.com>>

Sun, 05 Sep 2004 02:01:56 -0400

Nothing new, of course. If one is going to share a network with the world, and have no meaningful controls or security, the result is almost always going to result in the following type of news item.

Only 7,345 viruses in a day or two? Not all that bad, is it, if they were all stopped and did no damage, and we do NOT know what was defined as a virus, nor whether the code was viral, or simply backdoors and other junk.

South Korea's Incheon International Airport was reported to be highly vulnerable to online attacks from hackers and viruses. Incheon's computer

network is vulnerable because it's shared by private airlines and tourist

agencies located in the airport. The National Intelligence Service said

in a report that 7,345 computer viruses were detected May 3-4 in 116

businesses operating within the airport, and that electronic glitches

could lead to flight crashes or other accidents. "There is a high

possibility that Incheon International Airport will be exposed to online

attacks like computer viruses and direct hacking." [Source: UPI via

Korea Times, 4 Sep 2004, PGN-ed]

✶ Homeland Security Science&Technology BAA and Industry Day

<"Douglas Maughan" <Douglas.Maughan@dhs.gov>>

Wed, 15 Sep 2004 22:17:54 -0400

Cyber attacks are increasing in frequency and impact. These attacks continue to demonstrate that there are extensive vulnerabilities in information systems and networks, many with the potential for serious damage.

In an effort to reduce these vulnerabilities, the Department of Homeland Security's Science and Technology Directorate (DHS S&T) has issued a Broad Area Announcement (BAA 04-17) [see <http://www.hsarpabaa.com/>] for the research, development, and deployment of technologies to protect our nation's cyber infrastructure. DHS S&T intends to evaluate cyber security technologies for use in operational units within DHS, as well as

federal,
state, and local sectors -- for the purpose of increased
homeland security.
Many of these technologies will address security needs in the
larger public
Internet as well.

HSARPA anticipates that up to \$4.5M in funding in FY 2004 will
be available
for multiple awards via the solicitation, with a total
anticipated amount of
\$12-15M over the next 36 months. Copies of the BAA may be
downloaded from
the FedBizOpps web site at www.FedBizOpps.gov or at www.hsarpabaa.com. The
HSARPA CSRD BAA 04-17 solicits proposals that address at least
one of the
seven technical topic areas:

- TTA 1 - Vulnerability Prevention
- TTA 2 - Vulnerability Discovery and Remediation
- TTA 3 - Cyber Security Assessment
- TTA 4 - Security and Trustworthiness for Critical
Infrastructure Protection
- TTA 5 - Wireless Security
- TTA 6 - Network Attack Forensics
- TTA 7 - Technologies to Defend against Identity Theft

In addition, HSARPA will hold an Industry Day and Bidders
Conference for the
CSRD BAA on September 23rd at the Hilton Crystal City in
Arlington,
Virginia. All interested attendees must register online at
[https://www.enstg.com/signup/passthru.cfm?
ConferenceCode=DHS26146](https://www.enstg.com/signup/passthru.cfm?ConferenceCode=DHS26146) or linking
from www.hsarpabaa.com.

Douglas Maughan, Ph.D., Program Manager, Cyber Security R&D
Department of Homeland Security, Science and Technology
Directorate
Homeland Security Advanced Research Projects Agency
1120 Vermont Avenue, NW, 8th Floor, Washington, DC 20528
Phone: 202-254-6145 Fax: 202-254-6170 Cell: 202-360-3170

E-mail: Douglas.Maughan@dhs.gov

[I thought this item would be of interest to many RISKS readers -- not just those of you who might write proposals, but to the rest of you who have a keen sense of the vulnerabilities and threats that desperately need to be addressed more systematically. PGN]

Registration 'nightmare' at UMass

<Monty Solomon <monty@roscom.com>>

Wed, 15 Sep 2004 00:16:45 -0400

Computer woes keep many students from class sign-up
By Hiawatha Bray, **The Boston Globe**, 14 Sep 2004

For 25,000 students and faculty on the Amherst campus of the University of Massachusetts, last week's start of the new term was even more hectic than usual, thanks to a computer malfunction that prevented many students from signing up for classes. ... The university uses software from PeopleSoft Inc. to manage student registration. During the summer, campus computer administrators installed the latest version of the software but apparently something went wrong.

http://www.boston.com/business/technology/articles/2004/09/14/registration_nightmare_at_umass/

✶ Robert Heinlein Does it Again! (Re: e-voting)

<Paul Robinson <postmaster@paul.washington.dc.us>>

Sat, 28 Aug 2004 21:43:49 GMT

In the 1980s, when it was discovered that the wife of the leader of the free world was using an astrologer to chart her husband's political career, it was noted that the exact same practice was predicted by Robert A. Heinlein in his book, "Stranger in a Strange Land" which was published more than a generation before the revelations about Nancy Reagan.

Robert Heinlein also showed how you can steal an election without anyone being the wiser: you use a computer system to count votes, where the computer system's integrity is trusted and there is no means to provide a reliable audit trail outside of the computer system.

He wrote about that in "The Moon is a Harsh Mistress" which was first published in 1966. And nearly 40 years later, (almost) nobody seems to have remembered yet another of the late, great Bob Heinlein's prophetic views.

"The lessons of history teach us -- if the lessons of history teach us anything -- that nobody learns the lessons that history teaches us."

✶ E-Voting in Nevada

<"NewsScan" <newsscan@newsscan.com>>

Mon, 13 Sep 2004 08:34:11 -0700

Nevada \$9.3 million voting system worked well in last week's primary.

California official Marc Carrel, who observed the election, says, "They were

incredibly organized. I think California could pull off a similar election

if we had adequate training and education programs for poll workers and

voters." Printers attached to the systems offer assurances that elections

can be fully audited, and a spokesman for Sen. Dianne Feinstein says, "The

Nevada election demonstrates that you can have efficient electronic voting

machines yet at the same time have a paper trail so voters can be assured

they've voted accurately and their vote is being recorded accurately." But

Georgia elections director Kathy Rogers warns that the printers could have

unintended consequences, allowing unethical poll workers to determine how

individuals voted: "We seem to have traded a secret ballot for this piece of

paper." [AP/*USA Today*, 13 Sep 2004; NewsScan Daily, 13 Sep 2004]

<http://www.siliconvalley.com/mld/siliconvalley/9647591.htm>

✶ Electronic voting in Canada

<Richard Akerman <rakerman@chebucto.ns.ca>>

Sun, 12 Sep 2004 15:47:00 -0300 (ADT)

The Chief Election Officer ("CEO") of Ontario has produced a report "Access,

Integrity and Participation: Towards Responsive Electoral Processes for Ontario"

http://www.electionsontario.on.ca/usr_files/election_report_2003_en.pdf

in which he calls for the examination of "21st century automation" such as electronic and Internet voting.

I'm not sure what problem they're trying to fix. Cringely has said "My model for smart voting is Canada" because of our simple paper-based, hand-counted system.

<http://www.pbs.org/cringely/pulpit/pulpit20031211.html>

Unfortunately, many Canadian elections officials seem determined to bring in electronic voting technologies anyway.

There has already been Internet voting in Markham Ontario.

<http://tinyurl.com/2sv8j>

New Brunswick's chief electoral officer also is interested in electronic voting, which has already been tried in Saint John NB.

<http://tinyurl.com/7x3nj>

There doesn't seem to be any organized opposition to electronic voting in Canada.

I have written a summary of the current situation in my blog about the issue, Paper Vote Canada.

<http://tinyurl.com/3vqqu>

<http://blog.papervotecanada.ca/2004/06/summary-of-canadian-electronic-voting.html>

(This story has also been submitted to Slashdot.)

Richard Akerman <rakerman@chebucto.ns.ca> <http://www.akerman.ca/>

✶ Maryland rules against opponents of e-voting machines

<"NewsScan" <newsscan@newsscan.com>>

Wed, 15 Sep 2004 07:39:22 -0700

Maryland's highest court has rejected demands to allow citizens who distrust TouchScreen voting machines to use paper ballots to ensure the paperless devices are accurate and secure. Ryan Phair, attorney for the defeated plaintiff group called TrueVoteMD, complains: "We're basically playing Russian roulette. We know there is vulnerability. It is just a matter of time until it happens." TrueVoteMD vows to continue its legal battle to force the state to use printers on electronic machines in future elections.

[AP/*San Jose Mercury News*, 14 Sep 2004; NewsScan Daily, 15 Sep 2004]

<<http://www.siliconvalley.com/mld/siliconvalley/9662979.htm>>

✶ Washington State primary and voting machines

<"Below, Paul A" <paul.below@eds.com>>

Wed, 15 Sep 2004 13:24:09 -0400

Washington State was forced to implement a primary that required the voter to declare a party preference before voting for that party's candidates. In

addition, the ballot contained a nonpartisan section that all voters were supposed to be able to use, whether or not they declared a party preference.

News story:

http://seattletimes.nwsourc.com/html/localnews/2002036002_primary15m.html
<http://seattletimes.nwsourc.com/html/localnews/2002036002_primary15m.html>

After the machine returned his ballot, a poll supervisor at Hobart Community Church asked whether he had chosen a political party (he had not) and whether he had deliberately not chosen a party. His ballot was accepted only after the supervisor opened the machine and pressed a button overriding its programming. "So much for secret ballots," said Sterling, who claims that yesterday's voting procedures violate the state constitution's guarantee of "absolute secrecy" in preparing and depositing ballots. At some King County polling places, the override button either didn't function properly or workers didn't know how to use it. Stephen McCloskey watched a frustrated nonpartisan voter declare a party preference at St. Anne Church in Seattle because a poll worker couldn't find any other way to get a machine to accept the woman's ballot. When a voting machine wouldn't accept David Miller's nonpartisan ballot at Crown Lutheran Church in Seattle, a poll worker put his ballot on the side of the machine to be counted later. "This leaves my ballot unprotected for marking at a later time," Miller said.

✶ Order of names on electronic ballot

<"James Meade" <james.meade@siemens.com>>

Tue, 14 Sep 2004 12:47:13 -0700

As an IEEE member, I recently received my ballot to vote for various offices. The paper ballot very carefully says that "The order of candidate names indicates no preference. Ballots have been prepared so that the order randomly varies." You then have the option of voting on the paper ballot by traditional mail or voting electronically. Feeling adventurous, I went the electronic route and surprise, the electronic ballot has the candidates' names for each office in alphabetic order. The risk? The two voting methods (paper vs electronic) may provide different results, based on the spelling on the candidates' name. It's well-known that candidates listed at the top have an advantage over those listed further down. If my name were John Adams, I'd be pushing for people to vote electronically. Jim Meade /
Systems Engineer

✶ Re: Shutting the train door before the commuter has bolted ([R-23.52](#))

<Nick Brown <Nick.BROWN@coe.int>>

Fri, 10 Sep 2004 18:16:00 +0200

Standard GPS is nowhere near accurate enough for this sort of application.

It's possible that the designers assumed that they would be able to use EGNOS-enhanced GPS signals, which will give 1-2 metre accuracy, but at the time of writing, I don't think that the UK falls within the footprint of any EGNOS-transmitting satellite, due to a combination of EGNOS system implementation delays and a satellite launch problem (both well-known RISKS, of course).

The discussion as to whether or not a system with even this degree of accuracy, and the complexity of manual override described, is a good idea, is of course still equally valid.

⚡ Wired: Pentagon revives memory project

<"Joe Shead" <Joe@sheadprogramming.com>>

Mon, 13 Sep 2004 13:08:50 -0500

The Department of Defense is handing out contracts for a project to record what soldiers see and do in battle zones. The new initiative closely resembles another, called LifeLog, that the Pentagon scrapped months ago.

Wired.com article by Noah Shachtman:

[http://www.wired.com/news/privacy/0,1848,64911,00.html?
tw=wn_story_mailer](http://www.wired.com/news/privacy/0,1848,64911,00.html?tw=wn_story_mailer)

✦ **Re: More ID theft, via laptop (Lesh, [RISKS-23.52](#))**

<"F. Barry Mulligan" <mulligan@acm.org>>

Fri, 10 Sep 2004 23:35:59 -0400

When the Red Cross started asking for SSN, long before identity theft and data mining hit the popular lexicon, I refused and they just assigned an in-house number. What I remember is the nurse's immediate response: "Do you work for IBM?". When queried, she said that at blood drives at the IBM division headquarters none of the engineers and programmers would give their SSNs. When I suggested that perhaps they knew something she didn't, she acquired a rather thoughtful expression that lasted through the rest of the interview.

✦ **Updating the Screaming Telephone (DWW, [RISKS-23.51](#))**

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

Fri, 10 Sep 2004 16:29:13 +0200

I reported in [RISKS-23.51](#) on the Siemens 65 family of mobile phones that suffer from, if you will, terminal screaming (a painfully loud sound when the battery is empty).

Siemens rushed to put an update on its site, bringing down the wrath of many mobile phone providers who had had to pull the phones off their shelves and

had not yet tested the update. They forced Siemens to remove not just the link but also the files until they were happy with the fix.

On 9 Sep 2004, Siemens blanketed the print media with a very unconventional ad [2] - "Oops, that was our moose test" (DaimlerBenz had some problems 1997 with tests they performed on their A-class cars [1] - when doing the 'moose test', i. e. swerving to miss a big thing in the middle of the road, the cars had an annoying tendency to flip over).

In a very friendly, humorous but rueful tone the ad describes the "little technical problem" that is "extremely seldom", but we owe it to our customers etc. who expect quality products etc. etc. It then goes on: "We have learned that nobody is perfect. But one can learn from errors, and react honestly, openly, and fairly." [translations dww]

This is an amazingly open ad from a company that prefers rather cool, calm, and collected, buttoned-up ads. So even with the technical problems the company has had, they seem to have hired some good spin doctors.

The software update is at [3] - there are *10* different versions, one for each type of mobile phone. Wouldn't it make business sense to have just one sort of basic kind of program that was modular and would work on all of the different kinds of phone?

[1] <http://www.krisennavigator.de/mafa4-d.htm>

[2] http://www.gwa.de/modules/news/index.php?show=all&news_id=1439&pos=0

[3] http://www.siemens-mobile.de/cds/frontdoor/0,2241,de_de_0_66868_rArNrNrNrN,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/>

✉ **Re: German TollCollect System (DWW, [RISKS-23.51](#))**

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

Fri, 10 Sep 2004 17:04:13 +0200

The woes of the German TollCollect ([RISKS-23.51](#)) continue as the German government sues the consortium of Telekom and DaimlerChrysler to the tune of 4.5 billion Euros for damages arising because the toll system, which was supposed to start in August 2003, has now slipped to January 2005. The consortium vigorously denies needing to pay anything.

The **Berliner Zeitung** from 10 Sep 2004 quotes an internal report by DaimlerChrysler that states "The possibility of a late deployment was clear from the very beginning." These are normal, well-known "risks for the project development and project implementation". So we don't know how to do it any better?

The article goes on to report that both the German transport ministry and TollCollect now no longer doubt the technical feasibility of the system. (If they did have doubts, why were they building such a complicated and expensive system with tax dollars in the first place?!).

The reliability testing is now said to be at 99% (up from 97% 2 weeks ago, if this is indeed based on a test and not on a reporter's exaggeration). There need to be about 500 000 OBU (On Board Units) installed on trucks by the beginning of next year. Two weeks ago we had 37000 reported installed, now we have 45000 units reported installed. There are 15 more weeks in the year, so if they continue at this rate they will only have to put in about 280 000 units between Christmas and New Year's to have a functioning system....

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/>

✶ Re: German unemployment system

<Debora Weber-Wulff <weberwu@fhtw-berlin.de>>
Tue, 14 Sep 2004 08:51:42 +0200

Germany seems to be a hotbed of stuff like this at the moment. There is a monstrous disaster brewing over the new unemployment system. At the rate at which the politicians are assuring people that everything will work just fine on 1 Jan 2005, I am sure that it will be in the class of the toll collect woes. This one might just bring down the government, though, because the mob is angry. And if they don't get their unemployment checks cut on time, there will be hell to pay....

✈️ Re: U.S. air travel without government identification

<kathy gill <kegill@u.washington.edu>>

Tue, 14 Sep 2004 16:45:34 -0700

In response to Dan's story about air travel without an ID - here is a similar one originating in Seattle.

Last September (2003), my SO and I were flying from SEA to Charlotte NC where we planned to pick up a car and drive down to Georgia. When we were about 15 minutes from SeaTac -- and 20 minutes from home with a little more than an hour before our flight -- Mike realized he had left his wallet at home. We ride motorcycles, and he had put his wallet in his gear because he needed to buy gas. He forgot to put it back in his pants.

I phoned the airline, even though we knew we'd never make it if we drove home, got the wallet, and returned -- unless the plane was running late (an unusual occurrence for a red-eye flight). The person on the other end (United) said that the decision to let him fly or ground him would be made by both the check-in desk and security: in other words, two gauntlets.

He did have his Microsoft photoID, because he wears it on a retractable clip and it lives on his pants. Unlike Dan, Mike had NO ID other than his MSFT badge -- no credit cards, no SS card, not even a business card. Fortunately, I'd made the flight arrangements (and had ID and CC) and we had

our boarding passes, which were printed at home.

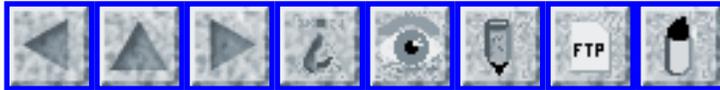
Like Dan, Mike was shuttled through a more invasive security check in.

"No ID?" was the question that greeted him as well. No other questions, even though he sports a ponytail.

We had a friend overnight mail the wallet (yeah FedX) the next day, because we were to be gone for a week, and we didn't want to chance his not being able to fly out of Charlotte. And yes, there were risks, there, too, but at the time, we thought they were the lesser of the two sets.

Kathy E. Gill, Department of Communication, University of Washington

<http://faculty.washington.edu/kegill/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 54

Sat 25 September 2004

Contents

- [Stupidsecurity](#)
[Richard Forno via Dave Farber](#)
- [Tests show cell phones don't disrupt navigation systems](#)
[NewsScan](#)
- [Railroad signal failure](#)
[Chuck Weinstock](#)
- [Breach Security, Inc. offers just that](#)
[Olin Sibert](#)
- [E-Vote Fears Soar in Swing States](#)
[wired.com via Monty Solomon](#)
- [Some times, new ideas are not good ideas](#)
[David Lesher](#)
- [Internet attacks jump significantly this year](#)
[NewsScan](#)
- [Don't worry about security holes ...](#)
[George Michaelson](#)
- [Re: LA ATC Failure](#)
[Paul Cox](#)
- [Re: 49.7 day "overloaded with data" in Los Angeles](#)
[John Dallman](#)

- [Nose-steered mouse](#)
[James Garrison](#)
 - [Java programs at risk from decompilers](#)
[Fiachra O'Marcaigh](#)
 - [REVIEW: "Systems Reliability and Failure Prevention", Herbert Hecht](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Stupidsecurity (via Dave Farber's IP)

<Richard Forno <rforno@infowarrior.org>>
September 21, 2004 3:43:47 PM EDT

Finally, someone is chronicling the stupidity that passes for
"stronger
security" post-September 11:
<http://www.stupidsecurity.com>

Topics include:

Teacher Arrested After Bookmark Called Concealed Weapon
Big Trouble For Mentioning a Plastic Explosive in the Airport
You Can't Hide In Chicago
Washington Post: Freedom's Light Hidden Under A Security Blanket
Government Asks Court to Keep ID Arguments Secret
Putting a Price Tag on US Visa Stupidity
TSA Cynicism
New York Convention
Barefoot toddlers delay Air NZ flight
Police Delay Departure From Plane to Catch A Dangerous Criminal
Cleveland Air Show In Danger....
It's Fun To See The Power Of Stupidity Turned On Its Sources...
Delete PIN When It Has Become Invalid
Nuclear Power Plants Security Gaps to be Withheld From Public
Let's Intimidate our Innocents -- That'll Scare the Terrorists!
High-Tech Wallpaper Keeps Wireless Wardrivers Out
HM department of vague paranoia

Dave's IP archives:

<http://www.interesting-people.org/archives/interesting-people/>

✶ Tests show cell phones don't disrupt navigation systems

<"NewsScan" <newsscan@newsscan.com>>

Thu, 23 Sep 2004 08:05:51 -0700

Recent tests by Airbus and American Airlines/Qualcomm indicate that, contrary to popular lore, cellular signals do not disrupt airplanes' navigational systems. The two results were similar for both the CDMA and GSM cellular technologies, but the Federal Aviation Administration and the Federal Communications Commission say the tests can't officially be considered in their review of the rules because they were conducted without government oversight. The agencies say they are moving ahead with their own tests. [*Wall Street Journal*, 23 Sep 2004; NewsScan Daily, 23 Sep 2004]

<http://online.wsj.com/article/0,,SB109589672706925579,00.html>

(sub req'd)

✶ Railroad signal failure

<Chuck Weinstock <weinstock@sei.cmu.edu>>

Fri, 17 Sep 2004 17:17:42 -0400

[Taken from an e-mail circulating on the net. Edited slightly for clarity. Chuck]

Hello my name is ... I'm an engineer in Sparks, Nevada. On August 28 about 5:25 am, my conductor and I heard slight conversations on the radio; we were about milepost 533. We heard Amtrak tell the dispatcher that they had a clear signal into a BNSF train and they did not think they were protected behind them. The engineer and conductor both said they were going to walk back their and see if the signal they went by was still clear. At that point we were about 8 minutes from them.

Well, I heard Amtrak tell dispatcher 76 that they were looking at a clear Signal at mp 524.1. At that point I was going by milepost 525.5 and had a clear signal there, so we took it upon ourselves to slow down and take caution for we were not quite sure what we were going to see. When we reached milepost 524.1 the engineer from Amtrak and the conductor were both standing below the signal, and of course we had a clear signal with Amtrak was only 25 cars on the other side of the signal.

Up until the point of us stopping at the clear signal, no one warned us about anything. When I told the dispatcher what we came across it seem to finally sink in, I guess. That's when everything came to a halt, signal management came over the radio and told no one to move. The whole reason the first train was stopped because of broken rail.

⚡ Breach Security, Inc. offers just that

<Olin Sibert <u9313@siliconkeep.com>>

Fri, 24 Sep 2004 11:08:55 -0400

A delightfully named company called Breach Security, Inc., (www.breach.com) has introduced a product called BreachView SSL that "is a unique add-on module for existing network IDS products that performs SSL traffic decryption without terminating the SSL session, or affecting non-repudiation in any way".

Judging from a ZDNet report (blogs.zdnet.com/index.php?p=531), the product operates by placing a piece of client software into every user's browser that informs Breach's IDS add-on module of every SSL session key. This allows the Breach module to decrypt the SSL session and provide plaintext to the IDS the analysis.

Aside from being reminiscent of the Clipper Chip, with its Faustian "give us your keys and we'll let you use encryption, and we promise to use our knowledge and power wisely" bargain, the RISKS of this technology should be clear.

Sure, if you can make a browser give up its session keys, you can read its SSL sessions--but if Breach's software can do that, then what's to stop some other software from doing the same thing? I'd also expect browser designers to consider this sort of thing a violation of sound security design principles and take steps to prevent it--making it ever more difficult for

Breach's product to work at all.

The flip side is that there IS a genuine problem here: if you rely on network-based intrusion detection as your network security mechanism, you can't inspect encrypted traffic to look for intrusions. However, "solving" this problem by preventing that traffic from being securely encrypted seems likely to introduce more fundamental risks. This approach should be yet another hint that network-based intrusion detection might not be the ideal answer for maintaining client system security.

This type of product seems more plausible on the inbound side of a system.

A company's server might well want to give up access its traffic for intrusion analysis before processing it, but as a filter for outbound traffic, it seems rather less desirable.

⚡ E-Vote Fears Soar in Swing States (wired.com)

<Monty Solomon <monty@roscom.com>>

Fri, 24 Sep 2004 08:00:56 -0400

Jacob Ogles, E-Vote Fears Soar in Swing States, *WiReD.com*, 23 Sep 2004

Roughly a third of the votes cast in the November presidential election will be made on controversial paperless electronic voting machines, but as any political analyst can tell you, the only votes that will matter a great deal will be cast in a handful of swing states. And just as the

Kerry and Bush campaigns are spending most of their efforts in those states where neither holds a heavy margin in the polls, voting advocacy groups concerned with the integrity of voting technology are devoting their resources toward the states which matter most. ...

<http://www.wired.com/news/evote/0,2645,65044,00.html>

✶ Some times, new ideas are not good ideas (Re: [RISKS-22.34](#))

<David Leshner <wb8foz@nrk.com>>
Mon, 20 Sep 2004 21:11:37 -0400 (EDT)

[RISKS-22.34](#) included my submission about Georgetown's adoption of this software. Looks like it was a mixed blessing after all:
<http://www.law.com/jsp/article.jsp?id=1095207119649>

Software Snafus Disrupt Law School Tests
Georgetown Law drops its exam software,
leading some to question the future of testing (excerpt)
Beth Hanson, **Legal Times**, 20 Sep 2004

After the Student Bar Association adopted a resolution to stop using the software and the Georgetown faculty agreed, the school dropped the software and asked students to sign an honor pledge during exams. The school also added extra proctors to each exam classroom. Now students are allowed to take their exams using an ordinary word processor.

[kudos to Sean Donelan for spotting the article...]

Also, there was no provision for Linux and Mac laptop owners. I knew one in the LLM program; she was forced to borrow a WinME machine, and yep, it crashed during the exam,

Internet attacks jump significantly this year

<"NewsScan" <newsscan@newsscan.com>>

Mon, 20 Sep 2004 10:49:40 -0700

The semiannual Internet Security Threat Report, which is based on monitoring by computer security firm Symantec, indicates that in the first six months of 2004 there were at least 1,237 newly discovered software vulnerabilities and almost 5,000 new Windows viruses and worms capable of compromising computer security. The numbers represent a dramatic increase over the same period in 2003. Even more troubling was the sharp rise in the number of "bot," or robot, networks, which comprise a large number of infected PCs that can then be used to distribute viruses, worms, spyware and spam to other computers. The survey notes that in the first half of 2004, the number of monitored botnets rose from fewer than 2,000 to more than 30,000. The botnets, which range in size from 2,000 to 400,000 "zombie" machines, are often "rented out" to commercial spammers who use them to distribute junk e-mail while concealing their identities. E-commerce was the industry most frequently targeted for attacks, accounting for 16% of the total, and report

authors note that phishing scams are responsible for pushing up the numbers in that category. "We're seeing a professional hand in development that was pretty startling in terms of malicious code," says Alfred Huger, senior director of engineering for security response at Symantec. The report's findings mirror those of recent government-supported research. [*The New York Times*, 20 Sep 2004; NewsScan Daily, 20 Sep 2004] <http://www.nytimes.com/2004/09/20/technology/20secure.html>

⚡ Don't worry about security holes ...

<George Michaelson <ggm@apnic.net>>

Thu, 23 Sep 2004 10:11:40 +1000

A quote from a *WiReD* article on the Diebold hack in VBS:

"...But speaking generally on the vulnerabilities Harris mentions, Diebold

spokesman David Bear said by phone that no one would risk manipulating

votes in an election because it's against the law and carries a heavy penalty. ..."

http://www.wired.com/news/evote/0,2645,65031-3,00.html?tw=wn_story_page_next2

I'm glad that's clear. We can all sleep better now knowing our money is safe in the banks, because nobody will risk stealing it since its against the law etc etc..

George Michaelson, APNIC, PO Box 2131 Milton, QLD 4064 Australia

+61 7 3858 3150 <http://www.apnic.net> ggm@apnic.net

✶ Re: LA ATC Failure ([RISKS-23.53](#))

<Paul Cox <pcox@eskimo.com>>

Thu, 23 Sep 2004 13:03:40 -0700

I'm an air traffic controller in Seattle Center, which is a facility just like the one in LA that had the crash.

To do their job, air traffic controllers need one thing above/beyond all:

They need the ability to communicate with the aircraft they're controlling.

We can control planes even without radar, because we can get position reports from the airplanes and provide safe separation via altitude, spacing, and so forth. But without comm, we're completely and utterly hosed.

(Some of the FAA spokesflacks had the audacity to suggest that the system was still safe, because the radar system continued working just fine. Sure, the controllers could still *see* the airplanes; they just couldn't do anything about it as they watched them get closer, and closer, and closer... they'd have had a wonderful view of the targets merging as the passengers were converted instantly a thin pink mist had the planes collided. But hey, the system was safe.)

The VSCS (Voice Switching Communications System) puts all of our communications into one spot- ground-to-ground calls to other facilities, calls within our own facility to other controllers, and air-to-ground comm.

It's a purely digital system; all the incoming feeds are converted to bits and bytes and switched through a series of servers and such until they're turned back into analog and put into the controller's ear through his headset.

Of course, this means that power to the system is absolutely critical, and we've had power failures in the past (see past RISKS for that info).

The VSCS system was designed and built by Harris Corporation, but their contract ran out some time ago. The FAA, coming to the end of the contract, decided to go a much less expensive route- and replace all the servers with Dell boxes and their own programming.

In theory, there's nothing wrong with this; do the required maintenance, and there's no problem. But the system does have the design flaws referred to in the RISKS articles.

Basically, the system needs to be reset about once a month- or more specifically, once every 30 days or so. I heard a rumor that part of the problem in LA was that they'd done the reset at the beginning of August, but had put it off for September... and were planning to do it at the end of the month.

There's a RISK right there; "once a month" probably means "once every 30 or so days", not "once in a calendar month" which could leave an interval as long as nearly 60 days in between resets.

(On a side note, the voice recordings are only kept for the past 15 days, and it's done by an entirely separate system. The main reason for the reset has to do with file and memory buffers overloading.)

Now, there's a backup system for VSCS. It's called VTABS, and is basically a reduced-capability server that normally runs the VSCS system on the ATC simulator that's used to train students.

The VTABS system, with much less server power, cannot run the entire control room and all of the frequencies that the control center has, so it's a hassle to go to VTABS.

When the reset on VSCS is done, you have to run on VTABS for a while, which usually means it's done on graveyard shifts to reduce the impact on live traffic. The downside to this is that the VTABS system also doesn't get a full workout.

So the next RISK pops up: The backup system isn't really fully checked out, and if/when ATC needs it... it might not work.

Sure enough, that happened. When VSCS died, LA Center switched to VTABS... which also didn't work right. Big trouble, now.

Finally, the FAA (in its infinite wisdom) a while back decided to remove a last-ditch backup system called EARS.

EARS was basically a hard-wired, all-analog system that only provided the most crucial thing- air-to-ground communications.

EARS required power to run, but the reason it had a big advantage over VSCS or VTABS is that if the power died for, say, 20 seconds, as soon as the power was back on EARS would work with no spool-up startup time. VSCS takes up to 45 minutes to completely start up, and VTABS has a significant delay in startup time as well.

Seattle Center (where I work) is the only facility of its type that still has EARS (our variant is called VEARS). We have it because a fairly wise manager asked our technicians to keep the system when it was slated for removal. The tech side agreed, and have kept VEARS going by moving a little money around in their budget (since FAA nationally cut VEARS, they don't provide any money to maintain the system to the facilities.)

Fortunately (and perhaps a bit unbelievably) VEARS costs very very little to maintain, because it's just a set of switches that sit there unused the huge majority of the time. We test them for functionality about once a week.

The LA failure was both ridiculous and scary. It's ridiculous on several levels; the fact that the system is designed to shut itself down is silly in a way, because from the user's perspective the system basically crashes to protect itself from crashing.

Well, when suddenly you can't talk to the airplanes, you don't

much give a damn whether it's an intentional shutdown or an accidental/buggy shutdown.

Therefore, they might as well remove this intentional design.

It's ridiculous that the technicians weren't doing the reset.

This issue is

NOT NEW, and has been known for some time... and had any of the 10 airplanes

(with 200 passengers each) managed to smack into another plane, you can bet

that the FAA would have been paying the families for a long, long, long

time.

It's ridiculous that the first backup system didn't work right simply

because people were too lazy/unmotivated to test it properly.

VTABS is an

acceptable backup; it's not perfect, but for the money it cost (essentially

nothing for hardware, some reprogramming costs for the servers) it's nearly

ideal.

It's ridiculous that a perfectly good SECOND backup was thrown away by the

FAA that cost even less. The technology in EARS has been around since, oh,

about as long as there's been radio; it's tried and true, and it's pathetic

that there's only one facility in the nation (out of 21) that still has

EARS.

And it's scary to think that this could've happened in an even busier

facility than LA. The morning crush of traffic in New York or Boston or

Indy or Cleveland Centers, for example, where there's even more traffic

packed into even less airspace than out west in LA.

The RISKS here are many and silly, because nearly all of them could have been easily avoided with some diligence and forethought.

RISK 1) programming the system to shutdown to try and prevent a shutdown.

If you don't expect it either way, it doesn't matter.

RISK 2) being lazy or not really understanding that "once a month" actually means "once every 30 days" and ensuring that a critical job is done, on time, and correctly.

RISK 3) having a backup system that isn't checked to see if it can actually do the job. You rely upon it, it better work, and if/when it doesn't, you're screwed.

RISK 3) throwing out a perfectly good second backup system because you think it's "old fashioned" and that the primary/secondary system you have now is so much better. Hey, the new stuff is all digital, it's gotta be better, right?

Finally, on a personal note, the manager at Seattle Center who managed to talk the technical guys into keeping our VEARS system should be considered a hero and an example for the rest of the FAA. He's already a hero to me - he's my father. :)

Paul Cox, Seattle Center

✶ Re: 49.7 day "overloaded with data" in Los Angeles

<jgd@cix.co.uk (John Dallman)>

Fri, 17 Sep 2004 22:46 +0100 (BST)

In [Risks 23.53](#), Keith Price quoted the *Los Angeles Times* thus:

> When the system was upgraded about a year ago, the original
> computers
> were replaced by Dell computers using Microsoft software.
Baggett
> said the Microsoft software contained an internal clock
> designed to
> shut the system down after 49.7 days to prevent it from
> becoming
> overloaded with data.

I really hope that this quote is a mistake. If it's true, it sounds very much like the issue in Windows 95 and Windows 98 that causes them to shut down every 49.7 days, described in Microsoft Knowledge Base article Q216641. It's caused by integer overflow of a 32-bit count of milliseconds, and "overflow" is something that could readily get misunderstood as "overloaded with data".

The idea that anything remotely connected with air traffic control was running on unattended Windows 9x causes me goosepimples of fear. Especially if it's Windows 9x without the long-available patches that fix the 49.7 day problem.

There are lesser 49.7 day issues in Windows NT 4.0 and Windows 2000 due to 32-bit counts of milliseconds wrapping around, but the Windows 9x one is the one where you have to reboot. The quote that Ben Moore had from the same paper:

> In the meantime, they required manual resetting of the
communications
> system -- a process they described as similar to rebooting a
personal
> computer.

makes me fear that the process is very similar indeed...

John Dallman, jgd@cix.co.uk, HTML mail is treated as probable
spam.

Nose-steered mouse

<James Garrison <jhg@athensgroup.com>>

Fri, 17 Sep 2004 14:52:01 -0500

New Scientist (16 Sep 2004) contains an article describing a
"Nose-Steered
Mouse" or "nouse" that uses a webcam to track nose movement, and
eye- blinks
for clicks. While the potential benefits to disabled users are
obvious,
there might be some interesting risks:

Files "Gone with the Wind"

Early technology adopter Joe Bloggs accidentally deleted a file
representing
several hours of work today while using the new "nouse" or nose-
activated
mouse. "I was moving a file to my desktop when I sneezed and
blinked at the
same time, accidentally opening the context menu, scrolling to
"delete" and
confirming the request. Mr. Bloggs' colleagues point out that
his sneezes
are particularly spectacular....

This new technology is obviously nothing to sneeze at :-)

James Garrison, Athens Group, Inc., 5608 Parkcrest Dr, Austin, TX 78731

<http://www.athensgroup.com> (512) 345-0600 x150

Java programs at risk from decompilers

<"Fiachra O'Marcaigh" <fiachraomarcaigh@amas.ie>>

Fri, 17 Sep 2004 17:30:26 +0100

Java programs at risk from decompilers

A new book shows that practically all Java programs are vulnerable to being decompiled back into the original source code. Author Godfrey Nolan says: "I know I could recover the source code from almost any Java application... and I'm pretty sure there are other people out there who could do the same."

There are several risks here. The programmer's work and intellectual property is vulnerable if the source code can be accessed relatively easily. There is also the danger that a cracker could decompile a popular piece of Java code, insert malicious functionality, and recompile the Java. This new version would be an exact copy of the original program, but with a malicious payload.

An experienced programmer himself, Godfrey Nolan says he wrote this book (Decompiling Java, Apress, August 2004) to explain exactly what decompilation means and what options programmers have to protect

their

work. The book includes building an obfuscator (to attempt to protect source code) and a decompiler (to expose source code).

There is also detailed description of the options open to programmers to protect their code.

<http://www.amazon.com/exec/obidos/tg/detail/-/1590592654/gid=1091398671/>

[sr=8-2/ref=sr_8_2/002-7737498-5564005?v=glance&n=507846](http://www.amazon.com/exec/obidos/tg/detail/-/1590592654/gid=1091398671/sr=8-2/ref=sr_8_2/002-7737498-5564005?v=glance&n=507846)

Fiachra Ó Marcaigh, Killiney View House, Newtownpark Avenue, Blackrock, Co Dublin, Ireland. +353 86 083 1880 fuom@online.ie

★ REVIEW: "Systems Reliability and Failure Prevention", Herbert Hecht

<Rob Slade <rslade@sprint.ca>>

Fri, 17 Sep 2004 11:57:53 -0800

BKSYRLFP.RVW 20040531

"Systems Reliability and Failure Prevention", Herbert Hecht, 2004,

1-58053-372-8, U\$79.00

%A Herbert Hecht

%C 685 Canton St., Norwood, MA 02062

%D 2004

%G 1-58053-372-8

%I Artech House/Horizon

%O U\$79.00 800-225-9977 fax: +1-617-769-6334 artech@artech-house.com

%O <http://www.amazon.com/exec/obidos/ASIN/1580533728/robsladesinterne>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1580533728/robsladesinterne)

<http://www.amazon.co.uk/exec/obidos/ASIN/1580533728/robsladesinte-21>

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1580533728/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1580533728/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1580533728/robsladesin03-20)

%P 230 p.

%T "Systems Reliability and Failure Prevention"

Chapter one is a very brief introduction: almost a preface.

Basic

statistical measures of failure and service are described in
chapter

two. "Organizational Causes of Failures," in chapter three,
tells

stories of some major disasters, but provides no structural
recommendations. Chapter four looks at analytical approaches to
failure prevention, covering the failure modes and effects
analysis

(FMEA) and fault tree analysis (FTA) methods that should be more
widely used in general risk assessment. The discussion of
testing

types, purposes, and analysis, in chapter five, raises some very
interesting questions: if a thousand versions of a part are
tested for

a thousand hours and only one fails, does this *really* support
the

vendor's assertion that the mean time between failures (MTBF) is
a

million hours--or is it equally possible that all of them start
failing shortly after a thousand hours, and one failed early?

Factors

such as partitioning, involved in implementing redundancy in a
system,

are reviewed in chapter six. The material on software
reliability, in

chapter seven, is rather disappointing: there is still an evident
hardware bias, little deliberation regarding the nature of
software,

and the techniques for stability are limited to UML (Universal
Modeling Language) analysis, which is, itself, only suitable to
object-oriented tasks. Chapter eight looks at the project life
cycle,

the preferred development models, reliability activities in
various

phases, testing, and reviews. In chapter nine Hecht addresses
economic considerations in preventing versus accepting failures

with a
good deal of math: a more practical illustration is provided in
chapter ten. Chapter eleven uses the techniques explained in
the book
in three example cases.

For those involved in risk analysis and operation continuity
work,
this text is a tutorial for a number of engineering principles
that
are not widely discussed in the available literature. However,
there
are a multitude of topics that sound interesting and useful, but
are
not presented in sufficient detail to be useful to the non-
engineering
professional. For those in the field, the book will definitely
be
worth reading, but it probably could have provided much more
assistance to those in the safety and security field.

copyright Robert M. Slade, 2004 BKS YRLF P.RVW 20040531
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

Volume 23: Issue 55

Thurs 30 September 2004

Contents

- [Federal Judge Strikes Down Part of PATRIOT Act](#)
[CDT via Monty Solomon](#)
- [Nationwide Radio Shack outage](#)
[George Coulouris](#)
- [Georgia's computer systems down for 16 hours](#)
[Bob Harbort](#)
- [Voter-verified paper trails vs. Internet voting](#)
[Lauren Weinstein](#)
- [Swiss tout success of Internet-voting test](#)
[NewsScan](#)
- [Dutch Internet elections](#)
[Erling Kristiansen](#)
- [Gov. Schwarzenegger signs CA paper trail bill into law](#)
[Kim Alexander](#)
- [JPEG/GDIplus vulnerability](#)
[Rob Slade](#)
- [Realtime keyword voice recognition... not just for the NSA anymore](#)
[Danny Burstein](#)
- [Software that knows your every move](#)
[Burt Helm via Monty Solomon](#)

- [The risks of zero feedback](#)
[Ian Chard](#)
 - [Free ISPs safe?](#)
[Dan Jacobson](#)
 - [Fraud e-mail detector risks](#)
[Danny Lawrence](#)
 - [Re: Java programs at risk from decompilers](#)
[Steve VanDevender](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Federal Judge Strikes Down Part of PATRIOT Act

<Monty Solomon <monty@roscom.com>>

Thu, 30 Sep 2004 00:36:06 -0400

Date: Wed, 29 Sep 2004 14:42:47 -0400 (EDT)

From: info@cdt.org

Subject: CDT Headline: Federal Judge Strikes Down Part of
PATRIOT Act

List-Archive: <<http://www.cdt.org/pipermail/cdt-announcements/>>

A federal judge today found unconstitutional a part of the USA
PATRIOT Act

that allows federal law enforcement officials to obtain
confidential

financial records without a court order or other safeguards.

The lawsuit,

brought by the ACLU, challenged the use of so-called "National
Security

Letters," a type of administrative subpoena power that was
expanded by the

USA PATRIOT Act.

For more on the USA PATRIOT Act:

<http://www.cdt.org/security/010911response.shtml>

For more information on the ACLU lawsuit [offsite]:

<http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15543&c=262>

⚡ Nationwide Radio Shack outage

<George Coulouris <george.coulouris@acm.org>>

Mon, 27 Sep 2004 08:56:26 -0400

On Sunday, September 26, I attempted to exchange a \$21.99 cable for a \$26.99 cable at my local Radio Shack. The manager informed me that all 7000 Radio Shack stores nationwide were unable to process transactions due to a computer outage. I asked if I could simply leave the \$5 difference in cash and let the store sort things out when they were back online, but I was told that this was not possible and to please come back in a couple hours.

⚡ Georgia's computer systems down for 16 hours (Re: [RISKS-23.52](#))

<bharbort@spsu.edu>

Thu, 30 Sep 2004 12:30:45 -0400 (EDT)

A note in [RISKS-23.52](#) about the state computers in Illinois being offline for an hour prompts me to send in the following. Georgia may be last in piddlin' stuff like SAT scores and teacher salaries, but we know how to have *major* downtime!

"A 16-hour shutdown of the state government's computer networks Tuesday

could have been prevented if officials had heeded an earlier warning that

the computers needed replacement batteries. The state's computers froze

for the entire business day Tuesday, shuttering tag offices and delaying

court-ordered child support payments to 516,000 Georgia children, among

other problems. The shutdown was caused by a power outage at Georgia

Power Co. as the remnants of Hurricane Frances swept through the state.

But the computers never should have been running on electricity. An April

report by a state consultant noted that batteries that normally power the

computers had gone bad and two backup generators had failed.

Officials with the Georgia Technology Authority told The Atlanta

Journal-Constitution that they learned of that consultant's report just

last month, and didn't have time to implement its recommendations before

this week's bad weather."

<http://wsbradio.com/news/090904statecomputercrash3a.html>

I particularly like the part about "the computers never should have been

running on electricity." White lightning, maybe?

Bob Harbort, Southern Polytechnic State U., CS/Software Engineering

1100 S. Marietta Pkwy. Marietta, GA 30060-2896 bharbort@spsu.edu
1.678.915.7405

✶ Voter-verified paper trails vs. Internet voting

<Lauren Weinstein <lauren@vortex.com>>

Wed, 29 Sep 2004 11:43:16 -0700

With California just wisely enacting a secure, voter-verified paper trail law relating to electronic voting machines, many other states following a similar path, and related federal legislation also being considered, it appears that this methodology is likely to become a fixture in many, most, or even all U.S. jurisdictions where touch-screen or other e-voting machines are in use.

However, I haven't seen discussion of a likely side-effect of this welcome trend -- its impact on proponents of voting over the Internet. If a secure, voter-verified paper trail is being required for e-voting machines operating in the theoretically "secure" environment of polling places, it's quite possible that we're finally putting a stake in the heart of the extremely ill-advised and highly risky idea of Internet-based voting, even if the laws regarding paper trails may not address this issue specifically.

Keep in mind that typical voter-verified paper trail systems permit the voter to inspect the receipt but not to handle or remove it -- the receipt must stay under the control of the voting authorities at all times. These twin requirements cannot be simultaneously met in remote Internet voting situations (e.g., people voting from their homes or offices, which are the big "selling points" for those persons pushing Internet voting).

No doubt the proponents of Internet voting will suggest all

manner of
bizarre schemes involving encoded receipts that could be
physically mailed
back to voting authorities or other similar completely
impractical ideas.

But the bottom line is that if a secure, voter-verified paper
trail is
needed for e-voting machines -- and it is -- then Internet
voting should be
considered to be dead on arrival for the foreseeable future at
least.

Lauren Weinstein lauren@pfir.org lauren@vortex.com
+1 (818) 225-2800 <http://www.pfir.org/lauren> <http://www.factsquad.org>

[Incidentally, the October issue of the *Communications of
the ACM*

has a special section with 8 papers devoted to voting
systems. PGN]

Swiss tout success of Internet-voting test

<"NewsScan" <newsscan@newsscan.com>>

Tue, 28 Sep 2004 09:12:02 -0700

Switzerland has declared Internet voting a success after being
used without
problems in a national referendum in which 2,723 people in four
Geneva
suburbs visited a special Web site to cast their votes on various
issues. Swiss officials says the test has proven their systems
are robust
and secure, but e-voting critic Avi Rubin of Johns Hopkins
University is
unconvinced: "Just because nobody attacked a referendum that
involved 2,723

people does not mean that it was secure. When these trials are viewed as successful and justify more in-depth electronic voting, eventually there will come a point where it will be worth someone's while to attack the election." Geneva's e-voting system uses software developed by local election authorities with the Swiss office of Hewlett-Packard Co. and the Geneva-based online security firm Wisekey. [AP/*USA Today*, 27 Sep 2004; NewsScan Daily, 28 Sep 2004]

http://www.usatoday.com/tech/news/2004-09-27-swiss-evotes_x.htm

🚀 Dutch Internet elections

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>

Sun, 26 Sep 2004 21:41:53 +0200

The Netherlands is currently holding the election for the Regional Water Management Boards (my translation of "Waterschappen"). One can vote by mail or by Internet. The latter attracted my curiosity, and I poked around the 'net a bit to see what people thought about the idea.

It appears that a test election was held in order to test the procedure and get some feedback from test voters. An often quoted feedback was that "Only 26% of the test voters expressed concern about the possibility of fraud". ONLY 26%?? This response seems to be interpreted as a vote of confidence for the system.

Another nugget: "The secrecy of the vote is guaranteed. The

relationship
between the voter identity and his login code is removed from
the file
before the votes are counted".

The FAQ also has an interesting statement. An independent body
(TNO) has
investigated the security of the voting method. They concluded
that "Voting
by Internet is not less safe than voting by mail or phone". This
formulation
implies that the procedure is actually not very safe, and they
know it.

I cast my vote today. And my wife's! With her permission, but I
could
equally well have voted for her without her knowing about it.
All you need
in order to vote is a couple of codes contained in a letter
delivered by
post. Since I happened to be the one emptying the mailbox
yesterday, I
retrieved my own ballot, my wife's and my daughter's. And what
about mail
delivered to the wrong address, that happens quite regularly.
But not today,
so, sadly, I was unable to vote on behalf of any of my
neighbours.

Slightly to my surprise, the voting web site worked well in
Netscape, except
that Netscape aborted just after I had completed the second vote.

At the end of the voting process, you get a code, consisting of
a total of
40 hex digits in 3 sub-fields. Allegedly, this code can be used,
after the
election has closed, to "check whether the vote was counted".
If you do not
take note of these codes here and now, they are lost for good,
there seems
to be no way to retrieve them later. The page displaying the
codes posts

the warning "Keep these codes secret, your vote can be derived from them".

It seems to me that there is no way to guarantee that "the vote was counted", only that it was registered somewhere. You have to take their word that this is actually the file that is counted, that nobody messed with it, and that counting is done correctly and honestly.

The Water Management Board election is not a very high-profile election, many show little interest in what these boards are doing. You vote for individuals, not for political parties, and the campaign preceding the election is not very intense, possibly because no party politics is involved. So it may not be very fraud-sensitive. But I am afraid that if this type of elections is declared a success, the technology may show up in more important elections.

Gov. Schwarzenegger signs CA paper trail bill into law

<cvfnewslst@calvoter.org>

Tue, 28 Sep 2004 10:47:00 -0700

Great news to share -- California Governor Arnold Schwarzenegger signed SB 1438 into law. This bill, co-authored by Senators Ross Johnson (R-Orange) and Don Perata (D-Alameda) requires there to be a voter verified paper record to back up every electronic ballot cast in California by 2006 Primary election.

California is the first state in the nation where paperless, electronic voting systems have been widely deployed that is requiring by law that the machines be retrofitted or replaced. With the enactment of SB 1438, California continues to lead the nation on electronic voting reform.

Two other states -- New Hampshire and Oregon -- have laws that mandate the use of voting systems that allow for manual recounts. Illinois passed a law that requires a voter verified paper trail for e-voting machines once that state begins purchasing them. Five Secretaries of State have elected to implement the voter verified paper trail. The first to do so is Dean Heller of Nevada, who is implementing the paper trail this election season. In addition, the Secretaries of State in Washington, Missouri, California, and Ohio will require the paper trail by 2006.

Although paper trail legislation was introduced in as many as 20 states this year, it appears that California is the only state so far to enact a paper trail law. SB 1438 essentially codifies California Secretary of State Kevin Shelley's November 2003 and April 2004 security directives, and advances the deadline for implementing the paper trail by one election. Under the Secretary of State's orders, California would have the paper trail by the November 2006 election. SB 1438 ensures the paper trail will be in place for the 2006 Primary.

The new law also prohibits the Secretary of State from

certifying any new,
paperless electronic voting systems after January 1, 2005, and
prohibits
counties from purchasing such systems after January 1, 2006.

Proclaimed "dead" just last month, SB 1438 was brought back to
life by its
authors in the 11th hour of the legislative session, and sailed
out of the
Legislature on unanimous votes of both houses.

For more information about SB 1438, visit
[http://www.leginfo.ca.gov/cgi-bin/postquery?
bill_number=sb_1438&sess=CUR&house=B&author=johnson](http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_1438&sess=CUR&house=B&author=johnson)
[http://www.leginfo.ca.gov/cgi-bin/postquery?
bill_number=sb_1438&sess=CUR&house=B&author=johnson](http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_1438&sess=CUR&house=B&author=johnson) [SPLIT
URL]

For past CVF-NEWS updates on SB 1438, visit
<http://www.calvoter.org/news/cvfnews/2004archive.html> .

-- Kim Alexander, President, California Voter Foundation
kimalex@calvoter.org, <http://www.calvoter.org>, 916-441-2494

Contact the California Voter Foundation: <http://www.calvoter.org>
530-750-7650
info@calvoter.org U.S. Mail - 503 4th Street, Suite 6, Davis,
CA 95616

JPEG/GDIplus vulnerability

<Rob Slade <rslade@sprint.ca>>
Sun, 26 Sep 2004 15:03:55 -0800

If you have not been living under a rock (in security terms),
you will
likely have heard something about the GDI+ vulnerability in the
past few

days. JPEGs and other files that may be handled in the same way are now potentially "dangerous" data files.

In 1994 a graphics file was spread via Usenet that contained oddities in the header, and at about the same time a virus warning hoax was created that warned of a viral JPEG file. Neither of these was, in fact, related to actual malicious software, but I did some study on the subject and found header structures in both formats that could, potentially, have been used as malware vectors, under certain conditions.

The specifics of the current JPEG/GDI+ vulnerability are very difficult to obtain, even when you have copies of the various "exploits" that have been released. However, it does seem to be simply your common or garden buffer overflow. As I write I am not aware of any specific exploits that have been released with the intent to use them maliciously. However, given the number of "exploit" samples that have been released I dare say that it will not be long before we see the real ones come out. It is unlikely that viruses will be created using this vulnerability, but it is quite probable that viruses will be created that carry graphics files (likely pornographic) that will use the vulnerability to open links to malware on Web sites, or simply open backdoors on machines for exploitation and amalgamation into botnets of various types.

Microsoft security bulletin MS04-028
(<http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx>)

has some links that, if you manage to follow them all the way through, will lead you to a patch. Affected systems use certain versions of the gdiplus.dll file. The most widespread of the affected versions of the file come with Microsoft Windows and Office, 2003 and XP versions. Other Microsoft, and other, products also have vulnerable versions of the file.

The file is fairly ubiquitous. I've got eleven copies (and two compressed copies) of five different versions of gdiplus.dll on my machine. The Microsoft site does provide details of which version numbers are vulnerable or not--but no information about file sizes or dates that might allow you to determine which versions are which. If you follow links through from that page there is also a "detection" tool--but it only tells you that you *are* vulnerable, rather than identifying specific instances.

SANS also has provided a scanning tool, at <http://isc.sans.org/gdiscan.php>.

(Actually two, a GUI version and a command line version. The GUI version, as provided, seems to want a disk in drive F:, but if you tell it to continue seems to function.) This tool identifies which versions are vulnerable and which are not, and also scans other filenames which are, in fact, renamed copies of the gdiplus.dll file, such as:

```
C:\I386\ASMS\1000\MSFT\WINDOWS\GDIPLUS\GDIPLUS.DLL
  Version: 5.1.3097.0 <-- Vulnerable version
C:\Program Files\ArcSoft\Software Suite\PhotoImpression
  5\Share\gdiplus.dll
  Version: 5.1.3097.0 <-- Vulnerable version
C:\Program Files\Common Files\Microsoft
```

Shared\OFFICE11\MSO.DLL

Version: 11.0.6360.0

C:\Program Files\Common Files\Microsoft Shared\VGX\vgx.dll

Version: 6.0.2800.1106 <-- Possibly vulnerable (Win2K SP2 and SP3 w/IE6 SP1 only)

C:\Program Files\Microsoft Office\OFFICE11\GDIPLUS.DLL

Version: 6.0.3264.0

Banning JPEGs is unlikely to be effective as a security measure. Untrained users will probably not know how to turn off the relevant functions, or be willing to so "cripple" their Web browsing. In any case, graphics files of various types can be renamed, and Windows will still identify them from internal structures, and run them through GDI+.

Microsoft has provided some new patches (patches for Office and Windows apparently have to be installed separately), and others will possibly do so as well. It may be difficult to find the appropriate patches for all applications. One would assume that all versions of gdiplus.dll could simply be replaced by the latest (safe) version, but, knowing the industry, one would probably be wrong.

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>

[Later update, Tue, 28 Sep 2004:]

a) I've seen at least one actual use of the exploit in what appears to be a malicious situation.

b) There are serious questions about whether the Microsoft updates (for both

Windows and Office) actually work.

✦ Realtime keyword voice recognition... not just for the NSA anymore

<danny burstein <dannyb@panix.com>>

Mon, 27 Sep 2004 13:04:30 -0400

"Phone a call centre and you are likely to spend ages on hold listening to canned music - and then find the operator cannot find the information you need. But an artificial intelligence system that hunts down the required information is aiming to slash the time people waste this way.

"Using a mixture of speech recognition and search engine technology, the system, being developed by IBM, will trawl a call centre's databanks for the information a customer wants and present it to the operator before the caller has finished explaining what they want. By giving operators rapid access to the right information, calls will be dealt with faster.

"The system works by listening in to the conversation and identifying keywords spoken by the customer....

<http://www.newscientist.com/news/print.jsp?id=ns99996430>

Risks: aside from the commercial aspects, how long before these programs start looking for any "disturbing" phrases in more and more communications, and then immediately redflagging the call and forwarding the info to Law Enforcement Agency of Your Choice?

✦ Software that knows your every move

<Monty Solomon <monty@roscom.com>>

Mon, 27 Sep 2004 02:55:33 -0400

Source: Burt Helm, *Business Week*, 23 Sep 2004

It's called Worklenz, and it can be a powerful management tool for tracking projects and people -- or a scary Big Brother

Look busy -- Worklenz is watching. Designed by privately held information-technology company Métier in Washington, D.C., Worklenz is software designed to help companies manage large projects and maximize efficiency. But unlike an enterprise resource program, which tracks a company's inventory, invoices, and assets, Worklenz tracks workers -- what they do, when they do it, and how long it takes.

And it's spreading fast. Métier says it has been profitable for just over two years and has won contracts with Lockheed Martin (LMT), BMW, Northrop Grumman (NOC), and the U.S. Agriculture Dept. In the next week, BusinessWeek Online has learned, Métier will announce a contract with the FBI to manage all of the bureau's IT-related projects.

In its essence, Worklenz uses an extreme form of micromanagement to help a company make broad decisions. The program can sync with each employee's Microsoft Outlook e-mail account, Microsoft Project scheduling software, and his or her PeopleSoft timesheet, to let a boss see everyone's

schedules,
what tasks they're working on, and how soon each employee will
complete his
or her work. ...

[http://www.businessweek.com/technology/content/sep2004/
tc20040923_0520_tc024.htm](http://www.businessweek.com/technology/content/sep2004/tc20040923_0520_tc024.htm)

✶ The risks of zero feedback

<Ian Chard <ian@chard.org>>
26 Sep 2004 17:08:03 +0100

Background: a Spanish bank issues its customers with a passbook
instead of an
ATM card on certain types of account (like UK building societies
used to
do). Its ATMs have a wide slot so that the passbook, open at a
certain
page, can be inserted. The book is about the size of a passport
and
contains a history of transactions on the account.

From a hotel window overlooking such an ATM, I recently watched
a woman
trying to use the service for the first time. She opened the
book and
inserted it correctly, and the machine pulled it completely
inside.
However, the screen stayed in what pinball machine designers
would call
"attract mode": it continued idly to display rolling adverts as
if nothing
had happened. Thirty seconds passed before a bank employee
noticed her
waving through the window and beckoned her inside. A few
seconds later, the
machine spat out the book saying it couldn't be read. It sat

hanging out of
the slot for a full minute before the woman came out and
retrieved it.

The risk is obvious, and I've also noticed in the last year or
so that newer
ATMs in the UK also exhibit this behaviour, leaving the customer
wondering
whether it even noticed that their card has been inserted. It's
so easily
mitigated ("Please Wait") that I find it hard to understand how
these things
ever passed their testing phase.

⚡ Free ISPs safe?

<Dan Jacobson <jidanni@jidanni.org>>
Sun, 26 Sep 2004 07:30:15 +0800

Here in Taiwan there are tons of free ISPs. One just dials up
with the
username and passwd from their ads. But how long before one of
them starts
snooping the data they pass for fun and profit?

⚡ Fraud e-mail detector risks

<Danny Lawrence <DanteMann@gmail.com>>
Wed, 29 Sep 2004 16:37:10 -0400

Citibank has an e-mail account to send fraud/Phishing messages
to,
presumably so that their security people can track down the
perpetrators. I

received an obvious (both to me and to my Spam catching software -- it was in my "probable spam" file) phishing message so I dutifully forwarded it to their address: emailspooof@citibank.com.

Later on I get a delivery failure: Error transferring to mail4.citigroup.com; SMTP Protocol Returned a Permanent Error 554 5.7.1 Virus present: Phish-BankFraud.eml

I suppose it is a good thing that Citibank has something that detects fraudulent e-mails, but wouldn't it be better if they didn't use it on messages coming into their fraud account?

✶ Re: Java programs at risk from decompilers (O'Marcaigh, [RISKS-23.54](#))

<Steve VanDevender <stevev@hexadecimal.uoregon.edu>>
26 Sep 2004 01:43:17 -0700

The risk here seems not to be the possibility that compiled programs can be decompiled (I've heard of decompilers for various languages and system architectures), but that there are people who wrongly think that a compiler somehow conceals the algorithms used in a program. Since a compiler's job is to translate a source specification of an algorithm into a machine-executable form, the compiler's job is to exactly preserve the programmer's "work and intellectual property" in that sense. The machine-executable form might be less human-readable, but it is still susceptible to analysis and reverse-engineering. Compiled machine code is

often easy to decompile, even by hand, because compilers tend to generate code with more conventional structure than human-written machine code.

> This new version would be an exact copy of the original program, but
> with a malicious payload.

How can such a program be "an exact copy" while having also been modified

"with a malicious payload"? If it's been modified, this modification will be easily detectable by comparison with the original.

At one time, "binary patching" (direct modification of machine code) was commonly used for fixing bugs in code which could not be conveniently recompiled or reassembled.

Apparently the now-ubiquitous use of compiled high-level languages is causing people to forget what compilers actually do, and ignorance of the details of low-level machine code leads to the erroneous idea that a compiled form of a program is somehow "protected" from modification or exposure of its inner workings.

[RISKS received a similar note from Russ Perry Jr., and another reminder of the futility of security by obscurity from Dave Minter. Scott Nicol

cited two Java decompilers

<http://kpdus.tripod.com/jad.html>

<http://jode.sourceforge.net/>

and observed that .Net code can also be decompiled. He also added

"Think how much easier Y2K fixes would have been if 1960's Cobol programs compiled into a form that was decompilable."

See a somewhat related article that has just appeared:

Huaiqing Wang and Shuozhong Wang,

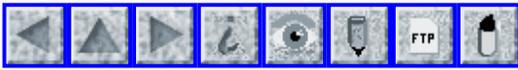
Cyber Warfare: Steganography vs Steganalysis,

Communications of the ACM, 47, 10, October 2004, 76--82.

PGN]



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 56

Tuesday 12 October 2004

Contents

- [VP Cheney shoots himself in the foot, URL-wise](#)
[Jim Griffith](#)
 - [Sabotage-induced power outage in Wisconsin](#)
[Sami Saydjari](#)
 - [Virus disables Colorado DMV for nearly a week](#)
[Brad Hill](#)
 - [Navy battle software unsafe](#)
[PGN](#)
 - [Runaway Renault risks](#)
[Alistair McDonald](#)
 - [Fire engine startup risks](#)
[Stephen Fairfax](#)
 - [Customs and Excise electronic returns](#)
[Ben Laurie](#)
 - [Power company sent too high voltage to customers](#)
[Jacob Palme](#)
 - [Terror alert from a "honey-pot"?](#)
[Bob Harbort](#)
 - [Glitch opens access to kids' records](#)
[Colleen Jenkins via Monty Solomon](#)
 - [Social security breach on Utah State University campus](#)
[Bob Heuman](#)
 - [Outsource firm sues in India](#)
[Karl Schoenberger via Monty Solomon](#)
 - [Internet voting](#)
[Martyn Thomas](#)
 - [Spam that asks you to delete it](#)
[Geoff Kuenning](#)
 - [Not all buffer overflow exploits are necessarily bad](#)
[Paul Robinson](#)
 - [Say goodbye to broken links](#)
[NewsScan](#)
 - [Info on RISKS \(comp.risks\)](#)
-

VP Cheney shoots himself in the foot, URL-wise

<Jim Griffith <griffith@dweeb.org>>

Wed, 6 Oct 2004 14:47:41 -0500

In last night's VP debate, Vice President Cheney countered an assertion made by Senator John Edwards and invited viewers to read a non-partisan analysis confirming his position by going to "FactCheck.com". Unfortunately, he meant to say "FactCheck.org", which is indeed a non-partisan election watchdog site run by the University of Pennsylvania. Worse for Cheney, it seems that FactCheck.com is a private advertising site, which is run by someone who is not a fan of the President. So to deal with the volume of traffic generated by Cheney's reference, the owner of FactCheck.com is now redirecting his traffic to www.georgesoros.com (George Soros being a billionaire who is actively campaigning to defeat the Bush/Cheney ticket). So anyone who follows Cheney's suggestion is presented with a partisan argument for voting for Kerry/Edwards.

http://story.news.yahoo.com/news?tmpl=story&e=2&u=/ap/20041006/ap_on_el_pr/debate_rdp

So always keep your URLs straight!

http://story.news.yahoo.com/news?tmpl=story&ncid=738&e=1&u=/ap/20041006/ap_on_el_pr/debate_web_sites

<http://story.news.yahoo.com/news>

?tmpl=story&ncid=738&e=1&u=/ap/20041006/ap_on_el_pr/debate_web_sites

Sabotage-induced power outage in Wisconsin (via Sami Saydjari)

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

Mon, 11 Oct 2004 15:32:12 PDT

On 9 Oct 2004, near Milwaukee, Wisconsin, an 80-foot-tall high-voltage electrical tower collapsed onto a second transmission tower, causing a four-hour power outage for 17,000 customers. Apparently someone had removed enough bolts from the base of the tower. Wires were still across railroad tracks the next day, delaying Amtrak and Canadian Pacific trains.

<http://www.cnn.com/2004/US/10/11/wisconsin.blackout.ap/index.html>

Virus disables Colorado DMV for nearly a week

<Brad Hill <hillbrad@gmail.com>>

Thu, 30 Sep 2004 17:16:01 -0600

The Department of Motor Vehicles in Colorado was disabled all of last week by a computer virus. New and renewed licenses and ID cards were unable to be issued during the time. Every computer in the system had to get fresh

software installs and nearly 4.5 million documents had to be reloaded. No cost estimates have been given for the outage and no details released about the nature or origin of the virus.

The risks of inadvertent disclosure and alteration of DMV records has been a frequent topic here over the years, but this is the first example I'm aware of involving a malware attack against such a huge and legally important government datasytem.

The risks of disclosure and modification of these data are obvious, but completely shutting down a major branch of state government for a week also provides a good case study of the possibilities of information warfare/sabotage.

<http://www.denverpost.com/Stories/0,1413,36~53~2417722,00.html>

✶ Navy battle software unsafe

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

Tue, 12 Oct 2004 09:02:47 -0400

[Source: Article by Neil Mackay, Investigations Editor, *Sunday Herald* (Scotland), 10 Oct 2004]

The Royal Navy's new, state-of-the-art destroyer has been fitted with combat management software that can be hacked into, crashes easily and is vulnerable to viruses, according to one of the system's designers who was fired after raising his concerns.

Gerald Wilson, who has 25 years' experience designing naval software, worked for Alenia Marconi Systems (AMS) in a joint venture with Bae Systems and the Italian company Finmeccanica on the combat system for the Type 45 destroyer, which will rely on Microsoft Windows 2000. System failure in action, he says, would leave the ship blind, defenceless, and as good as sunk.

Dismissed after voicing his fears to the Ministry of Defence and the Defence Procurement Agency (DPA), Wilson wants to give evidence to the parliamentary defence select committee about the software.

Last night he told Channel 4 news that "the use of Windows For Warships puts the ship and her crew at risk, and the defence of the realm".

There are also plans to install a similar Microsoft Windows-based computerised command system on Britain's nuclear submarines. Wilson said: "It is inconceivable that we could allow the possible accidental release of nuclear missiles. The people who survived such an exchange, if any, would certainly regard such a thing as a crime against humanity. And I can't help feeling that even planning to deploy such systems on Windows, with its unreliability and lack of security, is itself some sort of crime in international law."

Windows was chosen by AMS in order to cut costs, as the DPA has been encouraging a switch to off-the-shelf systems. Wilson says the Navy should stick to its current operating system, Unix, which is said to be more reliable. Designers can also customise Unix, which would allow unnecessary components to be removed to reduce risk.

A navy spokesman said: "Bae Systems, as the prime contractor for the Type 45, is responsible for ensuring that the warship meets the requirements placed on it by the DPA. Using Microsoft Windows within combat management systems was the subject of an independent review commissioned some while ago by the DPA. "The review found a proper engineering approach had been taken, both from a security perspective, as the system middleware isolated Windows from the remainder of the mission-critical systems, and from a safety perspective.

Comprehensive hardware mechanisms will be put in place where necessary to avoid any potential Windows-derived compromises. "We are satisfied that the solution recommended by the contractor will meet our requirements, as it has been subject to an independent review. This review was conducted by a team at the DPA who are independent of the Type 45 team."

✂ Runaway Renault risks

<"Alistair McDonald" <alistair@inrevo.com>>
Fri, 8 Oct 2004 13:14:34 +0100 (BST)

A driver of a Renault car fitted with an automatic speed regulator got more than they expected when the the regulator stuck on, giving him an hour-long drive at 125 MPH.

The Renault uses an electronic card instead of a key, and the driver finally stopped the car by pulling the card out. He had been in touch with police, who had used motorway warning signs to clear the road for him to drive past safely - but at one point he had to use the emergency lane, normally only used for recovery of broken-down cars.

http://www.theregister.co.uk/2004/10/07/satanic_renault/

I wonder if the driver had attempted to pull the card out earlier, and also wonder why Renault, the manufacturer, was allowed to "impound" the car for tests. I'd expect the police to be involved in any investigation.

The Register article includes links to previous stories where machines have "misbehaved" - it's worth a read.

Alistair McDonald, InRevo Ltd (<http://www.inrevo.com>)
Author of the SpamAssassin book: <http://www.spamassassinbook.com/>

[Lindsay Marshall noted this case as well:
http://www.iol.co.za/index.php?set_id=1&click_id=29&art_id=qw1096963740806B216
Also, recall "Runaway car from hell", a Pontiac Sunfire, in [RISKS-23.33](#). PGN]

✂ Fire engine startup risks

<Stephen Fairfax <fairfax@mtechnology.net>>
Thu, 26 Aug 2004 14:44:31 -0400

The risks of allowing a rushed ignition sequence to stall or significantly

delay an emergency vehicle are certainly breathtaking.

What I find interesting is that Toyota, which sells primarily in the free market rather than to government agencies, got this behavior pretty much correct. In the Toyota Prius, the computer controls the engine, the device the serves as the transmission, and of course the electric motor/generators and their associated power electronics. There is no starter motor, no reverse gear, and no cable between the accelerator pedal and the throttle, the computer monitors and controls everything.

The owners manual instructs you to turn the key to 'start,' wait for the 'OK' light in the instrument panel, then release the key. In the original Prius (up to 2004) the engine starts every time the ignition is activated in order to heat up the catalytic converter. I'm told the 2004 and later models will start in all-electric mode without the engine.

The beauty of the Prius is that Toyota engineers knows perfectly well that very few people read the owners manual. So you can just flip the key to start and immediately let it go. The computers go through their tests, and then start the engine. There's no way to manipulate the key in a way that will cause a delay or stall or require a reboot.

✂ Customs and Excise electronic returns

<Ben Laurie <ben@algroup.co.uk>>
Wed, 29 Sep 2004 13:05:52 +0100

Background, for non-Brits: Customs & Excise (C&E) is the government department responsible for collecting VAT (Value Added Tax), which is a European sales tax. Businesses report their VAT transactions quarterly to C&E, currently mostly on paper (a one page form, amazingly) - this is known as a VAT return.

For some time, C&E has been encouraging electronic VAT returns (cunningly named eVAT), but until recently required the use of an X509 client certificate to submit.

Presumably this has proved unpopular, since they are now permitting good old username/password to be used. But they seem to be a little confused...

From the eVAT FAQ:

[http://new.hmce.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?
_nfpb=true&_pageLabel=pageOnlineServices_ShowContent&id=HMCE_PROD_008287&propertyType=document](http://new.hmce.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pageOnlineServices_ShowContent&id=HMCE_PROD_008287&propertyType=document)

[http://new.hmce.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal
?_nfpb=true&_pageLabel=pageOnlineServices_ShowContent&id=HMCE_PROD_008287
&propertyType=document](http://new.hmce.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pageOnlineServices_ShowContent&id=HMCE_PROD_008287&propertyType=document) [SPLIT URL]

"Which is more secure -- using a Digital Certificate or User ID & Password?"

Both methods are secure, but they work in different ways."

From the Government Gateway Help pages:

http://www.gateway.gov.uk/help/help_template_non_secure.asp?content=%3A%2F%2Fwww.ukonline.gov

[uk%2FGateway%2FGatewayArticle%2Ffs%2Fen%3FCONTENT_ID%3D4013333%26chk%3DBQAvk3&languageid=0](http://www.gateway.gov.uk/help/help_template_non_secure.asp?content=%3A%2F%2Fwww.ukonline.gov.uk%2FGateway%2FGatewayArticle%2Ffs%2Fen%3FCONTENT_ID%3D4013333%26chk%3DBQAvk3&languageid=0)

http://www.gateway.gov.uk/help/help_template_non_secure.asp

?content=%3A%2F%2Fwww.ukonline.gov.uk%2FGateway%2FGatewayArticle%2Ffs%2Fen%3FCONTENT_ID%3D4013333%26chk%3DBQAvk3&languageid=0 [SPLIT]

"Certificates provide a higher level of security, which is required for certain services."

Nothing like singing from the same songsheet, eh?

Anyway, it gets better. Three types of certificate are permitted, SecureMark, SimplySign or Trust Services. Again from the eVAT FAQ:

- * SecureMark and Chamber SimplySign certificates can be used with either Internet Explorer 5.01 or higher, or Netscape Navigator.
- * Trust Services' certificates work with Microsoft Internet Explorer 5.0 or later and Netscape v 4.6 or higher (but not v6 or 7).
- * certificates can be used with Internet Explorer 5.01 or higher or Netscape Navigator 4.08 or later (but not v6 or 7). "

I dunno about you, but this is not exactly clear to me. Leaving that aside, let's look at the various CAs...

SecureMark, on a page amusingly titled "Does your Netscape Browser meet the minimum requirements?"

http://www.equifaxsecure.co.uk/digitalcertificates/Netscape_Response.html

"The minimum system requirements are:
Windows 95 or NT 4 (SP3) or higher
Internet Explorer version 5.01 or above
128-bit cipher strength"

I guess the answer will be "no", then! (My browser was Firefox, incidentally).

SimplySign - seems they actually admit that "Netscape" might work. But...

<http://www.simplysign.co.uk/support/ierootdownload.html>

"To make sure that your browser works with Trustis certificates the 'Trustis FPS Root CA' certificate should be installed. There is no danger in doing this and no programs will be downloaded to your computer."

No, of course, installing root CAs in your browser has no security implications whatever. And of course, you have to have the root CA to use a client cert. Not.

As for Trust Services. Well, I can't find them through Google (at least, not the one they had in mind) but much meandering around FAQs eventually yielded a link - turns out its BT and Verisign, but ... oops! "Note: Inland Revenue services have not yet been upgraded to allow the use of BT ID Certificates". So much for a simpler user experience.

Oh yeah, another gem from the eVAT FAQ:

"The Government Gateway and Digital Certificate authorities do not currently support the use of Digital Certificates on Apple Macintosh"

Well, of course not, because everyone knows that Apple X.509 is completely different from Microsoft X.509. Duh.

So, after all that, I totally understand why everyone thinks PKI is hard. I'm all for the username/password thing. Its free, too.

<http://www.apache-ssl.org/ben.html>

<http://www.thebunker.net/>

✂ Power company sent too high voltage to customers

<Jacob Palme <jpalme@dsv.su.se>>

Fri, 8 Oct 2004 21:15:14 +0200

A Swedish power company (Fortum) had a technical failure, causing it to send electricity to a hundred households with too high voltage.

Result: One fire destroying part of a house, Other houses got their electrical heating destroyed. When the fire company and police arrived, lots of people met them on the street, since all the houses were more or less affected.

[Source: Dagens Nyheter (largest Swedish morning paper), 6 Oct 2004]

This incident actually happened in May, but not until five months was it reported in the national newspapers. The power company refuses to pay for the damages, but the issue has not been settled in courts yet.

Power companies in Sweden were ten years ago mostly owned by the government or the local government. But in the privatization fervour of the 1990s, most of them have been "privatized". The private companies optimize profit at the expense of reliability. -- Jacob Palme <jpalme@dsv.su.se> (Stockholm University and KTH) for more info see URL: <http://www.dsv.su.se/jpalme/>

✂ Terror alert from a "honey-pot"?

<bharbort@spsu.edu>

Thu, 30 Sep 2004 13:46:42 -0400 (EDT)

Security at this past summer's Oshkosh AirVenture Fly-In was increased in response to what may have been a non-threat. USA Today reports that "...a suspicious Web posting was found referring to the city." The description of the posting reminds me a lot of what an anti-spam "honey pot" web page looks like:

"Winnebago County Sheriff Michael Brooks said the Milwaukee office of the FBI contacted him early Sunday regarding the Web site, which mentioned Oshkosh and Sunday's date in the text but contained no actual threat.

"Brooks said a California resident found the letter, which contained more than a full page of incoherent words, on a pharmaceutical Web site and notified the FBI. It also mentioned Auckland, New Zealand; Bangor, Maine and a couple other cities around the world, Brooks said.

" 'It was just a series of words that did not form a complete thought,' he

said. 'It contained today's date along with several names of cities -- one of which was Oshkosh -- so it becomes important for us to have heightened awareness...'

http://www.usatoday.com/tech/webguide/internetlife/2004-08-01-oshkosh-terror-warning_x.htm

Bob Harbort, Prof. of CS/Softw.Eng., Southern Polytechnic State U., 1100
S. Marietta Pkwy. Marietta, GA 30060-2896 1-678.915.7405 bharbort@spsu.edu

[I presume you heard about the Midwest Airline story of the flight from Milwaukee to SF that was aborted after takeoff because a passenger found a sheet of paper that looked like Arabic writing in the airline magazine. (It reportedly turned out to be a prayer-like message in Farsi.) PGN]

✂ Glitch opens access to kids' records

<Monty Solomon <monty@roscom.com>>

Mon, 4 Oct 2004 00:51:48 -0400

Officials say the problem has been fixed, but the error made thousands of confidential child-abuse and foster care files available to anyone on the Web.

[Source: Article by Colleen Jenkins, *St. Petersburg Times*, 1 Oct 2004]

A *Miami Herald* reporter alerted local child welfare authorities this week to a software glitch that made available thousands of confidential child-abuse and foster care records to anyone with Internet access.

Those files contained detailed information about the 3,966 children under the watch of Kids Central, the private consortium that handles foster care and related services for at-risk children in the Department of Children and Families' District 13, which includes Citrus, Hernando, Marion, Lake and Sumter counties.

Names of foster children, birth dates, Social Security numbers, photographs, case histories and even directions to children's foster homes were accessible with a password that had been published on Kids Central's Web site, the Herald reported.

DCF officials, who monitor the competitively bid contract with Kids Central, immediately ordered that the site be shut down after the reporter informed them of the security breach Wednesday morning. ...

http://www.sptimes.com/2004/10/01/Hernando/Glitch_opens_access_t.shtml

✂ Social security breach on Utah State University campus

<Bob Heuman <rsh@idirect.com>>

Mon, 11 Oct 2004 16:34:41 -0400

Do I need to say anything except that anyone who has been at USU in the past

8 years or more needs to be careful that their SSN is not misused? While it is reassuring to hear that it looks like no one has accessed the files in question, there is NO proof and can be no proof that this is the truth. Anyway, the following is from the campus newspaper. RSH

Social security breach on USU campus

Personal information leaked in USU database security breach

By Hilary Ingoldsby, hilaryi@cc.usu.edu

The Statesman, 11 Oct 2004, Email Edition TheStatesman@collegepublisher.com

<http://www.utahstatesman.com/news/749251.html&mkey=1022600>

The social security numbers of 16 Utah State University faculty and staff members were mistakenly made accessible on the Internet, leading to the discovery of thousands more, USU officials said. Over the weekend of Oct. 1 and 2, a faculty member looked up his name using the Google Internet search engine, John DeVilbiss, executive director of public relations and marketing, said. The search yielded results of a university site that contained his social security number, he said.

The site also contained the personal information of 15 other faculty and staff. The faculty member first notified the police and then Webmaster Charles Thompson was contacted, DeVilbiss said. "He [Charles] went right in and took immediate action," DeVilbiss said. Thompson said he immediately pulled the information off the server and began doing other searches. He said he also contacted Google who said they will shut down the sites but it will take a few weeks to do so completely.

Upon further investigation, 12 Excel spreadsheets were found on an open-access server. The spreadsheets contain more than 7,000 social security numbers of current and past faculty, staff and students, DeVilbiss said. An additional 11 files were also found containing sensitive information, Thompson said.

After much testing and searching DeVilbiss said they haven't found anything to lead them to believe that the spreadsheets were ever accessed on the Internet. So far, nothing shows that the other 11 files were indexed by search engines. However, the files containing the personal information of the 16 USU faculty and staff were accessed, DeVilbiss said. [...]

✦ Outsource firm sues in India

<Monty Solomon <monty@roscom.com>>

Fri, 27 Aug 2004 16:42:01 -0400

Outsource firm sues in India: Alleged Code Theft Highlights Foreign Risk
Karl Schoenberger, (San Jose) *Mercury News*, 26 Aug 2004

In a case that exposes the intellectual-property risks of outsourcing in India, a small San Carlos software company has sued Mumbai police for refusing to investigate the alleged theft of proprietary source code by an employee at its Indian subsidiary.

Sandeep Jolly, the founder and chief executive of Jolly Technologies, said U.S. technology companies should beware of the risks of doing business in his native land at a time when many are taking advantage of the cost savings of offshoring and entrusting sensitive software development and testing work

to Indian contractors. Protection of intellectual property is still a new concept for lawmakers, police and prosecutors, he said. ...

<http://www.siliconvalley.com/mld/siliconvalley/9500402.htm>

✂ Internet voting

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

Mon, 4 Oct 2004 10:18:35 +0100

Internet voting should not be considered secure until the electoral authorities are confident enough to give immunity from prosecution to anyone hacking the election, and to offer a substantial prize for anyone who can produce evidence that they have attacked it successfully.

✂ Spam that asks you to delete it

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

06 Oct 2004 20:44:34 +0200

I just got some spam from a biology company in Germany. The amusing thing is that it includes the now-popular (and legally meaningless) disclaimer:

```
> Important Note: This e-mail may contain trade secrets or privileged,  
> undisclosed or otherwise confidential information. If you have received this  
> e-mail in error, you are hereby notified that any review, copying or  
> distribution of it is strictly prohibited. Please inform us immediately and  
> destroy the original transmittal. Thank you for your cooperation.
```

So now spammers are sending us trade secrets and asking us to forget them?

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

✂ Not all buffer overflow exploits are necessarily bad

<Paul Robinson <postmaster@paul.washington.dc.us>>

Sat, 02 Oct 2004 13:18:59 -0400

There is a well-known buffer exploit for the X-Box game system. Basically it involves loading a savegame from an external storage device such as a USB key drive, the savegame overflows the font files used by the system, allowing the execution of arbitrary code and installation of an unauthorized program. (Generally programs on X-Box have to be digitally signed by Microsoft to run on the X-Box.)

The exploit is used to allow the arbitrary code to replace an item in the Dashboard of the X-Box.

And what is the "arbitrary code" and "unauthorized program"? The LINUX Operating System!

Using the game MechAssault one can modify older U.S. X-Box systems to allow Linux to be installed using a buffer overflow attack upon the font files used by the X-Box, by installing a cracked savegame from a USB keydrive. This modification only changes the software, allows the X-Box to continue to be used to play X-Box game disks, does not require opening the box or replacing any chips, and is fully reversible. The method is detailed here:

http://www.xbox-linux.org/Software_Method_HOWTO

I note that in newer X-Boxen, Microsoft HAS fixed this bug. :)

Isn't it interesting that when it is a problem for customers Microsoft can take months or be "unable" to fix exploits to their software, but when it's something that could cost them money (since someone can now purchase an inexpensive X-Box - which is sold by Microsoft as a loss-leader - and use the X-Box as a computer instead of a game console, which would mean a net loss to them) Microsoft is very quick to make fixes?

⚡ Say goodbye to broken links

<"NewsScan" <newsscan@newsscan.com>>
Mon, 27 Sep 2004 09:03:21 -0700

Interns at IBM's UK unit have developed a tool called Peridot that's designed to put an end to annoying broken links. It automatically maps and stores key features of Web pages so it can detect when the content changes. When deployed on a corporate intranet or Web site, it can then replace outdated links with the new ones. Currently, most of this work is done manually, which can result in work slowdowns or worse. Peridot's technical mentor Andrew Flagg says, "Internally, you have users who are trying to do their jobs and the intranet is there to facilitate that. If they can't get the information they cannot do their job properly. Externally, you have cases of companies that link to disreputable content which could seriously damage their reputation." Although there are similar tools that simply detect which links have been broken, Peridot's innovation is that it detects more substantial changes and has adjustable levels of autonomy, allowing staff to review changes before they're made or just allow the process to proceed on autopilot. The Peridot prototype has been tweaked so that it runs reliably over 100,000 pages, and intern James Bell predicts: "Peridot could lead to a world where there are no more broken links." The tool is named for the pale green gemstone which, according to legend, was used in ancient cultures to help people find something they had lost. [BBC News 24 Sep 2004; NewsScan Daily, 27 Sep 2004]

<http://news.bbc.co.uk/2/hi/technology/3666660.stm>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 57

Monday 25 October 2004

Contents

- [Nonexistent URL in comic strip leads to pornocopia](#)
[Conrad Heiney](#)
- [Fictional, but far too plausible](#)
[Paul Robinson](#)
- [Critical infrastructure cybersecurity risks](#)
[PGN](#)
- [South Korea vulnerable to cyber attacks from North](#)
[NewsScan](#)
- [Maryland Motor Vehicle Admin disabled](#)
[Pete Carah](#)
- [Cybersecurity largely ignored by individual users](#)
[NewsScan](#)
- [Tourist concerns: war, terrorism, computer problems](#)
[David Magda](#)
- [TV emits international distress signal](#)
[Mike Hogsett](#)
- [Is Windows up to snuff for running our world?](#)
[Richard M. Smith](#)
- [Of mice, snakes, and wiring](#)
[Brian Clapper](#)

- [Descent from privacy: a 'slippery slope'](#)
[NewsScan](#)
 - [A LAME PHISHING ATTEMPT: Please confirm your account](#)
[F.J. Reinke](#)
 - [Do vendors read their own security policies?](#)
[Vassilis Prevelakis](#)
 - [World Bank Technology Risk Checklist](#)
[Gideon T. Rasmussen](#)
 - [What the world needs is more lawyer-bots](#)
[NewsScan](#)
 - [Pre-election hanky-panky in Ohio](#)
[PGN](#)
 - [Re: Internet voting](#)
[Ray Todd Stevens](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ **Nonexistent URL in comic strip leads to pornocopia**

<Conrad Heiney <conrad@fringehead.org>>

Fri, 22 Oct 2004 09:06:45 -0700

"Regret the Error", a weblog that tracks media retractions, reports that a comic strip included a link to a nonexistent URL. Shortly after the strip hit the streets, the URL sprang to life, returning questionable content.

The risk of underestimating the Internet's reaction speed, plus a poor understanding of what an URL is, results in a media disaster similar to the Vice President's factcheck.com/org error recently. This reminds me of the dot-com days when marketers would print up thousands of glossy brochures with a vaporous address on them and then ask for the address to

exist as
they were handing them out at a trade show.

url: http://www.regrettheerror.com/2004/10/comic_porn.html

Conrad Heiney conrad@fringehead.org <http://www.contentgoeshere.com/>

✶ Fictional, but far too plausible

<Paul Robinson <postmaster@paul.washington.dc.us>>

Sat, 23 Oct 2004 00:40:13 GMT

Today on one of the satellite channels I saw an episode of the TV show 'JAG' in which a sailor in charge of a sophisticated command and control system for a battleship was murdered in Japan, in order to cause his replacement to be brought on, who was a long-term infiltrated double agent for North Korea.

Now, personally I would hope that most of the things the show claimed were possible were dramatic license, but with the published and publicly known use of Microsoft Windows in some military systems it implies that ordinary programs could be inserted into operating weaponry and/or ordnance.

In the story, the agent had inserted rogue code into the software for the ship's command, control and operational hardware. Initially a system test designed to perform simulated targeting activates live missiles that shoot down two aircraft (fortunately after the pilots are able to

eject.)

The new code essentially disables every weapons system and propulsion control, without capability of override, until it starts up a pre-programmed scheduled event: to sail the warship into North Korea, which would allow their military to obtain all of the technology on the ship, including the advanced control system.

The show points out that in an attempt to stop the system, a backdoor was attempted to be accessed - for use in just such an emergency - but it had been eliminated by the agent.

What I also noted about the system that they mentioned sounded plausible, and perhaps it is appropriate in view of the fact this is a warship (although having any system without an 'off' switch is a bad idea, in my opinion), but the thought is frightening if true. It stated that there is no means to disable the system to make it shut down dead; in the event of disconnect it stays in the last state it was in, which in the case of the ship would be in live fire mode, in which it would continue to target all aircraft or flying objects approaching the ship.

Again I wish to stress that I do understand it was a work of fiction and some of what is being stated may not be correct or is just dramatic license, but it still sounds reasonable as a potential way in which such systems might be designed and as such it is something we should be aware of.

More than two generations ago the book and movie 'Fail Safe' warned of the disastrous consequences of military systems designed such that they would lock down in a non-disable-able mode. If the examples given by this TV program are in any way even close to accurate it seems to indicate that not much has changed.

On a side note, with so many countries becoming democratic - or at least, somewhat less totalitarian - I suspect it's probably becoming harder and harder to find believable foreign enemies for TV shows and movies. We've lost Russia, East Germany and South Africa over the last twenty years, plus Iraq and Afghanistan in the last five, so basically there aren't a whole lot of believable bad-guy countries in the world left. I figure that won't last long, the U.S. Government will find some new country to target as the 'enemy of the month' or whatever period of time they need to distract the public.
:)

✶ Critical infrastructure cybersecurity risks

<"Peter G. Neumann" <neumann@csl.sri.com>>
Mon, 11 Oct 2004 12:09:07 PDT

[Source: Canada NewsWire, 9 Oct 2004; PGN-ed, starkly excerpted]

British Columbia Institute of Technology cyber security research leader Eric Byres testified for the U.S. Congressional Subcommittee on Technology,

Information Policy, Intergovernmental Relations and the Census in Washington D.C. on 1 Oct 2004, warning that hacker attacks on North America's critical industrial infrastructure [power, etc., and of course the information technology on which they all depend] could soon become as commonplace as the practice of hacking Web pages. Particularly vulnerable are the Supervisory Control and Data Acquisition (SCADA) systems used ubiquitously for operation and maintenance. They efficiently enable the collection and analysis of data and control of equipment from remote locations.

There is a growing concern that this reliance on computers and computer networks raises the vulnerability of critical infrastructures to attack by cyber terrorists. A recent National Research Council report has identified "the potential for attack on control systems" as requiring "urgent attention."

In May, a researcher at a British conference showed how by remotely adjusting overload settings on a grid's power transformers during the warm summer months, it is possible to destroy millions of dollars of equipment and shut the grid for days.

As early as 1997, a six-month vulnerability assessment by the White House's National Security Telecommunications Advisory Committee found basic security flaws in the computerized systems that control generators, switching stations and electrical substations. Among other things, the committee reported that operational networks controlling critical portions

of the grid were accessible through electric companies' corporate LANs (local area networks). Some digital circuit breakers could be remotely tripped by anyone with the right phone number. Fixed passwords for remote vendor access went unchanged for years. Not enough has changed since then, Byres notes. While getting into a critical control system might not be easy, it is certainly not impossible. Said Byres, "As we like to say in the lab, 'crunchy on the outside, soft on the inside.'"

[Canadian and British media seem to be more interested in these problems than U.S. media. My Website includes Senate and House testimonies on this subject from 1996 and 1997, but those and other warnings and recommendations seem to be largely ignored by the U.S. authorities. PGN]

South Korea vulnerable to cyber attacks from North

<"NewsScan" <newsscan@newsscan.com>>

Tue, 05 Oct 2004 10:50:03 -0700

South Korea's defense ministry says that North Korea has trained hundreds of computer hackers who could launch a cyber-war on South Korea, the US or Japan. Because South Korea has the world's highest usage of broadband services yet maintains relatively low levels of Internet security, the country is especially vulnerable to network attacks.

[*Financial Times*,
4 Oct 2004; NewsScan Daily, 5 Oct 2004]

<http://news.ft.com/cms/s/3d592eb4-15f0-11d9-b835-00000e2511c8.html>

✶ Maryland Motor Vehicle Admin disabled

<Pete Carah <pete@altadena.net>>

Thu, 14 Oct 2004 13:44:31 -0700

[Re: Virus disables Colorado DMV for nearly a week]

Within a day or so of the initial appearance of Blaster in Aug 2003, the Maryland MVA (Motor Vehicle Administration, DMV equivalent) was totally disabled (statewide) for most of a week.

I saw no explanation in the local papers of how it got inside the security perimeter but in the networks I admin'd at the time it mostly got in via carried laptops. (or, maybe Blaster had a mail variant, though I thought it didn't, or maybe the firewall wasn't good enough, or....) (for those who don't know, Blaster and its successor Nachi (or Welchia) were direct-transmission worms that attacked the NT DCOM software. As usual, MS had released a patch for at least part of the buffer-overflow in question before the worms appeared in the wild, but it was not widely applied.) In the risks list at the time, someone noted that a very easy vector for these worms was a laptop on a hotel (or other open) network using a VPN to connect in to the internal network.

Of course, trying to apply the removal tool and patch online

were usually
fruitless since the reinfection rate was faster than the time it
took to
download the patch... This led on my networks, to everyone in
the support
group madly running around the campus with CDs doing clean
+patch...

And MS finally got the message with XP SP2 that the software
firewall should
default to ON, only years late, and I don't know if they do this
yet in Win
2K or Server 2003 (or do those even ship with an internal
firewall?)

🔥 Cybersecurity largely ignored by individual users

<"NewsScan" <newsscan@newsscan.com>>

Mon, 25 Oct 2004 08:01:44 -0700

A new study by America Online and the National Cyber Security
Alliance
indicates that about 80% of home PCs are infected with spyware,
but most
users aren't even aware of it. And while 85% of users had
installed
antivirus software, two-thirds of those had not updated it in
the past
week. In addition, about 20% had an active virus on their
machines and
two-thirds did not have a firewall installed. AOL chief trust
officer
Tatiana Gau says the results highlight just how vulnerable the
average
online user is to malicious hackers. "No consumer would walk
down the street
waving a stack of cash or leave their wallet sitting in a public
place, but
far too many are doing the exact same thing online. Without basic

protections like antivirus, spyware and firewall software, consumers are leaving their personal and financial information at risk." [CNet News.com, 24 Oct 2004; NewsScan Daily, 25 Oct 2004]

http://news.com.com/Plague+carriers+Most+users+unaware+of+PC+infections/2100-1029_3-5423306.html

✶ Tourist concerns: war, terrorism, computer problems

<David Magda <dmagda@ee.ryerson.ca>>

Tue, 12 Oct 2004 21:36:47 -0400

I was looked at perhaps taking a package tour. I ran across a site that had some interesting options and decided to read the terms & conditions. One sentence stuck out:

> Additionally, responsibility is not accepted for losses or expenses due to
> sickness, lack of appropriate medical facilities or practitioners,
> weather, strikes, theft or other criminal acts, war, terrorism, computer
> problems, or other such causes.

http://www.historytelevision.ca/travel/containers/terms_conditions.asp

I found it amusing that computer problems were listed right beside war and terrorism. Was someone bitten by this issue and thus decided to do a CYA, or are people becoming more aware the complexity of digital systems?

⚡ TV emits international distress signal

<Mike Hogsett <michael.hogsett@sri.com>>

Tue, 19 Oct 2004 09:36:04 -0700

An Oregon man discovered earlier this month that his year-old Toshiba Corporation flat-screen TV was emitting an international distress signal picked up by a satellite, leading a search and rescue operation to his apartment in Corvallis, Oregon, 70 miles south of Portland. More in the article:

<http://www.cnn.com/2004/SHOWBIZ/TV/10/18/odd.television.reut/index.html>

⚡ Is Windows up to snuff for running our world?

<"Richard M. Smith" <rms@computerbytesman.com>>

Sat, 23 Oct 2004 10:27:56 -0400

[RMS also contributed this to bugtraq. PGN]

The Microsoft Windows operating system is increasingly being used in devices which run our world. Some examples include cash registers, ATMs, electronic voting machines, and factory control computers. But is the Windows operating system really reliable and secure enough for these kinds of applications? A small incidence at the Atlanta airport last May makes me wonder.

I was flying home to Boston from Atlanta on Delta Airlines. When I got to my gate at the Atlanta airport, I immediately noticed that there was a Windows error alert box in the middle of the large display screen over the gate door. I walked around the terminal and saw that many of the gate display units had the same error alert box being displayed. In many cases, the display units were no longer usable since the alert boxes covered up critical information on the screens.

Here are some photos I took of the problem:

<http://www.ComputerBytesMan.com/atlanta>

The problem existed for at least 30 minutes, but no one from Delta seemed to be interested in fixing it. I wanted to click the "Okay" button myself, but I couldn't find a mouse. ;-)

I even recognized the software package that was failing at the Delta terminal. It is a customer support package that a number of computer makers ship with their home PC systems. This same software package was pre-installed on my Sony laptop but I removed it after discovering that it contained a number of ActiveX controls with serious security holes. These security holes can potentially be used by a virus writer to take over a Windows PC using simple script code.

The customer support software was failing because it couldn't find a standard Microsoft ActiveX control which ships with Windows. My impression is that the Windows operating system in control of a display unit had

somehow been corrupted. Ironically this customer support package is designed to diagnose and fix these kinds of problems with home PCs. Why Delta was running consumer-grade PCs for this application is bit hard for me to fathom.

I sure that this is not the first time a Windows system has failed in a dedicated application. If you have any interesting photos of similar Windows failures, please send them along to rms@computerbytesman.com.

Richard M. Smith <http://www.ComputerBytesMan.com>

Links

Microsoft server crash nearly causes 800-plane pile-up
<http://www.techworld.com/opsys/news/index.cfm?NewsID=2275>

Car crazy: Microsoft in the driver's seat
<http://tinyurl.com/6s24a>

ATMs in peril from computer worms?
http://www.theregister.co.uk/2004/10/20/atm_viral_peril/

Shifting cyber threats menace factory floors
<http://www.securityfocus.com/news/9671>

Software vendors just don't "get" ActiveX security
<http://archives.neohapsis.com/archives/fulldisclosure/2003-q3/0043.html>

⚡ Of mice, snakes, and wiring

<Brian Clapper <bmc@clapper.org>>
Fri, 22 Oct 2004 11:04:58 -0400

Here's a slight twist on an old RISKS favorite.

For the last couple weeks, We've been experiencing intermittent DSL

"drop-outs", for thirty seconds at a time, a few times a day.

The light on

the modem would start blinking, and the Internet connection would become

unresponsive. Then, shortly thereafter, the modem would "find" the signal

again, and everything would come back. This is an unusual situation for us.

In the almost five years we've had ADSL, it has rarely gone out for any

appreciable amount of time.

I initially figured the DSL problems were transient--someone working at the

C.O., or something. But then, a few days ago, the home phone line (which

carries the the DSL signal) started having some audible static, sometimes

bad enough to make it nearly impossible to hear. I plugged a phone into the

jack at the network interface box, and I heard the static there, too. At

that point, I figured it was time to call Verizon.

Verizon sent someone out this morning. The woman who came out to check the

wiring found that the pedestal down the street--where all the phone lines

on the street connect--had become a shelter for mice, and the mice had

chewed through some of the wires, including ours. The inevitable corrosion

was having predictable effects on the electrical signals.

The woman told me that sometimes, when she goes to service larger boxes

that handle hundreds of phone lines for an entire community,

she'll find
that those boxes have also become infested with mice. At that
point, she
made a face, and said, "It's pretty disgusting." But then, she
said, it
gets worse, because the snakes come along. (Free mouse buffet!
Come and get
it!) After telling me that, she made a another face, and said,
"Y'know, I'm
not especially fond of snakes."

Brian Clapper, <http://www.clapper.org/bmc/>

✶ Descent from privacy: a 'slippery slope'

<"NewsScan" <newsscan@newsscan.com>>

Fri, 22 Oct 2004 08:13:23 -0700

Pam Dixon, executive director of the World Privacy Forum, warns:
"Most
consumers don't fully understand the tradeoffs they're making
with privacy."
As an example, she argues that the potential widespread use of
the VeriChip
-- a tiny radio transmitter inserted under a person's skin -- is
"a
nightmare situation" for privacy, because at first workers might
be induced
to wear the devices simply to get high-security jobs but that
eventually the
transmitters would be much more broadly required: "All of a
sudden it
becomes mandatory for certain classes of people. I just see this
as an
extremely slippery slope." [**Christian Science Monitor**, 21 Oct
2004;

NewsScan Daily, 22 October 2004]

<http://www.christiansciencemonitor.com/2004/1021/p13s01-stct.>

[html](#)

⚡ A LAME PHISHING ATTEMPT: Please confirm your account

<"reinke, f. j. \ (Yahoo)" <reinkefj@yahoo.com>>

Fri, 22 Oct 2004 12:23:10 -0400

[This might have worked (not very likely) if I even had an account at Citibank. It's tiring to see these. The fact that this lame attempt might even work is really frustrating to this security pro. John]

-----Original Message-----

>From: Citibank [mailto:rosend@sullcrom.com]

Sent: Thursday, October 21, 2004 5:08 PM

To: John

Subject: Please confirm your account

<<http://218.4.196.49/signin/citifi/scripts/login2/header.gif>>

Dear valued Citibank member,

Due to concerns, for the safety and integrity of the online banking community we have issued the following warning message.

It has come to our attention that your account information needs to be confirmed due to inactive customers, fraud and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to confirm your records may result in your account suspension.

Once you have confirmed your account records your Internet banking service will not be interrupted and will continue as normal.

Please click here

<<http://218.4.196.49/signin/citifi/scripts/login2/index.html>> to confirm your bank account records.

Thank you for your time,
Citibank Billing Department.

<http://218.4.196.49/signin/citifi/scripts/login2/citi_lsm.gif>
Citibank.com <<http://www.citibank.com>>
<http://218.4.196.49/signin/citifi/scripts/login2/mem_citi.gif>
Citigroup <<http://www.citibank.com/privacy/promise.htm>> Privacy
Promise
Terms, <<http://www.citibank.com/citibank/disclaim.htm>>
conditions,
caveats and small print
Copyright C 2004, Citicorp

⚡ Do vendors read their own security policies?

<Vassilis Prevelakis <vp@cs.drexel.edu>>
Fri, 22 Oct 2004 00:18:01 -0400 (EDT)

Now everybody is "committed to security", with almost every site giving security advice. But do these people ever bother to read their own security policies or to ensure that their procedures are compatible even with common-sense security policies.

Two examples:

1) Paypal

In their "Security Center" web page

(https://www.paypal.com/cgi-bin/webscr?cmd=_security-center-outside)

PayPal advises (in big letters next to a "hazard" icon):

Avoid Fake Websites

Log in safely to your account. Open a new web browser (e.g., Internet

Explorer or Netscape) and type in the following: <https://www.paypal.com/>

So far so good, but why do they also advice customers to

This recipient only accepts PayPal payments through their website. To make

this payment, please go to <http://www.auctionworks.com/pay.asp>

This web site encourages users to fill-in their order details and then jumps

to the paypal web site so that the customer can log on and authorize the payment.

THIS IS EXACTLY THE MO USED BY TRICKSTERS, because the user cannot verify the URL used to perform the redirection.

2) Roxio

I really like this message:

If you are having trouble downloading, disable any firewalls such as Personal Firewall(TM) or Gauntlet(TM) and disable any download managers such as RealDownload(TM) or GetRight(TM).

Vassilis Prevelakis, Computer Science Dept, Drexel University, Philadelphia, PA

World Bank Technology Risk Checklist

<"Gideon T. Rasmussen" <lists@infostruct.net>>

Mon, 25 Oct 2004 16:56:16 -0400

"The World Bank Technology Risk Checklist is designed to provide Chief

Information Security Officers (CISO), Chief Technology Officers (CTO), Chief

Financial Officers (CFO), Directors, Risk Managers and Systems Administrators with a way of measuring and validating the level of security

within a particular organization."

<http://www.infragard.net/library/pdfs/technologyrisklist.pdf> (31 pages)

⚡ What the world needs is more lawyer-bots

<"NewsScan" <newsscan@newsscan.com>>

Wed, 13 Oct 2004 11:01:15 -0700

Mark Rasch, founder and former head of the U.S. Justice Department's

computer crimes unit, says that the increasing trend toward lengthy,

tiny-font policy "agreements" that users must click on before they can

access a Web site are generating the need for more legal oversight.

"Increasingly, companies have been putting some pretty nasty things into

their clickwrap agreements -- such as that they can collect and sell your

detailed personal information or install software that will capture your

every keystroke This is not legal boilerplate, the kind that everybody orney

general's assents to when renting a car or buying a ticket to a

ball

game. It affects the privacy, security, and operability of all of the information you access online." Rasch says what's desperately needed is a law robot -- "a browser-based automaton that could be adjusted to match your tolerance for legal mumbo-jumbo. Once you establish privacy settings, your browser would > transfer personal data (after prompting you) only to sites that conform with your privacy requirements." Rasch says such technology would go a long way toward eradicating such online nuisances as porn spam and spyware. "We will never fully automate the reading of contracts or agreements online. Nor would we want to -- after all, Internet lawyers need jobs, too. But by automating the vetting of clickwraps or implied agreements we could make everybody sleep a little easier." [Wired.com, Oct 2004;

NewsScan Daily, 13 Oct 2004]

<http://www.wired.com/wired/archive/12.10/view.html?pg=2>

Pre-election hanky-panky in Ohio

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

Sat, 23 Oct 2004 14:56:25 PDT

1. Columbus voters report fake elections board calls

Completely bogus phone calls claiming to be from the Franklin County Board of Elections have been received by voters, informing them that their polling place had been changed from one precinct to another.

[Source: Suzanne Hoholik, Voters report fake calls: Instructions to change polling place don't come from board of elections *The Columbus Dispatch*, 22 Oct 2004; PGN-ed]

<http://www.dispatch.com/election/election-local.php?story=dispatch/2004/10/22/20041022-A1-00.html>

2. Thieves steal campaign computers with sensitive information

Thieves broke in to Lucas County Democratic headquarters in Toledo, Ohio, stealing computers with sensitive campaign information -- including e-mail messages on campaign strategy, candidates' schedules, financial information, and phone numbers of party members, candidates, donors, and volunteers.

[Source: Robin Erb, Thieves hit Democratic Party offices; computers containing sensitive data removed; PGN-ed]

<http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20041013/NEWS03/410130378>

✶ Re: Internet voting (Thomas, [RISKS-23.56](#))

<"Ray Todd Stevens" <raytodd@kiva.net>>

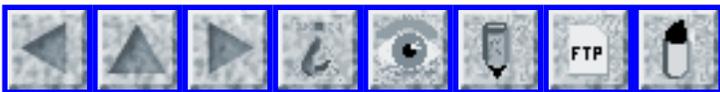
Wed, 13 Oct 2004 09:36:57 -5

I don't know I would go this far, on the other hand I would go farther.
Companies and governments wanting to implement Internet voting should be required to first publish all the information that hackers over time could acquire about the system, and then setup several test elections. You know vote for you favorite disney character, vote for your favorite

ice cream
flavor, etc. All attempts to hack these elections should be
encouraged, and
there should be a big prize for doing it. Once it goes live I
am a little
iffy on allowing hacking. How do you tell the difference
between someone
hacking to get the prize and who will immediately admit their
activities,
and one who is going to secretly hack the election and allow
phony results
to stand?. How about the problem of denial of service? This
had already
been an issue with regard to some electronic voting.

Maybe there should have to be a test election just before and
just after
every real election where hacking is permitted, and rewarded.
In fact maybe
all electronic voting systems should be subject to this form of
"audit".
There should be someone you can go and try to break the system.
But it should never be during a real election.

[I continue to be amazed that folks persist on focusing only
on the risks
of penetrations by outsiders. Insiders are by far the
greatest concern
here. PGN]



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 58

Thurs 4 November 2004

Contents

- [Some thoughts on the 2004 U.S. election process](#)
[PGN](#)
- [Touchscreen voting spawns glitches](#)
[NewsScan](#)
- [Preferential voting software breaks down in San Francisco](#)
[PGN](#)
- [Clocks set back a week too early](#)
[Dave Stringer-Calvert](#)
- [Nuclear Regulatory Commission lab info on Web](#)
[Dave Brunberg](#)
- [Battlefield Robotics are risk to the world public](#)
[Edward G. Nilges](#)
- [Spyware epidemic threatens to stall computer industry](#)
[NewsScan](#)
- [Swedish Hospital forces persons to change names](#)
[Peter H](#)
- [Election candidates' web pages hacked during Finnish election](#)
[Erka Koivunen](#)
- [Re: Internet voting](#)
[Hamilton Richards](#)

- [Address-form glitch proves an easy scam](#)
[Gabe Goldberg](#)
 - [Re: TV emits international distress signal](#)
[Steve Summit](#)
 - [Re: Is Windows up to snuff for running our world?](#)
[Atom 'Smasher'](#)
 - [Re: Do vendors read their own security policies?](#)
[jmeissen](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ **Some thoughts on the 2004 U.S. election process**

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

Wed, 3 Nov 2004 18:21:20 PST

It is important to recognize that the election process is a long and arduous one in which Election Day is just one highly visible manifestation. The integrity of our elections depends on almost every step along the way. That obviously includes the actual casting of ballots and the creation, evaluation, certification, testing, and maintenance of voting equipment. But it also includes the registration of voters; identification, authentication, and challenging of voters; creation of the actual appearance of ballots and setting up the voting machines; distribution and handling of ballot and polling-place information, absentee ballots, and especially provisional ballots; processing of ballots; tabulation and collection of results; and proper assurance that voters' ballots are treated with adequate respect for privacy -- along with oversight of each of the steps in the

entire process.

Historically, many past elections have encountered serious anomalies. (See my Illustrative Risks document, <http://www.csl.sri.com/neumann/illustrative.html> and click on Election

Problems; that summary of RISKS cases will eventually be upgraded to include the most relevant of a large number of reported November 2004 anomalies.)

Yesterday's election reminds us once again that each of the steps in the overall election process represents various potential weak links with

respect to security, system integrity, accountability, recountability, privacy -- and, indeed, the democratic process. For example, some exit

polls differed rather substantially from the actual results in some states.

However, in the absence of meaningful audit trails, it is impossible to determine definitively whether this was the result of a lack of integrity

and accuracy in the exit polls or in the election systems themselves; a

voter's intent remains unknown in the absence of voter-verified audit trails

when using unauditible machines. On the other hand, having to believe in

exit polls to evaluate whether the unauditible electronic machines were

accurate and noncompromised is also a ludicrous proposition.

When everything comes down to one state -- in it did again this year -- we

are left with unanswered and indeed unanswerable questions about the

integrity of the unauditible all-electronic machines in Ohio.

Among other

vendors, Diebold is known for numerous transgressions. We have previously

noted here that in California in 2002, the software that was used by Diebold in 17 counties was not the software that had been certified; the actual versions in use were different. In Georgia in 2002, Diebold's had unmonitored dedicated lines into computer systems during the election process (in case it was necessary to fix (!) problems). (This is also true of other vendors, and is apparently used to download software upgrades and offload results.) In Ohio in 2003, Diebold's CEO Wally O'Dell wrote to would-be contributors that he is "committed to helping Ohio deliver its electoral votes to the President next year." Overall, the use of unauditable machines is of particular concern when it is impossible to determine the presence of bad software, human error, and intentional fraud -- unless the anomalies are totally egregious, as in the case in Boone County, Indiana, of 144,000 votes being recorded when only 5,352 people had voted ([RISKS-23.03](#)) or where -16,022 votes were reported in Volusia County, Florida ([RISKS-22,93,94](#)). Of course, other voting machine companies are also involved in many other irregularities, so Diebold is not the only source of problems.

Returning to the notion that the voting problem is a total-system problem, here are a few more issues.

* The federal election standards are inherently incomplete and extremely weak. This is true of the 2002 standards that replaced the 1990 standards, although most of the current systems were evaluated against

the even weaker old standards.

- * The evaluation process is normally secret, and funded by the voting machine purveyors themselves -- some of whose employees have felony conviction records or otherwise questionable backgrounds.
- * Many state election officials are overtly partisan, some also serving in party positions (as in Ohio).
- * The National Institute of Standards and Technology is supposed to be involved in setting standards, but its funding is grossly inadequate for this task.
- * The U.S. Election Assistance Commission has also been seriously shortchanged in its funding.
- * Legislation cannot reflect all of the possible things that can go wrong, but it is absolutely essential that nonpartisan actions and guidelines be as carefully and proactively constructed as possible.
- * In the 2004 national election, it is already clear that numerous irregularities have occurred leading up to and during the election (including a variety of what might be called "dirty tricks"), some of which even appear to have been illegal. For example, numerous efforts to disenfranchise or harass legitimate new voters were reported in various states. Further complicating the need for a level playing field, there were many reports of long lines -- with some voters having to wait two hours or four hours to vote, and even a few who had to wait for 9.5 hours!

The fact that some voters persevered despite such discouraging circumstances is truly amazing.

* There were also reports from New Orleans that all of the Sequoia machines throughout the city had failed (for example, could not be booted up), and that there were inadequate paper backups.

* Training of precinct workers is also a significant problem under confusing conditions, as was misinformation and a lack of standards regarding provisional ballots mandated by the Help America Vote Act.

* The Election Incident Reporting System (<https://voteprotect.org>) is currently showing 29007 reported incidents (many of which were relatively minor, but the total of which suggests some real problems), with Pennsylvania, Florida, California, New York, and Ohio leading the pack in that order.

And I feel as if I have only scraped a little off the top of the iceberg.

Correcting all of these and other problems is not an easy task, and requires objective approaches. But the primary lesson from this election --

irrespective of the eventual outcome -- is that we still urgently need meaningful election reforms. It is not too early to do this for the future.

🔥 Touchscreen voting spawns glitches

<"NewsScan" <newsscan@newsscan.com>>

Wed, 03 Nov 2004 09:52:25 -0700

U.S. voters across the country reported some 1,100 problems with e-voting machines, bearing out scientists' concerns that touchscreen machines are prone to tampering and unreliable unless they're equipped to print out paper records for recounts. Some problems were blamed on factors as mundane as power outages and incompetent poll workers, but there were a number of voters in six states -- especially Democrats in Florida -- who said that although they voted for John Kerry, when the computer asked them to verify their choice, it indicated that they had voted for President Bush. One voter in Clearwater reported that it took her about 10 tries and a quick touchscreen clean-up with a wet-wipe towel before she could successfully select Kerry. A spokesperson for Sequoia Voting Systems said the machines' monitors may need to be recalibrated periodically to ensure the touchscreen is sensitive enough to record users' votes. [AP/CNN.com 3 Nov 2004;

NewsScan Daily, 3 Nov 2004]

<http://www.cnn.com/2004/TECH/11/03/electronic.voting.ap/index.html>

⚡ Preferential voting software breaks down in San Francisco

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

Thu, 4 Nov 2004 10:07:12 PST

In the election of 2 Nov 2004, San Francisco's district supervisor election used ranked-choice voting for the first time. It went just fine on Tuesday during the election. Preliminary results showed candidates in three districts had won by a majority (so no reranking is needed), whereas the other four seats remained to be determined by the preferential ballot counting process. However, the computer processing broke down completely on Wednesday afternoon when election workers began to merge the first, second, and third choices into the program that is supposed to sequentially eliminate low-vote candidates and redistribute voters' second and third choices accordingly. However, no San Francisco ballots were lost, because each ballot has a paper trail.

The software is provided by ES&S (Election Systems and Software, in Omaha). This system has undergone federal and state testing, as well as pre-election testing in which everything seemed to work perfectly. [No surprise to RISKS readers there.] The results of four contested supervisors' races are expected to be delayed up to two weeks. [Source: Suzanne Herel, *San Francisco Chronicle*, 4 Nov 2004, front page continued on A7; PGN-ed]

⚡ Clocks set back a week too early

<Dave Stringer-Calvert <david.stringer-calvert@sri.com>>

Thu, 28 Oct 2004 19:20:13 -0700

Brussels has been "blamed" for bringing winter a week early to parts of the country. About 2,000 clocks on public buildings and railway stations across the UK have gone back an hour seven days too soon. An EU directive dictating clocks should change on the last Sunday of October has been blamed by clock makers. Traditionally, clocks changed on the fourth Sunday of October and most were pre-programmed to do so. There are five Sundays in October this year. [...] [Source: BBC News]

⚡ Nuclear Regulatory Commission lab info on Web

<"Dave Brunberg" <DBrunber@FBLEOPOLD.com>>

Wed, 20 Oct 2004 08:46:35 -0400

Today's cnn.com (<http://www.cnn.com/2004/US/10/19/terror.nrc/index.html>) has a story on floor plans, chemical lists, and other "sensitive" data on licensed nuclear facilities in the U.S. being made available through the Nuclear Regulatory Commission's web site.

The article discusses what types of information are available, and how it may be useful to terrorists planning attacks against such facilities, or raids to obtain radioactive material. Interestingly enough, little is said about why the information was up in the first place. The reason is likely regulations requiring disclosure of hazardous substances and publication of

floor plans for use in fire/rescue training and other safety-related regulations.

While most of us can agree that security through obscurity is a dead end, the article's author seems mildly outraged and disbelieving that such information would ever be publicly available.

However, it's nice to know that some people who are discussing physical security understand the failures of security through obscurity: Money quote:

"It [the Web site] may help a little, but if someone's determined to do this, it won't help them much. If someone wanted to find this out, they can," said David Albright of the Institute for Science and International Security.

"If secrecy is your only security, then you don't have it. Because everybody that has a brain knows that physics departments use radioactive sources ... and it's not that hard to find where they are," he said.

It's always a delicate balance, when you have to weigh government secrecy against the public right to know what's going on in their government. In my mind, it's better to err on the side of public knowledge, while implementing true security measures. The alternative is to try to hide everything and then have to explain to a few thousand people why their loved ones died in an attack that could have been prevented by a security policy driven by the assumption that the enemy can find out whatever they need. The

latter takes
more work, but it's more honest and more reliable.

David W. Brunberg, Engineering Supervisor, The F.B. Leopold
Company, Inc.

✶ Battlefield Robotics are risk to the world public

<spinoza111@yahoo.com (Edward G. Nilges)>
25 Oct 2004 21:03:51 -0700

http://news.yahoo.com/news?tmpl=story&u=/ap/20041025/ap_on_bi_ge/battle_ready_robot

No consideration appears to be given here by the John Deere
corporation
(engaged enthusiastically in beating plowshares into high-tech
swords) that
battlefield robots may represent the existing hazards of land
mines to
children and others...raised to a power.

Dazzled by the glitter of the hardware and the apparent
perfection of the
software in the showroom, we seem to systematically forget what
happens to
old systems of this nature.

The unusable laptop, that boots up to a Blue Screen of Death and
is too
expensive to repair, becomes closet clutter as does the desktop
outdated by
the next big thing.

But what happens to military hardware, as is evident from the
known problem
of unexploded ordnance (still a problem in northern France,
almost a century

after the First World War), is much more serious.

It becomes an attractive nuisance for children growing up in former battlegrounds.

A partially functional, unmanned and unaccounted for battlefield robot will attract children, but since it is logically impossible to program these pernicious things with Asimov's First Law (see below), its partially corrupted software (corrupted by low power and environmental stress causing memory losses, for example) may well interpret the random actions of children as a threat...especially when the children play "war", as children tend to do in real war zones.

Boom...and, as usual, nobody is responsible: the great good John Deere corporation has moved on.

It is logically impossible to program these things with Asimov's First Law, which was never to harm a human being. That's because their whole purpose is to harm human beings.

Software people make mistakes, called bugs, all the time. Perhaps this inures them to not admitting what may be The Grand Fallacy of software.

This is that one is not morally accountable for all phenomena of the software system one has fabricated, including "unexpected" phenomena. Of course, an early lesson, learned and taught by hero computer scientist Dijkstra, was that one was indeed responsible for outlier conditions.

We have been told that cruise missiles are pinpoint accurate even though they have destroyed innocent lives. The destruction is explained away as unusual combinations of circumstances or operators who in the heat of battle misprogram the final parameters.

Trivially, there is no boundary between field modification of parameters, whether of a cruise missile on board a naval vessel or behind the lines.

More important, it can be concluded that the seriousness of a final result (a child's life destroyed) when considered as a number makes the final ratio of our "input" to the magnitude of the crime something which has to be taken into account.

Of course, for this reason, many software and hardware engineers simply avoid defense work. But one hopes that the military types write all their own goddamn software all the way down so that Open Source coders are not indirectly responsible.

There is some fantasy that if we put enough steps between our actions and a final result, the amplitude of the moral signal, the level of our guilt, is attenuated and not amplified into a cry to heaven.

But September 11 may have brought home to many Americans that other people do not feel the same way. Other people, if we implement battlefield robotics and after the battle they are running amuck, will ask us why we constructed such cowardly and unnecessary devices.

🔥 Spyware epidemic threatens to stall computer industry

<"NewsScan" <newsscan@newsscan.com>>

Mon, 01 Nov 2004 10:08:46 -0700

Computer makers say that their technical support lines are lit up by consumers frustrated over sluggish performance and increasingly they're tracing the problems back to one culprit: spyware. Companies are concerned about the cost of the calls, but they're even more worried that that customers will wrongly blame them for performance deficiencies. Russ Cooper, senior scientist with TruSecure Corp., says now that spyware has become epidemic, it's time for Microsoft and other technology companies to launch a public education campaign along the lines of the old "Only *you* can prevent forest fires" concept. The industry's incentive is pure survival, says Cooper. Microsoft officials blame rogue software for up to a third of applications crashes on Windows XP computers and AOL estimates that just three such programs together cause about 300,000 Internet disconnections per day. Forrester Research analyst Jonathan Penn says spyware-related customer support can cost \$15 to \$45 per phone call, but it's worth it. "Security is a component of loyalty. People, they want all these various services, but they expect security to come with it." [AP, 31 Oct 2004; NewsScan Daily, 1 Nov 2004]

<http://apnews.excite.com/article/20041031/D862JARG0.html>

✶ Swedish Hospital forces persons to change names

<Peter H <prisk@ipsec.se>>

Fri, 29 Oct 2004 20:27:52 +0200 (CEST)

Swedish hospital forces users to change their officially registered name!

According to an article in "Computer Sweden" (29 oct 2004) the users at karolinska university hospital have adopted a rigorous naming-scheme, that uses **only** a person's name with spelling and order as existing in official population register. Bad, you think? Well it is even worse; many people has several given names, among which most persons pick one and use it for everyday life. But this hospital's administrators refuse to use the chosen name, instead insisting on using the first given name + surname as e-mail address.

Reason? "It's about making sure it's the right person logging in and it's also important with law and order."

For those unhappy souls not recognizing their names, the IT department has ready-made forms for changing the official population register (which costs money in sweden, something the unhappy souls is not reimbursed for).

The article does not mention that some persons still has to use

other

combinations, there is two cases where the "dream-scheme" does not work (not even in sweden):

(1) for the duplicates (or do they refuse employment for these??)

(2) for the persons christened to names containing non-ascii characters.

Orwell, you are way behind !

✶ Election candidates' web pages hacked during Finnish election

<"Erka Koivunen" <Erka.Koivunen@iki.fi>>

Thu, 28 Oct 2004 09:07:55 +0300

The web pages of two candidates from the Finnish National Coalition Party were hacked last Thursday, just three days before the Finnish municipal elections. The pages were a part of a public service provided by Finnish Broadcasting Company YLE. The candidates were supposed to type in their answers along with opinions for predefined multiple-choice questions. In turn, the citizens could compare the candidates' answers against their own preferences. The service has grown to be quite popular during the latest Finnish elections - at least I found my candidate by using the service!

According to YLE's project manager Erkki Vihtonen, somebody had gotten hold of the party's passwords and used a PC in a public library to log in and type in bogus answers for two candidates who hadn't completed the

questionnaire. The material was distinctively racist and sexist.

The webmasters were finally notified on the eve of the election by a tip from the public and bogus answers were removed. The police is currently investigating the suspected crime.

The service contained information about 16,000 candidates and it was visited 250,000 times before the election. No information about hits to the bogus pages was released. According to Mr. Vihtonen, they have "7,000 suspects".

For the record: the two candidates - one in Helsinki, the other in Kemi - didn't win.

Link to the original news story, dated 2004-10-27 (only in Finnish):

<http://www.helsinginsanomat.fi/tuoreet/artikkeli/1076154360595>

Erka.Koivunen@iki.fi +358-50-5066317 <http://iki.fi/Erka.Koivunen/>

✉ **Re: Internet voting (Stevens, [RISKS-23.57](#))**

<Hamilton Richards <ham@cs.utexas.edu>>

Wed, 27 Oct 2004 14:24:12 -0500

PGN's comment on a couple of proposals to stage Internet-election hacking contests --

[I continue to be amazed that folks persist on focusing only on the risks of penetrations by outsiders. Insiders are by far the greatest concern here. PGN]

-- is well-taken as it applies to all software that's involved in ballot counting, but Internet voting is a nonstarter for reasons that are more fundamental.

The problem is that Internet voting compromises the secret ballot's secrecy. Although it's often assumed that ballot secrecy is a matter of individual privacy, it's more than that. Ballot secrecy benefits not only the individual voter whose ballot is secret, but all other citizens, who can be sure that their fellow citizens can't be bribed or coerced into voting contrary to their true preferences. The voter is alone in the voting booth, and takes away nothing that she could use to prove how she voted.

Now picture a voter casting his ballot, via the Internet, from the comfort and convenience of his home or office. How do we know that his employer, or a party official with pockets full of cash, is not watching over his shoulder?

It's true that absentee ballots have already opened this door a crack, but that's no reason to throw it open wide.

Hamilton Richards, Senior Lecturer, Dept. of Computer Sciences, UT Austin

[... not to mention that you have to trust everything along the way. PGN]

✶ Address-form glitch proves an easy scam

<Gabe Goldberg <gabe@gabegold.com>>

Mon, 25 Oct 2004 22:07:27 -0400 (EDT)

Credit-card thieves find sneaky way to beat fraud checks

<http://www.msnbc.msn.com/id/6297815/>

It's a harmless-looking part of every a Web site retailer's checkout page.

The form filled out by customers ordering products almost always has a

second line -- sometimes it's used for apartment numbers or other

information; it's usually left blank. But that innocuous-looking second

line could become a big headache for Internet merchants soon, says one

fraud expert. Credit card criminals have figured out a simple way to use

that second line to foil the most basic anti-fraud measures online

merchants use. [...] Designed long ago, most address verification

systems only check numerical values at the beginning of the address and

zip code fields in the billing address form. Letters, such as street

names and cities, are ignored. That means if the legitimate address is

123 Elmwood Street, and a criminal enters "123 XXTRTWW," the fraud

software will return a "yes" value, indicating the address is valid. [...]

This is of course not a "glitch", it's people specifying, designing, coding,

approving, and *continuing to use* a system in which "letters, such as

street names and cities, are ignored". And then being all shook up when

something bad happens.

Gabriel Goldberg, Computers and Publishing, Inc., 6580 Bermuda

Green Court,
Alexandria, VA 22312-3103 <http://www.cpcug.org/user/gabe> 1-703-
941-1657

✶ Re: TV emits international distress signal (Hogsett, [RISKS-23.57](#))

<Steve Summit <scs@eskimo.com>>

Fri, 29 Oct 2004 20:00:06 -0400

Mike Hogsett wrote about a flat-screen TV in Corvallis, Oregon, that inadvertently summoned a search-and-rescue operation.

I just heard a similar story about the Civil Air Patrol in New York.

Evidently they get repeated calls which can be traced to a United Parcel

Service depot in the Bronx. Now, it turns out that a company that makes

Emergency Locator Transmitters is serviced out of that UPS depot, and these

ELTs are often returned via UPS for repair. But sometimes the boxes get

dropped, at which point the supposedly malfunctioning ELT inside senses the

high-G impact of a "crash" and starts to transmit.

And then there's the story (perhaps an urban legend) about people mailing

supposedly-defective electronic toll tokens back to the issuing highway

authority, and being billed for the tollbooths the mail truck passed

through...

✶ Re: Is Windows up to snuff for running our world? (Smith, [R-23.57](#))

<"Atom 'Smasher'" <atom@suspicious.org>>
Wed, 27 Oct 2004 01:02:18 -0400 (EDT)

About a week ago i stopped by a local bank to cash a check and their windows computers where all down. they had no way to determine if the account had sufficient funds to cash the check. when i asked how often the system went down, they replied "once or twice a day" for 10-20 minutes.

They have a computer system that spends 10-40 minutes of every workday taking a siesta!

Apparently they knew the owner of the account that i was cashing the check from, and determined that he never writes bad checks so it should be OK to give me the money and sort it out later. hmmm... might there be a risk of someone trying to cash a bad check during a hectic time?

related link - Is Microsoft Licensing Forcing Banks to Break The Law?

http://www.ciupdate.com/article.php/10493_1485861

✶ Re: Do vendors read their own security policies?

<jmeissen@aracnet.com>
26 Oct 2004 23:26:02 GMT

I have the same problem with Fidelity Investments. Their

official website is
at <http://www.fidelity.com>. Yet in spite of having the problem
pointed out
to them they continue to send email that directs the recipient
to various
pages at m0.net, such as
<http://fidelity2.m0.net/m/s.asp?HB16244124889X4152973X503473>

The domain 'm0.net' is owned by Digital Impact in San Mateo.
There is no way
on the face of it to know that this is legitimate. For some
reason they
don't think it's a problem. The risk, of course, is that users
won't be able
to recognize a phishing attempt by the URL.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 59

Monday 8 November 2004

Contents

- [New Standards for Elections](#)
[NYT editorial summarized by PGN](#)
- [Some 2004 voting anomalies](#)
- [Bidding up prices on online auctions](#)
[NewsScan](#)
- [Identities stolen in seconds](#)
[Timothy L. O'Brien via Monty Solomon](#)
- [Pirates see video games before paying customers do](#)
[NewsScan](#)
- [Music industry on the wrong course](#)
[NewsScan](#)
- [Cahoot online banking security issue](#)
[Nik Barron](#)
- [Westpac Internet Banking problems](#)
[Tim Chmielewski](#)
- [Banks and their marketing/PR departments](#)
[Henk Langeveld](#)
- [Re: TV emits international distress signal](#)
[John Levine](#)
- [Re: Clocks set back a week too early](#)

[Martin Hepworth](#) [Mike Causer](#)

● [Re: Is Windows up to snuff for running our world?](#)

[Ron Bean](#)

● [Re: Battlefield Robotics are risk to the world public](#)

[Geoff Kuenning](#)

● [Book on malicious cryptography](#)

[J.H. Haynes](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **New Standards for Elections**

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

Sun, 7 Nov 2004 9:45:22 PST

The New York Times lead editorial on 7 Nov 2004 is titled
`New Standards for Elections'.

"... the mechanics of our democracy remain badly flawed. From untrustworthy electronic voting machines, to partisan secretaries of state, to outrageously long lines at the polls, the election system was far from what voters are entitled to."

Here is my PGN-ed summary of their recommendations:

1. Election day should be a holiday (rather than penalizing employees for having to take time off to vote).
2. Early voting can allow people to vote when it is convenient for them.
3. Voter-verified audit trails, source code accessibility to election officials, spot checks of code on Election Day (as is done in Nevada's slot machines!)

4. Shorter lines at the polls, standards for numbers of voting machines and
poll workers.
5. Impartial election administrators, and restrictions on insiders endorsing
candidates.
6. Uniform and inclusive voter registration standards.
7. Accurate and transparent voting roll purges.
8. Uniform and voter-friendly standards for counting provisional ballots.
9. Upgraded voting machines and improved ballot design.
10. Fair and uniform voter ID rules.
11. An end to minority vote suppression, disenfranchisement, harassment,
dirty tricks.
12. Improved absentee ballot procedures, e.g., downloading absentee ballots
from the Internet, but avoiding the ballot-by-scan/fax/e-mail with
explicit loss of privacy.

The full editorial as well as the entire series can be found at nytimes.com/makingvotescount .

✶ Some 2004 voting anomalies

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

Mon, 8 Nov 2004 16:01:13 PST

For those of you interested in following a collection of

reported problems
more carefully, here are just a few reported anomalies,
collected from a
variety of sources:

* Palm Beach County logged 88,000 more votes than people who had
voted in
the presidential race. (Teresa LePore of 2000 Butterfly
Ballot fame is
the County supervisor of elections there.)

* A Franklin County Ohio machine error gave Bush 3,893 extra
votes in a
precinct in Gahanna. The correct totals were 365 for Bush,
260 for Kerry.

* In Broward County FL, in balloting for Amendment 4, ES&S
software for
tabulating absentee ballots began counting BACKWARDS once a
total of
32,767 [$2^{15} - 1$, in a signed 16-bit field] votes had been
reached in a
precinct. When this was discovered, the corrected totals for
the precinct
went from 166,000 to 240,000, and actually caused the
statewide results to
be reversed on this amendment. Apparently the same flaw was
detected two
years ago in the same software, and remained uncorrected.
Nick Simicich wondered in a long message to RISKS:
Do you suppose that they "fixed" this by making the 16 bit
field
unsigned? Or do you suppose that they counted the numbers
separately
using, say, floating point so that they could check the
results for
large discrepancies? Or maybe that they checked the before
and after to
see that the numbers increased when they added to them...or
anything
else that they could do to make this self auditing? Nah...
frankly, I'm
scared by the stupidity of this error. This is a problem

that needs an
open source solution.

* The failure of the ES&S ranked-choice vote-counting software in the San

Francisco Supervisors' election that I noted in [RISKS-23.58](#) turns out to

have been a hard-coded constant maximum number of voters that was set too

low. The fix was utterly trivial, but wisely required recertification by

the State. [Perhaps the same programmer wrote the Broward software?]

* Bev Harris reported that ``Jeff Fisher, the Democratic candidate for the

U.S. House from Florida's 16th District said he was waiting for the FBI to

show up. Fisher has evidence, he says, not only that the Florida election

was hacked, but of who hacked it and how... In Baker County, for example,

with 12,887 registered voters, 69.3% of them Democrats and 24.3% of them

Republicans, the vote was only 2,180 for Kerry and 7,738 for Bush.... Dick

Morris [famous consultant to both parties, now with Fox News] wrote "So,

according to ABC-TVs exit polls, for example, Kerry was slated to carry

Florida, Ohio, New Mexico, Colorado, Nevada, and Iowa.... Exit polls

cannot be as wrong across the board as they were on election night. I

suspect foul play." '' [See <http://www.blackboxvoting.org> , *NOT* .com]

* Incidentally, Ralph Barone noted an article on the internal database

structures of the Diebold voting machines, plus how to hack an election

and cover your trail afterwards.

<http://www.blackboxvoting.com/scoop/S00065.htm>

* There were numerous reports of screens "jumping" votes in ES&S and Hart

InterCivic machines, where casting a straight-party subsequently changes the vote for the President before exiting.

* Also reported were many cases of long lines and long waits only in certain

politically skewed precincts, many legitimate voters who claim they were

disenfranchised, voters who were given special optical scan pens that were not capable of being tallied, and so on.

Many Web sources provided running lists of reported anomalies, such as

<http://www.votersunite.org>

<http://fairvote.org/easttwest.pdf>

<https://voteprotect.org>

<http://www.verifiedvoting.org/eirs/>

<http://www.electionprotection2004.org/coalition.htm>

<http://www.blackboxvoting.org>

⚡ Bidding up prices on online auctions

<"NewsScan" <newsscan@newsscan.com>>

Mon, 08 Nov 2004 07:57:29 -0700

Eight eBay sellers who bid up products online to inflate their prices have

been ordered by the New York Attorney General's office to pay almost \$90,000

in restitution and fines. More than 120 people will receive money from the

settlement of the three cases. One man will receive a check for \$3,089 after

overpaying for a 1999 Jeep Cherokee sport-utility vehicle he

bought from an
eBay seller in 2002. [**The Washington Post**, 7 Nov 2004;
NewsScan Daily, 8
Nov 2004]

<http://www.washingtonpost.com/wp-dyn/articles/A32944-2004Nov7.html>

Identities stolen in seconds

<Monty Solomon <monty@roscom.com>>
Sun, 24 Oct 2004 03:51:42 -0400

Timothy L. O'Brien, (**The New York Times**, 24 Oct 2004)

Pausing in the foyer of a comfortable suburban home two days before Halloween in 2002, Kevin Barrows, a special agent with the F.B.I., could not bring himself to open the front door. He and a team of agents had just spent several hours searching every room in the house, in New Rochelle, N.Y., but they were leaving empty-handed. Months of investigating had led Mr. Barrows to believe that someone was orchestrating a huge fraud from the house, yet he had not found a single scrap of evidence.

Still, something bothered him about the furniture in one of the bedrooms. It seemed oddly oversized. So he headed back upstairs for a second look, and his attention focused on an expansive canopy over the bed. When he pushed at the draping, he found that it was weighed down with files. They contained reams of confidential financial information about hundreds of individuals

whose identities had been pilfered in an intricate scheme that illicitly netted more than \$50 million.

Two years later, the New Rochelle home has emerged as a linchpin in what federal law enforcement authorities describe as the biggest case of identity theft ever uncovered in the United States. The scheme was essentially masterminded by just two people: Linus Baptiste, who lived in the house and had contacts with a sprawling ring of Nigerian street criminals, and Philip A. Cummings, his former brother-in-law, who worked as a help-desk clerk at a Long Island software company. At least 30,000 people nationwide were victimized, according to law enforcement authorities and court documents.

...
<http://www.nytimes.com/2004/10/24/business/yourmoney/24theft.html>

🚨 Pirates see video games before paying customers do

<"NewsScan" <newsscan@newsscan.com>>

Mon, 08 Nov 2004 07:57:29 -0700

Pirated copies of the sci-fi action title "Halo 2" and games such as "Grand Theft Auto: San Andreas" and "Half-Life 2" have been circulating on file-sharing networks, news groups and Web sites even before their official release to consumers. Brian Jarrard of Microsoft's Bungie Studio, which produced "Halo 2," complains: "You spend three years of your

life pouring
everything you have into this project, and then somebody gets
their hands on
the game and gives it away to the world for free. We made this,
and these
guys had no right to give it out to the public." Douglas
Lowenstein,
president of the Entertainment Software Association, admits:
"The problem
and challenge with piracy is that there are people out there on
a worldwide
basis who've identified piracy as a very profitable enterprise.
You don't
end this problem overnight." [AP 8 Nov 2004; NewsScan Daily, 8
Nov 2004]

<http://apnews.excite.com/article/20041108/D867MSU80.html>

⚡ Music industry on the wrong course

<"NewsScan" <newsscan@newsscan.com>>

Mon, 25 Oct 2004 08:01:44 -0700

Wharton business professor Joel Waldfogel says the music
industry is
mistakenly pursuing a short-term strategy in backing the Inducing
Infringement of Copyrights Act of 2004, which would hold liable
any entity
that "intentionally aids, abets, induces or procures"
copyrighted material.
Rather than fighting technological advances through litigation,
the music
industry must come up with new business models -- for instance,
taking
advantage of the Internet to slash its distribution costs.
"Instead of
putting out CDs and shipping them on trucks, they can send them
directly at
a very low cost. That does suggest a very different business

model than charging \$15 or \$20 for a CD. It might be a much more attractive way to do things. Stuff that is easy to distribute wants to be free. Given that force, I think [the recording industry] needs to come up with a new model for generating income," says Waldfogel. [Knowledge@Wharton, Oct 20-Nov 2 2004; NewsScan Daily, 25 Oct 2004]
<http://knowledge.wharton.upenn.edu/index.cfm?fa=viewArticle&id=1066>

⚡ Cahoot online banking security issue

<Nik Barron <Nik.Barron@pennantplc.co.uk>>
Fri, 5 Nov 2004 08:23:15 -0000

The UK's BBC Breakfast news reported a security issue with the Cahoot Internet bank. Apparently due to a recent system upgrade 12 days ago it was possible to access other users' accounts with only their user ID (normally, a password and set of "memorable information" is required before access is granted).

The report did not reveal the full details for obvious reasons, but implied that it was necessary to know the user's login name, which certainly for other banks is not directly related to the user's name. It was also confirmed by Cahoot that it would not be possible to transfer any money without knowledge of the password and memorable information.

Cahoot reacted promptly when the issue was confirmed, closing the site for ten hours while the cause was investigated and resolved. The system is now up and running and the vulnerability has been removed.

Although no financial loss was possible, this was a serious confidentiality breach albeit mitigated by ease of access to the user's login name. Needless to say the bad publicity will probably cause confidence problems for Cahoot and other online banks. Lessons to be learned include the need for comprehensive regression testing of security after system upgrades, and the difficulty in bolting on session security to web-based systems.

Full details are on the BBC's web site at <http://news.bbc.co.uk/1/hi/programmes/breakfast/3984641.stm>

Surprisingly, Cahoot have no statement on their site regarding the issue. The FAQ on "Security" states "However, we can reassure you that the site is tested regularly by independent security experts who are satisfied that the site is secure".

[Also noted by Michael Bacon. PGN]

Westpac Internet Banking problems

<"Tim Chmielewski" <tim@humanedge.biz>>
Mon, 8 Nov 2004 08:19:12 +1100

The Australian bank Westpac decided to implement its promised security

upgrade to their internet banking service on the weekend, only to have something go wrong and lockout thousands of customers (I would know as my Dad called me not long after I had the same problem.)

As their support line is only open 8am to 5pm during the week there was no one I could call to report the problem. When I rang this morning there was a recorded message regarding the problem with the service (I suspect they had to put it up or else their support line would be flooded.)

They tout their online banking service as being 24/7, but if they don't have the support to go with it, what is the use of having it?

Also, if they were going to require a change of passwords for a system upgrade, I think they should have sent a message out by mail at least two weeks in advance.

At least I haven't had any money stolen from me via the online banking service like what happened to service National Australia Bank customers last year.

Tim Chmielewski Webmaster, Human Edge Software <http://www.humannedge.biz>

✶ Banks and their marketing/PR departments

<Henk Langeveld <hlangeveld@mailworks.org>>
Fri, 05 Nov 2004 11:42:55 +0100

Re: Do vendors read their own security policies?
<jmeissen@aracnet.com>

I get frequent mailings from two Dutch banks, who apparently use the same PR company to send out their mailings. Both the mailings and the URLs (for special offers) refer to sites *not* under the control of the bank.

⚡ Re: TV emits international distress signal (Hogsett, [RISKS-23.57](#))

<John Levine <johnl@iecc.com>>
5 Nov 2004 00:43:55 -0000

>And then there's the story (perhaps an urban legend) about people mailing >supposedly-defective electronic toll tokens back to the issuing highway >authority, and being billed for the tollbooths the mail truck passed >through...

It's well documented. E-ZPass toll transponders contain a battery which eventually wears out, so every few years they send you a new pass and tell you return the old one. They provide a conductive bag that prevents the pass from responding, but a certain number of people don't bother to put the pass in the bag and it gets read on the way to the service center. The specific cases I've heard about were on the NJ Turnpike on the way to the Staten Island service center, but since all of the E-ZPass centers are close

to the roads or bridges they serve, it happens all the time.

[Yes. Paul Schreiber notes Susan Landau's item in [RISKS-23.01](#) on this very subject. Sorry I neglected to interject that. PGN]

⚡ Re: Clocks set back a week too early ([RISKS-23.58](#))

<Martin Hepworth <martinh@solid-state-logic.com>>
Fri, 05 Nov 2004 10:04:27 +0000

Since 1996, when the UK changed it's 'daylight saving' schedule to be in line with continental Europe, it's always been the last Sunday of March and October when this change occurs. That was 8 years ago!

<http://wwp.greenwichmeantime.com/time-zone/rules/eu.htm>

<http://www.nmm.ac.uk/site/request/setTemplate:singlecontent/contentTypeA/conWebDoc/contentId/344>

The risk seems to be people 'interpreting' the 'last Sunday' to mean the 'fourth Sunday', and not taking into account a month with 5 Sundays...

Martin Hepworth, Senior Systems Administrator, Solid State Logic Ltd
tel: +44 (0)1865 842300

⚡ Re: Clocks set back a week too early ([RISKS-23.58](#))

<Mike Causer <mikec@mikecauser.com>>

Fri, 5 Nov 2004 18:34:30 +0000

[...] The BST to GMT switch happened on the 5th Sunday of October in 1950, 1961, 1967, 1971, 1972, 1978, 1989, 1999, and 2000. (Source: <http://wpp.greenwichmeantime.com/info/bst2.htm>)

Mike Causer <http://www.mikecauser.com> mikec@mikecauser.com

⚡ Re: Is Windows up to snuff for running our world? (Smith, [RISKS-23.58](#))

<rbean@shell.core.com (Ron Bean)>

Sat, 6 Nov 2004 23:08:57 -0500

> But is the Windows operating system really reliable and secure enough for
> these kinds of applications?

Apple is missing out on a huge market here by not allowing their OS to run on other vendors' hardware. Nobody's going to buy a Mac to run an ATM or a cash register, but they might buy the OS if they thought it would work better.

⚡ Re: Battlefield Robotics are risk to the world public ([RISKS-23.58](#))

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

04 Nov 2004 23:40:42 +0100

To be fair to John Deere, as far as I can tell this particular robot is intended to be used purely for surveillance and will not have offensive capabilities. But Edward Nilges is still correct in his analysis of the risks of offensive robots. I especially agree with the analogy to land mines.

I recall a science fiction story from nearly 50 years ago that warned of the problems of a killer robot still searching for targets long after the war had happened. Perhaps we should insist that everyone in the Pentagon read old SF?

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

🔥 Book on malicious cryptography

<jhhaynes@earthlink.net>

Sat, 6 Nov 2004 15:43:06 -0600 (CST)

The October issue of Cryptologia has a review of "Malicious Cryptography: Exposing Cryptovirology" by Adam L. Young and Moti Yung, about the use of cryptography by crackers.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 60

Saturday 27 November 2004

Contents

- [Another telco equipment theft](#)
[David Lesher](#)
- [The coming catastrophe in German social services](#)
[Debora Weber-Wulff](#)
- [BMW series 5 disables Dynamic Stability Control and ABS](#)
[Stefan Lesser](#)
- [Business risks of software development](#)
[Peter B. Ladkin](#)
- [Recent fiasco with computer system at Child Support Agency](#)
[Pete Mellor](#)
- [Software is no substitute for thought: yet another instance](#)
[Robert Allan Zeh](#)
- [Wanted by police: a few good icons...](#)
[David Lesher](#)
- [Texas officials wary of plan to hunt by Internet](#)
[Arthur Goldstein](#)
- [Whites Only websites?](#)
[Dan Jacobson](#)
- [Re: Battlefield Robotics are risk to the world](#)
[Edward G. Nilges](#)

- [Increasing sophistication of phishing spammers](#)
[Dan Wallach](#)
 - [Scott Sagan: The Problem of Redundancy Problem](#)
[PGN](#)
 - [REVIEW: "WarDriving: Drive, Detect, Defend", Hurley/Thornton/Puchol](#)
[Rob Slade](#)
 - [Computers, Freedom & Privacy Conference 2005, Call for Proposals](#)
[Bruce R Koball](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Another telco equipment theft

<David Leshner <wb8foz@nrk.com>>
Sat, 27 Nov 2004 09:59:14 -0500 (EST)

911 service was disrupted for seven hours for some 25,000 customers in parts of Westchester County NY. Reportedly, police were sent to a telco building in White Plains to investigate, but as they arrived two men were seen wheeling a luggage cart out of the building. It turns out that the men had stolen \$1 million worth of computer parts -- whose removal had effectively shut down 911 service. The computer chip boards were valued from \$5,000 to \$70,000 each. The men were arrested. Apparently, no ambulance delays or other serious consequences were reported. [Source: AP item, 26 Nov 2004: PGN-ed]

⚡ The coming catastrophe in German social services

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

Fri, 26 Nov 2004 22:04:39 +0100

On 1 Jan 2005 Germany will switch over from two systems for compensating people who do not work (Arbeitslosenhilfe and Sozialhilfe, money for people who have worked but their unemployment insurance has run out and social services payment for the poor) to a new one, Arbeitslosengeld II, called ALG II or Hartz IV (after the guy who chaired the commission that thought this mess up).

In order to make sure that no one hides any assets there is a 16-page application form that needs to be filled out and all sorts of documentation supplied. It takes an official at the public offices about an hour to put all of this information into the central system just for one person. Germany's jobless rate is at about 10% of the population, or 4.2 million people officially registered, I could not find the number of people on Sozialhilfe.

The system, however, was not finished on time. The time for starting the data entry kept being slipped. When the data entry began, not all of the workers could enter data at the same time, because the system overloaded. The system has to be rebooted every day at lunch time, because otherwise it would be too slow in the afternoon. (Anyone hear hanging processes screaming?). The data connections are very slow, and sometimes die, taking all of the data entered up until now with them. It can take up

to an hour for the data entry station to permit a new logon.

If data entered is incomplete (and it often is, as someone missed one of the many questions) the system automatically deletes the record after about three or four weeks. Last week, a software update was put on the central system in Nürnberg, crashing the system so completely, that the backup had to be restored a day later. (At least they had one!).

In desperation some office managers pleaded with their workers to do overtime and come in on the weekend to enter data. But there was a fire in the central computing system and no data could be entered at all.

Amazingly, they have managed to calculate some of the payouts and send the information to the people receiving them. But since they do not yet have all of the forms and cannot put in all of the data in time, many offices are being forced to just pay people some money in January and figure out later if it was too much or too little.

So we pretty much have a great example of everything going wrong that possibly can - one wonders perhaps why Germany has so many of these projects at the moment: this, the TollCollect scheme, the health card proposed for 2006, etc.

There's a nice article in c't (in German) on why large software projects don't work in Germany: (c't 23/2004, IT-Großprojekte: Warum so viele Vorhaben scheitern, S. 218) It ranges from people without knowledge of systems deciding what to implement to the politics of

procurement. And, of course, a good bit of wishful thinking - hoping that computers can cure problems that have deeper causes.

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, Treskowallee 8, 10313 Berlin
Tel: +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

✶ BMW series 5 disables Dynamic Stability Control and ABS

<Stefan Lesser <stefan.lesser@burdadigital.de>>
Mon, 8 Nov 2004 23:59:42 +0100 (W. Europe Standard Time)

After two accidents involving police cars of Berlin, Germany, at first the drivers were blamed and appointed to a security training. But taking into consideration the driver's nearly identical reports, which claimed that the cars on-board drive dynamic control systems had failed, BMW took on and inspected the case. The result was: Yes, after an emergency brake exceeding a certain preset pressure on the pedal, all stability systems are disabled and can only be re-enabled by switching off the ignition for five seconds...

Originating report (German only):
<http://www.daserste.de/plusminus/beitrag.asp?iid=254>

Follow-Ups (German ditto):
http://www.autobild.de/aktuell/neuheiten/artikel.php?artikel_id=7348
<http://www.autoservicepraxis.de/sixcms4/sixcms/detail.php?id=81192&topnavi=32454&zielcb=>

Stefan Lesser, Muenchen, Burda Digital Systems GmbH, Am
Kestendamm 2,
77652 Offenburg, Germany +49 89 9250-3433 [http://www.
burdadigital.de](http://www.burdadigital.de)

✶ Business risks of software development

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Sat, 13 Nov 2004 08:30:43 +0100

Another data point from the *International Herald Tribune*
<http://www.ihf.com/articles/2004/11/11/business/siemens.html>

The large German engineering conglomerate Siemens AG held a news conference Thursday 11 November 2004 in Munich, in which it said inter alia that its mobile phone division lost €141m in the fourth quarter 2003 (July-September) compared with a profit of €14m in the same quarter 2002. Siemens is reported as saying that the main reason for the loss was a delay in selling the S65 phones to correct a software defect.

University of Bielefeld, Germany <http://www.rvs.uni-bielefeld.de>

✶ Recent fiasco with computer system at Child Support Agency

<Pete Mellor <pm@csr.city.ac.uk>>
Fri, 19 Nov 2004 21:43:54 +0000 (GMT)

The Child Support Agency is a UK Government organisation set up

some years ago to trace absent parents and extract maintenance payments to the parents of the children they have abandoned. (In the way of the world, the absentees are usually the fathers, and the abandoned are usually the mothers, but the opposite can occur.)

The CSA has never worked well. Under the 'old legislation', the calculation of payments due was complicated and time-consuming, and left little time for staff to trace the absentees and enforce payment.

Under the 'new legislation', which went into effect on 3 Mar 2003, the algorithm for calculating payments was simplified to allow more effort to be concentrated on enforcement. To implement the new rules, a computer system was procured from EDS under a contract valued at GBP 456 million over 10 years.

On the BBC Radio 4 'Today' news and current affairs programme this morning (Fri 19 Nov 2004), the Work and Pensions Secretary, Alan Johnson, stated that the new computer system is "problematic", but, under pressure from the interviewer, John Humphrys, he admitted that "disastrous" might be a better word.

The backlog of cases is growing at 30,000 per month, and has now reached around 250,000 cases. The CSA's debt (money owed to abandoned parents and children) stands at GBP 720 million, and, in addition, GBP 1 billion has been "written off". Of 478,000 absent parents, 417,000 "have not paid a

penny". (I presume that these statistics cover the whole life of the CSA under both the 'old' and 'new' systems, and reflect the great difficulty of tracing those who owe the maintenance and enforcing payments, rather than being due solely to recent computer problems.)

Applicants are regularly told that their cases cannot be progressed, since certain "incidents cannot be resolved" on the new computer system. So far, only new cases have been entered. 95,000 cases are still stuck on the 'old system'. These applicants should have received interim payments of GBP 10 per week since March 2003, but the 'new system' cannot cope with this, either.

Two employees of the CSA were interviewed anonymously. It appears that once an incident has occurred while processing a case, no further work can be done on that case. (For "incident" read "system failure".) One interviewee claimed that the new system "cannot cope with change". For example, if a couple decide to get back together (which happens, and which means that maintenance payments no longer need to be enforced), there is no way of entering this information into the system.

The underlying problem seems to be an inadequate requirements specification.

Alan Johnson blames EDS. (The CSA has withheld GBP 1 million per month from payments due to EDS under the contract, to a total of GBP 12 million so far.) Tony Collins of Computer Weekly said that, in his opinion, the responsibility lay 50/50 between customer and contractor, and

that CSA probably did not know what they wanted, and their requirements were therefore unstable.

On Wednesday, Alan Johnson faced tough questions in Parliament. On Thursday, the chief executive of the CSA resigned. According to Johnson, this was just because he had been in post for four years. (Presumably he wanted to spend more time with his family!)

Another triumph for UK Government IT procurement!

The official CSA website is:

<http://www.csa.gov.uk/>

This includes a description of the method of calculating payment due.

To hear the brief report from the Today programme on Wed 17 Nov 2004, visit:

http://www.bbc.co.uk/radio4/today/listenagain/zwednesday_20041117.shtml

To listen to a summary of the background to the problem, and (in a later item) the Work and Pensions Secretary, Alan Johnson, wriggling on a hook, on Friday 19th November, visit:

<http://www.bbc.co.uk/radio4/today/listenagain/>

and follow the links.

Peter Mellor, Centre for Software Reliability, City University, London EC1V 0HB +44 (0)20 7040 8422 Pete Mellor <p.mellor@csr.city.ac.uk>

✶ Software is no substitute for thought: yet another instance

<Robert Allan Zeh <razeh@earthlink.net>>

Sun, 21 Nov 2004 13:13:58 -0600

I live in River Forest, IL, a Chicago suburb. The November 10th, 2004 edition of our local paper, The Wednesday Journal, contained coverage of a development review board meeting for some new construction.

The architect for the construction had done a computerized "Shadow Study" to determine how the new construction would impact the area. The study simulated conditions on Jun 20 and Dec 20. Here is the section relevant to RISKS:

When Nimesh said that long shadows were present at 6 p.m. in the 20 Dec simulation, DRB chairman Frank Martin look at him for a second, then said 'It's dark at 6 p.m. in December.' "The software's not perfect," replied Nimesh after a moment's hesitation.

I would suggest that the user needs a little work too. Checking your answers for reasonableness is always a good practice, even if you aren't using a computer.

And old physics teacher of mine enjoyed showing a physics problem to students to see if they'd spot what didn't make sense. The problem, which involved a door, had originally used English units, but was later converted to metric.

However, the units were changed without changing the values. The door was 7 meters tall, with a doorknob 3 meters up.

✶ Wanted by police: a few good icons...

<David Leshar <wb8foz@nrk.com>>
Sat, 13 Nov 2004 19:30:49 -0500 (EST)

Wanted by the Police: A Good Interface,
Katie Hafner, *The New York Times*, 11 Nov 2004
<http://www.nytimes.com/2004/11/11/technology/circuits/11cops.html?pagewanted=print&position=>
<http://www.nytimes.com/2004/11/11/technology/circuits/11cops.html>
<http://www.nytimes.com/2004/11/11/technology/circuits/11cops.html>
<http://www.nytimes.com/2004/11/11/technology/circuits/11cops.html>

San Jose has a reputation as one of the safest large cities in the nation, with the fewest police officers per capita. Yet a number of the 1,000 officers in this city of 925,000 in the heart of Silicon Valley have been worrying about their own safety of late. Since June, the police department has been using a new mobile dispatch system that includes a Windows-based touch-screen computer in every patrol car. But officers have said the system is so complex and difficult to use that it is jeopardizing their ability to do their jobs. [...]

This article reads like a casebook for your class Risks 201: "How NOT to build a system..."

"Do you think if you're hunkered down and someone's shooting at you in your car, you're going to be able to sit there and look for Control or Alt or Function?" said Sgt. Don DeMers.

A) Single-tasking. Recall the Star Trek spoof when Data can't shoot back

because his console has a rotating hourglass as he raises shields....?

B) Non-intuitive.

C) Too much data for the audience.

D) No consultation with end-users. "We know what's best for you.."

Now I'll grant cops can be tough crowd for technology; I recall decades ago

explaining to several, in slow detail, how you adjusted the squelch control,

and yes, it DOES matter if you put the mike up to your mouth.

[Several would

leave it on the dash and just yell...]

But the vendor should KNOW that.

PS: As for Sgt. DeMers, maybe Mr. Clippy will show up and help him out....

✶ Texas officials wary of plan to hunt by Internet

<arthur.goldstein@att.net>

Wed, 17 Nov 2004 15:44:47 +0000

This just strikes me as having a risk:

http://reuters.excite.com/article/20041117/2004-11-17T134519Z_01_N15284347_RTRIDST_0_ODD-LIFE-HUNTING-DC.html

http://reuters.excite.com/article/20041117/2004-11-17T134519Z_01_N15284347_RTRIDST_0_ODD-LIFE-HUNTING-DC.html

Hunters soon may be able to sit at their computers and blast away at animals

on a Texas ranch via the Internet, a prospect that has state wildlife officials up in arms. A controversial Web site, <http://www.live-shot.com>, already offers target practice with a .22 caliber rifle and could soon let hunters shoot at deer, antelope and wild pigs, site creator John Underwood said on Tuesday. Texas officials are not quite sure what to make of Underwood's Web site, but may tweak existing laws to make sure Internet hunting does not get out of hand.

[Excerpted from Jeff Franks, Reuters, 17 Nov 2004]

[Guncams instead of webcams as the next rage? AG]

[Don't forget the Internet Web-enabled Thai robot that could aim and fire a gun ([RISKS-21.02](#)). PGN]

⚡ Whites Only websites?

<Dan Jacobson <jidanni@jidanni.org>>
Fri, 19 Nov 2004 01:20:33 +0800

First it was blocking e-mail from countries one never expects to get mail from (even though one unwittingly sends mail to there, expecting replies). Now some websites don't even allow browsers from lesser countries to connect. "Who from there would need to read our website? They're all just spam bots." So next time you go abroad, you might find yourself locked out of familiar websites, and not just during elections, e.g., <http://news.bbc.co.uk/1/hi/technology/3958665.stm>

✶ Re: Battlefield Robotics are risk to the world (Kuenning, [RISKS-23.59](#))

<spinoza1111@yahoo.com (Edward G. Nilges)>
12 Nov 2004 23:01:10 -0800

No, I don't think the brass hats should read old SF. They'd curl up with Heinlein and the next thing you know, hard service in Iraq would be a prerequisite for citizenship. They'd read the first chapter of Ursula LeGuin's *The Left Hand of Darkness* and throw up at the very idea of people changing their sex.

I'd recommend the *Cambridge History of Iraq*, instead, because therein one reads of British redcoats, roaring about the desert in the exact same way as us, in 1921, egged on by lunatics including T. E. Lawrence and Gertrude Bell.

An analysis of what it means to be "responsible" for a software system is needed, including the ways in which digital systems designers have historically limited their liability.

It would show that no bright line can be drawn between "my responsibility" and "someone else's".

A simple example from the history of ordinary software illustrates. When I started coding, my boss of course had me do a lot of maintenance in addition to development, and I was shocked to see that the older

programmers' code
had all sorts of bugs causable by invalid input. I extended my
own boundary
and that of the legacy code by adding error checks, thereby
gaining a
reputation in some jobs as an ivory tower theorist, or
something, despite
the fact that error checking is grubby praxis, and not theory.

I believe that the Bush administration wants power without
responsibility,
and in software this has been the typical administrative/MIS
gesture of
authorizing the development of crud.

In dark moments I wonder if the whole purpose of software is not
rhetorical
and not logical, to manufacture a post-Enlightenment consent
which
necessarily contains the memory of Enlightenment.

Military standards, of course, are much higher, as shown in the
Ada
language. But the very precision of the process draws a bright
line around
responsibilities which have in the past, excluded military
responsibility
for "legacy code" in the form of land-mines and unexploded
ordnance.

And as a confirmed civilian, watching Marines fire over
Najulla's walls
exactly as they were filmed at the Citadel in 1968, I find it
hard to
believe that they are worried about the existing laws of war, or
will pick
up after themselves when the battle is over, if it ever is.

We may discover that one's responsibility extends so far in fact
and in
ethics that the only RATIONAL response is an end to war. Gee,
how about
that.

✶ Increasing sophistication of phishing spammers

<Dan Wallach <dwallach@cs.rice.edu>>

Tue, 23 Nov 2004 10:08:28 -0600

I recently received a spam message claiming to be a response, forwarded to me via eBay, in regards to an item I was auctioning. Of course, I have no auction going on eBay, making it obviously fake. The message was an HTML message and included numerous in-lined images from pics.ebaystatic.com, helping make the message appear more real. A link at the bottom, attacked to a "Respond Now" button (which users might presumably click to helpfully say "you got the wrong person") takes you to an IP address that has nothing to do with eBay and which feeds you a recent JavaScript exploit against Internet Explorer. That JavaScript appears to be in Unicode (making it annoying to look at with Emacs), and further contains a hex-encoded message which is decoded with JavaScript's "unescape" operator. The exploit is designed for Internet Explorer, but caused Firefox 1.0 to wedge. I had to restart it.

This particular spam seems intended to take over machines, presumably for zombie purposes. I've gotten other spams that similarly inlined "real" images to lure unsuspecting users toward credit card information phishing sites.

Issue #1: eBay and similar companies should eliminate these public servers that serve up static images for e-mail and should pay attention to referrer information to refuse images being sent to pages other than their own. Make the spammers work harder to make their pages look "real". They'd either need to set up their own static image servers, or they'd need to embed the images in the spams as MIME attachments, making the spam larger and reducing the number of spams they can send with a given amount of bandwidth.

Issue #2: I get plenty of legitimate e-mail from companies with which I do business, such as my preferred airline, car rental, and credit card vendors. All of them have my e-mail address and occasionally have real reason to send me messages (e.g., I like getting an e-mail copy of my travel itinerary). Even those companies, however, occasionally send me "promotional" messages and such, even though I always go out of my way to select the "don't e-mail me" option. As long as we're using e-mail for business purposes (either in response to actual business, like when I reserve a plane ticket, or "promotional"), then we're going to have spam that imitates this legitimate mail. Probably the only true answer is for eBay, my credit card company, and all of these other vendors to start digitally signing their mail. S/MIME has been integrated in modern e-mail systems since 1996 or 1997. It's time for these firms to use it.

✦ **Scott Sagan: The Problem of Redundancy Problem**

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

Thu, 18 Nov 2004 20:46:44 PST

Scott Sagan has written a fascinating article entitled
The Problem of Redundancy Problem: Why More Nuclear
Security Forces May Produce Less Nuclear Security,
which appears in the current issue of **Risk Analysis**.
This article is quite provocative, and also illustrative of the
profound
difficulties we have in designing trustworthy organizations to
manage highly
dangerous technologies.

After a little browsing, I found this paper noted on his Web
site at

<http://cisac.stanford.edu/people/2223/>

Scott has long been studying and writing about risks-related
issues
that transcend the scope of what normally appears in RISKS.

Scott D. Sagan, Professor of Political Science
ssagan@stanford.edu

Co-Director, Center for International Security and Cooperation
(CISAC)

Stanford Institute for International Studies, Encina Hall
616 Serra Street, Stanford University, Stanford, CA 94305-6165
(650-725-2715) phone <http://cisac.stanford.edu>

✦ **REVIEW: "WarDriving: Drive, Detect, Defend", Hurley/Thornton/ Puchol**

<Rob Slade <rslade@sprint.ca>>

Thu, 11 Nov 2004 10:31:44 -0800

BKWARDRV.RVW 20040823

"WarDriving: Drive, Detect, Defend", Chris Hurley/Frank Thornton/Michael Puchol, 2004, 1-931836-03-5, U\$49.95/C\$69.95

%A Chris Hurley
 %A Frank Thornton
 %A Michael Puchol
 %C 800 Hingham Street, Rockland, MA 02370
 %D 2004
 %G 1-931836-03-5
 %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/1931836035/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/1931836035/robsladesinte-21>
 %O <http://www.amazon.ca/exec/obidos/ASIN/1931836035/robsladesin03-20>
 %P 495 p.
 %T "WarDriving: Drive, Detect, Defend"

Chapter one is an introduction to the concept, with a discussion of required components, and the relevant characteristics thereof. Installing NetStumbler is described in chapter two, with operating instructions in three (which also repeats some of the earlier advice on component choice). Kismet installation is detailed for Slackware in chapter four, Fedora in five, and the operations are listed in six. Screenshots of using StumbVerter (and Microsoft MapPoint) or DiGLE to produce maps with the data previously obtained are shown in chapter seven.

Chapter eight describes, in detail, how to organize your own wardriving contest (including an eight page Perl script for scoring results). Simple means of attacking and connecting to wireless networks are given

in chapter
nine. Screenshots of dialogue boxes for enabling basic security
features on
the major wireless routers are listed in chapter ten. Some
features
providing more advanced security are discussed in chapter eleven.

The material provided in the book is clear, and will provide you
with enough
information to start wardriving and connecting to other
networks. The
content is fairly rudimentary, though, without the background
information of
a work like "Wireless Hacks" (cf. BKWLSHCK.RVW), by Rob
Flickenger, which
would allow the reader to go further in both understanding the
technology
and defending wireless networks.

copyright Robert M. Slade, 2004 BKWARDRV.RVW 20040823
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)

✦ Computers, Freedom & Privacy Conference 2005, Call for Proposals

<Bruce R Koball <bkoball@well.com>>
Sun, 14 Nov 2004 19:29:16 -0800 (PST)

COMPUTERS, FREEDOM, AND PRIVACY CONFERENCE: Panopticon 2005
12-15 Apr 2005, Westin Hotel, Seattle, WA
<http://www.cfp2005.org>

The 15th annual conference on Computers, Freedom & Privacy takes
place
from Wednesday 12 Apr to Friday 15 Apr 2005, in Seattle,

Washington.

The Program Committee is now accepting proposals for conference sessions and speakers for CFP2005. The deadline for submissions is 31 Dec 2004.

CFP serves as an internationally recognized forum for the members of the technical, government, hacker, legal, business, education, media, cyber-rights, and non-profit communities to address cutting edge technical, business, legal and cultural issues. Programs, topics, and speakers from prior years' CFP conferences can be found at: www.cfp.org

The CFP2005 Program Committee welcomes proposals on all aspects of technology, freedom and privacy. We are particularly interested in receiving proposals that ask the hard questions about privacy and freedom in emerging surveillance societies, and challenging those assumptions. For example, how much surveillance is too much? When does surveillance cease making us more secure and begin to change the fabric of society?

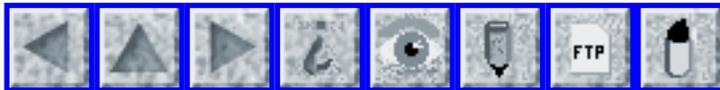
The theme of the 15th CFP is "Panopticon 2005." Over time, and particularly recently, surveillance of ordinary citizens has increased to dramatic levels. Not only are governments watching more aspects of their citizens' lives, but those in the private sector are increasing surveillance of people as well. Often lost in the race to "increase intelligence" are discussions about different approaches to address problems like the threat of terrorism that are equally or more effective, but do not involve extensive and constant surveillance.

Other areas of interest include:

1. domestic and international travel issues
2. communications surveillance
3. children and young adults growing up in a surveillance society
4. social networking
5. the flourishing of free speech (i.e. blogging) in spite of increased watchfulness
6. RFIDs and other emerging technologies
7. Intellectual property issues

All submissions must be received by 31 Dec 2004. Complete submission

instructions appear on the CFP2005 Web site: www.cfp2005.org



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 61

Weds 8 December 2004

Contents

- [Group urges Government to focus on cybersecurity](#)
[NewsScan](#)
- [UK "Government department wiped out by IT upgrade disaster"](#)
[Bob Heuman](#)
- [Cyberspace activism](#)
[NewsScan](#)
- ["Midway scare is blamed on glitch"](#)
[D. McKirahan](#)
- [Defibrillator maker issues recall, goes out of business](#)
[Caleb Hess](#)
- [Exploding cell phones](#)
[PGN](#)
- [Air Traffic Control blacked out by rodent](#)
[D. Joseph Creighton](#)
- ['Virus-throttle' software from HP](#)
[NewsScan](#)
- [E-mail notification](#)
[Drew Dean](#)
- [When e-commerce and poor translation meet... terrorism?](#)
[Harry Neumann](#)

- [Job posting follies](#)
[Stephen Cohoon](#)
 - [Re: New Standards for Elections](#)
[Atom 'Smasher'](#)
 - [Re: new standards for elections; voting anomalies](#)
[J.E. Cripps](#)
 - [More on the electoral process](#)
[J.E. Cripps](#)
 - [Voter touch-screen no good? Here's a pen!](#)
[Joel Garry](#)
 - [Re: Is Windows up to snuff for running our world?](#)
[Sander Tekelenburg](#)
 - [Deworming the Internet: addressing computer security market failure](#)
[Douglas Barnes](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ **Group urges Government to focus on cybersecurity**

<"NewsScan" <newsscan@newsscan.com>>

Wed, 08 Dec 2004 10:22:59 -0700

The Cyber Security Industry Alliance is calling on the Bush administration to beef up its cybersecurity operations, starting with elevating the position of national cybersecurity director to assistant secretary level. "There is not enough attention on cybersecurity within the administration. The executive branch must exert more leadership," says Alliance director Paul B. Kurtz, who's a former senior cybersecurity official in the Bush administration. Kurtz was joined by Amit Yoran, the former director of Homeland Security's National Cyber Security Division who resigned in September. Meanwhile, a provision in the recently

passed intelligence overhaul bill that would have raised cybersecurity's profile in the Homeland Security Department was stripped out before passage. The Alliance's recommendations mirror those outlined in a report issued Monday by the House subcommittee on cybersecurity, which also calls for the administration to consider tax breaks and other incentives for businesses that make computer security a top priority. In addition, both groups are urging the Homeland Security Department to take the lead in creating a disaster recovery and response plan, should the U.S. suffer debilitating digital sabotage. [*The Washington Post*, 8 Dec 2004; NewsScan Daily, 8 Dec 2004]

<http://www.washingtonpost.com/wp-dyn/articles/A45622-2004Dec7.html>>

Report says "Government department wiped out by IT upgrade disaster"

<"R.S. (Bob) Heuman" <rsh@idirect.com>>

Fri, 26 Nov 2004 10:23:00 -0500

This is from the United Kingdom, and I really have to wonder how anyone can download an 'incompatible system' to 80,000 computers in this day and age. It boggles the mind! Recovery in a day is not shabby, either, if true.

The Department of Work and Pensions (DWP) has suffered what has been

described as the biggest computer crash in government history after a software upgrade that is believed to have downloaded an incompatible system throughout the entire DWP network. The government department lost 80 per cent of its roughly 100,000 PCs following a "routine software upgrade", a DWP spokeswoman confirmed today. The problem lasted all of yesterday but the "majority of our system is up and running now", she said. Microsoft and EDS run the DWP's network as part of a 2-billion pound IT contract. The situation had apparently been largely rectified by the next day.

[Source: Government department wiped out by IT upgrade disaster;

Another massive computer cock-up, this time at Work and Pensions.

<http://www.techworld.com/opsys/news/index.cfm?NewsID=2695&Page=1&pagePos=2>

By Laura Rohde, IDG News Service, 26 Nov 2004; PGN-ed]

R.S.(Bob) Heuman, Toronto, ON, Canada Independent Computer Security Consulting
Web Site Auditing for Compliance with Standards rheuman@rogers.com

Cyberspace activism

<"NewsScan" <newsscan@newsscan.com>>

Wed, 01 Dec 2004 09:07:27 -0700

The German-based Web portal Lycos Europe is offering a screensaver program that chokes spam servers by flooding them with junk traffic. The company argues that what it's doing is perfectly legal, but former FCC

chief

technologist David Farber comments: "You don't stop a bad thing by being bad yourself. The idea of somebody coming and hitting you and you hitting back, you both end up very hurt. It just aggravates an already serious problem."

And noted computer security expert Dorothy Denning, a professor of defense

analysis at the Navy Postgraduate School, points out that cyberspace

activism of the kind offered by Lycos Europe is likely to have only minimal

impact on spam because "the cost of adding extra bandwidth may be worth the

reward" that spammers get from their activities. She adds: "The interesting

question is whether or not that company [an anti-spam activist company]

might be liable under some law, and would probably be liable, certainly, at

least under a lawsuit by the spammers." [AP 30 Nov 2004; NewsScan Daily, 1

Dec 2004]

http://www.usatoday.com/tech/products/2004-11-30-lycos-attack-spam_x.htm?csp=34

🔥 "Midway scare is blamed on glitch"

<"D. McKirahan" <dmckirahan@comcast.net>>

Tue, 23 Nov 2004 05:39:43 -0600

Errors by screeners--not random computer glitches that the federal

government previously blamed--were responsible for false alarms over weapons

that sparked the recent evacuation of Midway Airport and two other U.S.

airports, according to the Transportation Security Administration.

The confusion that led to the terminal evacuation on 15 Nov was prompted by a hand grenade appearing on an X-ray scanner. The image of the grenade, part of an exercise used to test screeners, should have been stored in a computer file by a security agency staff member as part of standard procedure before an employee shift change at the screening checkpoint, said Amy von Walter, spokeswoman for the security agency.

Federal security officials initially said a malfunction in a software program used to test screener performance prompted a computer-generated image of the grenade to appear randomly on the X-ray screen. A screener operating the X-ray scanner thought the grenade, artificially projected inside a carry-on bag, was real.

If the screener were being tested, the grenade image would have disappeared when the screener tapped a button on the device's console to acknowledge seeing the item. In this case, the grenade did not vanish. But the passenger was able to leave the security checkpoint with the suspect bag before screeners could search its contents, leading to the evacuation order.

[DMcK submitted two items, a week apart. This is PGN-ed from the more recent and more accurate. Source: Jon Hilkevitch, Screeners blamed for bomb scare, *Chicago Tribune*, 23 Nov 2004]

<http://www.chicagotribune.com/news/local/chi-0411230350nov23,1,4870091.story>

?coll=chi-newslocal-hed

✶ Defibrillator maker issues recall, goes out of business

<Caleb Hess <hess@cs.indiana.edu>>

Fri, 12 Nov 2004 13:29:55 -0500

A manufacturer of Automated External Defibrillators (AED) recently announced a recall due to failure modes in which AEDs failed to deliver a shock when needed, or "turned themselves on" and subsequently failed to function (presumably due to drained batteries?). The maker claimed a failure rate of less than one percent, although it is not clear how that figure was obtained (many of these units are deployed in public buildings or other settings where few of them will actually be called upon to operate).

Aside from the risk of shipping an inadequately tested product, the article below raises some other interesting points:

The manufacturer says that no patient has died because of either failure mode - which should be obvious, since an AED is only to be applied to a patient who is already technically dead (pulseless).

A fire chief cites the obvious concern of carrying a piece of equipment that may not work when needed.

An EMS director notes that, where units cannot be immediately replaced, their removal turns a 1% probability of not defibrillating into a 100%

probability.

The AP article is at

<http://cms.firehouse.com/content/article/article.jsp?sectionId=17&id=36601>

✶ **Expoding cell phones**

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

Wed, 24 Nov 2004 9:30:01 PST

Exploding Cell Phones a Growing Problem;
Injuries From Exploding Cell Phones Prompt Recalls;
Bad Batteries or Chargers Often the Culprit (ABC News, AP item,
24 Nov 2004)

Safety officials have received 83 reports of cell phones exploding or catching fire in the past two years, usually because of bad batteries or chargers. Burns to the face, neck, leg and hip are among the dozens of injury reports the Consumer Product Safety Commission has received. The agency is providing tips for cell phone users to avoid such accidents and has stepped up oversight of the wireless industry. There have been three voluntary battery recalls, and the CPSC is working with companies to create better battery standards. U.S. phone makers and carriers say most fires and explosions are caused by counterfeit batteries and note that in a country with some 170 million cell phone users, the number of accidents is extremely low. [PGN-abst]

✂ Air Traffic Control blacked out by rodent

<"D. Joseph Creighton" <djc@cc.umanitoba.ca>>

Fri, 19 Nov 2004 10:27:30 -0600

Some local wildlife decided to get warm and intimate with power lines, blowing a transformer, and causing a cascade shutdown of substations across much of the city of Winnipeg, Canada.

http://winnipeg.cbc.ca/regionalnews/caches/mb_hydro20041118.html

This left every plane in central Canada (Saskatchewan, Manitoba, NW Ontario) flying blind for some eight minutes as YWG Center went down. Although power was restored after one minute -- backup power also failed -- the radar and communication systems took seven more minutes to restart.

http://winnipeg.cbc.ca/regionalnews/caches/mb_powerout20041118.html

D. Joseph Creighton [ESTP] | Info. Technologist, Database Technologies, IST

Joe_Creighton@UManitoba.CA | University of Manitoba Winnipeg, MB, Canada, eh?

✂ 'Virus-throttle' software from HP

<"NewsScan" <newsscan@newsscan.com>>

Wed, 01 Dec 2004 09:07:27 -0700

Software engineers at Hewlett-Packard are developing "virus-

throttling"
software to slow the spread of viruses and worms on the Internet
by
identifying suspicious behavior. HP chief technology officer
Tony Redmond
says, "Any worm or virus that depends on its ability to spread
itself will
be hurt by this technology." Alan Paller, director of research
at the SANS
Institute, says the overall idea "makes sense," and adds, "It's
an arms
race, not a simple war. I've been hearing people talk about the
notion of
throttling for a long time, and it's a spectacular idea if HP
can get it to
work." [*The Washington Post*, 30 Nov 2004; NewsScan Daily, 1
Dec 2004]

<http://www.washingtonpost.com/wp-dyn/articles/A23527-2004Nov30.html>

✶ E-mail notification

<Drew Dean <drew.dean@sri.com>>

Fri, 3 Dec 2004 13:21:22 -0800

I recently received e-mail from Southwest airlines informing me
of an
e-ticket. The only problem is that I didn't make the
reservation, and it's
not for me.

While there's a Reply-To: header in the message, with the same
address
as the From: header, there's a note at the bottom saying please
don't
reply to this address, and the message provides no way to reach
Southwest's customer service department.

I suppose I can dig around their website, or call their general toll-free number to try and remedy this, but why on earth don't they include a customer service contact in their e-mail?

[To Southwest's credit, they did NOT include a credit card number in the e-mail.]

Drew Dean, Computer Science Laboratory, SRI International

✶ When e-commerce and poor translation meet... terrorism?

<bo025@freenet.carleton.ca (Harry Neumann)>

Sat, 04 Dec 2004 14:00:43 -0500 (EST)

I was recently looking to purchase some items from an online grocer in Germany, www.lila-se.de, which offers service in both English and German. Everything seemed relatively straightforward until I examined the section labelled "Shipping Cost Informations". Zone 1 countries and regions were listed as follows:

(from the English-language part of the site)

Generally Shipping Costs for Delivery Zone 1 (EU)
Zone 1 - EU(European union) Andorra, the Azores, Belgium, Denmark, Faeroer (DK), Finland, France, Greece, Greenland, Great Britain (inclusive Isle OF one), Guernsey, Ireland, Italy, jersey, Korsika, Liechtenstein, Luxembourg, larva Irish Republican Army, Monaco, the Netherlands (Holland), Northern Ireland, Austria, Poland, Portugal,

San Marino, Sweden, Switzerland, Slowakei, Spain (inclusive Balearen),
Tschechien, Vatikanstadt.

vs. the German version (listed under "Versandkosten")

Zone 1 - EU (Europäische Union) Andorra, Azoren, Belgien, Dänemark,
Färöer (DK), Finnland, Frankreich, Griechenland, Grönland, Großbritannien (inklusive Isle of Man), Guernsey, Irland, Italien,
Jersey, Korsika, Liechtenstein, Luxemburg, Madeira, Monaco, Niederlande (Holland), Nordirland, Österreich, Polen, Portugal, San
Marino, Schweden, Schweiz, Slowakei, Spanien (inklusive Balearen),
Tschechien, Vatikanstadt.

Note the entry in the English-language page: "larva Irish Republican Army",
between Luxembourg and Monaco. This is definitely a puzzle until one looks
at the corresponding entry on the German page: Madeira. What presumably has
happened is that the word "Madeira" has been split in two for some reason,
becoming "Made" and "ira". Then "Made" was translated, becoming "larva",
whereas "ira" was not translated but expanded to become "Irish Republican
Army.". (Why other place names were not subjected to this treatment remains
a mystery).

Three risks (at least):

1) The usual hazards of doing a literal, contextless translation, magnified
by an unexplained parse-split-translate procedure, leading to a result
that, in this case, can be described without exaggeration as "weird" (not
to mention inaccurate).

2) That a potential customer will see these idiosyncratic translations and

assume that they're just the tip of the iceberg in terms of sloppiness,
and take his or her business elsewhere.

3) While no reasonable person will see this site as "terrorist-related"

there's a real risk that blocking software could spot the phrase "Irish

Republican Army", and categorize this site as "Political Extremism-related", for no evident reason. The RISKS to even cautious

web-surfers living under authoritarian regimes, of accidentally viewing

"Political Extremism" sites need no further explanation.

⚡ Job posting follies

<Stephen Cohoon <risks@cohoon-tx.com>>

Mon, 29 Nov 2004 17:15:25 -0600

While perusing some job posting web sites I found an interesting commentary.

I suspect the comments are intended for either in-house or external recruiters who just posted it using select-all copy & paste resulting in text that probably was not intended for public view. Particularly the set of competitors to raid.

Required: C Plus Plus; Perl; Network Protocols; Linux; TCP/IP;
Yes I will

notify you guys in the case that anything else even gets warm.
Right now I

don't even have any other recruiters working on this but that may change

by the end of the week. Companies to Pinpoint Recruit from include: <List of competing companies> (my former boss at <one of the competitors> is now the VP of Engineering here)

✶ Re: New Standards for Elections ([RISKS-23.59](#))

<"Atom 'Smasher'" <atom@suspicious.org>>
Wed, 10 Nov 2004 02:06:21 -0500 (EST)

> 7. Accurate and transparent voting roll purges.

or doing away with purges... if convicted felons are allowed to write the proprietary software that the machines run and manage the company that manufactures the machines
<<http://www.blackboxvoting.com/modules.php?name=News&file=article&sid=132>>,
then convicted felons should be allowed to use the machines.

> 11. An end to minority vote suppression, disenfranchisement, harassment,
> dirty tricks.

to a large extent, it can be argued that purging voters *is* a form is suppression, disenfranchisement, harassment, and dirty tricks. purging felons from voting roles was devised as a "jim crow" law, and it can be argued that jim crow is still proud of it.

this article
<<http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/20040708/COLUMNIST36/407080376>>
points out how the purge can be used as a precision weapon in

the war
against democracy.

✶ Re: new standards for elections; voting anomalies ([RISKS-23.59](#))

<"J.E. Cripps" <cycmn@nyct.net>>
Wed, 10 Nov 2004 04:59:04 -0500 (EST)

Regarding the summary of the NYT editorial, I do not see any requirement that voters be citizens of the U.S. or any identification requirement.

[Citizens, yes. That is understood. Identification? It varies from place to place, and is seriously abused in some, one way or the other.
PGN]

Appalled as I am at the allegations regarding the 2004 elections, I do not think that these .orgs address all the anomalies. For example:

Laying the Groundwork: A Study Of Voter Registration In Missouri
<http://cf.townhall.com/linkurl.cfm?http://www.centerforethics.org/VoterRegistrationStudy.htm>

Moreover, a more fundamental threat was not addressed in the editorial at all. Both parties are at fault here, recalling the Bush amnesty:

Carrying out the Mandate: Get Borders and Illegal Immigration Under Control
<http://cf.townhall.com/linkurl.cfm?http://www.humaneventsonline.com/article.php?id=5718>

As PGN stated in an earlier issue of RISKS:

[including] the actual casting of ballots and the creation, evaluation, certification, testing, and maintenance of voting equipment. But it also includes the registration of voters; identification, authentication, and challenging of voters; creation of the actual appearance of ballots and setting up the voting machines; distribution and handling of ballot and polling-place information, absentee ballots, and especially provisional ballots; processing of ballots; tabulation and collection of results; and proper assurance that voters' ballots are treated with adequate respect for privacy -- along with oversight of each of the steps in the entire process. comp.[risks 23.58](#), November 4, 2004, (emphasis added)

Many of these are not matters of technology (rushing a polling place in the last minutes) but surely fall within the ambit of comp.risks. But if either major party has consistently addressed any of these, I've missed it.

I find the Democratic inattention to the deficiencies of the 2004 technologies before election very perplexing.

Appalling as the allegations which have appeared in sources quoted on this list are (some of which find corroboration in the RISKS archives), I am afraid that the proposals, laudable as many of them are, in the NYT editorial insufficient.

More on the electoral process

<"J.E. Cripps" <cycmn@nyct.net>>
Wed, 10 Nov 2004 05:10:40 -0500 (EST)

Here's another longstanding anomaly:
Nearly 50,00 duplicate registrations: Florida Redux?
<http://www.eagleforum.org/column/2004/oct04/04-10-27.html>

Here's a Republican warning about technological deficiencies, in
May:
Don't Let Judges Jimmy Elections
<http://www.eagleforum.org/column/2004/may04/04-05-12.html>

The most serious risk: The Scam of Voting by Noncitizens and
Felons
<http://www.eagleforum.org/column/2004/aug04/04-08-18.html>

If this isn't fixed, the system will be broken.

More predictions of the current debacle, from someone with
first-hand experience as a local office candidate:
<http://www.NewsWithViews/Devvy/kidd72.htm>

Mark my words: We will never know the true vote count next month
no matter
how many times the ballots are run through a machine or how many
lawsuits
the Democrats file against the Republicans and visa versa. ...

As someone who has run for public office, put their whole heart
into the
effort, along with all the volunteers and the financial
generosity of so
many, I would rather have waited four or five days for a real
vote count
than be cheated. I don't want election results at the speed of a
button, I
want a true vote count. ...

A must is to get rid of the insidious Motor Voter Law of 1993.
All states of
the Union must purge their voting rolls and start over from

scratch. There is a two year period between elections. That's more than enough time for anyone who has a real desire to vote, to obtain a certified birth certificate and personally get down to the county clerk's office to register. If someone can't find those few minutes over a two year period, then fine, keep them out of the voting booth.

⚡ Voter touch-screen no good? Here's a pen!

<"Joel Garry" <joelgarry@anabolicinc.com>>

Mon, 8 Nov 2004 17:26:09 -0800

As I write this, the extremely close vote for mayor of San Diego is still up in the air. From http://www.signonsandiego.com/uniontrib/20041107/news_lm7frye.html :

"But she clearly benefited from the unusual technical aspects of this election. Because of problems in the March primary with a touch-screen voting system, the county shifted to optical-scan ballots, which required voters to fill in bubbles next to their choices. That meant all voters were handed a pen when they got their ballot, a remarkable turn of luck for Frye."

This highlights a risk of computerized voting: More difficult to write in a candidate, and conversely, if a fallback system is used, that can stimulate a change in vote. Also, the web page that shows the results

<http://www.sdcounty.ca.gov/voters/Eng/Eindex.html> is a bit difficult to figure out the vote tally, whoever wrote it didn't seem to consider the possibility of a write-in - so there is a separate link to see the slowly increasing Frye vote, as opposed to the regular candidates and "write in."

[Re: Is Windows up to snuff for running our world? \(Bean, RISKS-23.59\)](#)

<Sander Tekelenburg <tekelenb@euronet.nl>>

Tue, 9 Nov 2004 22:29:56 +0100

> Apple is missing out on a huge market here by not allowing their OS to run
> on other vendors' hardware. Nobody's going to buy a Mac to run an ATM or a
> cash register, but they might buy the OS if they thought it would work
> better.

Apple being wrong about not letting their OS run on non-Apple hardware is an age-old argument. The age-old counter argument is that part of the quality of Apple's OS is the fact that Apple controls the hardware. That gives them an enormous advantage when it comes to guaranteeing some level of quality to customers. Without it, when Mac OS X would have to run on any (and *cheap*) third-party hardware, Apple cannot guarantee the hardware quality, customers with crappy hardware will blame Apple for problems, Apple loses its name of offering quality products.

If you want quality, you need to be willing to pay for it. It's that simple.

It seems Apple understands that.

Of course that doesn't mean some enterprising bank could not try to get

Apple interested in working together on building ATM hardware running Mac OS

X. Steve Jobs might like the challenge. But it seems to me that something

like Mac OS X is way overkill for an ATM machine... Possibly Darwin. But

then there's other BSDs too to choose from.

Sander Tekelenburg, <<http://www.euronet.nl/~tekelenb/>>

✶ Deworming the Internet: addressing computer security market failure

<"Douglas Barnes" <salguod@mail.utexas.edu>>

Sat, 20 Nov 2004 10:38:15 -0600

I thought RISKS folks might be interested in a paper I've written which is just now available on SSRN. In part it's a response to the periodic calls for "liability" (notably from Bruce Schneier) as a mechanism for solving computer problems. The upshot is that I think Bruce is right that there is a need for a regulatory response, but that extending, say, tort liability to software would be a disaster. In addition to my more complicated law & economics argument for why this is, I point out in passing that ordinary tort liability could crush open source software, which has the

potential to act as a positive force in addressing the underlying market failure.

Douglas Barnes <http://www.salguod.com>

Abstract:

Both law enforcement and markets for software standards have failed to solve the problem of software that is vulnerable to infection by network-transmitted worms. Consequently, regulatory attention should turn to the publishers of worm-vulnerable software. Although ordinary tort liability for software publishers may seem attractive, it would interact in unpredictable ways with the winner-take-all nature of competition among publishers of mass-market, internet-connected software. More tailored solutions are called for, including mandatory "bug bounties" for those who find potential vulnerabilities in software, minimum quality standards for software, and, once the underlying market failure is remedied, liability for end users who persist in using worm-vulnerable software.

<http://papers.ssrn.com/abstract=622364>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 62

Tuesday 21 December 2004

Contents

- [Flaw in Google's New Desktop Search Program](#)
[John Markoff via Jim Schindler](#)
- [A chess-playing "bankomat"](#)
[Lothar Kimmeringer](#)
- [GPS Shutdown "during national crisis"](#)
[Jim Youll](#) [Atom 'Smasher'](#)
- [French motorist obeys GPS navigation, makes U-turn into traffic](#)
[Peter G Capek](#)
- [Colorado welfare system computer problems](#)
[Mike A](#)
- [Automated medication worse than the disease?](#)
[NewsScan](#)
- [Strange S&P numbers](#)
[Dawn Cohen](#)
- [Judge slams spammers with \\$1-billion judgment](#)
[NewsScan](#)
- [Unintended effects of RFID devices](#)
[Paul Wallich](#)
- [Medical records-sharing in Massachusetts](#)
[NewsScan](#)

- [Satellite TV broadcast pirated](#)
[Erling Kristiansen](#)
 - [Live television banner hacked](#)
[Matthew Schie](#)
 - [ATM spits out Canadian Tire "money"](#)
[Paul Schreiber](#)
 - [New browser vulnerability targets non-IE models, too](#)
[NewsScan](#)
 - [Re: When e-commerce and poor translation meet... terrorism?](#)
[Ulf Lindqvist](#)
 - [Re: Is Windows up to snuff for running our world?](#)
[Ben Galehouse](#)
 - [Re: More on the electoral process](#)
[D.F. Manno](#)
 - [Screensaver tackles spam websites](#)
[Amos Shapir](#)
 - [Freeze on anti-spam campaign](#)
[Amos Shapir](#)
 - [Re: ACM Needs Your Feedback](#)
[James Garrison](#)
 - [Increasing sophistication of phishing spammers](#)
[Jonathan de Boyne Pollard](#) [Dan Wallach](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ **Flaw in Google's New Desktop Search Program**

<"Jim Schindler" <Jimschin@pacbell.net>>

Mon, 20 Dec 2004 00:25:13 -0800

John Markoff, Rice University Computer Scientists Find a Flaw in Google's

New Desktop Search Program, *The New York Times*, 20 Dec 2004

[PGN-ed]

<http://www.nytimes.com/2004/12/20/technology/20flaw.html>

Prof. Dan Wallach and two of his students at Rice University discovered a potentially serious security flaw in the desktop search tool for personal computers that was recently distributed by Google. The flaw could permit an attacker to secretly search the contents of a personal computer via the Internet, and is referred to as a composition flaw -- a security weakness that emerges when separate components interact. Dan Wallach said, "When you put them together, out jumps a security flaw. These are subtle problems, and it takes a lot of experience to ferret out this kind of flaw."

✂ A chess-playing "bankomat"

<Lothar Kimmeringer <lothar@kimmeringer.de>>

Wed, 08 Dec 2004 21:24:44 +0100

In German banks you find more and more machines, where you can check your account's balance and do money-transfers. To be able to do this, there is a keyboard available instead of the 11+4 keys for the standard-cash-points.

It seems that the program running on these machines is a simple window and that it's possible to get the underlying "desktop" with "clicking" (the screen is a touchscreen) onto the corresponding place where the minimize-icon resides. Thanks to the available keyboard it's possible to do everything you're used to do with every other computer with a shell.

Somebody took the opportunity to play a little bit around with these machines and documented everything with a digital camera.

The pictures can be watched at

<http://www.ulm.ccc.de/projekte/bankomat/>

where the machine ends with a game of chess against itself running

instead of the application originally intended to be run on it.

Lothar Kimmeringer

E-Mail: spamfang@kimmeringer.de

✶ GPS Shutdown "during national crisis"

<Jim Youll <jim@agentzero.com>>

Thu, 16 Dec 2004 10:51:29 -0500

Just consider how much of our world now relies on GPS for ordinary day-to-day operation... what if it just "went away" during a time of crisis?

The EU has been planning its own version of GPS called Galileo... progress was hampered for years by all sorts of bickering, but the project recently announced that deployment would happen by 2006. The threat of a US GPS shutdown may motivate that project, but Galileo is already bound up in agreements with the Americans and would probably be turned off as well in cooperation, via NATO, on American orders... all this so "terrorists" can't... I'm not sure what terrorists do with GPS that they can't do without GPS.

On the bright side, I guess times of national crisis will also be free days on the GPS-metered toll roads now being tested in Oregon and elsewhere.

This seems like a great example of the sort of "solution" that turns a regular-size crisis into an impressively crippling crisis. I don't understand why reinstating Selective Availability isn't considered an option this time. [It dumbs down the accuracy, and was stopped by President Clinton in 2000. PGN]

President Bush has ordered plans for temporarily disabling the U.S.

network of global positioning satellites during a national crisis to prevent terrorists from using the navigational technology. He also

instructed the Defense Department to develop plans to disable, in certain

areas, an enemy's access to the U.S. navigational satellites and to

similar systems operated by others. The European Union is developing a

\$4.8 billion program, called Galileo.

The military increasingly uses GPS technology to move troops across large

areas and direct bombs and missiles. Any government-ordered shutdown or

jamming of the GPS satellites would be done in ways to limit disruptions

to navigation and related systems outside the affected area, the White

House said.

[Source: Ted Bridis, Bush prepares for possible shutdown of GPS network in

national crisis The Associated Press, 15 Dec 2004, excerpted]

<http://www.securityfocus.com/news/10140>

[http://cnn.netscape.cnn.com/ns/news/story.jsp?](http://cnn.netscape.cnn.com/ns/news/story.jsp?id=2004121521290001739682&dt=20041215212900&w=APO&coview=)

[id=2004121521290001739682&dt=20041215212900&w=APO&coview=](http://cnn.netscape.cnn.com/ns/news/story.jsp?id=2004121521290001739682&dt=20041215212900&w=APO&coview=)

GPS Shutdown "during national crisis"

<"Atom 'Smasher'" <atom@suspicious.org>>

Mon, 20 Dec 2004 01:59:12 -0500 (EST)

Great... if there's another 9/11, they can turn off GPS so the "terrorists" can't use the system. of course, if there's another 9/11, the terrorists will be dead before we know what happened. that will leave police, fire, rescue, 911, red cross, air traffic, media, utility workers, etc all left without their bearings, since they rely heavily on consumer-grade GPS receivers. this is just brilliant.

But why stop there? how about turning off all cell phones, land-lines, Internet connections, electricity and water? we don't want terrorists to be aided by any of these things immediately following an attack. [...]

French motorist obeys GPS navigation, makes U-turn into traffic

<Peter G Capek <capek@us.ibm.com>>

Fri, 3 Dec 2004 08:28:32 -0500

A 78-year-old driver, on a 130 km/h road near Nancy, and not realizing the

limitations of the navigation system, turned around when instructed to do so. He and the occupants of the car he collided with were, amazingly, unhurt. Police said this wasn't the first such incident they'd experienced.

[Source: News Interactive at http://www.news.com.au/common/story_page/0,4057,11553850%255E15306,00.html]

Peter G. Capek, IBM Thomas J. Watson Research Center,
Yorktown Heights, NY 10598-0218 (+1 914) 945-1250

[Maybe that's a reason why GPS should be turned off? PGN]

✶ Colorado welfare system computer problems

<mikea <mikea@mikea.ath.cx>>
Wed, 8 Dec 2004 14:20:47 -0600

On the National Public Radio program "Morning Edition" this morning, a story by Elaine Korry on how, "Due to a crashed computer network, Colorado is unable to distribute Medicaid and welfare benefits this holiday season. Food banks are picking-up the slack."

According to the story, numerous benefit applications are still waiting to be processed after the Federally-mandated 30 day processing deadline, and food banks are serving unprecedented numbers of households: one food bank served 157 in one day, where their typical monthly load has been about

150.

⚡ Automated medication worse than the disease?

<"NewsScan" <newsscan@newsscan.com>>

Tue, 21 Dec 2004 07:57:23 -0700

A report from U.S. Pharmacopeia (USP), a nonprofit group that sets standards for the drug industry, says that as more hospitals have implemented automated systems for administering drugs the number of errors associated with them has risen. USP vice president Diane Cousins says, "It would seem logical that applying computer technology to the medication use process would have a significant positive impact in preventing medication errors. Yet, depending on the computer's design or user competence, new points of potential errors can emerge." Kenneth Kizer of the National Quality Forum agrees with Cousins: "Technology offers great opportunity to reduce errors, but it's not a panacea. You can't just throw a computerized system in and expect that everything's fixed. It has to be done right. The technology is only as good as the people who use it." [*The Washington Post*, 20 Dec 2004; NewsScan Daily, 21 Dec 2004]
<<http://www.washingtonpost.com/wp-dyn/articles/A15178-2004Dec20.html>>

⚡ Strange S&P numbers

<"Cohen, Dawn" <dcohen@ets.org>>

Tue, 21 Dec 2004 17:11:13 -0500

I just checked Yahoo's finance website and was rather surprised to learn that the S&P had fallen nearly 870 points today. I thought perhaps it was a Yahoo issue, but I also checked the Fidelity web site and found the same numbers. So either a very strange anomaly has occurred causing S&P to lose 73% of its value while the Dow and Nasdaq gained 1% OR something's gone funny in some database or application that reports S&P numbers.

I have screen shots.

I'm a RISKS reader. I'm voting for database corruption or data entry issue.

✶ Judge slams spammers with \$1-billion judgment

<"NewsScan" <newsscan@newsscan.com>>

Mon, 20 Dec 2004 11:47:08 -0700

A federal judge in Iowa has awarded a small ISP more than \$1 billion in damages in what's believed to be the largest judgment ever against spammers. The case was brought by Robert Kramer, whose company provides e-mail service to about 5,000 customers, and who filed suit after his inbound mail servers were jammed with as many as 10 million spam-mails a day in 2000. Citing federal racketeering laws (RICO) and the Iowa Ongoing

Criminal Conduct Act, U.S. District Judge Charles R. Wolle
ordered AMP

Dollar Savings of Mesa, Ariz., to pay \$720 million; Cash Link
Systems of

Miami, Fla., \$360 million; and TEI Marketing Group, also of
Florida,

\$140,000. "It's definitely a victory for all of us that open up
our e-mail

and find lewd and malicious and fraudulent e-mail in our boxes
every day,"

said Kramer, who is unlikely to ever collect on the judgments.

[AP/*Wall

Street Journal*, 20 Dec 2004; NewsScan Daily, 20 Dec 2004]

<http://online.wsj.com/article/0,,SB110349923676804327,00.html>

(sub req'd)

✶ Unintended effects of RFID devices

<Paul Wallich <pw@panix.com>>

Tue, 07 Dec 2004 20:41:48 -0500

(or has this been done already?)

As anyone who has recently become a parent knows, hospitals are
very serious

about making sure that no one leaves the premises with a baby
not their

own. RFID anklets on the infant, combined with RFID scanners and
existing

magnetic locks on maternity-ward doors seem like a good idea:
chipped

infants can't leave, and only Authorized Personnel can remove
the chips.

RFID is no respecter of walls, so a strategically placed baby in
the nursery

can effectively lock down the maternity-ward exit until someone
figures out

why the doors aren't opening -- which could be anywhere from a few minutes to an hour or more. In a real emergency, the magnetic locks of course fail open, but there are plenty of other urgent situations where not being able to open the maternity-department doors (and not knowing why) could complicate hospital operations significantly.

This isn't exactly an unintended effect, since the system is operating exactly as intended (baby within range of RFID door scanner yields non-opening door), but rather an imprecise specification ("within range" doesn't mean what the implementors thought it meant). As RFID-based security becomes more common, it will be interesting to see just how many more such snafus crop up.

Medical records-sharing in Massachusetts

<"NewsScan" <newsscan@newsscan.com>>
Tue, 07 Dec 2004 08:31:37 -0700

If a new Massachusetts "eHealth" pilot project is successful, physicians in that state will be able to access patients' records from any hospital or clinic by computer. Gov. Mitt Romney says that switching from paper records to easily shared electronic records could save the state millions of dollars while improving patient safety and quality of care. He has given assurances that the system will have strict controls to allow patients to control who

sees their records. [AP/*Los Angeles Times*, 7 Dec 2004;
NewsScan Daily, 7
Dec 2004]

[http://www.latimes.com/technology/ats-
ap_technology14dec07,1,1268455.story?coll=sns-ap-toptechnology](http://www.latimes.com/technology/ats-ap_technology14dec07,1,1268455.story?coll=sns-ap-toptechnology)
[http://www.latimes.com/technology/ats-
ap_technology14dec07,1,1268455.story](http://www.latimes.com/technology/ats-ap_technology14dec07,1,1268455.story)
?coll=sns-ap-toptechnology

✶ Satellite TV broadcast pirated

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>
Tue, 21 Dec 2004 21:12:27 +0100

According to *Space News*, 29 Nov 2004, a TV broadcast via the AsiaSat satellite was pirated for 4 hours on 20 Nov. A broadcast targeted at mainland China was superseded by an unknown source transmitting a signal with higher power than the legitimate programme towards the satellite transponder, thus replacing the intended programme . The pirate broadcast concerned the Falon Gong spiritual organization that is outlawed in China.

The source of the pirate signal is unknown, but is believed to originate in Taiwan. (Is this a political or a technical assessment??)

Calculations by AsiaSat suggest that the signal could be generated by a 250 Watt transmitter on a 4.5-meter dish, or 100 Watt on a 7-meter dish. Such capabilities are quite standard in medium-sized Earth stations.

AsiaSat eventually decided to switch off the transponder for

some hours.

The pirate signal was gone when the transponder was re-started.

This event underscores the vulnerability of, in this case, satellite TV broadcast. But similar attacks could be launched on many other types of (satcom) services. The equipment needed is commercially available and within financial reach of even rather small organizations. The attack can be launched from anywhere within the footprint of the satellite which, in most cases, includes neighbouring countries, some of which may be less than friendly.

At least with bent-pipe satellites ("dumb" transponders that receive and re-broadcast anything within their frequency band), the most common technology today, very few defenses exist against such attacks. Also, locating the perpetrator is difficult since the signal is transmitted upwards in a highly directive beam and therefore is undetectable at ground level unless you are very close to the transmitter.

QinetiQ of Britain claim to have a method to determine the position of a transmitting station by comparing the signal with weaker copies of the same signal transponded through nearby satellites. Little detail of their satID system is given in the article.

Live television banner hacked

<Matthew Schie>

Tue, 30 Nov 2004 12:34:26 -0500 (EST)

A television station in Raleigh, North Carolina (U.S.A.) created a Web interface so local businesses could submit closure information during inclement weather. Although participants had to register and receive human approval, there was apparently no further review of the submissions before they appeared on-air. Judging from the screenshots the hack went on for many hours before being discovered.

Gallery

<http://www.networksynapse.net/gallery/News14?page=1>

Discussions

<http://www.securityfocus.org/news/8191>

<http://www.lostremote.com/archives/000366.html>

⚡ ATM spits out Canadian Tire "money"

<Paul Schreiber <shrub@mac.com>>

Thu, 2 Dec 2004 10:43:29 -0800

<http://www.cbc.ca/story/canada/national/2004/12/01/CanadianTire-ATM.041201.html>

[For the non-Canadians out there, an intro to Canadian Tire money:

<http://www2.canadiantire.ca/CTenglish/ctmoney.html>]

A CIBC cash machine at a mall near Moncton, New Brunswick, Canada dispensed an assortment of 11 Canadian Tire bills in denominations ranging from 10 cents to \$2 instead of legitimate Canadian cash. The bogus cash

reportedly
must have originated from business customers. [Source: CBC.CA,
2 Dec 2004]

✶ New browser vulnerability targets non-IE models, too

<"NewsScan" <newsscan@newsscan.com>>

Tue, 30 Nov 2004 09:06:22 -0700

Since its debut, Microsoft's Internet Explorer browser has been plagued by a steady stream of "flaw discovery" announcements followed by the requisite patches. Usually those flaws are exclusive to the Microsoft model, but a new vulnerability also affects the Mozilla Browser, Mozilla Firefox, Opera and Apple Safari browsers. This latest bug, called the Infinite Array Sort Denial of Service Vulnerability, causes the affected browsers to execute an infinite JavaScript array sort, which in turn causes a crash. The flaw was discovered by independent security researcher Berend-Jan Wever, who also uncovered the IFRAME vulnerability that affects banner ads. [*InternetNews*, 29 Nov 2004; NewsScan Daily, 30 Nov 2004]
<http://www.internetnews.com/security/article.php/3440971>

✶ Re: When e-commerce and poor translation meet... terrorism?

<Ulf Lindqvist <ulf.lindqvist@sri.com>>

Thu, 9 Dec 2004 09:15:48 -0800 (PST)

(Harry Neumann, [RISKS-23.61](#))

I pasted the German version into three free translator sites:
Google Language Tools http://www.google.com/language_tools?hl=en
Altavista Babelfish <http://babelfish.altavista.com/babelfish/tr>
Freetranslator <<http://freetranslation.com/>>

Google gives the same English version as the one Harry Neumann had noted, so that is probably what was used. Altavista's result is just as weird except for "Vatican city", while Freetranslator seems to do a much better job (although not perfect).

> (Why other place names were not subjected to this treatment
> remains a mystery).

It seems like some of them were:

Isle of Man -> Isle of one

Jersey -> jersey (lower case indicates clothing, not island or cow)

Ulf Lindqvist, Computer Science Laboratory, SRI International

⚡ Re: Is Windows up to snuff for running our world?

<Ben Galehouse <bgalehouse@spamcop.net>>

Wed, 8 Dec 2004 23:37:16 -0500

I have always assumed that the tendency to use Windows for everything stems from a perception that development is less expensive for the more standard systems. This perception might even be correct. However, I'm not sure I'd want a programmer who couldn't learn a new environment writing a glass cockpit, and I have seen Windows based glass cockpits advertised.

Recently, several people have mentioned using OS X, and now other BSD derivatives for special purpose turnkey systems such as ATMs. The basic quality might be higher, but these general purpose projects still spend a lot of time developing and adding features irrelevant here. It seems to me that the QNX and its competitors are meant for such applications and would have serious advantages. I'd especially expect more stability and better long term support.

✶ Re: More on the electoral process

<"D.F. Manno" <dfm2a3l0t2@spymac.com>>

Thu, 09 Dec 2004 20:44:23 -0500

In [Risks Digest 23.61](#), "J.E. Cripps" <cycmn@nyct.net> wrote:

> If someone can't find those few minutes over a two year
> period, then fine,
> keep them out of the voting booth.

I don't know about your neck of the woods, but here in Pennsylvania, USA, we have elections in April and November of every year. I don't think six months is sufficient time to overhaul the electoral process in the way you suggest.

By the way, your suggestion would disenfranchise me. Since I'm disabled and homebound, I would be unable to present my birth certificate in person at the office of the Board of Elections.

✶ Screensaver tackles spam websites

<"Amos Shapir" <amos083@hotmail.com>>

Tue, 30 Nov 2004 11:38:15 +0200

I found the following on the BBC's site. The RISK here is, of course, did Lycos take care of all the (mainly legal) aspects of such a sponsored DoS attack against spammers? Knowing how spammers work, they would either find a way to make someone else pay for their increased bandwidth, or sue Lycos for lost revenues (or both). After all, the targeted sites are probably quite legal, and it may be easier to associate the attacking screensavers with Lycos, than to associate the targeted sites with the spam that advertises them.

A screensaver targeting spam-related websites could help drive spammers out of business.

Full story:

<http://news.bbc.co.uk/go/em/-/2/hi/technology/4051553.stm>

✶ Freeze on anti-spam campaign

<"Amos Shapir" <amos083@hotmail.com>>

Sat, 04 Dec 2004 11:54:50 +0200

It seems that what I had predicted just 2 days ago has already

happened;
again from the BBC's site:

A controversial anti-spam campaign by Lycos Europe appears to have been put on hold.

Full story:

<http://news.bbc.co.uk/go/em/-/2/hi/technology/4065751.stm>

✶ Re: ACM Needs Your Feedback

<James Garrison <jhg@athensgroup.com>>

Tue, 07 Dec 2004 14:53:56 -0600

I received the following today. My response is below.

acmsurvey@acm.org wrote:

> Dear ACM Member,

>

> We are redesigning parts of the acm.org website to make it more member-friendly, informative, and easily navigable, and we would like your

> assistance in this effort.

>

> You can help us by taking a moment to complete our ACM website survey

> located at:

> <http://www.surveymonkey.com/s.asp?u=71148761076>

>

> The survey should take no more than 10 minutes to complete, and your

> answers will be kept confidential and considered only in aggregate

> form. Your participation will help us to identify ACM's most valuable

> content and functionality, and at a later time, you will also have the

> opportunity to provide feedback on actual suggested website

redesigns.

Are you aware that this request is indistinguishable from a phishing scam?

The link you provide is NOT within the acm.org domain, and the message is

not authenticated (i.e., in PGP-signed). My guess is it's probably

legitimate, but you are contributing to the problem by not making it

possible for recipients to unambiguously distinguish this from phishing. I

continue to be extremely disappointed by ACM's apparent ivory-tower

unawareness of what actually goes on in the real world.

[Increasing sophistication of phishing spammers \(Wallach, RISKS 23.60\)](#)

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

Wed, 01 Dec 2004 12:42:50 GMT

W> eBay and similar companies should eliminate these public
W> servers that serve up static images for e-mail and should pay
W> attention to referrer information to refuse images being sent
to

W> 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).

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: Increasing sophistication of phishing spammers ([RISKS-23.60](#))

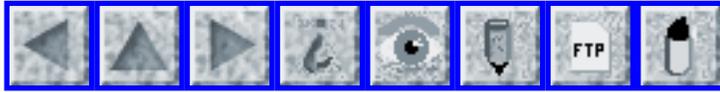
<Dan Wallach <dwallach@gmail.com>>
Mon, 29 Nov 2004 20:15:57 -0600

> JIM HORNING responded: I also suspect that we are probably
going to have
> to give up the use of html in e-mail.

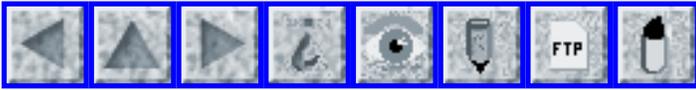
I seem to get an awful lot of legitimate HTML e-mail. I don't

think that

HTML is the problem. My hope is that some of the "low hanging fruit" (e.g., servers like static.ebaypics.com) can be fixed, at least increasing the marginal cost of business for spammers. These guys are all about thin marginal profits multiplied by huge numbers of messages. If you can make those messages even a little more expensive, you hurt the spammers.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 63

Sunday 26 December 2004

Contents

- [Patients not notified due to computer glitch](#)
[Jim Bruce](#)
- [Comair cancels all flights 25 Dec](#)
[Jeremy Epstein](#)
- [Restarting a reactor with a flawed part](#)
[Ken Knowlton](#)
- [Wrong braking algorithm causes trains to overrun stops](#)
[Mark Brader](#)
- [Banksys solves cash card mystery](#)
[David Kennedy](#)
- [Y2K? Never heard of it...](#)
[Dag-Erling Smørgrav](#)
- [The new NASA calendar](#)
[Tom Nimitz](#)
- [Flaw in Google's New Desktop Search Program](#)
[John Markoff](#)
- [Windows into the world](#)
[Monty Solomon](#)
- [The Graphing Calculator Story](#)
[Ron Avitzur](#)
- [Why adding more security measures may make systems less secure](#)
[Don Norman](#)

- [Re: GPS Shutdown "during national crisis"](#)
[Pat Place](#)
 - [Re: Unintended effects of RFID devices](#)
[cogg](#)
 - [Re: Strange S&P numbers](#)
[Dawn Cohen](#)
 - [Re: Whites Only websites?](#)
[Jonathan de Boyne Pollard](#)
 - [Software Engineering for Secure Systems: SESS05](#)
[Gene Spafford](#)
 - [REVIEW: "Network Security Hacks", Andrew Lockart](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Patients not notified due to computer glitch

<Jim Bruce <jim.bruce@sympatico.ca>>

Wed, 22 Dec 2004 09:16:19 -0500

The *Toronto Sun* reported this morning that a computer bug is being blamed for the fact that over 14,000 radiology reports were not printed and sent to doctors. This occurred at a newly built hospital in the Montreal area from 7 Jan 2004 until 17 Dec 2004! The reports were not destroyed, but because they were never printed, doctors did not follow up with the patients. The reports included abnormal radiology results, so some patients may have cancer and not know it.

I suspect that most patients assumed that if they heard nothing then there was nothing to worry about.

<http://www.canoe.ca/NewsStand/TorontoSun/News/2004/12/22/793248-sun.html>

[Taj Khattrra noted that the same article referred to the health

status of
579 Quebec patients.]

✈ Comair cancels all flights 25 Dec

<Jeremy Epstein <jeremy.epstein@cox.net>>
Sat, 25 Dec 2004 20:43:48 -0500

CNN reports that "Comair, which flies an average of 30,000 people per day, called off all 1,160 daily flights for both Saturday and Sunday. It will resume a limited schedule Monday, Comair spokesman Don Bornhorst said. The computer system Comair uses to book pilots for flights broke down, he said. Comair could not pinpoint a reason for the computer crash and could not say why there was no backup system." [Comair flies flights in the eastern and midwest US as Delta Express.]

<http://www.cnn.com/2004/TRAVEL/12/25/flights.canceled/index.html>

Comair's web page admits that they are "currently experiencing computer problems, resulting in cancellation of flights through December 26th, 2004. This includes, but is not limited to, flights to/from Cincinnati, Ohio."

We shouldn't be surprised that computer failures (whether hardware, software, a combination, or something else) is causing problems, but this is the first case I can recall where it's caused an airline to cancel *all* of their flights for days.

Between failures like this and the nasty weather in the midwest, I'm sure

glad to be home this holiday weekend!

[A short squib in the Palo Alto California Sunday *Daily News* noted that the 30,000 passengers span 118 cities, although *The New York Times* article said 119. Also of note were the USAir baggage-handling problems in Philadelphia, where an estimated 8 to 10 thousand luggage items piled up; USAir canceled 65 flights on Thursday, 176 on Friday, and 143 on Christmas Day, due to bad weather, sick baggage handlers in Philadelphia, etc. PGN]

✈ Restarting a reactor with a flawed part (via Ken Knowlton)

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

Wed, 22 Dec 2004 17:29:24 PST

Ken Knowlton noted an article by John Sullivan in *The New York Times* Metro Section, 12 Dec 2004 (PGN-ed here), that I somehow missed in my morning musing/newsing that day. Ken's comment: ``Here's a fantastic way to fix a serious technical problem: change the location of the sensors that have indicated it!''

Despite opposition, managers of the Salem nuclear power station (second largest in the U.S.A.) are planning to restart operations after discovery of a flaw in a critical recirculation pump first that helps cool three reactors, just south of Wilmington, Delaware. This flaw was first noted in April 2003, when it was noted that seals were wearing out

too rapidly. Then, in November 2004, an engineering team determined that the steel drive shaft was probably cracked -- and at certain speeds ``bangs like a freight train.'' New Jersey's top regulator (which has no regulatory role in Delaware) advises fixing the pump before restarting the shutdown Hope Creek reactor, which had to be shut down on 10 Oct 2004 because of a broken steam pipe. Sensors were added to the pump that showed lower vibration readings than historical records, although those sensors were in different places than those producing earlier diagnostics (which had previously showed an almost doubling in vibrations between 2000 and 2002!). The operators are concluding that the pump is now safe (without having had any repairs). The state regulators are recommending replacing the bent drive shaft, but the final decision is up to the U.S. Nuclear Regulatory Commission.

✶ Wrong braking algorithm causes trains to overrun stops

<msb@vex.net (Mark Brader)S>

Wed, 22 Dec 2004 14:46:00 -0500 (EST)

The December 2004 issue of "Modern Railways" reports a series of incidents with the Pendolino electric trains, which earlier this year began operating at 125 mph on the West Coast Main Line in England.

In one case, with the train moving at about 7 mph, the driver attempted a normal brake application to bring it to a stop just short of the end of

track as usual -- but it did not slow. By the time the emergency brake had been applied, there wasn't enough track left, and the train rammed the buffer stop at 4 mph. This was repeated a few days later. Another case involved a SPAD (signal passed at danger) after all axles on the leading car locked up as the train approached the red signal: the speedometer read 0 while the train was moving. The driver released and reapplied brakes, but could not stop in time.

As on many modern electric trains, the conventional friction braking on the Pendolino is supplemented by regenerative braking: the train's motors become generators, feeding much of its kinetic energy back into the power supply for use by other trains.

In this case the choice of braking mode is made by computer control. When the train is moving at speed, a normal command for brakes activates the regenerative braking first, with the friction brakes added as braking demand increases. But the train only has motors on 1/3 of its axles, so the regenerative braking is more prone to slipping in poor rail conditions, and it can take up to 6 seconds for the computer to balance everything and reach the desired braking level after a normal brake application. So at lower speeds, when even a light brake application might be intended to stop the train in a short distance, the friction braking is brought on immediately. (Presumably emergency braking also does this, although the article doesn't actually say.)

The manufacturer, Alstom, had used this "braking and traction

package"
successfully on other trains; the problem with the Pendolino (or
maybe just
with this particular version -- there are Pendolinos in other
countries) was
simply that the speed threshold for immediate friction braking had
been
lowered from 20 to 7 mph, and that was too low. It looks to me as
though
someone just didn't understand the way that trains are driven at
low speeds.

Rocket, 1829: The first 30 mph train. TGV-A, 1989: The first 300
mph train.

✶ Banksys solves cash card mystery

<David Kennedy CISSP <david.kennedy@acm.org>>

Sat, 18 Dec 2004 01:21:23 -0500

http://www.expatica.com/source/site_article.asp

?subchannel_id=24&story_id=14880&name=Banksys+solves+cash+card
+mystery
9 Dec 2004

Last weekend's catastrophic failure of bank card readers and
cashpoints
across Belgium was caused by a chain of small technical errors and
not a
computer virus, it has been discovered. "(A)n unfortunate sequence
of minor
hiccups in the internal Banksys system was aggravated by the large
number of
bank card payments made by shoppers."

220K bank card transactions failed as did 60K credit card
transactions
representing 20M Euros. Banksys announced that all transactions
will be
free on 18 December as a measure of consideration. "But it is

still denying
overall responsibility for the blunder."

David Kennedy CISSP Risk Analyst Cybertrust Corp.
<http://www.cybertrust.com>

✶ Y2K? Never heard of it...

<des@des.no (=?iso-8859-1?q?Dag-Erling_Sm=F8rgrav?=)>
Thu, 23 Dec 2004 11:27:50 +0100

According to www.lexpress.fr (the website of a leading French news magazine), today's date is Jeudi 23 décembre 104. The date is generated by the following snippet of ECMAScript:

```
var tj= new Array
("Dimanche", "Lundi", "Mardi", "Mercredi", "Jeudi", "Vendredi", "Samedi");
var tm= new Array("janvier", "f&eacute;
vrier", "mars", "avril", "mai", "juin", "juillet", "ao&ucirc;
t", "septembre", "octobre", "novembre", "d&eacute;
cembre");
d= new Date();
document.write( tj[d.getDay()] + " " + d.getDate() + " " + tm[d.
getMonth()] + " " + d.getYear()) ;
```

One wonders how long this has been so, and how much longer it will take before they realize that they need to add 1900 to the year (and start reading manuals).

Dag-Erling Smørgrav - des@des.no

✶ The new NASA calendar

<Tom Nimitz <tnimitz@cox.net>>
Tue, 21 Dec 2004 20:47:08 -0500

One of the Web sites I occasionally visit on the web is <http://spaceflight.nasa.gov/realdata/sightings/cities/index.cgi> -- which allows you to pick a city and find out when there will be an pass by the International Space Station. The site is updated weekly.

This week the header at the top of the pages reads "THE FOLLOWING ISS SIGHTINGS ARE POSSIBLE FROM MON DEC 20 TO SAT JAN 32".

Fortunately, the only a risk would be using the same logic for calculating a trajectory for landing a probe on Titan.

✂ Flaw in Google's New Desktop Search Program

<"Peter G. Neumann" <neumann@csl.sri.com>>
Mon, 20 Dec 2004 10:34:06 PST

Rice University Computer Scientists Find a Flaw in Google's New Desktop Search Program

By John Markoff, *The New York Times*, 20 Dec 2004
<http://www.nytimes.com/2004/12/20/technology/20flaw.html>
[Also noted by Jim Schindler; PGN-ed]

Rice University professor Dan Wallach and two of his graduate students, Seth Fogarty and Seth Nielson, have discovered a potentially serious security flaw in the desktop search tool for personal computers that was recently distributed by Google. The flaw could allow an attacker to clandestinely search your PC via the Internet. This is an example of a composition flaw, which results from putting two components together.

✶ Windows into the world

<Monty Solomon <monty@roscom.com>>

Fri, 24 Dec 2004 20:51:02 -0500

Researchers warn of multiple unpatched Windows holes;
Vulnerabilities could leave systems open to remote attacks

Paul Roberts, IDG News Service, 24 Dec 2004

Symantec Corp. warned its customers about a number of critical holes in Microsoft Corp.'s Windows operating system that surfaced late yesterday and that could make Windows systems vulnerable to compromise by remote attackers. Symantec acted after security researchers published the details of the heap overflow vulnerabilities in messages posted to online security news groups Thursday, including the Bugtraq mailing list, and on xfocus.net. The flaws affect most supported versions of Windows, but Microsoft has not yet issued a patch for the newly disclosed holes. Windows users are vulnerable to Internet based attacks until patches are issued, Symantec said.

<http://www.computerworld.com/securitytopics/security/holes/story/0,10801,98532,00.html>

Three Serious Windows Vulnerabilities Surface,
David Morgenstern, eweek.com, 24 Dec 2004

Symantec Corp.'s Security Response service on Friday confirmed that unpatched Windows vulnerabilities could pose a serious risk for exploits via malicious Web pages and e-mail messages. One of the three security vulnerabilities involves image handling—a source of recent exploits on Windows and Unix operating systems. The other two risks are found in the

Help system and in Window's ANI (Automatic Number Identification) authentication. Symantec said the Microsoft Windows LoadImage API Function

Integer Overflow Vulnerability could be exploited via browsers or e-mail

client software. Users who open an HTML message or Web page bearing the

image could face security risks. ...

<http://www.eweek.com/article2/0,1759,1745642,00.asp>

Exploits released for new Windows flaws

Robert Lemos, CNET News.com, 23 Dec 2004

A Chinese security group has released sample code to exploit two new unpatched flaws in Microsoft Windows. The advisory comes in the week before

Christmas, a time when many companies and home users are least prepared to

deal with the problems. Security firm Symantec warned its clients of the

vulnerabilities on Thursday, after the Chinese company that found the flaws

published them to the Internet.

One vulnerability, in the operating system's LoadImage function, could

enable an attacker to compromise a victim's PC when the computer displays a

specially crafted image placed on a Web site or in an e-mail. The other

vulnerability, in the Windows Help program, likewise could affect any

program that opens a Help file. ...

<http://news.com.com/2100-1002-5502534.html>

✶ The Graphing Calculator Story

<Ron Avitzur <avitzur@PacificT.com>>

Wed, 22 Dec 2004 02:20:21 -0800

This is an old story, but I've only told it in person before. Now that I've put it in print, I wanted to share it with other readers of Risks. I'll leave enumerating the risks as an exercise for the reader.

"It's midnight. I've been working sixteen hours a day, seven days a week. I'm not being paid. In fact, my project was canceled six months ago, so I'm evading security, sneaking into Apple Computer's main offices in the heart of Silicon Valley, doing clandestine volunteer work for an eight-billion-dollar corporation."

The story behind the Macintosh Graphing Calculator is at

<http://www.PacificT.com/Story>

✚ Why adding more security measures may make systems less secure

<"Don Norman" <norman@nngroup.com>>
Tue, 21 Dec 2004 22:07:45 -0800

In [RISKS-23.60](#), Peter Neumann recommended a paper by Scott Sagan entitled:

"The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security" <http://cisac.stanford.edu/publications/20274/>

I want both to second the recommendation and also to expand upon it. Many attempts by both experts and amateurs in the world of security and safety actually weaken their systems.

Sagan provided three major reasons why this might be so: I add a fourth. Sagan's three reasons were:

1. Common-mode problems. Adding redundancy only makes things more secure or safe if the new items are truly independent of the existing ones. They seldom are, and accident after accident demonstrates the common mode problem, where one accident takes out all the supposedly redundant system. (Classic example: redundant hydraulic lines in a DC-10, but an accident destroyed the part of the fuselage that held all three lines. Poof. No more hydraulics.)

2. The "shirking" problem (also known to psychologists as "bystander apathy"). The more people that are asked to check upon a system, the less thorough any individual is apt to be. Think about it -- will you take extra steps to check something if you know that "n" people have already vetted it and "m" more will do so after you? But if everyone shirks their duty, the reliability goes to zilch. In Social Psychology, "bystander apathy" refers to the experimentally validated observation that the more people that witness a crime, the less likely it is to be reported.

3. The overcompensation problem. This can be phrased as "the system is now safer, so I can take more risks" problem. Make a system more safe or more secure and people learn they can take chances. Add seat belts in automobiles and people drive faster. Add a secondary limit detector on a mechanical system, and people are willing to go beyond the first limit ("because the backup will catch any problem").

I want to emphasize the importance of these problems, while adding an equally important fourth one:

4: The Dedicated Worker problem. If the security or safety requirements get

in the way of doing the work, then the most dedicated workers will defeat them. Put in locked doors, and they will prop them open with waste baskets. Require long, lengthy, hard-to-guess passwords, changed frequently, and they will write them down and post them in easy to reach places. After all, security and safety are risks, not realities (and usually low-probability at that. (*) Getting the work done on time is a reality, and these extra steps invariably make it harder to do the work. Hence, the most dedicated workers will remove whatever tends to block getting the work done.

----- (*) This is what I have sometimes called the "one in a million" problem. Low probability events are often judged to be non-existent, or at least, that happen to others. I've named it after the pilot who decided that all three of his engines could not be failing because "the chance of this happening is one in a million." My observation is, "yes, you are correct, and you are that one." Actually, with some 7 million flights a year, one in a million is not nearly good enough, but that is a different argument.

----- Item one of these four is a technical issue: the other three are psychological ones. When attempting to increase security and safety of systems, it is essential that the psychology of the people be considered to be of equal or greater importance than the purely technical analysis. Note, the most obvious response of security and safety people is "more training is necessary." Yes, proper training is always useful, but don't count on it solving these problems. These issues happen despite training. They often are present in the best, most well motivated, most effective people

in the organization. Indeed, professionals in the security and safety industry have succumbed to just these issues. ("I know my home computer isn't secure, but it was absolutely essential that I finish this report, ..."). The correct solution lies in ensuring that the security and safety measures take into account both the technical and the psychological factors.

Don Norman norman@nngroup.com www.jnd.org

✶ Re: GPS Shutdown "during national crisis"

<Pat Place <prhp@andrew.cmu.edu>>

Thu, 23 Dec 2004 10:25:05 -0500

There are many services that depend on GPS so shutting it down in a national crisis appears to be foolhardy. On the other hand, a GPS unit trivializes the development of a guidance system. For example, <http://www.buzzle.com/editorials/6-3-2003-41208.asp> discusses how inexpensive it is to build such a system. I'm sure that there are plenty of other applications that risks readers can think of that use GPS for guidance that might, indeed, be the basis for future attacks in the US or elsewhere.

✶ Re: Unintended effects of RFID devices (Wallich, [RISKS-23.62](#))

<cogg@copper.net>

Sat, 25 Dec 2004 09:32:30 -0500

I recall that Richard Feynman found a similar issue with the storage of radioactive material in adjacent rooms. Neither room had a dangerous mass of material, but when the material is stacked back-to-back on the same wall in different rooms, it was possible for the mass to become critical.

✶ Re: Strange S&P numbers (Cohen, [RISKS-23.62](#))

<Dawn Cohen <dcohen@ets.org>>

Wed, 22 Dec 2004 09:30:00 -0500

[PGN asked Dawn: "Any follow-up?"]

As of this morning, I see that the S&P is at 1205, rather than 324. I wonder how many automated trading systems saw that 324 and tried to create orders.

✶ Re: Whites Only websites? (Jacobson, [RISKS 23.60](#))

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

Wed, 01 Dec 2004 12:42:46 GMT

DJ> Now some websites don't even allow browsers from lesser countries

... like the U.K., in the George W. Bush case ...

DJ> countries to connect. "Who from there would need to read our DJ> website? They're all just spam bots."

The problems of determining country from the IP address of the connecting client are known, of course, although less well than they should be, it seems. IP addresses simply don't map reliably onto countries. Most approaches rely upon tables derived from coarse-grained data, and are thus either inaccurate or incomplete. For example: Dan Bernstein provides an example DNS service that returns different answers depending from the continent (It doesn't even aspire to determining the specific country.) of the client (strictly: the resolving proxy DNS server) performing the lookup. Perform a "TXT" lookup for "clientcontinent.cr.yip.to." to see it in action. The service is based upon the 2001 IANA IPv4 address space allocation list. Even accounting for the datedness of the source data, there are vast swathes of IP address space for which it cannot even determine the *continent* of the client IP address. One might blame the coarseness of the IANA source data, but finer grained approaches suffer from other problems, such as errors caused by address assignment churn. And that's not to mention other factors such as VPNs, caching proxy servers, and the cases, common in years gone by although less so today, of people who make international calls for PPP access.

And of course, there are always the humorous consequences of people trying to determine country from IP address. *The Register* covered the George W. Bush website block, for example, and noted that Canada was deemed to be part of the United States by the Bush Campaign. (<URL:http://www.theregister.co.uk/2004/10/28/letters_politics/>)

Software Engineering for Secure Systems: SESS05

<Gene Spafford <spaf@cerias.purdue.edu>>

Thu, 23 Dec 2004 19:56:27 -0500

Software Engineering for Secure Systems (SESS05)
Building Trustworthy Applications
<http://homes.dico.unimi.it/~monga/sess05.html>

May 15-16, 2005
St. Louis, Missouri USA

An ICSE 2005 workshop
<http://www.cs.wustl.edu/icse05>

This workshop will provide a venue to discuss techniques that enable the building and validation of secure applications. We are especially interested in (1) design and implementation approaches that make it easier to deal with security requirements, and (2) program analysis techniques that enhance the trustworthiness of applications.

Areas of interest include, but are not limited to:

- o Security requirements management
- o Architecture and design of trustworthy systems
- o Architecture and design of protection systems
- o Separation of the security concern in complex systems
- o Secure programming
- o Black box components trustworthiness
- o Security testing
- o Trustworthiness verification and clearance
- o Defining and supporting the process of building secure software
- o Deployment of secure applications

** Submission of 7-page-max workshop papers 21 Feb 2005

[Excerpted for RISKS. See the Web site for full details. PGN]

✦ REVIEW: "Network Security Hacks", Andrew Lockart

<Rob Slade <rslade@sprint.ca>

Wed, 22 Dec 2004 13:42:37 -0800

BKNTSCHK.RVW 20041106

"Network Security Hacks", Andrew Lockart, 2004, 0-596-00643-8,
U\$24.95/C\$36.95

%A Andrew Lockart

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 2004

%G 0-596-00643-8

%I O'Reilly & Associates, Inc.

%O U\$24.95/C\$36.95 707-829-0515 fax: 707-829-0104 nuts@ora.com

%O <http://www.amazon.com/exec/obidos/ASIN/0596006438/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0596006438/robsladesinterne)

<http://www.amazon.co.uk/exec/obidos/ASIN/0596006438/robsladesinterne>
[21](http://www.amazon.co.uk/exec/obidos/ASIN/0596006438/robsladesinterne)

%O <http://www.amazon.ca/exec/obidos/ASIN/0596006438/robsladesinterne>
[20](http://www.amazon.ca/exec/obidos/ASIN/0596006438/robsladesinterne)

%P 298 p.

%T "Network Security Hacks"

Chapter one lists twenty 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 ten 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. Almost all of the network security tools discussed in chapter three are for UNIX, although some do have Windows versions. The same is true with the logging tips in chapter four, although there is mention of arranging to have Windows report to a syslogd. Network monitoring, and some analysis thereof, is in chapter five. Tunnels and VPN (Virtual Private Network) products are detailed in chapter six. Most of the network intrusion detection material in chapter seven concerns

Snort.

(You are not my NIDS, you are a Snort!) Chapter eight 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 BKNTSCHK.RVW 20041106
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

Volume 23: Issue 64

Tuesday 28 December 2004

Contents

- [New Year's Privacy Resolutions](#)
[Marc Rotenberg](#)
- [Tsunami: Natural Disaster Imminent: Whom to tell? How? E-mail!](#)
[Dan Vergano via Harry Crowther](#)
- ["April Fools and Ho-Ho-Ho" Combo](#)
[James Bauman](#)
- [More on computer glitches and laboratory result reporting](#)
[Robert L Wears](#)
- [Cell phones for eavesdropping - finally some public "chatter"](#)
[Gadi Evron](#)
- [T-Mobile Cripples the Blackberry](#)
[Jason D. O'Grady via Monty Solomon](#)
- [Did a 16-bit counter shut down Comair?](#)
[Dan Foster via Richard M. Smith](#)
- [Re: Y2K? Never heard of it...](#)
[Scott Nicol Ray Blaak](#)
- [Re: Pirates, Automeds](#)
[Charles Jackson](#)
- [Re: Why adding more ... may make systems less secure](#)
[R. Geoffrey Newbury](#)

● [Re: RFIDing babies](#)

[Ray Todd Stevens](#)

● [Info on RISKS \(comp.risks\)](#)

✶ New Year's Privacy Resolutions

<Marc Rotenberg <rotenberg@epic.org>>

Thu, 23 Dec 2004 16:51:21 -0500

[Thanks to Chris Hoofnagle for compiling.]

Protect Your Privacy in The New Year:
Privacy Tips from the Electronic Privacy Information Center
(EPIC)

Top Ten Consumer Privacy Resolutions

1. Engage in "privacy self defense." Don't share any personal information with businesses unless it is absolutely necessary (for delivery of an item, etc.). Don't give your phone number, address, or name to retail stores. If you do, they can sell that information or use it for telemarketing and junk mail. If they ask for your information, say "it's none of your business," or give "John Doe, 555-1212, 123 Main St." Don't return product warranty cards. Don't complete consumer surveys even if they appear to be anonymous. Profilers can build in barely-perceptible codes that link you to the survey, and this data goes straight to direct marketers.

2. Pay with cash where possible. Electronic transactions leave a detailed dossier of your activities that can be accessed by the government or sold to

telemarketers. Paying with cash is one of the best ways to protect privacy and stay out of debt.

3. Install anti-spyware, anti-virus, and firewall software on your computer.

If your computer is connected to the Internet, it is a target of malicious viruses and spyware. There are free spyware-scanning utilities available online, and anti-virus software is probably a necessary investment if you own a Windows-based PC. Firewalls keep unwanted people out of your computer and detect when malicious software on your own machine tries to communicate with others.

4. Use a temporary rather than a permanent change of address.

If you move in 2005, be sure to forward your mail by using a temporary change of address order rather than a permanent one. The junk mailers have access to the permanent change of address database; they use it to update their lists. By using the temporary change of address, you'll avoid unwanted junk mail.

5. Opt out of prescreened offers of credit. By calling 1-888-567-8688, you

can stop receiving those annoying letters for credit and insurance offers.

This is an important step for protecting your privacy, because those offers can be intercepted by identity thieves.

6. Choose Supermarkets that Don't Use Loyalty Cards. Be loyal to supermarkets that offer discounts without requiring enrollment in a loyalty

club. If you have to use a supermarket shopping card, be sure to exchange it with your friends or with strangers.

7. Opt out of financial, insurance, and brokerage information sharing. Be sure to call all of your banks, insurance companies, and brokerage companies and ask to opt out of having your financial information shared. This will cut down on the telemarketing and junk mail that you receive.

8. Request a free copy of your credit report by visiting <http://www.annualcreditreport.com>. All Americans are now entitled to a free credit report from each of the three nationwide credit reporting agencies, Experian, Equifax, and Trans Union. You can engage in a free form of credit monitoring by requesting one of your three reports every four months. By staggering your request, you can check for errors regularly and identify potential problems in your credit report before you lose out on a loan or home purchase. Currently, these reports are available to residents of most western states. By September 2005, all Americans will have free access to their credit report.

9. Enroll all of your phone numbers in the Federal Trade Commission's Do-Not-Call Registry. The Do-Not-Call Registry (<http://www.donotcall.gov> or 1-888-382-1222) offers a quick and effective shield against unwanted telemarketing. Be sure to enroll the numbers for your wireless phones, too.

10. File a complaint. If you believe a company has violated your privacy, contact the Federal Trade Commission, your state Attorney General, and the Better Business Bureau. Successful investigations improve privacy protections for all consumers.

Available online at <http://www.epic.org/privacy/2004tips.html>

For more information about privacy, visit the Electronic Privacy Information Center at <http://www.epic.org/>

⚡ Tsunami: Natural Disaster Imminent: Whom to tell? How? E-mail!

<"Harry Crowther" <crowther@ziplink.net>>
Tue, 28 Dec 2004 11:18:17 -0500

[There are huge lessons for disaster recovery in the aftermath of the Sumatra earthquake/tsunami. PGN]

[Following item by Dan Vergano, *USA TODAY*, PGN-ed]

Suppose you know a disaster is imminent, but don't know whom to tell?
Or how to tell them? Is e-mail the answer? Suppose those to be effected have no plans to deal with impending disaster?

Minutes after a massive earthquake rocked the Indian Ocean on Sunday, international ocean monitors knew that a tsunami would likely follow. But they didn't know whom to tell. "We put out a bulletin within 20 minutes, technically as fast as we could do it," says Jeff LaDouce of the National Oceanic and Atmospheric Administration. LaDouce says e-mails were dispatched to Indonesian officials, but he doesn't know what happened to the information.

The problem is that Sunday's earthquake struck the unmonitored Indian Ocean. An international system of buoys and monitoring stations - the Pacific Tsunami Warning Center based in Hawaii - spans the Pacific, alerting nations there to any oncoming disasters. But no such system guards the Indian Ocean. [where there are many earthquakes, although detector buoys used elsewhere are not deployed there; also risks of false alarms, as the evacuation in Hawaii in 1986, which reportedly cost more than \$30 million...; also the critical needs for evacuation plans and training]

[Source: Scientists in USA saw tsunami coming, by Dan Vergano, *USA TODAY*]

http://www.usatoday.com/news/world/2004-12-28-tsunami_warning_usat_x.htm

✶ "April Fools and Ho-Ho-Ho" Combo

<"Bauman, James" <James.Bauman@safety-kleen.com>>
Tue, 28 Dec 2004 10:25:40 -0500

Alek Komarnitsky, a computer specialist, two years ago created a Web site that supposedly allowed browsing users to turn his outdoor Christmas lights on and off, blinking on command. However, it turns out it was a hoax, intended "to spread holiday cheer", as he recently confessed to *The Wall Street Journal*. At first, he used a series of still photographs with lights on or off, and varying amounts of snow. This year, his wife manually

controlled the lights while a TV helicopter even hovered overhead. [Source: `Web-controlled' Christmas lights just a holiday hoax, *Chicago Tribune*, 28 Dec 2004; PGN-ed]

✶ More on computer glitches and laboratory result reporting

<"Robert L Wears, MD, MS" <wears@ufl.edu>>

Mon, 27 Dec 2004 09:37:20 -0000

I'd like to add one more case to the series of computer glitches causing failures in reporting patients' laboratory results to the proper people (see [RISKS-23.63](#) and 23.19, at least).

A hospital recently changed its method for testing for a sexually transmitted disease (GC); the new instrument reported its results into the hospital information system in a free text field, where it could be viewed by clinicians looking up an individual patient's result.

The system for ensuring no results were missed was based on a custom report written locally (because the vendor's report packaged with the system was too difficult to manage). This report covered all bacteriology cultures, not just those for the GC, and looked at a binary field for a positive or negative value for GC, reporting only the positives. Under the new system, that field was empty, and so no cases positive for GC were listed by the report. Because the other cultures were still being reported normally, the

report superficially looked normal (ie, it was not entirely empty).

The person who normally reviewed the report to follow up on all positive, untreated cases was away on vacation during this change. Some time after returning, she began to think it odd that no positive GC cases were showing up, and discovered the foregoing. A corrected report showed that several hundred cases positive for GC had been missed and had also not been treated with antibiotics; a non-negligible proportion were in children (where a positive result might be an indication of abuse).

There are organizational level, management level, and programming level risks here. At the organizational level there is the risk of increasing dependency on computer systems in an industry whose experience with these systems is immature (compared to other settings) and whose investment in informational infrastructure is low. At the management level, one failure is not tracking dependencies among system modifications. And at the programming level, the classic mistake of assuming a missing value means negative, instead of unknown. (I'm reminding of the aphorism that database programming would be much easier if missing values did not exist).

The case also indicates the value of experienced workers, who know what the normal pattern of laboratory abnormalities looks like and have some insight into the potential seriousness of anomalies. Although it did take them some time to become aware that something was persistently odd, I'm

not sure how
or when it would have been detected otherwise.

Bob Wears, Robert L Wears, MD, MS, University of Florida
wears@ufl.edu
and Imperial College London +44-(0)791-015-2219 r.
wears@imperial.ac.uk

⚡ Cell phones for eavesdropping - finally some public "chatter"

<Gadi Evron <ge@linuxbox.org>>
Mon, 27 Dec 2004 20:39:48 +0200

/Pun intended on the subject line!/

Okay, so, we have all known cell phones are "dangerous".

Stepping out of the cellular protocols security and vendor-side systems, and forgetting for a second about interception of transmissions through the air, Trojan horses/worms that may install themselves on the cell phone and even bluetooth risks, there is the long talked of risk of "operating" a regular un-tampered cell phone from a far and the risk of modified devices.

Sorry for stating the obvious, but cell phones are transmitters.

For years now paranoid people and organizations claim that eavesdropping through a cell phone is a very valid risk. Much like somebody pressing "send" by mistake during a sensitive meeting is a very valid yet different risk.

Some of the stricter organizations ask you to do anything from

(top to bottom) storing the cell phone in a safe, through shutting it off or removing the battery, and all the way to *only* "don't have that around here while we are in a meeting". Then again.. *most* haven't even heard of this risk.

Forgetting even this risk, many of us even ignore the obvious. I usually ask people who talk to me while I'm on the phone "even if the NSA (for example) is not interested in what I have to say or not capable of intercepting it and even that I don't care if they heard my conversations... Should the person I talk to hear our conversation?"

Lately there seems to be some more awareness about the "dangers" of cell phones. Knowing which risk is more of a threat than the other is another issue.

It seems to me that other than in the protocols, where there has been a serious learning curve (and GPRS seems very promising), cellular companies keep doing the same mistakes, and we can see the security problems of the PC world reappearing in cell phones, much like those of the main frames re-appeared in PC's (to a level).

History repeated. Heck, I can't even disable Java or the web browser in most cellular computers (we really should refer to them as computers now).

Here are some URL's on the subject:

Here is one about modified cell phones, which also mentions the

risk of
eavesdropping through a cell phone as mentioned above:
<http://www.interesting-people.org/archives/interesting-people/200206/msg00031.html>

Here is a product for sale, a cellular phone BUILT for
eavesdropping:
<http://wirelessimports.com/ProductDetail.asp?ProductID=347>

Also, check out the IEEE Pervasive article that mentions this
problem area,
although discusses more the issue of malware:
<http://csdl.computer.org/comp/mags/pc/2004/04/b4011abs.htm>

Or Google for "symbian +virus", for example.

Thanks go to David Dagon for the links.

⚡ T-Mobile Cripples the Blackberry

<Monty Solomon <monty@roscom.com>>
Wed, 22 Dec 2004 17:11:50 -0500

T-Mobile Cripples the Blackberry
Jason D. O'Grady, powerpage.org, 23 Dec 2004

In his article "T-Mobile Tells BlackBerry Users: GetLess!"
PowerPage editor
Emory Lundberg reports about how T-Mobile effectively crippled
the
Blackberry smartphone on its network by disallowing outbound
requests on TCP
port 80. A real sin considering that T-Mo Blackberry users pay US
\$40 per
month for "BlackBerry Unlimited w/Enterprise E-mail" that
includes
"Unlimited Web Browsing." ...

<http://www.powerpage.org/cgi-bin/WebObjects/powerpage.woa/wa/story?newsID=13375>

⚡ Did a 16-bit counter shut down Comair?

<"Richard M. Smith" <rms@computerbytesman.com>>

Mon, 27 Dec 2004 17:24:23 -0500

Date: Mon, 27 Dec 2004 02:53:06 +0000 (UTC)

>From: Dan Foster <use...@evilphb.org>

Newsgroups: comp.os.vms

Subject: Re: OT: anybody know the details on the COMAIR debacle?

Message-ID: <slrnctuucj.gd7.usenet@gaia.roc2.gblx.net>

In article <41CF6AC4.8030...@prodigy.net>, CJT <abujl...@prodigy.net> wrote:

>JF Mezei wrote:

>>So I wouldn't blame this on a computer breakdown. Just a scale of a

>>problem that had not been planned for.

>

>They said the computer crashed. That's different from saying the

>software couldn't find a feasible solution in an acceptable time.

Yeah, well. I wouldn't necessarily take a news report as gospel for a

technical event when lacking details and not reported through a technical

source.

This is unverified, and could be a wild rumor, but sounds credible

(especially since it has better details and someone else with firsthand

knowledge of Comair IT operations whom vouched for the report), and was seen

on a Slashdot thread:

Re:Fire away! (Score:5, Informative)

by [Xorian] (112258) on Sunday December 26, @12:56PM (#11185556)

Someone from Comair (who shall remain anonymous) provided me with some details which people here would be interested in:

The computer system in question runs AIX. The box itself is still up and running just fine; this is purely an application error. This application was not written in-house at Comair, but by another large aerospace company -- SBS (<http://www.sbsint.com/> [sbsint.com], owned by Boeing.) This bit of software does not use an external database, it tracks everything itself. It is a dedicated system responsible only for flight crew assignments. (The blather in the original submission about passenger reservations is way off-base. Those functions are handled by a completely different system.)

The great majority of Comair's traffic flows through the midwest, and the central base of operations is in Cincinnati. The midwest was hit by a major snowstorm this week, causing many, many crew reassignments. It appears right now that the application in question has a hard limit of 32,000 changes per month (ouch). Consider that Comair runs 1,100 flights a day and there are usually 3 crew members on each aircraft. A big storm like this can cause problems for days after the snow stops falling. That's a whole lot of crew changes.

In Comair's defense, this has never happened before and is

unlikely to happen again. The crew system was already on the chopping block long before this incident, with its replacement scheduled to go live in January. If this freak storm had happened a month later, this likely never would have occurred.

[The 2**15 exhaustion has been confirmed. For example, see:
<http://www.cincypost.com/2004/12/28/comp12-28-2004.html>
PGN]

✶ Re: Y2K? Never heard of it... (DES, [RISKS-23.63](#))

<Scott Nicol <snicol@apk.net>>
Sun, 26 Dec 2004 18:06:08 -0500

This is one of those little problems that never should have been a problem.

It was a bad design, but the subsequent fixes created the problem. It appears that lexxpress.fr tests their site using Internet Explorer, since the year will display correctly with this browser.

date.getYear() is supposed to return "year - 1900", so if you want to display "1999", you should add 1900 to date.getYear() before displaying it.

However, many lazy programmers displayed the date using the string "19" and tacked on the result of date.getYear(). On January 1 2000, many web sites showed the year as "19100".

Recognizing the problem, Netscape added date.getFullYear() in javascript 1.1

(but their documentation says it was added in 1.3), which returns the full year. However, nobody wanted to use it because not every browser in use supported it (even now, but especially in 2000).

Microsoft also recognized the problem, and "fixed" `date.getYear()` by making Internet Explorer return 99 in 1999, but 2000 in 2000, breaking compatibility with almost every other browser. It would be easy to blame Microsoft for this, except that Netscape itself made this same "fix" in some (but not all) versions of navigator 3.

So for the first week of 2000, various web sites displayed 2000, 19100, 3900, 20100, 192000, 202000, or nothing, depending on what browser you were using and how the code was written (and rewritten, again and again, as different browser users complained).

The correct fix is to call `date.getYear()` and add 1900 to it if the result is less than 1999. You won't find that in any reference manual, however.

✶ Re: Y2K? Never heard of it... (DES, [RISKS-23.63](#))

<Ray Blaak <rAYblaaK@STRIPCAPStelus.net>>

Sun, 26 Dec 2004 21:49:11 GMT

And how much longer will it take before broken libraries finally stop having `getYear()` return such unintuitive results?

It is not a precision problem.

The only "zero" year should be 0 BC/AD, and nothing else.

[Quite correct, even though there WAS NO ZERO YEAR. Whoever decided on the BC to AD shift was certainly not a mathematician. PGN]

✶ Re: Pirates, Automeds ([RISKS-23.62](#))

<"Charles Jackson" <chuck@jacksons.net>>

Wed, 22 Dec 2004 09:43:52 -0500

Re: Satellite TV Broadcast Pirated

There was a similar occurrence in the USA about 10 or 15 years ago. Someone seized the uplink of a C-band satellite service (Playboy channel, IIRC) and inserted their own programming. Technical details of the attack were quite similar to those described in the item in RD.

Upshot, the miscreants were convicted in US Federal District Court for some violation of the Communications Act.

Re: Automated medication worse than the disease.

I can't tell from the quote if the problem is (1) "automated medication is worse than perfect" or (2) "automated medication is worse than non-automated medication." The headline would indicate (2) but the text only supports (1). Could it be that the real problem with automated medication that it permits easy collection of data on medication errors?

✦ Re: Why adding more ... may make systems less secure (Norman, [R-23.63](#))

<"R. Geoffrey Newbury" <newbury@mandamus.org>>

Mon, 27 Dec 04 19:13:03 -0500

> These issues happen despite training. They often are present
in the best,
> most well motivated, most effective people in the organization.

These issues also happen BECAUSE of training and
competitiveness. Here's
an example.

Over the holiday, I caught up on my TV arrears by watching a
program I had
taped from the History Channel. This program involved a group
whose
objective was finding and diving on the wreck of the Queen Mary
(or
Indefatigable or Invincible...I don't remember which one). The
wreck is that
of a battlecruiser, hit by a German shell during the Battle of
Jutland, May
31, 1916. The battlecruiser exploded and sank, with the death of
all hands
but a very lucky few. It was known that the German shell had
struck through
to some magazine area, but the size and nature of the explosion
indicated
that something more had happened. The blast was too large to be
explained by
the magazine alone exploding, or one of the turret ready rooms.
They were
designed to contain any blast resulting from a shell incursion.

An alternate theory was that the blast-proof fire traps between

the magazine
and gun turrets had failed.

The dive revealed that there were blast effects in both the
turret ready
rooms, underneath the forward turrets, and in the main magazine
for the
forward guns. In addition, there were unexploded cordite bags
all along the
corridor between the magazine and the turret ready rooms. And
the blast
doors were not closed...

In order to keep the guns firing "efficiently", the gunners
(obviously with
officer knowledge and implicit consent) were storing cordite in
the corridor
right up to the ready room blast trap, which they were not using
anyway.....

Serving the six forward turret guns with three 50 pound plus
bags of cordite
per gun per shot, and attempting to fire at the same rate as
could be
attained when using the ready room stores alone... meant not
just ignoring,
but subverting the very safety measures which were intended to
make the ship
safe. As best the divers could tell, the German shell exploded
in one of the
ready rooms. The blast should have been contained there, but...

The physical design did not allow for a quick enough
replenishment and
serving of the guns, when the 'safe' method was used. So it was
not.

The sailors knew that the captain depended upon them to serve
the guns and
keep them firing as quickly as possible. Inter-ship competition
at gunnery
meant that every possible advantage had been discussed and
explored. And

wouldn't a captain be peeved if his crew could fire a broadside once every say 2 minutes during training, but only every 3 minutes in battle....

There's a picture of the Queen Mary explosion at www.gwpda.org in the naval photos page.

R. Geoffrey Newbury, Barrister and Solicitor, Mississauga, Ontario, Canada
1-905-271-9600 newbury@mandamus.org

✶ Re: RFIDing babies (cogg, [RISKS-23.63](#))

<"Ray Todd Stevens" <raytodd@kiva.net>>

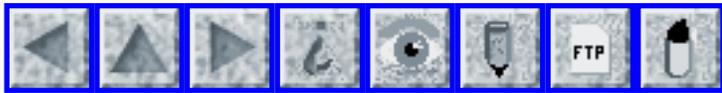
Sat, 25 Dec 2004 14:41:02 -5

Interesting. I have another idea to try. I would suspect that the software is implemented as "test for existence of an RFID tag in the control area" not "test for the existance of an RFID tag that is programmed as an active baby" So happens when you take an RFID that is not attached to a baby and bring it near the door? How about an RFIDed package that is being delivered? Given the nature of RFID, this would happen sooner rather than later.

Also that I know of there has been no real attempt in RFID to prevent denial of service as far as reading the tags. I wonder if a fairly low powered device of the right frequency could override the primary IF amp in the RFID

receiver and allow one to prevent the tag from being read, therefore prevent the system from locking the doors. So I wonder if this is such a great security device.

Ray Todd Stevens Specialists in Network and Security
raytodd@kiva.net
Suite 21, 3754 Old State Rd 37, N Bedford, IN 47421 (812) 279-9394



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 65

Tuesday 4 January 2005

Contents

- [Tsunami: natural disaster imminent?](#)
[Harry Crowther](#)
- [Tsunami warnings and spam](#)
[Geoffrey Brent](#)
- [New Year's Privacy Resolutions](#)
[Bernard Peek](#)
- [A deaf Hubble...?](#)
[David Lesher](#)
- [Missile interceptor doesn't even leave its silo](#)
[Vassilis Prevelakis](#)
- [Two German projects: Toll and Dole](#)
[Debora Weber-Wulff](#)
- [The effects of mistaking left- for right-fill](#)
[Jan Vorbrüggen](#)
- [Ars Team Prime Rib finds fourth-largest prime number ever](#)
[Monty Solomon](#)
- [Walgreen Overcharges, Reimburses Customers](#)
[Monty Solomon](#)
- [Thieves take brain remote control](#)
[Charles Williams](#)

- [Year Zero of Length Zero](#)
[Sam'l Bassett](#)
 - [Re: Cell phones for eavesdropping - finally some public "chatter"](#)
[Bill Stewart](#)
 - [Re: RFID'ing babies](#)
[Jerry Leichter](#)
 - [REVIEW: "High Tech Crimes Revealed", Steven Branigan](#)
[Rob Slade](#)
 - [RAID: Recent Advances in Intrusion Detection](#)
[Deborah A. Frincke](#)
 - [30 Joint CS & CE conferences in Las Vegas, 20 Jun 2005](#)
[H.R. Arabia](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Tsunami: natural disaster imminent?**

<"Harry Crowther" <crowther@ziplink.net>>
Wed, 29 Dec 2004 04:36:37 -0500

It is a dubious rationalization to complain about 'lost productivity' costs after '3 of 4 tsunami warnings' (in Hawaii?) prove false. Are evacuation drills and similar preparation, or planning related to disaster response also be considered too costly, if tsunamis do not occur on some obliging schedule? (Perhaps.) At some point, technology related to detection and warning is also 'too costly'. Particular care needs to be taken to appropriately balance 'lost productivity' costs with the cost of real damage and lost lives.

Obviously, while an hour's warning is inadequate in many situations, a

six-hour warning could do quite a bit of good given the vast reach of a tsunami. Presumably the detectors necessary for a one hour warning would be that same ones required for the six hour warning.

Harry Crowther (hdcrowther@alum.rpi.edu)

See: Sounding the Alarm on a Tsunami Is Complex and Expensive
John Schwartz, *The New York Times*, 29 Dec 2004
<http://www.nytimes.com/2004/12/29/international/worldspecial4/29warn.html>

If only people had been warned. An hour's notice for those living and vacationing along the coastlines of the Indian Ocean might have saved thousands of lives. But predictions, and acting on them, are not simple, geoscience experts say. ... According to a NASA Web site devoted to tsunamis, three of four tsunami warnings issued since 1948 have been false, and the cost of the false alarms can be high. ... An evacuation in Hawaii could cost as much as \$68 million in lost productivity, according to the National Oceanic and Atmospheric Administration. Since the 1960's, there have been two warnings of tsunamis in Hawaii that ended in evacuations, and both were false alarms.

🔥 Tsunami warnings and spam

<Geoffrey Brent <g.brent@student.unsw.edu.au>>
Wed, 29 Dec 2004 09:08:55 +1100

Around 1 Dec 2004, I and several people I know received this spam:

> THIS IS AN OFFICIAL WARNING!

> A huge 300 ft. high ocean wave is moving towards your
continent. Your and
> many other cities are in a real danger. Approximate wave
moving speed is
> 700 km/h.

> Please read more about this catastrophe here: [plausible-
looking URL
> snipped] We are strongly urging you to evacuate yourself and
your family
> as soon as possible, even though you may live far away from
your city. The
> tsunami will reach the continent in approximately FOUR hours.

I didn't check the URL then; aside from the "how would you know
what city
I'm in?" aspects, I'd previously received very similar messages
using other
shock announcements ("Terroract in Australia!") to lure people
to their
sites. And indeed, this one was also spam.

But in the wake of this week's tragedy, it reminds me that there
is no end
to opportunism. I'm sure we'll see that particular message
recycled;
spammers aside, there are several obvious reasons why somebody
might find it
convenient to trigger a mass evacuation. (Looting, terrorist
attack on
traffic choke points, etc etc...)

We know what false alarms do to the effectiveness of warning
schemes. Any
warning system needs to incorporate authentication - which also
means
limiting its distribution to people who *will* check
authenticity rather

than taking it on trust.

✦ New Year's Privacy Resolutions (Rotenberg, [RISKS-23.64](#))

<Bernard Peek <bap@shrdlu.com>>

Tue, 28 Dec 2004 23:03:39 +0000

It's common for RISKS posts to point out unintended consequences of well-meaning actions, so some response to Marc's post seems called for.

Having worked in the advertising and marketing industries and having run marketing campaigns I should point out some unexamined assumptions. The main one is that enhanced privacy is an unalloyed benefit. It isn't, there are costs.

Advertisers use targeted advertising because they have no desire to advertise to people who are not going to buy the product. The phrase I coined while in the industry was "Every ad a wanted ad." Targeting isn't perfect but the more information an advertiser has the better their targeting and the less they have to advertise to people who aren't interested.

If consumers don't provide that information, the advertisers will use less efficient, more expensive, advertising media including large blanket mailshots. Because all advertisers would be equally affected I would expect them to be free to pass on the extra costs to their customers.

Privacy is a
laudable aim, but not a zero cost option.

I need to add that part of the warning does not apply in the UK where I am. In general if you provide personal information to a European company they are not free to sell it on. The European model assumes that you own the data and when you "give" it to a company what they receive is a limited license to use that data. Unlicensed use of the data is a criminal offence. As a database manager I, and my company directors, could do jail time for buying or selling names and addresses. Adopting a similar legislative framework in the USA would do more to protect electronic privacy than any other measure.

Bernard Peek, London, UK. DBA, Manager, Trainer & Author

✶ A deaf Hubble...?

<David Leshner <wb8foz@nrk.com>>
Sun, 2 Jan 2005 20:24:25 -0500 (EST)

James Oberg wrote a great piece on the Cassini-Huygens mission that reminds us: it's the things we DON'T test that can really bite us.

<http://www.spectrum.ieee.org/WEBONLY/publicfeature/oct04/1004titan.html>

[This is a rather remarkable story of Boris Smeds, whose discovery of a flaw in Cassini's receiver and subsequent persistent

apparently
has saved the mission. PGN]

✶ Missile interceptor doesn't even leave its silo

<vp@cs.drexel.edu (Vassilis Prevelakis)>
Tue, 4 Jan 2005 09:16:29 -0500 (EST)

>From Aviation Week and Space Technology December 20/27, 2004,
pp. 34-36:

The trial began Dec. 15 around 00:45 EST when the target (for the
interceptor) was fired from Kodiak, Alaska. However, about 16
min later,

the interceptor at the Kwajalein missile range in the South
Pacific shut

down 23 sec. prior to launch owing to a still unspecified
anomaly. It was

the first test of Boeing's ground-based midcourse missile
defense system

using the operational Orbital Sciences Corp. interceptor.

Pentagon officials are still assessing why the missile defense
test

failed, but are pressing ahead anyway with the next round of
enhancements.

Are they simply going through the motions because nobody expects
this system
to be used against an actual enemy?

Vassilis Prevelakis, Computer Science Department
Drexel University, Philadelphia, Pennsylvania

Two German projects: Toll and Dole

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

Tue, 04 Jan 2005 09:09:57 +0100

Germany introduced not one, but two big projects on 1 Jan 2005. This was not by design, but because the toll collection scheme on the autobahns was delayed by about 18 months.

1) Toll collection

The government is happy to report that all is well, they collected some real money and there were no problems reported. Spiegel, however, (<http://www.spiegel.de/wirtschaft/0,1518,335367,00.html>) reports on its on-line edition that 10 % of all attempts to use the system ended in failure or in people just not paying the toll.

The system started with just 320.000 "On-Board Units" (OBU) installed that calculate the tolls using a complicated, satellite-based scheme. If a trucker does not have an OBU they must either purchase a ticket by mobile phone (costly) or at a toll booth in a rest stop. The problems here are that many truckers do not know exactly what exit they will be getting off at. In addition, if there is a traffic jam or other problems and they have to take a detour, they must change their toll ticket.

A personal observation from a rest stop visit on Sunday: there were 2 people posted at the terminal to help people use the system. The costs for this need to be factored into a success evaluation. The proof of the pudding will be when there are no helpers around anymore, just the machine with its

rather intricate user interface.

Other media have noted that now other EU countries are jealous and are considering their own toll systems. We will probably soon see trucks having to be completely rebuilt in order to accommodate the 25 or so different toll collection registration units.....

2) The new dole: Arbeitslosengeld II

The new dole system in Germany began on Jan. 1, 2005. The government has admitted to a "computer problem" in the direct deposit scheme that left about 5 % of the recipients without money. The computer on-line news system Heise Online reports in <http://www.heise.de/newsticker/meldung/54690> that the error was with account numbers that were less than the now standard 10 digits. The program was of course supposed to put in *leading* zeros, for example "0012345678". Instead, the zeros were added at the end ("1234567800") causing the payments to be unassignable to the recipient.

The government had to set up an emergency payment scheme to hand out 100 Euros to people who could show that they had not received the money properly. It seems strange that there would only be 5 % of people affected, as only people with newer banking accounts actually have a 10-digit account number and many people do not put in the leading zeros when they put their account number in a form.

The company that produced the software, T-Systems (a company that used to be part of the German telephone company) insists that the error is

not theirs,
but in the bookkeeping software of the government that sent them
the account
numbers already in the incorrect form. This software has been
working for
years, however, so the witch-hunt for the guilty continues.

Since the bank workers tend to still be on Christmas holiday and
the ones
left at the bank are concerned with getting the year-end
bookkeeping cleaned
up, the money had just been transferred to temporary accounts
where it
awaits someone to come along and sort it out.

Meanwhile, the scheme -- which was supposed to save the
government money so
that it could use the money to find work for people - has turned
out to
actually *not* save money yet. The government requested many
personal
details from people in the hopes of denying them money. But
instead of the
expected 23%, only 6.5% of the 2.7 million applications for
money were
rejected.

<http://www.berlinonline.de/berliner-zeitung/tagesthema/409437.html?2005-01-04>

There are very few people available for helping people find new
jobs, as all
of the available personnel have been concerned with getting the
payment
system to work.

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/>

[The second system problem also noted by Jan Vorbrüggen,

excerpted

next. PGN Correction of 6,5 added later]

✶ The effects of mistaking left- for right-fill

<=?ISO-8859-15?Q?Jan_Vorbr=FCggen?= <jvorbrueggen-not@mediasec.de>>

Tue, 04 Jan 2005 16:05:51 +0100

[...] Among the various media reports, see for instance (in German)

<http://www.spiegel.de/wirtschaft/0,1518,335141,00.html>.

A comment: Interbank transfers are ubiquitous in Germany - you can even use them to pay at the supermarket for your groceries. Certainly, everybody earning a salary receives it that way. It seems almost inconceivable that a programmer living here would not know that right-filling of account numbers is the wrong thing to do. Oh, and have they ever heard of testing?

✶ Ars Team Prime Rib finds fourth-largest prime number ever

<Monty Solomon <monty@roscom.com>>

Tue, 4 Jan 2005 17:12:35 -0500

Eric Bangeman, 4 Jan 2005, arstechnica

An anonymous member of Ars distributed computing Team Prime Rib has found the fourth-largest prime number discovered to date as part of the Seventeen

or Bust effort. The number, $28433 * 2^{7830457} + 1$, was found after over two days of processing by the computer that found it. ...

<http://arstechnica.com/news.ars/post/20050104-4497.html>

⚡ Walgreen Overcharges, Reimburses Customers

<Monty Solomon <monty@roscom.com>>

Sat, 1 Jan 2005 04:17:36 -0500

Bloomberg News, 1 Jan 2005

<http://www.latimes.com/business/la-fi-rup1.4jan01,1,4107985.story>

Walgreen Co., the largest U.S. drugstore chain, accidentally overcharged as many as 4 million customers buying gifts and decorations the two days before Christmas because its payment-processing system malfunctioned from overuse.

Walgreen discovered the error on Christmas Day and electronically reimbursed customers whose credit or debit cards had been incorrectly double- and triple-charged, said company spokesman Michael Polzin. Some credits may not post on customers' accounts until early next week, he said.

⚡ Thieves take brain remote control

<Charles Williams <C.D.H.Williams@exeter.ac.uk>>

Tue, 4 Jan 2005 12:07:19 +0000

Reported in several UK newspapers:

Thieves steal a device which allows a woman to sleep by switching off an implant in her brain.

<http://news.bbc.co.uk/go/em/fr/-/1/hi/uk/4142183.stm>

"... she is hopeful, but not certain, that the hospital caring for her - the National Hospital for Neurology and Neurosurgery in central London - will be able to replace the device."

✶ Year Zero of Length Zero (Re: Y2K?, [RISKS-23.63,64](#))

<"Sam'l Bassett" <samlb@samlb.ws>>
Tue, 28 Dec 2004 14:35:45 -0800

I have been saying for years that we should define a Virtual Year 0 of Length Zero, both for computer programming purposes, and to make decades and centuries come out right -- i.e. the 1960s would run from 1960 to 1969, not 1961 to 1970, and the 20th Century from 1900 to 1999.

✶ Re: Cell phones for eavesdropping - finally some public "chatter"

<"Stewart, William C \ (Bill)\, RTSLS" <billstewart@att.com>>
Tue, 28 Dec 2004 15:31:00 -0600

I **have** accidentally eavesdropped on a meeting using a cell

phone. I used the phone to check my voicemail before going into my meeting, which uses the same phone number as my phone, turned the ringer to vibrate-only, and forgot to lock the keypad when I put it into my briefcase. At some point the send button got bumped, and since I hadn't dialed a number, it called the last number I'd called, which was my phone. It was busy, so it connected to voicemail and recorded for ~15 minutes. My briefcase wasn't designed for acoustics, so it was pretty muffled, but relatively understandable.

✶ Re: RFID'ing babies (Stevens, [RISKS-23.64](#))

<Jerry Leichter <jerroldleichter@mac.com>>

Tue, 28 Dec 2004 23:56:40 -0500

Ray Todd Stevens, continuing and expanding on an assumption made by Paul Wallich back in [RISKS-23.62](#), describes possible problems with RFID tags used to lock doors in hospital neonatal units.

These measures have been around for years. I recall them from when my 3 1/2 year old was born, and I'm pretty sure they were in place when my 9 1/2 year old was born - and probably even before that. RFID refers to a specific technology which didn't exist 3 years ago, much less 9 years ago. I would be surprised if they are used today. RFID tags are cheap and disposable.

The tags used in neonatal units are on lock-on bracelets. As I

recall, they are re-usable. They don't need to provide true identification, only proximity detection. There will certainly be pressures, once a big RFID infrastructure is in place, to use RFID chips as the "standard" alternative, but they will have to battle an incumbent "standard" that's been in place for years. Change is unlikely to be quick, because the advantages of using RFID seem minimal.

As for "dumb" readers that just check if any RFID tag is present: Why would anyone even build such things? It's hard to come up with situations where they would ever be useful, and anyone who deployed such a device will quickly be swamped by random tags - and the cost advantages will be minimal, given how cheap true RFID readers will likely be in a short time. (Early targets for RFID tags are medicine bottles. A hospital is likely to have tons of the things moving around its halls pretty soon, whether or not it actually uses them for anything.)

In any case, it's easy to come up with failure modes, but that doesn't make them risks. They become risks when people don't deal with them appropriately. The systems I saw in action were pretty reliable. There was a clear marking in the hallway of how far you could go before setting off an alarm. It was quite accurate - we accidentally set the alarm off by walking a couple of steps too far. (My older one was helping push the younger one's carrier.) Determining the source of the problem wasn't that big a deal. (There was more running around by the staff, checking *all* the

exits, than
was really called for. This undoubtedly was partially a
reflection of the
rarity of such events. I only saw the alarm go off that once.
Once could
also argue that checking all the exits is prudent in any case,
since the
alarm could be an attempt at a distraction.)

There were two rooms adjacent to the exit door, and they were
clearly used
all the time without problems with the system. Radio waves may
not respect
room boundaries, but systems can be designed to allow for that.

🔥 REVIEW: "High Tech Crimes Revealed", Steven Branigan

<Rob Slade <rslade@sprint.ca>>
Wed, 29 Dec 2004 08:21:37 -0800

BKHTCRRV.RVW 20041016

"High Tech Crimes Revealed", Steven Branigan, 2005, 0-321-21873-
6,

U\$29.99/C\$42.99

%A Steven Branigan steveb@cyanline.com

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

%D 2005

%G 0-321-21873-6

%I Addison-Wesley Publishing Co.

%O U\$29.99/C\$42.99 fax: 416-443-0948 800-822-6339 bkexpress@aw.
com

%O [http://www.amazon.com/exec/obidos/ASIN/0321218736/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0321218736/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0321218736/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0321218736/robsladesinte-21)

%O <http://www.amazon.ca/exec/obidos/ASIN/0321218736/>

[robsladesin03-20](#)

%P 412 p.

%T "High Tech Crimes Revealed"

The title is a wee bit misleading: it is not the crimes that are revealed

here as much as it is the investigations, and investigative techniques and

tips. As such, the initial material in the book is more valuable than many

of those that do concentrate on the crimes themselves.

Chapter one deals with an insider attack at a telephone company. Branigan

tells the story well (if sometimes a bit flippantly) and also provides

"rules" for an inquiry as the account progresses. The narrative points out

errors that were made (or fortuitously missed) and notes what might have

been done better. A simple case of ISP (Internet Service Provider) banner

defacement turns out to have larger ramifications in chapter two. But, the

supply of rules seems to dry up, although there are notes reiterating or

expanding on them. Some accidental discoveries result in the discovery of a

pornographic service, in chapter three. Chapter four outlines a hacker

sting operation.

Identity theft is superficially reviewed in chapter five, but the "case" is

minor, and only used as a lead in. There are interviews with a couple of

blackhats (which, if you've read Denning's, Gordon's, or Taylor's work,

don't teach very much) in chapter six. Chapter seven examines the motives

of different types of blackhats. It is difficult to say that this material

will help in understanding attacks or protecting systems. There

is a brief history of information technology in chapter eight. The essay on high tech crime in chapter nine is a bit redundant at this point. There is also some questionable material, retailing myths such as Al-Qaida's use of steganography and the salami scam. Chapter ten describes some common mistakes in an investigation, and eleven lists an overall, if simplistic, investigative outline. Chapter twelve finishes off by recapping miscellaneous thoughts.

The reports of investigations that begin the book are interesting, particularly since all too many books about computer crime concentrate on technical details, and forget the legal realities (or, like Kovacich's and Boni's "High Technology Crime Investigator's Handbook" (cf. BKHTCRIH.RVW) concentrate on the career and forget the job). It is disappointing that Branigan's work trails off into more vague generalities.

copyright Robert M. Slade, 2004 BKHTCRRV.RVW 20041016
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>

RAID: Recent Advances in Intrusion Detection

<"Deborah A. Frincke" <frincke@moscow.com>>
Wed, 29 Dec 2004 11:13:37 -0800

RAID 2005, CALL FOR PAPERS and PANELS
Eighth International Symposium on Recent Advances in Intrusion

Detection

Seattle, Washington, USA, 7-9 Sep 2005

Deadlines:

31 Mar 2005: Paper & practical experience submissions

30 Apr 2005: Panel submissions

15 Aug 2005: Deadline for poster session submissions

www.conjungi.com/RAID/

www.raid-symposium.org

✶ 30 Joint CS & CE conferences in Las Vegas, 20 Jun 2005

<hra@cs.uga.edu>

Sun, 26 Dec 2004 15:00:23 -0500 (EST)

Call For Papers and Call For Session Proposals

The 2005 International Multiconference in

Computer Science and Computer Engineering

(composed of 16 Joint Conferences)

June 27-30, 2005, Las Vegas, USA

The 2005 World Congress in Applied Computing

(composed of 14 Joint Conferences)

June 20-23, 2005, Las Vegas, USA

[Excerpted for RISKS by PGN]

The 2005 International Multiconference in Computer Science and
Computer

Engineering is composed of the following 16 conferences (all
will be held

simultaneously, same location and dates: June 27-30, 2005, Las
Vegas, USA):

1. The 2005 International Conference on Parallel and
Distributed Processing
Techniques and Applications (PDPTA'05)
2. The 2005 International Conference on Artificial Intelligence
(ICAI)
3. The 2005 International Conference on Software Engineering

Research and

Practice (SERP'05)

4. The 2005 International Conference on Internet Computing (ICOMP'05)
5. The 2005 International Conference on Computer Design (CDES'05)
6. The 2005 International Conference on Wireless Networks (ICWN'05)
7. The 2005 International Conference on Modeling, Simulation and Visualization Methods (MSV'05)
8. The 2005 International Conference on Foundations of Computer Science (FCS'05)
9. The 2005 International Conference on Imaging Science, Systems, and Technology: Computer Graphics (CISST'05)
10. The 2005 International Symposium on Web Services and Applications (ISWS'05)
11. The 2005 International Conference on Pervasive Systems and Computing (PSC'05)
12. The 2005 International Conference on Machine Learning; Models, Technologies and Applications (MLMTA'05)
13. The 2005 International Conference on Communications in Computing (CIC'05)
14. The 2005 International Conference on Engineering of Reconfigurable Systems and Algorithms (ERSA'05)
15. The 2005 International Conference on Programming Languages and Compilers (PLC'05)
16. The 2005 International Conference on Embedded Systems and Applications (ESA'05)

The 2005 World Congress in Applied Computing is composed of the following 14 conferences (all will be held simultaneously, same location and dates 20-23 Jun 2005, Las Vegas, USA):

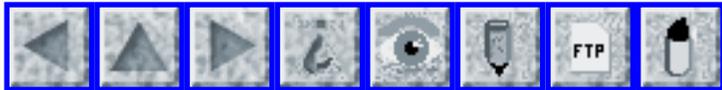
1. The 2005 International Conference on Grid Computing and Applications
(GCA'05)
2. The 2005 International Conference on e-Business, Enterprise Information Systems, e-Government, and Outsourcing (EEE'05)
3. The 2005 International Conference on Biometric Authentication (BIOAU'05)
4. The 2005 International Conference on Computers for People with Special Needs (CPSN'05)
5. The 2005 International Conference on Data Mining (DMIN'05)
6. The 2005 International Conference on Human-Computer Interaction (HCI'05)
7. The 2005 International Conference on Computer Vision (VISION'05)
8. The 2005 International Conference on Scientific Computing (CSC'05)
9. The 2005 International Conference on Information and Knowledge Engineering (IKE'05)
10. The 2005 International Conference on Security and Management (SAM'05)
11. The 2005 International Conference on Mathematics and Engineering Techniques in Medicine and Biological Sciences (METMBS'05)
12. The 2005 International Conference on Algorithmic Mathematics and Computer Science (AMCS'05)
13. The 2005 International Conference on Data Fusion - From Multi-Source Data to Information (FUS'05)
14. The 2005 International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS'05)

(a link to each conference's URL can be found at <http://www.world-academy-of-science.org> - currently under construction.)

GENERAL CHAIR AND COORDINATOR:

H.R. Arabnia, PhD, The University of Georgia, Department of
Computer Science
415 Graduate Studies Research Center, Athens, Georgia 30602-
7404, U.S.A.
Tel: (706) 542-3480 Fax: (706) 542-2966 E-mail: hra@cs.
uga.edu

Deadline for submission of papers 16 Feb 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

Volume 23: Issue 66

Friday 14 January 2005

Contents

- [A Comedy of Errors](#)
[Leslie Lamport](#)
- [30,000 personal records stolen in GMU server compromise](#)
[James Bauman](#)
- [New FBI software not usable](#)
[NewsScan](#)
- [Wal-Mart Stung in \\$1.5 Million Bar-Code Scam](#)
[Evan Schuman via Monty Solomon](#)
- [Attack on T-Mobile](#)
[NewsScan](#)
- [Risks of /pseudo-?/random alphanumeric generation](#)
[Joe Thompson](#)
- [Risks of lenient parsing](#)
[Jim Horning](#)
- [Heisenberg at work? Ranking cardiologists](#)
[David Lesher](#)
- [Ticket not in computer system: your insurance rates may increase](#)
[Joyce Scrivner](#)
- [eBay open invitation to phishing scammers](#)
[Thomas L. Jones](#)

- [Honest, General, it was only a little glitch](#)
[Jeremy Epstein](#)
 - [Microsoft AntiSpyware beta - quick review](#)
[Rob Slade](#)
 - [Re: Why adding more security measures may make systems less secure](#)
[Ron Bean](#)
 - [Re: New Year's Privacy Resolutions](#)
[Erling Kristiansen](#)
 - [REVIEW: "Net Crimes and Misdemeanors", J. A. Hitchcock](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ A Comedy of Errors

<Leslie Lamport>

Wed, 5 Jan 2005 09:55:36 -0800

The TLA+ specification language uses a common notation in which strings are enclosed in double-quotes. Special characters within a string, such as double-quote and backslash, are quoted by preceding them with a backslash. Thus, the string consisting of the five characters a " b \ c is written "a\"b\\c". The string "a\"b" appearing in a specification should traverse the following circuitous path if it is printed by the model checker:

1. The parser should convert the string "a\"b" to the list ('a', '"', 'b') of the three characters a " b.
2. The printing routine should convert ('a', '"', 'b') to the string "a\"b".
3. The pretty-printer, which inserts spaces and line breaks to format the output, should leave the string "a\"b" unchanged.

In the current version, none of these steps is performed correctly.

Instead, they do the following:

1. The parser converts the string "a\"b" to the list ('a', "\", "'", 'b') of the four characters a \ " b.
2. The printing routine, which should covert ('a', "\", "'", 'b') to "a\\\\"b", instead converts it to "a\"b".
3. The pretty printer, which should leave the string "a\"b" unchanged, instead prints it as "a\".

What is remarkable is that these three transformations are performed by code written by three different people. The programmers are all PhD researchers at different institutions--one at a university and the other two at two different industrial research labs.

Quoted characters are one of only two special cases that occur in handling strings. (The other, the empty string, should be handled automatically by any competently-written code.) Yet three different people forgot about that case when writing code. (I presume that the first transformation is done in two steps--the first identifying the string and the second converting it to a list--and the programmer forgot about quoted characters only in the second step.)

This comedy of errors shows that smart people can overlook even obvious cases. One hopes that, had this been production code written by professional programmers rather than research-project code written by researchers, then so simple an error would have been caught. But programs contain many problems that are not so simple. This incident points out the limitation of code reviews. It also calls into

question the use of multi-version programming as an alternative to verification for building highly reliable systems.

<http://lamport.org>

⚡ 30,000 personal records stolen in GMU server compromise

<James Bauman <James.Bauman@safety-kleen.com>>

Tue, 11 Jan 2005 14:59:32 -0500

The server at George Mason University in Virginia was compromised by crackers who stole personal information ("names, photos, Social Security numbers and (campus ID) numbers of all members of the Mason community who have identification cards") on 30,000 students, faculty, and staff.

The mega-risk here is obvious -- tens of thousands of people who may become victims of identity theft, one of the fastest growing crimes in America.

A system alert is posted on the University web site -->

<http://www.gmu.edu/prod/alerts/supportcenter/index.jsp?ID=1157>

For more details, see http://news.com.com/2100-7349_3-5519592.html

⚡ New FBI software not usable

<"NewsScan" <newsscan@newsscan.com>>

Thu, 13 Jan 2005 08:49:59 -0700

A new FBI computer system called Virtual Case File, designed to help agents share information to ward off terrorist attacks, may have to be discarded because it doesn't work as designed. The agency will be soliciting proposals for new software from outside contractors for new software. Sen. Judd Gregg (R-N.H.), chairman of the Senate appropriations subcommittee, calls the development "a stunning reversal of progress" and adds: "If the software has failed, that sets us back a long way. This has been a fits-and-starts exercise, and a very expensive one for a very long time. There are very serious questions about whether the FBI is able to keep up with the expanding responsibility and the amount of new dollars that are flowing into it. We have fully funded it at its requested levels." Science Applications, the company that developed the system, says it "successfully completed" delivery of the initial version of the Virtual Case File software last month. [*Los Angeles Times* 13 Jan 2005, NewsScan Daily, 13 Jan 2005]

[http://www.latimes.com/technology/la-na-fbi13jan13,1,2171776.story?](http://www.latimes.com/technology/la-na-fbi13jan13,1,2171776.story?coll=la-headlines-technology)

[coll=la-headlines-technology
http://www.latimes.com/technology/la-na-fbi13jan13,1,2171776.
story?coll=la-headlines-technology](http://www.latimes.com/technology/la-na-fbi13jan13,1,2171776.story?coll=la-headlines-technology)

[VCF is part of a four-year, \$.5 billion overhaul of the FBI's ``antiquated'' computer systems. PGN]

Wal-Mart Stung in \$1.5 Million Bar-Code Scam

<Monty Solomon <monty@roscom.com>>

Fri, 7 Jan 2005 01:49:49 -0500

By Evan Schuman January 5, 2005

In a scheme that leveraged a little technology but relied on inattentive cashiers, Tennessee authorities have arrested two couples on charges that they used bogus bar codes to steal at least \$1.5 million from hundreds of stores--some belonging to Wal-Mart--in 19 states. The group is slated to appear in court Wednesday.

Although the accused are said to have spent a lot of time and effort organizing colleagues in various parts of the country, the technology portion of their scheme was quite simple. They are accused of visiting a retailer and purchasing a low-priced item. The group would then scan the bar codes and simply print out duplicate bar codes, said Thomas Dean, the assistant Sumner County (Tennessee) district attorney who is assigned to the case.

The accused--Michael Poore, 29, and Julie Marie Simmons, 35, also known as Julie Poore; and Dewey Howerton, 39, and Laura Howerton, 39--would then go back to the store, tape the duplicate bar code on a higher-priced item and purchase the more expensive item at the lower scanned price, Dean said in an eWEEK.com interview.

One of the accused, according to the police complaint, would

then remove the bogus tag and try to return the item to the store for the full purchase price. Instead of cash, the defendants would often ask for gift cards, Dean said. "Wal-Mart will more quickly put it on a gift card than hand you cash," he said. ...

<http://www.eweek.com/article2/0,1759,1748274,00.asp>

✶ Attack on T-Mobile

<"NewsScan" <newsscan@newsscan.com>>

Thu, 13 Jan 2005 08:49:59 -0700

A network vandal broke into the network of wireless carrier T-Mobile over a seven-month period and read e-mails and personal computer files of hundreds of customers -- including those of the Secret Service agent investigating the hacker himself. The online activities of the vandal, 21-year-old computer engineer Nicolas Lee Jacobsen of Santa Ana, were traced to a hotel where he was staying in Williamsport, N.Y. Although Jacobsen was able to view the names and Social Security numbers of 400 customers (all of whom were notified in writing about the break-in), customer credit card numbers and other financial information never were revealed, and T-Mobile says it "immediately took steps that prevented any further access to this system."

[AP, 12 Jan 2005; NewsScan Daily, 13 Jan 2005]

<http://www.siliconvalley.com/mld/siliconvalley/10633193.htm>

✶ Risks of /pseudo-?/random alphanumeric generation

<Joe Thompson <kensey@gmail.com>>

Thu, 6 Jan 2005 13:50:16 -0500

The Cabbage Patch doll, known to legions of kids from the 80s on, comes with

"adoption paperwork" including a unique, randomly-generated serial number.

However, apparently the company's random number generator was, from a

certain point of view, a little too random:

Girl Gets Cabbage Patch Doll With Obscene Message

<http://www.10news.com/news/4050756/detail.html>

Apparently, purely by chance -- or so the company insists, at any rate --

one serial number included a six-letter string commonly considered obscene,

especially so in the context of children's toys. The slide show on the

linked new story page has a shot of the string in question (with the first

letter helpfully covered up to avoid further offense). That it was given as

a Christmas gift seems particularly unfortunate.

Many are the tales of large computer systems where user account names

are fully or partially randomized to avoid embarrassing formations

from pieces of names or other data. Even in such cases, some basic

filtering is needed; in fact given the audience for the product I'm

surprised no one at Play-Along has realized this in twenty years.

People easily forget that 0000, 1111, 2222, etc. are as random as any

other four-digit string in certain contexts.

✶ Risks of lenient parsing

<Jim_Horning@McAfee.com>

Fri, 07 Jan 2005 4:26 PM

Yesterday I had a frustrating experience trying to help track down a problem in a post to a blog I subscribe to, <<http://www.cra.org/govaffairs/blog/index.php>>. It ended happily enough when we were able to locate a syntax error in the HTML of the post, but not before we had explored several blind alleys.

For the gory details, see

<http://horning.blogspot.com/2005/01/risks-of-lenient-parsing.html>

So what is the lesson? There was clearly a syntax error, so what we got is what we deserved, right? I think not.

Given the frequency of errors in HTML, it would be unreasonable for renderers to refuse to display pages with errors. (There is an error somewhere in my blog post on this that I am still looking for.) However, we stumbled around blindly because *none* of the browsers we were using gave any hint that there was a syntax error on the page. Each just silently "corrected" the error. Unfortunately, but predictably, they didn't all "correct" it in the same way, meaning that Peter and his testers were consistently getting one result, and I was consistently getting

another.

I contend that **all** of the browsers were wrong not to indicate clearly the presence of a syntax error. A friendly browser would even have made some attempt to indicate the approximate location on the page of the error.

Although it was published more than thirty years ago, I think my advice on "What the Compiler Should Tell the User" (in **Compiler Construction, an Advanced Course**, F. L. Bauer and J. Eickel (eds.), Springer-Verlag, pp. 525-548, 1974) is still pertinent to those who build compilers and other formal language interpreters. Those who do not study the past are very likely not to learn its lessons, and therefore to repeat old mistakes, such as silently "correcting" syntax errors.

⚡ Heisenberg at work? Ranking cardiologists

<David Leshner <wb8foz@nrk.com>>
Tue, 11 Jan 2005 07:52:25 -0500 (EST)

Cardiologists Say Rankings Sway Choices on Surgery, Marc Santora, 11 Jan 2005

An overwhelming majority of cardiologists in New York say that, in certain instances, they do not operate on patients who might benefit from heart surgery, because they are worried about hurting their rankings on physician scorecards issued by the state, according to a survey released

yesterday.

I am reminded of the {alleged} quota scheme in the FBI. For years, no agent would willingly undertake terrorism cases, as such are long, time consuming and fraught with failure. Stick to the meat & potatoes of doofus bankrobbers, and you'll get promoted.

So the PHB's made terrorism cases carry more weight... Result? Now jaywalking and felony mopery are charged as terrorism...

✈ Ticket not in computer system: your insurance rates may increase

<Joyce Scrivner <kscriv@earthlink.net>>
Thu, 06 Jan 2005 16:19:07 -0600

<http://www.boingboing.net/2005/01/05/a_kafka_day_at_the_1.html>
http://www.boingboing.net/2005/01/05/a_kafka_day_at_the_1.html

Mark Frauenfelder: In November, my wife, Carla Frauenfelder, was driving home when a Los Angeles Police officer pulled her over. He ticketed her for making an illegal left turn.

The next day, with her ticket in hand, I entered the url for the website listed on the ticket (lasuperiorcourt.com). I wanted to pay the fine and sign her up for driving school so our car insurance rates wouldn't increase. The website couldn't find the ticket. I tried searching for it both by entering the ticket number and by entering my wife's

driver license

number. No luck. So I called the phone number on the ticket. The woman who answered said there was no record of the ticket. She said my wife would have to drive to the ticket office on Penfield St, in Chatsworth to take care of it.

So, my wife drove there on January 5th and showed the woman at the counter the ticket. The woman entered the ticket number and nothing came up. She scratched her head for a minute, and then noticed that the police officer forgot to write a date on the ticket. Apparently, that screws everything up.

The woman told my wife what the fine is (about \$135), but told her that she could not accept payment for the fine, because the ticket is not in the database. My wife is not allowed to attend driving school, either, because the ticket isn't in the database.

The woman instructed my wife to call the court every day week, to find out if the ticket had been entered into the computer yet. Once it shows up, she is supposed to drive to the ticket office the very next day to take care of it. And once the ticket has been entered, she is going to be hit with a penalty and possibly a warrant for her arrest, because once the information goes into the computer it'll see that she hasn't paid the fine yet, and it will be flagged as delinquent. My wife will then have to explain the situation to another helpful city employee.

My wife asked the woman how it long will take for the ticket to

be entered
into the computer system. The woman said she had no idea. My
wife asked her
if she is going to have to call every day week for the next
several years.
She shrugged and said "Well, it might take a week, it might take
six
months, I don't know."

My wife asked again if she could just pay the fine and have it
apply to the
ticket when it finally does show up. Woman: "Nope."

I'm at a loss for what to do here. If you have a good idea please
<mailto:mark@boingboing.net>email me and let me know if you do!

✶ eBay open invitation to phishing scammers

<"Thomas L. Jones" <DrJones@alum.mit.edu>>

Sun, 2 Jan 2005 05:23:20 -0500

Recently I received an e-mail from eBay.com involving something
called = "My
Messages." The e-mail directs the user to click on a link and
enter = his or
her password. Thus it is indistinguishable from a phishing scam,
= and
eBay.com will have only itself to blame when its customers fall
= victim to
scammers.

Thomas L. Jones, Ph.D., Computer Science

cc: Federal Trade Commission <reportphishing@antiphishing.org>

✶ Honest, General, it was only a little glitch

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

Thu, 13 Jan 2005 8:18:22 -0500

As has been widely reported, the DoD's missile interceptor test failed miserably in December, building on a rather impressive history of failures. According to Pentagon brass, the problem was "with an automated pre-launch check of the communications flow between the interceptor and the main flight control computer. Detecting too many missed messages, the system shut down automatically, as designed. [so] the Pentagon will increase the pre-launch tolerance for missed messages. [General] Obering said the tolerance level was set too low; increasing it will not risk a flight guidance failure".

Well, that makes me feel better. The system ran into problems, so it generated errors. Rather than figuring out what the problem was, let's ignore the errors. Not unlike turning up the radio in your car so you can't hear it falling apart.

The general went on to say "Statistically, it's a very rare occurrence and most likely would not happen again."

Gee, I feel safer every minute.

<http://www.cnn.com/2005/TECH/01/12/missile.defense.ap/index.html>

Microsoft AntiSpyware beta - quick review

<Rob Slade <rslade@sprint.ca>>

Fri, 7 Jan 2005 13:49:15 -0800

The beta version of Microsoft's Anti-Spyware program (purchased from Giant)

is available at

<http://www.microsoft.com/downloads/details.aspx?familyid=321cd7a2-6a57-4c57-a8bd-dbf62eda9671&displaylang=en&Hash=5BMW635>

The beta version is about a 6.4 meg download, and can be downloaded as a file in order to copy and install it onto other machines. That's very nice, and a departure from Microsoft's often heavy-handed approach.

Installing offers you a few options: do you want to set it to automatically update (I did), do you want it to install real-time protection (I did: so far it hasn't interfered with much, but I haven't used it much, either), and do you want to join Spynet. Spynet is not an invitation to join a kind of corporate CIA, but will report on "suspect" files. There is a fair amount of information on what it collects, if you ask for it. It seems to send information about file sizes and an MD5 hash back to HQ, but not, seemingly, the suspect file itself. In any case, there wasn't enough information on what it **doesn't** collect for me to feel comfortable, so I turned it off. (I hope.)

The installation seems to default to a reasonably protected mode: the defaults are for auto updating, real-time protection, and

scheduled scans
(although the schedule is for 2 am).

When you start up the program, it is initially set for a quick scan. I changed that to a full scan, which took about half an hour on my machine.

>From a quick test, the MS antispyware, at least in beta, falls between Spybot S&D and Adaware in terms of detection. Spybot is fairly conservative, and only deals with stuff that is pretty certain to be spy/adware, whereas Adaware will detect a bunch of other stuff. The MS product detected one copy of BackWeb (inactive) that Spybot had not, and detected about 38 copies of 15 versions of other stuff from my samples directory. (Adaware quarantined about 60.) The items detected all seem to have a least some remote access component, even if it is rather limited (such as BadTrans.B, that drops a keylogger). Oddly, it only detected two of my extensive collection of Bagles.

You can ask the program to deal with individual threats in different ways, although seemingly not individual files. (As a researcher, I like that. In terms of protection, I'm not as sure.) The options are to remove, quarantine, ignore, or always ignore. The program usually defaults to quarantine, although some threats are considered more serious, and marked to remove. The explanation of "always ignore" is not detailed enough, as far as I am concerned: does this mean always ignore this particular file, or always ignore this threat?

You can also specify certain directories to scan, or to ignore. Again, as a researcher I really appreciate the ability to tell it so ignore my sample directory. Unfortunately, this option doesn't work properly: it scans directories you tell it to ignore, regardless. When I told it to scan *only* my sample directory, it seemed to scan a fair amount of other stuff as well. Again, from a protective standpoint, this is probably a good thing.

At the moment, after a very quick test, I'd provisionally recommend the use of the MS/Giant antispyware program, at least in fairly restricted and manual mode. I'd be interested in hearing from others who have tested the real-time operations more extensively, and particularly from anyone who has tested the Spynet capabilities, and what information is returned thereby.

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

✶ Re: Why adding more security measures may make systems less secure

<rbean@shell.core.com (Ron Bean)>
Wed, 29 Dec 2004 00:17:01 -0500

"Don Norman" <norman@nngroup.com> writes in [RISKS-23.63](#):

> 4: The Dedicated Worker problem. If the security or safety requirements

> get in the way of doing the work, then the most dedicated
workers will
> defeat them.

> Note, the most obvious response of security and safety people
is "more
> training is necessary."

There is training, and then there is operant conditioning. If
defeating a
safety and/or security system results in an "attaboy" for
increased
productivity, the employee is being "trained" to defeat the
system,
regardless of anything that may have been said in the official
training
session.

The only way I see around this is to continually emphasize the
value of
safety/security systems, and to somehow downplay the all-too-
obvious value
of defeating them (possibly by making them less awkward to use--
don't
assume this is impossible).

A lot of safety training focuses on reviews of "one in a
million" accidents
that actually happened, so people will remember why the safety
systems are
there in the first place. The book "Construction Failure" by
Feld & Carper
(Wiley 1997) notes that many construction accidents are caused by
"unexpected" weather conditions, that statistically are not
"unexpected" at
all. This may be true of computer security issues as well.

It would also help if the security message were coming from the
people
responsible for production rather than from a separate
department. In many
companies, the people in charge of safety and/or security are
seen purely as

obstacles, because they don't seem to be of any help when it comes to actually getting things done.

🔥 **Re: New Year's Privacy Resolutions (Peek, [RISKS 23.65](#))**

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>

Thu, 06 Jan 2005 21:14:53 +0100

Bernard Peek sets as a goal "Every ad a wanted ad". But he thereby excludes those people who feel that "Every ad an unwanted ad". For those of us who belong to this group, Rotenberg's Resolution seems a better starting point.

Peek advocates the view that the more complete trail of your actions you leave, the better can advertising be targeted. I would like to ask: What kind of trail am I supposed to leave in order to get the message across that I do not want any unsolicited ads at all? The only answer I can think of is: Leave as little trail as possible. Which is exactly what Rotenberg suggests.

🔥 **REVIEW: "Net Crimes and Misdemeanors", J. A. Hitchcock**

<Rob Slade <rslade@sprint.ca>>

Mon, 10 Jan 2005 15:33:56 -0800

BKNTCRMD.RVW 20041016

"Net Crimes and Misdemeanors", J. A. Hitchcock, 2002, 0-910965-57-9,

U\$24.95/C\$37.95

%A J. A. Hitchcock

%C 143 Old Marlin Pike, Medford, NJ 08055

%D 2002

%G 0-910965-57-9

%I Information Today Inc.

%O U\$24.95/C\$37.95 609-654-6266 custserv@infotoday.com

%O <http://www.amazon.com/exec/obidos/ASIN/0910965579/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0910965579/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0910965579/robsladesin03-20>

%P 359 p.

%T "Net Crimes and Misdemeanors"

This book is not about net crimes in general, but about cyberstalking and online harassment.

Chapter one details Hitchcock's own experience with cyberstalking and harassment, an extremely unpleasant case of deliberate personal attack by fraudsters she had exposed. Three other cases are briefly described in chapter two, along with some basic advice on header analysis. Spam is delineated, and some helpful sites for dealing with it are listed, in chapter three (which also contains the usual, not terribly useful, suggestions for keeping your address off the net). Chapter four lists some urban legends and chain letters, which are hardly criminal material.

Chapter five lists various types of online scams, but really only addresses credit card theft. The utility of the advice varies: the book suggests that you only deal with vendors with a professional

looking website (hardly a guarantee of virtue), but also gives fairly detailed descriptions of indicators for a secure HTTP (HyperText Transfer Protocol) session. Online auction fraud is covered in chapter six, from the perspective of both buyer and seller. The story of adoption fraud, in chapter seven, is particularly distressing. Chapter eight give some account of identity theft, but the initial "case" is more related to harassment, and the material never really looks at more usual identity theft situations. More cases of cyberstalking are listed in chapter nine, with not as much helpful content. Chapter ten discusses trolls, flames--and more harassment.

Chapter eleven examines chat and harassment. Other means of harassment are discussed in chapter twelve. Child exploitation is reviewed in chapter thirteen. Chapter fourteen looks at various issues in the workplace. Statements from various law enforcement personnel are given in chapter fifteen--along with an odd mention of the Sam Spade program. Harassment at universities is covered in chapter sixteen. There is a terse mention of the PGP program in seventeen. Chapter eighteen describes viruses and firewalls, but not very well. Tips on investigating harassment are in chapter nineteen.

The book does provide some helpful resources on certain topics. It could have provided more, if it didn't keep returning to the same topic over and over again.

copyright Robert M. Slade, 2004 BKNTCRMD.RVW 20041016
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

Volume 23: Issue 67

Monday 17 January 2005

Contents

- [Loss of data from Huygens Probe](#)
[John Murrell](#)
- [130 most common bugs -- and counting](#)
[Peter Ludemann](#)
- [Cellery worm plays games with victims](#)
[NewsScan](#)
- [Hollywood Sign Security](#)
[Bruce Schneier](#)
- [Problems with Chicago-area toll road transponders](#)
[jhhaynes](#)
- [GPS used to arrest snowplow driver](#)
[David Tarabar](#)
- [Re: A Comedy of Errors](#)
[Rex Black](#)
- [Yet another route map software problem](#)
[Nick Brown](#)
- [MapPoint explains Vikings?](#)
[Adam Shostack](#)
- [Re: Risks of lenient parsing](#)
[Doug McIlroy](#) [Walter Roberson](#) [Roger Burton West](#) [Jonathan Kamens](#) [Russell Smiley](#)

[Sander Tekelenburg](#)

● [Copyright and reverse engineering](#)

[Rob Slade](#)

● [Re: High Tech Crimes Revealed"](#)

[Steven Branigan](#)

● [Re: A Kafka day at the Los Angeles traffic ticket office](#)

[Paul Robinson](#)

● [Info on RISKS \(comp.risks\)](#)

✶ **Loss of data from Huygens Probe**

<"John Murrell" <johnmurrell@compuserve.com>>

Sat, 15 Jan 2005 20:38:57 -0000

It appears that data was only received from one of the two semi-redundant communications channels from Huygens by the Cassini spacecraft. At this morning's press conference it appears that one of the two receivers on Cassini was not turned on due to a software error.

This has not caused a major loss as most data was duplicated between channels - the only two losses are that 50% of the images are lost but most of these will overlap with images sent on the other channel.

Also the 'Doppler Wind' experiment relied on the carrier signal from the channel that was not switched on however it is believed that this information can be reconstructed from the radio telescope observations that were tracking Huygens.

ESA has set up a board of enquiry into why the receiver was not turned on.

It is interesting to know why 'end to end' system tests did not

find this.

✶ 130 most common bugs -- and counting

<Peter Ludemann <p_ludemann@yahoo.com>>

Sat, 15 Jan 2005 12:13:33 -0800

Bruce Tognazzini has started collected well-known bugs at <http://asktog.com/Bughouse/index.html> ... many of these have shown up

before in Risks, such as "Harassing Confirmations & Missing Confirmations" and "'Smart' functions that aren't smart".

Readers might also enjoy (if that's the right word) Tognazzini's article

on Security D'oh!ts: <http://asktog.com/columns/058SecurityD'oh!ts.html>

and an older article on how inconvenience and security are confused:

<http://asktog.com/columns/051AirSecurity.html>

✶ Cellery worm plays games with victims

<"NewsScan" <newsscan@newsscan.com>>

Fri, 14 Jan 2005 06:19:58 -0700

Users are being warned about the Cellery worm -- a Windows virus that

piggybacks on the hugely popular Tetris game. Rather than spreading itself

via e-mail, Cellery installs a playable version of Tetris on the user's

machine. When the game starts up, the worm seeks out other

computers it can infect on the same network. The virus does no damage, but could result in clogged traffic on heavily infected networks. "If your company has a culture of allowing games to be played in the office, your staff may believe this is simply a new game that has been installed -- rather than something that should cause concern," says a spokesman for computer security firm

Sophos. [BBC News, 13 Jan 2005; NewsScan Daily, 14 Jan 2005]

<http://news.bbc.co.uk/1/hi/technology/4170903.stm>

Hollywood Sign Security

<Bruce Schneier <schneier@counterpane.com>>

Sat, 15 Jan 2005 02:50:05 -0600

From Bruce's CRYPTO-GRAM, January 15, 2005

http://www.schneier.com/blog/archives/2004/12/physical_access.html

In Los Angeles, the "HOLLYWOOD" sign is protected by a fence and a locked gate. Because several different agencies need access to the sign for various purposes, the chain locking the gate is formed by several locks linked together. Each of the agencies has the key to its own lock, and not the key to any of the others. Of course, anyone who can open one of the locks can open the gate.

This is a nice example of a multiple-user access-control system. It's simple, and it works. You can also make it as complicated as you

want, with
different locks in parallel and in series.

[Ah, a wonderful new use for the switching theory of relay
circuits that

takes me back to Howard Aiken's switching course in 1953!
Boolean

switching functions and even bridge networks, where current
can flow in

either direction in some links, provide for nifty multilock
combinations.

PGN]

⚡ Problems with Chicago-area toll road transponders

<jhhaynes@earthlink.net>

Wed, 5 Jan 2005 12:03:06 -0600 (CST)

[Source: Activating I-PASS hits a roadblock; Online demand
blamed for delay

Virginia Groark, *Chicago Tribune*, 4 Jan 2005; PGN-ed]

<http://www.chicagotribune.com/technology/chi-0501040029jan04,1,5273675.story?coll=chi-techtopheds-hed>

The Illinois State Toll Highway Authority raised the tolls at
12:01 on New

Year's Day 2005 for drivers paying cash, which caused floods on
both the

phone lines (with typically a 15-minute wait) and the Web site,
with 65,000

requests for I-PASS accounts over the weekend. Officials warned
that it

might take up to eight hours for activated transponders to work.

⚡ GPS used to arrest snowplow driver

<David Tarabar <dtarabar@acm.org>>

Tue, 11 Jan 2005 18:39:03 -0500

For the past several years, the Massachusetts Highway Department has required that private snow-removal contractors carry a GPS equipped mobile phone. The purpose is to allow the department to better schedule plowing and to verify that the roads are actually being plowed.

"The state found another use for the global positioning satellite network

...", according to the **The Boston Globe**, 11 Jan 2005. At 3:45 AM on 10

Jan, a snow-removal truck stopped at a local coffee shop, where the driver

ordered coffee and allegedly exposed himself to a female employee. The

Highway department tracked a truck from a local depot and by later that

day, the driver had been arrested and charged with multiple offenses.

✶ Re: A Comedy of Errors (Lampport, [RISKS-23.66](#))

<Rex Black <rexblack@ix.netcom.com>>

Sat, 15 Jan 2005 19:39:16 +0200

I don't know about whether all professional programmers would necessarily catch this error, but any programmer doing competent unit testing and/or any tester doing competent input-handling testing would have caught it.

Equivalence class partitioning would identify at least three

classes of
strings:

1. Null string (sometimes valid)
2. Non-null strings that contain no special characters (valid)
3. Non-null strings that contain at least one special characters (valid)
4. Malformed string (always invalid)

In each those classes--excepting perhaps the null string--a competent programmer or tester should be able to identify multiple subclasses and other interesting tests (e.g., using boundary value analysis), such as the non-null string of minimal length, the non-null string of maximum length, the non-null string exactly one character longer than the maximum length, a non-null string long enough to overflow a buffer, etc.

Since these types of tests tend to be effective at finding bugs during system testing by independent test teams, I conclude that many programmers do not cover these tests during unit testing. With the advent of some of the so-called agile methodologies, that may well change, provided that programmers take the time to study and apply well-established testing techniques.

Rex Black Consulting Services, Inc., 31520 Beck Road, Bulverde,
TX 78163 USA
1 830 438-4830 www.rexblackconsulting.com
rex_black@rexblackconsulting.com

🚧 Yet another route map software problem

<Nick Brown <Nick.BROWN@coe.int>>

Sat, 15 Jan 2005 00:31:13 +0100

This kind of thing has been discussed in RISKS before ([20.62](#), [23.20](#)), but

apparently the problems are still there:

1. Go to <http://mappoint.msn.com/DirectionsFind.aspx>
2. In the Start section, select "Norway" from the listbox and enter "Haugesund" into the "City" field
3. In the End section, select "Norway" from the listbox and enter "Trondheim" into the "City" field
4. Click on "Get Directions"

Interestingly, inverting the cities in the request produces "less spectacular" results.

What was fundamentally the same service (Microsoft Expedia Maps, now called MSN MapPoint) figured in article in [RISKS 20.62](#), more than five years ago.

MapPoint explains Vikings?

<Adam Shostack <adam@homeport.org>>

Sat, 15 Jan 2005 12:06:55 -0500

(Or, that wrong turn at Djupaskarvegen again!)

When going from Haugesund, Rogaland, Norway, to Trondheim, S=F8r-Tr=F8ndelag, Norway, be aware that following Microsoft MapPoint's

directions, will take you through England, France, Belgium, the Netherlands, Germany, Denmark, Sweden, and finally back into Norway.

While this may be culturally sensitive and respectful of historic Viking routing, rooting, or looting, it is somewhat less

efficient than
other routes, as a quick glance at a map will show.

Start: Haugesund, Rogaland, Norway

End: Trondheim, S=F8r-Tr=F8ndelag, Norway

Total Distance: 1685.9 Miles, Estimated Total Time: 47 hours, 31
minutes

(This is listed as the "quickest" route.)

[.gif file deleted]

✶ Re: Risks of lenient parsing (Horning, [RISKS-23.66](#))

<Doug McIlroy <doug@cs.dartmouth.edu>>

Sun, 16 Jan 2005 16:05:39 -0500

Following up on Jim Horning's remarks that rightfully blame the
prevalence
of bad HTML, which works here but not there, on browsers'
silently "fixing"
errors, I note that this behavior was officially encouraged:

HTML user agents should be liberal except when verifying code.

- Berners-Lee, Connolly et al, "HyperText Markup Language
Specification - 2.0", Internet Draft, November 28, 1994

Browsers -- the only ubiquitous tools for seeing that a web page
works --

are rarely built for verification, and this sentence lets them
off the hook.

It has always ranked high on my list of misguidances in language
design.

[Doug's message is right on. Jim's posting created quite a
flurry, both

in-band and out-of-band. I have selected a few, despite some

overlap,

which by no means covers the waterfront, but may exhaust the reader. PGN]

✶ Re: Risks of lenient parsing (Horning, [RISKS-23.66](#))

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

Sat, 15 Jan 2005 02:07:48 -0600 (CST)

In [RISKS-23.66](#), Jim Horning contended that "**all** of the browsers were wrong not to indicate clearly the presence of a syntax error."

In my experience, pages **without** HTML syntax errors are quite uncommon.

I usually use an older browser that does less automatic fixups of incorrect HTML. If I hand-edit nonconformant HTML to make it compliant, the browser almost always works.

I find that an increasing number of sites are insisting on IE6, or Firefox, or Netscape 7, supposedly because "We use advanced HTML features not supported in older browsers". In **every** such case that I have investigated, if I grab the content otherwise and fix its broken HTML, the pages have worked fine on the old browser.

Sites almost never fix their HTML in response to my reports. It has become clear to me that requiring IE6 has become a euphemism for "Our HTML is nonconformant and we have no intention of fixing it."

⚡ Re: Risks of lenient parsing (Horning, [RISKS-23.66](#))

<Roger Burton West <roger@firedrake.org>>

Sat, 15 Jan 2005 12:52:42 +0000

Mr Horning may find it useful to be aware of the Dillo browser (<http://www.dillo.org/>), which not only gives detailed information on errors in HTML but uses a clearly-specified set of heuristics in trying to correct them.

⚡ Re: Risks of lenient parsing (Horning, [RISKS-23.66](#))

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

Mon, 17 Jan 2005 10:21:29 -0500

I had a "those who fail to learn from history" moment when I read Jim Horning's account of his difficulty tracking down an HTML syntax error because all of the browsers used to display the page with the error silently corrected it.

Years ago, early on in the browser wars when Netscape was still king, I heard a similar rant from one of my friends who is an SGML / XML / HTML expert. The very controversial question the browser developers and early adopters were asking then was, should HTML be treated as a structured language which must parse correctly to be displayed, or should it be treated

as a markup language which browsers should obey as much as possible even when it's broken?

Clearly, the browsers have chosen the latter. As uncomfortable as that decision may make the technology purists among us, it is a reasonable application of Postel's rule to "Be generous in what you accept and conservative in what you generate."

Developers who regularly encounter difficulties with HTML syntax errors which the browsers make difficult to locate may wish to avail themselves of one of the numerous free and commercial HTML validation tools that are available.

✶ **Re: Risks of lenient parsing (Horning, [RISKS-23.66](#))**

<"Russell Smiley" <smiley@nortelnetworks.com>>

Mon, 17 Jan 2005 11:01:18 -0500

> A friendly browser would even have made some
> attempt to indicate the approximate location on the page of
the error.

Personally I'd be rather annoyed if my favourite browser started generating prompts for "general syntax error at line x" on every poorly formed web page out there and I suspect most general users would as well.

It seems to me that browsers try to cleanly and silently work around problems in HTML to ease the experience for users who simply

don't understand the issues with writing good HTML, or don't want to. In a general sense this seems particularly reasonable when most of the time the error can be worked around without any noticeable problem for the user.

However Mr Horning's experience suggests there is a specific class of users who actually need the error reporting to validate the HTML they are generating. Rather than "enhancing" browsers to report all errors as Mr Horning suggests I would suggest that browsers should have a debug mode which is by default disabled to facilitate the present user-friendly experience. When enabled the debug mode could report all HTML errors for the benefit of those users who need to know about such errors.

✉ **Re: Risks of lenient parsing (Horning, [RISKS-23.66](#))**

<Sander Tekelenburg <tekelenb@euronet.nl>>

Sat, 15 Jan 2005 13:45:05 +0100

> So what is the lesson?

The 3 lessons are:

1. There is no excuse for publishing invalid HTML as there are plenty of HTML validators available. (Once you use them you will notice that there are (almost?) no CMS tools, blogs, 'WYSIWYG HTML editors', etc. that output valid HTML. At best they output minor errors (like not encoding ampersands))

but usually they'll just output crap, relying on browsers' ESP engines to guess what was meant.)

Note that some of those tools, like HTMLTidy, are useful but are not *validators*.

2. When a Web page shows a problem, the first thing to do is make sure its HTML is valid. It's no use wasting time on any other aspect as long as it is not. For some reason most Web designers seem to be unaware of this.

3. You were using the wrong tools. (iCab, see below, would have been a right tool.)

> Given the frequency of errors in HTML, it would be unreasonable for
> renderers to refuse to display pages with errors.

IMO this is open for debate still. Browsers refusing to display invalid HTML would be the ideal solution, as it would force authors to ensure valid HTML.

However, I recognise that, given that easily 95% of the Web contains broken HTML, a user agent that would refuse to display such pages would never become popular. It is simply too late now. Users expect Web pages to 'just work'. They expect browsers to guess what the author meant, and to guess right.

Still, indicating to the user that a page contains invalid HTML, and that therefore what is rendered is no more than a best guess at what the author intended *would* be realistic. It would be a very useful tool for those who care, and it would not get in the way of those who don't. Give

it time, and more users will hopefully begin to realise that indeed it does matter. The Web browser iCab has offered this for many years.

A way to make this even more useful, perhaps even to popularise this, might be to have browsers score pages. The less HTML errors, the better the score, thus indicating that the user can be more confident that what is being displayed is what the author intended.

If that becomes popular enough, then maybe, just maybe we can finally arrive at a point where users will appreciate browsers that refuse to display invalid Web pages. Probably the right way (both to make it a smooth step from the previous step, and to popularise it) would be to allow users to define the threshold at which their browser should simply refuse to display a page.

Of course you would need to come up with a sensible algorithm to be able to score HTML in a useful way. This won't be easy given that 1 error will influence the effect of another error...

> We stumbled around blindly because *none* of the browsers we were using
> gave any hint that there was a syntax error on the page.

There is at least one browser that does contain a HTML syntax checker, and has so for many, many years: iCab. See <<http://www.icab.de/>>. When it considers a document's HTML to be good, it shows a green smiley in the toolbar. When it considers a document to contain 1 or more errors, the green smiley turns into a red sad face, which you can click to get a

list of all
the errors it found (including a hint as to what is wrong about
it and
sometimes even what it probably should have been) and in turn
double-clicking individual errors makes it show the document's
source code,
with the relevant portion highlighted.

This tool has been available since about 1998 (provided you have
a Mac to run
it on). AFAIK to this date no other browser vendor has been
smart enough to
copy this function.

iCab 3.0, which is currently in 'limited public beta testing'
phase not only
validates HTML 4.0.1 but also XHTML 1.0, CSS 2.1 and javascript.

> Each just silently "corrected" the error. Unfortunately, but
predictably,
> they didn't all "correct" it in the same way, meaning that
Peter and his
> testers were consistently getting one result, and I was
consistently
> getting another.

Although I agree, IMO you're forgetting an even more (and far
more common)
danger: that silently fixed HTML errors can easily lead to
output that is
wrong, but *not obviously wrong*.

Also note that this goes beyond just HTML. For instance, many
Web sites do
not provide any or the correct character repertoire that applies
(and
sometimes even claim 2 different charsets!), and browsers will
often silently
guess which character repertoire to use. This can lead to
outright nonsense
which is easily recognised, but can just as well lead to just
the odd
character being wrong. You bet that in some cases that 'wrong'

character
could make perfect sense and can thus go by undiscovered, even
though it
could change the meaning of the content completely. AFAIK no
browser will
warn the user in this case.

So use iCab, and/or put pressure on the makers of your favourite
browser to
make their product useful.

Sander Tekelenburg <<http://www.euronet.nl/~tekelenb/>>

✶ Copyright and reverse engineering

<Rob Slade <rslade@sprint.ca>>

Tue, 11 Jan 2005 11:31:25 -0800

> [http://www.zdnet.com.au/news/security/0,2000061744,39176657,00.
htm](http://www.zdnet.com.au/news/security/0,2000061744,39176657,00.htm)

>
> A French security researcher who published exploit codes that
could
> take advantage of bugs in an anti-virus application, could be
> imprisoned for violation of copyright laws.

I warned ya.

OK, well not quite the same situation, but on page 21 of
"Software
Forensics" I noted that this type of situation might one day
result in a
malware author challenging evidence obtained by forensic
examination on the
basis of the laws supposedly supporting copyright by inveighing
against
reverse engineering.

rslade@vcn.bc.ca
niu.edu

slade@victoria.tc.ca

rslade@sun.soci.

<http://victoria.tc.ca/techrev/~rslade>

or

<http://sun.soci.niu.edu/~rslade>

✦ **Re: High Tech Crimes Revealed" (Slade review, [RISKS-23.65](#))**

<Steven Branigan <steveb@cyanline.com>>

Sun, 16 Jan 2005 18:21:10 -0500

I am honored by the fact that Robert Slade took the time to do a review of my book, "High Tech Crimes Revealed", back on December 29th, 2004. It covers a few high tech crime cases from "inside the investigation", based upon actual cases with which I was involved.

I believe that these stories are very relevant in today's society. We need just look at the recent story about hackers breaking into T-Mobile to read e-mails of an ongoing investigation to see that hackers are still getting past computer security.

<http://www.cnn.com/2005/LAW/01/12/cellular.hacker.ap/>

I just wanted to address a couple of small points that I spoke with Robert about prior to his publishing this review.

(1) steganography

The quote from my book is... "Rumors persist that Al-Qaeda style terrorist groups have used steganography to hide their communications out in the open. Using steganography, a person can hide a secret message

inside a picture that is sent via e-mail or even posted on a website. All that is needed from the person receiving the picture is to extract the hidden message from it."

Rumors do persist that terrorist have looked at using steganography for clandestine communication.

<http://www.fitug.de/news/newsticker/old/2001/newsticker200901125229.html>

<http://www.heise.de/tp/r4/artikel/11/11004/1.html>

Let me state that I have not seen any conclusive evidence that steganography has been used for terrorist communications. I do wish to point out, though, that some in the government are concerned about it and are not looking into it.

(2) Salami scam

I had a discussion with Robert and I believe that his view is that the salami scam is all hype because there are very few documented cases of it.

I respect that point of view, but I believe that the following documented cases are sufficient to be concerned about it as a potential crime.

<http://www.collyerbristow.com/site/default.asp?s=55&cID=301&ctID=13&bhcp=1>

<http://www.nwfusion.com/newsletters/sec/2002/01467137.html>

✶ Re: A Kafka day at the Los Angeles traffic ticket office (R.23-66)

<Paul Robinson <ohshitidontknow@verizon.net>>

Mon, 17 Jan 2005 11:14:44 -0500

[Open letter to Mark Frauenfelder:]

I saw the discussion of your problem with your wife's traffic ticket which was also reported in [RISKS-23.66](#). I am not a lawyer but I have some idea on what your wife needs to do if you can't resolve the ticket because the system won't record it:

Call (or preferably write) the headquarters office for the district attorney for Los Angeles County. If you write, you explain the situation; if you call you ask to speak to the district attorney or get an appointment, .saying you need to discuss the disposition of a court case. You do not inform the secretary of what the case is unless she says she has authority to negotiate a plea bargain herself (which she won't of course). You'll get some lawyer in the office but that's fine, because that's what you want..

If you can get a lawyer on the phone or you get an appointment, you explain the circumstances of the situation and ask them to agree to dismiss the charge and not prosecute this particular ticket because the case office is not posting the ticket and you can't be put in a position where you are "twisting, turning in the wind," waiting for an unknown and unknowable filing to be made which places you in jeopardy of even more serious criminal penalties when you can't get the current one resolved.

If they won't or you can't get someone, you file suit in

Superior Court

against the District Attorney's office (you will probably have to sue the D.A. personally by name) for a writ of mandamus prohibiting them from prosecuting the original ticket. You may even be able to sue for damages but I think all you're interested in is to get rid of the matter, either by converting it off of a moving violation or getting it dismissed. I don't think it would be that difficult to file for an order even without a lawyer since you're only trying to solve the problem and the government, by its incompetence or misconduct is placing you in a position in which you are being denied the right to a constitutionally guaranteed speedy trial and quite possibly to equal protection and possibly other issues. Even if you don't get the order you've got grounds to have any potential penalty for not paying the ticket and not appearing canceled.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 68

Weds 26 January 2005

Contents

- [Risk Analysis and the War on Terrorism](#)
[Curt Sampson on James Fallows](#)
- [FBI axes Carnivore, eats investment](#)
[NewsScan](#)
- [E-waste is piling up](#)
[NewsScan](#)
- [Drug histories exposed](#)
[PGN](#)
- [A-List Jury](#)
[Howard M Israel](#)
- [A-Train in New York City disabled](#)
[Ken Knowlton](#)
- [F/A-22 crash](#)
[Peter B. Ladkin](#)
- [Figure this out: system configuration](#)
[Lindsay Marshall](#)
- [HTTPS .ne. secure](#)
[Jeremy Epstein](#)
- [No e-mail return address](#)
[Louise Pryor](#)

- [PayPal contradicting its own security advice](#)
[Tim Huckvale](#)
 - [Re: eBay open invitation to phishing scammers](#)
[Drew Dean](#)
 - [REVIEW: "Outsourcing Information Security", C. Warren Axelrod](#)
[Rob Slade](#)
 - [REVIEW: "Degunking Your Email, Spam, and Viruses", Jeff Duntemann](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Risk Analysis and the War on Terrorism

<Curt Sampson <cjs@cynic.net>>
Wed, 19 Jan 2005 13:38:10 +0900 (JST)

In the January/February 2005 issue of The Atlantic Monthly there is an article by James Fallows entitled "Success Without Victory," discussing risk management as it applies to the war on terror.

One key point is that there are people out there who, in the tradition of RISKS readers themselves, take a sensible and scientific approach to the war on terror, seeing it as an exercise in risk management rather than something that can be "won," causing all of the risks to go away:

There will always be a threat that someone will blow up an airplane or a building or a container ship.... But while we have to live in danger, we don't have to live in fear. Attacks are designed to frighten us even more than to kill us. So let's refuse to magnify the damage they do. We'll talk

about the risk only when that leads to specific ways we can make ourselves safer. Otherwise we'll just stop talking about it, as we do about the many other risks and tragedies inevitable in life.

We cannot waste any more time on make-believe....measures that seem impressive but do not make us safer, such as national threat-level warnings and pro forma ID checks. The most damaging form of make-believe is the failure to distinguish between destructive but not annihilating kinds of attack we can never eliminate but can withstand and the two or three ways terrorist groups could actually put our national survival in jeopardy. We should talk less about terrorism in general and more about the few real dangers.

Screening lines at airports are perhaps the most familiar reminder of post-9/11 security. They also exemplify what's wrong with the current approach. Many of the routines and demands are silly, eroding rather than building confidence in the security regime of which they are part.

[Daniel] Prieto argues that the roughly \$4 billion now going strictly toward airline passengers could make Americans safer if it were applied more broadly in transportation -- reinforcing bridges, establishing escape routes from tunnels, installing call boxes, mounting environmental sensors, screening more cargo. All these efforts combined now get less than \$300 million a year, which will drop to \$50 million next year.

Where the article gets really interesting, however, is in pointing out the political barriers to doing the rational thing from a risk-analysis point of view. For example, spending less on airline security in order to spend more on land and water transportation:

Rationally, this is an easy tradeoff: less routine screening of passengers who don't call out for special attention (watch lists, travel and spending patterns, and other warning mechanisms can be improved), in exchange for more and faster work to reduce the vulnerabilities of bridges, tunnels, and ports. In wartime a commander would easily make such a decision to protect his troops. But politically this decision is almost impossible. Such a tradeoff would make it likelier that some airplane, somewhere, would be blown up. If that happened, whoever had recommended the change would be excoriated -- even if more people had been spared equally gruesome fates in subways or near ports.

And even examples of where this is already happening:

[Terror and counter-insurgency experts] understand that this struggle will be with us for a very long time, that success will mean reducing rather than absolutely eliminating the threat of attacks, and that because there is no enemy government or army to surrender, there can be no clear-cut moment of victory. "Ironically, when President Bush said this in the campaign, he was immediately jumped upon," Jenkins said. "It was a moment of truth for which he was promptly punished. Senator Kerry had

a similar

moment, when he said that the objective was to reduce terrorism to no more

than a nuisance. Conceptually that was quite accurate, even if it was not

the most felicitous choice of words. And he was punished too. In a

campaign with a great deal of nonsense about the threat of terrorism,

these two moments of truth were mightily punished, and the candidates had

to back away and revert to the more superficial and less supportable

assertions."

The article goes on with some general and specific recommendations for improving the security of America against terror attacks.

The approach will be nothing new to RISKS readers, though the details may be. But I find it very hopeful that articles like this are appearing in general interest magazines rather than just specialized forums like this.

The article is available on-line to The Atlantic Monthly subscribers at

<http://www.theatlantic.com/doc/200501/fallows>

If you are not a subscriber but know one, he can e-mail you a link that will make the full article available to you for three days.

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

🔥 FBI axes Carnivore, eats investment

<"NewsScan" <newsscan@newsscan.com>>

Wed, 19 Jan 2005 09:08:42 -0700

The FBI has abandoned its custom-built Internet surveillance technology, dubbed Carnivore, and is now using commercial software to eavesdrop on computer network traffic during investigations of suspected criminals, terrorists and spies. In addition, it's asking Internet service providers to conducting wiretaps on targeted customers, when necessary. Carnivore initially was developed because commercial tools available in 2000 were inadequate, but FBI spokesman Paul Bresson says the Bureau moved a while ago to using popular commercial wiretap software because it's less expensive and has improved in its ability to copy e-mails to and from a specific Internet account without affecting other subscribers. "We see the value in the commercially available software; we're using it more now and we're asking the Internet service providers that have the capabilities to collect data in compliance with court orders," says Bresson. The FBI didn't disclose how much it had spent on Carnivore, but outside experts estimate expenditures at somewhere between \$6 million and \$15 million. [AP, 18 Jan 2005; NewsScan Daily, 19 Jan 2005]

<http://apnews.excite.com/article/20050119/D87MS3CO0.html>

⚡ E-waste is piling up

<"NewsScan" <newsscan@newsscan.com>>

Fri, 21 Jan 2005 10:14:49 -0700

Consumers' penchant for constant upgrades -- new cell phones, a sleeker laptop -- is causing havoc in the environment, and with technology products now accounting for as much as 40% of the lead in U.S. landfills, e-waste has become one of the fastest-growing sectors of the U.S. solid waste stream. The International Association of Electronics Recyclers estimates that Americans dispose of 2 million tons of electronic products a year -- including 50 million computers and 130 million cell phones -- and China, which has served for years as the final resting place for Americans' unwanted TVs and computers, is becoming overwhelmed by the volume. Some high-tech companies are taking matters into their own hands -- Hewlett Packard and Dell job out their e-waste handling to environmentally sensitive recyclers such as RetroBox -- but such efforts are still quite limited and unable to cope with a problem that's reaching crisis proportions. Meanwhile, the U.S. is the only developed country not to have ratified the 1992 Basel Convention, the international treaty that controls the export of hazardous waste. "There's a real electronics-waste crisis," says Basel Action Network coordinator Jim Puckett. "The U.S. just looks the other way as we use these cheap and dirty dumping grounds." [*The Washington Post*, 21 Jan 2005;

NewsScan Daily, 21 Jan 2005]

<http://www.washingtonpost.com/wp-dyn/articles/A24672-2005Jan20.html>

⚡ Drug histories exposed

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

Wed, 26 Jan 2005 17:35:17 PST

An investigation by **The Harvard Crimson** was reported in that newspaper on 21 Jan 2005, noting that a Harvard University website, iCommons Poll Tool, for months had contained confidential information on the drug purchase history of students and employees that was easily accessible to outsiders. After **The Crimson** demonstrated this to university officials, the website was immediately shut down. Authentication information required for access was based on a Harvard ID and birthdate that were easily available on the Web. In addition, the Family Educational Rights Privacy Act (FERPA) requires that students may request a special security status for total privacy, and that status was not properly enforced. The university's drug insurer, PharmaCare, also had the same problems -- which still existed at the time of the article in **The Crimson**. This is seemingly a violation of the HIPAA legislation, which prohibits unauthorized disclosure of individual's medical records.

[I suppose if medicinal uses of marijuana were covered by insurance, someone might have found the situation HIPAA-pot-amus-ing. PGN]

⚡ A-List Jury

<Howard M Israel <hisrael@avaya.com>>

Mon, 17 Jan 2005 16:35:46 -0500

http://abclocal.go.com/ktrk/news/bizarre/011405_Apsn_jury.html

A computer glitch at the state Office of Jury Commissioner alphabetized names of potential jurors, rather than shuffling them, before summonses were sent out. That created a jury pool of people whose last names mostly begin with the letter "A".

Howard Israel, Avaya Global Services, Avaya, Inc. 1-732-852-3353

[Suffolk Superior Court, Massachusetts. That must be as random as anything else they do. None of the lawyers objected! PGN]

⚡ A-Train in New York City disabled

<Ken Knowlton <KCKnowlton@aol.com>>

Tue, 25 Jan 2005 09:48:54 EST

On 25 Jan 2005, a homeless man trying to keep warm (says the early report) started a fire that wiped out a control room, disabling New York City's 'A' subway line indefinitely, and seriously curtailed service on several other lines; it may take months, possibly years, to repair the damage. The subway controls destroyed are those that automatically prevent closely-

spaced
trains from colliding.

F/A-22 crash

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Wed, 19 Jan 2005 08:34:41 +0100

On 20 Dec 2004, an F/A-22 crashed on takeoff from Nellis Air Force Base, Nevada (*Aviation Week*, 3 Jan 2005, pp21-22). According to *Aviation Week* (10 Jan 2005, p19), based on preliminary data, "Pentagon leaders believe" that the cause was a problem in the digital flight control system (DFCS).

The short article quotes an unnamed official that, after an apparently normal takeoff roll, once airborne the pilot had "no control over pitch, yaw or roll." Those are the names for the movements about the three axes which constitute the aircraft's movement in the air. The pilot apparently received no warning of a failure.

According to the 3 Jan article, in September an F/A-22 was stressed to 10-11g when flying through the wake of an F-16 while carrying external fuel tanks. The operational limit on the aircraft is 9g. The incident was put down to a feature in the DFCS software producing a violent pitch reaction. The pitch gain was calibrated for low-altitude operations, but the aircraft was manoeuvring at high altitude. The SW was modified. The incident aircraft was grounded, and it is uncertain whether it

will fly
again.

The F/A-22 is the U.S.'s new stealthy air superiority fighter. The program is notorious for its tardy and expensive SW development, and thereby ran into funding difficulties with the U.S. Congress, indeed I believe it was threatened with cancellation.

The crash of a prototype YF-22A aircraft at very low altitude (just off the runway) was reported by Leveson (citing an article in *The Washington Post* by Gellman) in [RISKS-13.46](#) in 1992, and followed in [RISKS-13.47](#) and [13.50](#) by some speculative commentary.

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

⚡ Figure this out: system configuration

<"Lindsay Marshall" <Lindsay.Marshall@newcastle.ac.uk>>
Mon, 24 Jan 2005 21:37:03 -0000

A neighbour of mine just bought a new Epson printer and were trying to install it on their laptop. They had a problem : they rebooted their system and it said "Not a system disk". They gave me a call and I wandered up to have a look. I hit a few keys and suddenly it booted again. Odd I thought (not having noticed a crucial event!). I got in as Administrator and installed the software for them and we connected up the printer

and
rebooted. "Not a system disk". I thought for a bit and looked in
the BIOS
and lo and behold, the first boot item was a USB disc, and the
printer does
indeed have a USB disc feature so that you can access camera
memory cards
via the printer. Unplug the printer and the system boots fine,
plug it and
no dice. (What I hadn't noticed above was that my neighbour had
unplugged
the printer from the USB as I was hitting keys)

How could anyone expect everyday users with no experience of
systems
internals to deal with a situation like that? Why should a
printer look like
a disc anyway (at least by default), and why have the default
BIOS setting
to boot from USB first? A disaster waiting to happen and it
happened.

HTTPS .ne. secure

<Jeremy Epstein <jeremy.epstein@cox.net>>
Fri, 21 Jan 2005 7:25:35 -0500

I recently filed a change of address for some Qwest stock I
own. Qwest uses
The Bank of New York (www.stockbny.com) to manage stock
accounts, so I went
to their web page, and filled out the form using name, address,
SSN, and
account number. Checked for the padlock indicating HTTPS, and
convinced
there was **some** degree of due diligence, submitted the form.
The
confirmation screen starred out all but the last four digits of
the SSN

(i.e., ***-**-9999), which seemed reasonable.

Last night I got back an e-mail that they couldn't process my change request (the reason is unimportant), and included in the text of the message my name, e-mail address, account number, and SSN. No stars this time to shield sensitive information. Seems like a pretty useful e-mail to intercept!

What kind of security policies allow including this sort of information?

The security & privacy policies don't say anything about safeguarding customer information.

If anyone has a privacy/security contact at Bank of New York, I'd certainly be interested in talking to them!

(This is certainly not a new type of problem; see [RISKS 21.83](#) for another example I wrote about 3 years ago.)

✶ No e-mail return address

<Louise Pryor <pryor@pobox.com>>

Tue, 18 Jan 2005 15:04:48 +0000

Many automated e-mails have no usable e-mail return addresses. For example, Verizon include the following rubric at the bottom of their messages: "This message was sent from a notification-only e-mail address that cannot accept incoming e-mail messages. Please do not reply."

I know this because I have now received five messages from Verizon intended for somebody who shares my last name and probably has a similar e-mail address. I now know this person's mailing address and telephone number, and that they have ordered Verizon's DSL service. I know that the DSL service is now available.

I've been receiving these e-mail messages for about a month now (there was a delay in getting the DSL service operational, apparently, for which Verizon have apologised). I have tried e-mailing postmaster@verizon.com, but have no effect. I could, I suppose, telephone or write to the intended recipient, but I don't see why I should make a transatlantic phone call to someone I don't know. For obvious reasons, I don't have an e-mail address for this person.

The risks here are obvious. Verizon presumably have a disgruntled customer, frustrated with not having heard from them. I have personal information about somebody else that I am not entitled to have (at least they didn't sent the account username and password through by e-mail) and get a small amount of unwanted e-mail.

Louise Pryor pryor@pobox.com www.louisepryor.com

PayPal contradicting its own security advice

<"Tim Huckvale" <tim@huckvale.net>>
Tue, 18 Jan 2005 12:30:15 -0000

I just received an e-mail from PayPal warning me that my credit card was about to expire. Naturally my first thought was that it was a phishing trip, but closer inspection showed it to be genuine.

It ended with the following warning:

```
- - - - -  
- - -  
  
                PROTECT YOUR PASSWORD  
  
    NEVER give your password to anyone and ONLY log in at  
    https://www.paypal.com/. Protect yourself against fraudulent  
websites  
    by opening a new web browser (e.g. Internet Explorer or  
Netscape) and  
    typing in the PayPal URL every time you log in to your account.  
  
- - - - -  
- - -
```

Typing in the URL is excellent advice. Such a shame that they defeated it by making the link clickable.

⚡ Re: eBay open invitation to phishing scammers ([RISKS-23.66](#))

<Drew Dean <drew.dean@sri.com>>
Mon, 17 Jan 2005 16:18:03 -0800

> ... Thus it is indistinguishable from a phishing scam, ...

The amusing thing is that this is actually meant as an anti-phishing tool, and it started from a good idea: eBay would communicate with its

customers
via an area on its website rather than e-mail. The (reasonable)
assumption
being that it is somewhat harder (though, of course, not
impossible) to
spooof eBay's website than a piece of e-mail. But you have to
get started,
so how do you communicate this new policy to your customers?

Presumably eBay would have been better off sending plain text e-
mail
providing a link only to <http://www.ebay.com>, or even better,
telling people
to type that into their browser, or use a pre-existing bookmark,
but plain
Jane e-mail might cause people to think it was a phishing
attack, or other
folks probably don't know how to enter a URL directly into a
browser -- all
of which would drive up eBay's technical support costs.

This appears to be one of those cases in which you just can't
win.

Drew Dean, Computer Science Laboratory, SRI International

REVIEW: "Outsourcing Information Security", C. Warren Axelrod

<Rob Slade <rslade@sprint.ca>>
Thu, 20 Jan 2005 08:23:18 -0800

BKOSINSC.RVW 20041210

"Outsourcing Information Security", C. Warren Axelrod, 2004,
1-58053-531-3, U\$85.00/C\$119.50

%A C. Warren Axelrod

%C 685 Canton St., Norwood, MA 02062

%D 2004
%G 1-58053-531-3
%I Artech House/Horizon
%O U\$85.00/C\$119.50 800-225-9977 artech@artech-house.com
%O [http://www.amazon.com/exec/obidos/ASIN/1580535313/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1580535313/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/1580535313/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1580535313/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/1580535313/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1580535313/robsladesin03-20)
%O tl a rl 1 tc 1 ta 3 tv 2 wq 2
%P 248 p.
%T "Outsourcing Information Security"

The author states that he intends to raise issues involved in outsourcing security in such a way that those working through the process will not neglect important areas of concern.

Chapter one reviews reasons for outsourcing. Lists of threats and vulnerabilities, in general, are given in chapter two. Costs are examined in chapter three, as a basic discussion of justification for outsourcing. Chapter four looks at risks that might be associated with outsourcing. Various types of costs, such as intangible, subjective, and indirect, are contemplated in chapter five, and costs related to different stages of the evaluation process in chapter six. Chapter seven investigates a number of issues surrounding the development of requirements for system or project development. The first chapter that actually seems to talk in detail about security outsourcing, rather than just outsourcing itself, is chapter eight, which goes through the ten domains of the CISSP (Certified Information

Systems Security Professional) CBK (Common Body of Knowledge) (and some subdomains), determining which of them are particularly appropriate for outsourcing, and which are not. Chapter nine outlines the outsourcing process as a sequence of steps.

Axelrod has provided a very solid and useful framework for dealing with the many areas that need to be considered if outsourcing is sought. Very little is directly relevant to the security function itself, but that may simply expand the market for the book. It is probably futile to expect that any more guidance could have been provided, since the possibilities are so immense, but the summary given here still leaves the potential outsourcer with an enormous amount of work to do.

copyright Robert M. Slade, 2004 BKOSINSC.RVW 20041210
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>

[For those of you interested in security implications, see Table 7.1 of my recent report, which summarizes the pros and cons of both outsourcing and offshoring:
<http://www.csl.sri.com/neumann/chats4.html> for browsing,
Section 7.10.2
<http://www.csl.sri.com/neumann/chats4.pdf> and .ps otherwise,
page 133
PGN]

★REVIEW: "Degunking Your Email, Spam, and Viruses", Jeff Duntemann

<Rob Slade <rslade@sprint.ca>>

Wed, 26 Jan 2005 08:14:12 -0800

BKDYESAV.RVW 20041205

"Degunking Your Email, Spam, and Viruses", Jeff Duntemann, 2004, 1-932111-93-X, U\$24.99/C\$37.99

%A Jeff Duntemann feedback@paraglyphpress.com

%C Suite 115 4015 North 78th Street, Scottsdale AZ 85251

%D 2004

%G 1-932111-93-X

%I Paraglyph Press

%O U\$24.99/C\$37.99 602-749-8787 ssayre@paraglyphpress.com

%O <http://www.amazon.com/exec/obidos/ASIN/193211193X/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/193211193X/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/193211193X/](http://www.amazon.co.uk/exec/obidos/ASIN/193211193X/robsladesinte-21)

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/193211193X/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/193211193X/](http://www.amazon.ca/exec/obidos/ASIN/193211193X/robsladesin03-20)

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/193211193X/robsladesin03-20)

%O tl i rl 3 tc 3 ta 4 tv 4 wq 3

%P 334 p.

%T "Degunking Your Email, Spam, and Viruses"

Lots of books have "quick tips" at the front these days. Usually these are nothing more than promotional fluff, designed to convince you that the author Knows Important Stuff. However, when I perused the suggestions for what to do about email and viruses if you had limited amounts of time, I was quite impressed that Duntemann had, in fact, carefully selected those tasks that would give the most protective value for the temporal coin. I could cavil at a few, but generally this list is very well chosen for those readers who do need to get started right away.

Chapter one is an introduction, defining the various problems, and outlining the "12-step" program that structures most of the rest of the book.

Although chapter two is supposed to be about creating an email strategy it doesn't go quite that far. But Duntemann does provide guidance on the type of email user you are, and notes the importance (which varies) of having alternative email addresses. Various email clients, and important features, are reviewed in chapter three. The advice is good (although I don't know why he is dissing Pegasus :-). Chapter four outlines good email habits, and effective practices for using and managing email. The advice on maintaining contact and synchronization on the road, given in chapter five, is helpful to travelers although I am not sure that it a) applies to everyone, and b) is a "gunky" problem. Chapter six provides valuable advice for managing stored or saved messages.

Chapter seven describes the situation with regard to spam, and suggests the standard actions to avoid it. The concepts and tools for spam filtering are outlined in chapter eight. Chapter nine walks the reader through the installation and "training" of POPfile, while ten lists arguments against non-Bayesian spam prevention filters and systems.

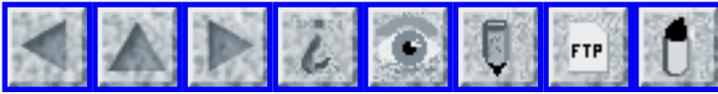
Chapter eleven is a good introduction to the broad categories of malware.

The choice and evaluation of antiviral programs, given in chapter twelve, is quite decent, although the space and precedence given to the "three sisters"

seems to be excessive: companies like Sophos, F-Prot, and Avast turn out technically superior products and are hardly "obscure." Spyware and adware, as well as suggestions to limit them and products to deal with them, are covered in chapter thirteen. Chapter fourteen has good advice about dealing with worms (although I'm surprised that Duntemann did not mention turning off DCOM, which would probably have saved his friend some grief). Chain letters and scams are discussed in chapter fifteen. (I was teaching in Nigeria when I read this book, so I found the coverage of the 419 scam ironic. Nigeria isn't in chaos: it just seems that way.) Chapter sixteen finishes off with advice on what to do if you *have* been hit with something nasty.

The book has a lot of very practical and useful information. It is written at a level that any intermediate user, and many intelligent novices can use directly without further experimentation. (A few items could use more detail: how do you turn an .iso file into a bootable CD?) I would recommend this as an excellent reference to have to hand for pretty much any computer user.

copyright Robert M. Slade, 2004 BKDYESAV.RVW 20041205
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 69

Tuesday 1 February 2005

Contents

- ['Thief-proof' car key cracked. What, already?](#)
[Chris Leeson](#)
- [Incredible Hulk No-Coaster](#)
[Frank Carey](#)
- [Tiger triggers the car window?](#)
[Wendell Cochran](#)
- [Search engine risks](#)
[Marcos H. Woehrmann](#)
- [German Toll Collect - an exercise in Graph Theory](#)
[Debora Weber-Wulff](#)
- [It's a feature, not a bug! The saga of the German dole continues](#)
[Debora Weber-Wulff](#)
- [Oops: 'Can Spam Act' seems to be no-can-do](#)
[NewsScan](#)
- [The joys of auto-complete](#)
[Thom Kuhn](#)
- [Panix.com domain name hijacking](#)
[Cyrus R Eyster](#)
- [Are *you* on a list of aggressive drivers? You could be, if I say so!](#)
[Dawn Cohen](#)

- [Most identity theft occurs offline](#)
[NewsScan](#)
 - [Grocery store robot scanner a royal pain](#)
[Mark Rockman](#)
 - [American Express or Phishing?](#)
[John Pettitt](#)
 - [Re: HTTPS .ne. secure](#)
[Robert Ellis Smith](#)
 - ['Hot' URLs in e-mail](#)
[Jay R. Ashworth](#)
 - [REVIEW: "Open Source Security Tools", Tony Howlett](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ 'Thief-proof' car key cracked. What, already?

<"LEESON, Chris" <chris.leeson@atosorigin.com>>

Tue, 1 Feb 2005 10:55:50 -0000

According to an article in **The Register**, the security on RFID devices used in car keys and petrol pump payment systems has been broken (the article actually says "Researchers have discovered cryptographic vulnerabilities in the RFID technology...")

http://www.theregister.com/2005/01/31/rfid_crypto_alert/

The encryption uses "an unpublished, proprietary cipher that uses a 40-bit key".

The researchers managed to reverse-engineer the system and program a microchip to do the decoding in 10 hours. Using 16 of the chips in parallel

reduced the search time to 15 minutes. At about \$200 per chip that's not an expensive brute force attack.

The article notes that although potential criminals could make fraudulent petrol charges and deactivate vehicle immobilisation systems, they would still have to get past physical locks in the car.

Provided that the car has them, of course.

I can't resist quoting from the last two paragraphs:

"The team recommends a program of distributing free metallic sheaths to cover its RFID devices when they are not being used in order to make attacks more difficult.

The company that markets ExxonMobil's SpeedPass system has said it has no knowledge that any fraudulent purchases have ever been made with a cloned version of its device."

The Risks? Well, apart from the fairly obvious security/fraud issues, it does seem to me that this is using technology for technology's sake. When I want to disarm the alarm on my car, I point the remote at it and press the button. I don't need an "always on" control...

Incredible Hulk No-Coaster

<Frank Carey <Carey1938@aol.com>>

Sat, 29 Jan 2005 10:07:47 EST

Several riders were assisted to safety [28 Jan 2005] after a car became stuck on the Incredible Hulk Coaster at Universal Orlando's Islands of Adventure theme park, according to Local 6 News. A Universal spokesman said a computer glitch stopped the train at one of three braking points. Twenty riders walked to safety. Four others in the front of the car were forced to wait until firefighters arrived. There were no injuries reported.
[*Florida Today* 29 Jan 2005, p. 8B]

✶ Tiger triggers the car window

<Wendell Cochran <atrypa@eskimo.com>>
Sun, 30 Jan 2005 08:12:08 -0800

'A stripper mauled by a tiger in an Ontario safari park has won \$650,000 in damages ... 'Jennifer-Anne Cowles was driving through the park ... with her boyfriend when a tiger jumped into their car and tried to drag them away. The two insisted their windows had been shut when the tiger charged ... 'The judge accepted the couple's testimony that the power windows had been inadvertently lowered when one of the big cats bumped against the car. The boyfriend was awarded \$1.37 million. [Source: Reuters item in the *Seattle Times*, 29 Jan 2005. The Times doesn't believe in copyediting wire-service stories, even those from Reuters. WC]

We may indeed have here a computer-related risk, but another

possibility
is gullible-judge risk.

✶ Search engine risks

<"Marcos H. Woehrmann" <marcos@panix.com>>
Tue, 1 Feb 2005 14:36:33 -0500 (EST)

Microsoft today (02/01/05) announced a new and more precise search engine (<http://www.imagine-msn.com/search/tour/moreprecise.aspx>).

As part of the announcement they gave some example searches, one of which was "What is the mass of Jupiter?".

The search.msn.com result for that search does indeed return the mass of Jupiter: "Answer: Jupiter mass: 318 Earth masses". But what is an "Earth mass"?

Entering "What is the mass of Earth?" into search.msn.com produces "Answer: World: mass: 1 Earth masses". I suppose that answer doesn't violate the definition of precise (though to be even more precise they could have said "1.0000 Earth masses"). Entering "What is an Earth mass?" produces the same, meaningless, result.

BTW, entering "What is the mass of Saturn?" into search.msn.com produces: "Saturn: Mass: 5.69x10", which since it's missing its units doesn't seem precise to me (and it's probably not accurate either, unless the missing

units are 10^{25} kilograms).

Just to demonstrate that this isn't too hard I did the same searches on

Google, which produced more reasonable results:

mass of Earth = 5.9742×10^{24} kilograms

mass of Saturn = 5.6851×10^{26} kilograms

mass of Jupiter = 1.8987×10^{27} kilograms

The risk here is that if you give an example search to demonstrate your new search engine capabilities, you should test to see if related searches work

as well. [Or, if you pardon a pun on the ambiguity of "as well",

if they work as poorly. PGN]

Marcos H. Woehrmann marcos@panix.com <http://www.panix.com/~marcos>

German Toll Collect - an exercise in Graph Theory

<Debra Weber-Wulff <weberwu@fhtw-berlin.de>>

Fri, 28 Jan 2005 20:35:40 +0100

The German IT magazine c't reports in its number 2/2005 on the current state

of the German Toll Collect system, which does appear to be functioning and

raking in some money, much to the glee of the politicians who are now

dreaming of exporting this technology.

A few highlights not making the daily newspapers:

* Checking trucks to make sure they paid the toll is easy if the truck has

an OBU (On Board Unit) - mobile checkers can query the box

without stopping
the truck. Trucks without the OBU pass occasional bridges that
photograph
the truck, recognize the license plate, calculate the truck
geometry to
determine the axle count, and then check if this bit is paid for
in the
central data base. There are pull-off areas that were specially
built so
that offenders can be pulled off and fined on the spot.

Unfortunately, when calculating the distance between the bridge
and the
pull-off area the engineers used an optimistic assumption on the
time needed
for the calculations, and used the *middle* of the rest area for
calculating
the distance between the bridge and the rest area. But actually,
if you want
to flag down a truck you have to have someone standing a good
bit before the
rest area.

Since neither moving the pull-off area nor the bridge are
options, traffic
is slowed at these points to give the computers time to grind....

* The mobile checkers have a few problems of their own. Heise
reports in
<http://www.heise.de/newsticker/meldung/mail/55332> that the
checkers use
infrared communication. They have to drive in front of the truck
they are
checking and are having problems during fog and snow. The
company producing
this device insists, however, that there are no problems.

* c't tried to make sense of the public database listing the
autobahn
crossings and the tolls assessed. There is no obvious connection
between the
numbers for the exchanges and the exchanges, some (in different
parts of the

country) even have the same number. Other bits of autobahn are only listed in one direction, not in both. Some crossings have multiple numbers, other multiple names. They used the data to build a graph of the German autobahn (> 2000 edges), a nice exercise for students of computing to then calculate the shortest path between A and B. Interestingly, 23 of the edges are listed as being 0,0 km long. Toll Collect says that these are bits of non-autobahn that connect up isolated autobahn portions.

c't concludes that it will be difficult for a company to prove that they have been charged the wrong toll - and in a new law rushed through in December the government has stated exactly that - Toll Collect does not have to prove that they charged the correct toll, but a shipper has to prove that they were charged the wrong toll.

For those interested in the database:

<http://www.mauttabelle.de/maut.html> (in German)

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

[Slight typo fixed in archive copy. PGN]

⚡ It's a feature, not a bug! The saga of the German dole continues

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

Sun, 23 Jan 2005 15:57:03 +0100

Germany switched to a new dole system on 1 Jan 2005 and has been coping with problems ever since. Many people who submitted their paperwork back in October still do not have money - because the paperwork was "misplaced". [Maybe they were just entering in the data LIFO... --dww]. The media in Germany are enjoying finding problems with the system, especially as the officials are announcing it all a roaring success.

The Heise Ticker (<http://www.heise.de/newsticker/meldung/55427>) notes that the "problem" of the software only counting 360 days to a year is a feature and not a bug. According to spokespeople, it lets them figure the amount of the dole much faster [I didn't realize that the isLeapYear routine took *that* much time to compute.... --dww]. The Westfälischen Nachrichten reported the computation, which is also discussed in Spiegel-online at <http://www.spiegel.de/wirtschaft/0,1518,338133,00.html> will save government about 100 million Euros a year because the payments are done according to a daily rate. All months are now fixed at 30 days.

Other fun games: In order to keep people who just barely earn too much from making themselves eligible for money by purchasing health insurance (which is deductible) they are apparently paying people 1 cent a month so they can keep their cheaper public health insurance.

The problems with the system are being collected in a database in Nürnberg and are sent out in a non-printable PDF file to keep people from printing it

out and giving it to the press. The file has, however, grown larger than 2 MB and is now being rejected by the mail servers throughout the work payment administration. This is the only problem that the officials will admit to in public.

The saga will continue!

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

✶ Oops: 'Can Spam Act' seems to be no-can-do

<"NewsScan" <newsscan@newsscan.com>>

Tue, 01 Feb 2005 07:57:15 -0700

The Can Spam Act went into effect in January of last year, yet unsolicited commercial e-mail on the Internet is now estimated to account for at least 80% of all e-mail sent -- a figure up from 50-60% percent of all e-mail before the law went into effect. A number of critics of the law had argued that it would make the spam problem worse by effectively giving bulk advertisers permission to send junk e-mail as long as they followed certain rules. Steve Linford, the founder of the UK-based Spamhaus Project, says the law "legalized spamming itself." The law's chief sponsor, Senator Conrad Burns (R- Montana) says the problem isn't the law but the ineffective

enforcement of the law: "As we progress into the next legislative session, I'll be working to make sure the FTC utilizes the tools now in place to enforce the act and effectively stem the tide of this burden."
Anne Mitchell
of the Institute for Spam and Internet Public Policy comments:
"Most people say it's a miserable failure, but I see it as a lawyer would see it. To think that law enforcement agencies can make spam stop right away is silly. There's no such thing as an instant fix in the law." [*The New York Times 1 Feb 2005; NewsScan Daily, 1 Feb 2005]
<http://www.nytimes.com/2005/02/01/technology/01spam.html?hp&ex=1107320400&en=f7486f68b21cb2cc&ei=5094&partner=homepage>

The joys of auto-complete

<"Thom Kuhn" <tkuhn@mail.acponline.org>>
Thu, 27 Jan 2005 19:54:57 -0500

A while ago I was listening to a public affairs program on NPR. One of the speakers was representing a trade association, and his comments really got to me. I Googled him and sent him a somewhat venomous e-mail. A few hours later I got an even more venomous reply. End of story? Not quite. My e-mail address was now in his shortcut list. A few weeks later I was copied on what was clearly meant to be an internal and confidential e-mail from this gentleman to this colleagues.

✶ Panix.com domain name hijacking

<Cyrus R Eyster <cyruse@MIT.EDU>>

Mon, 17 Jan 2005 16:55:09 -0500

Quoting from <http://www.panix.com>:

>Panix's main domain name, panix.com, was temporarily hijacked
>over the
>weekend by parties unknown. The false information for the panix.
>com
>domain was present at the top-level Internet domain servers
>from 04:30
>Saturday morning Jan 15 until 6 PM Sunday Jan 16 (US-EST), when
>the
>domain was returned to us. As a result of this attack, mail, Web
>access, and other connectivity to the panix.com domain was
>disrupted.

and

>Panix's main domain name, panix.com, was hijacked by parties
>unknown. The registration of the panix.com domain was moved to a
>company in Australia, the actual DNS records were moved to a
>company
>seemingly in the United Kingdom (but with servers in Canada and
>corporate registration in Delaware), and panix.com's mail was
>redirected to servers in Canada. None of the systems exploited
>to
>perform this hijacking were under Panix's control.

>

>It's not supposed to be possible to transfer a domain name from
>one
>registrar to another without notifying both the current
>registrar and
>the current domain owner, but that's what seems to have
>happened.

>

>As the hijacking occurred over the weekend, we had great trouble
>reaching responsible parties at the other companies involved.

The
>domain was not returned to us until the beginning of the
business day
>in Australia on Monday. None of the companies involved had
support
>numbers that were available over the weekend, or even emergency
>contact numbers.

More info at <http://www.panix.com:> and <http://www.panix.net/hijack-faq.html>

⚡ Are *you* on a list of aggressive drivers? You could be, if I say so!

<"Cohen, Dawn" <dcohen@ets.org>>
Tue, 18 Jan 2005 14:33:03 -0500

Apparently several websites have come up that allow random drivers to report other random drivers for aggressive driving. See a story by Charisse Jones, USA TODAY

http://story.news.yahoo.com/news?tmpl=story&cid=710&e=35&u=/usatoday/20050118/pl_usatoday/websitesletdriversflagroadragers

unsafedriver.com will allow you to register for free, which entitles you to enter reports about other cars. However, you must pay \$24.99 for the first vehicle, and \$14.99 for each additional vehicle, in order to (and these are quotes from the web site)

- * Receive the details of the driving complaints made against your registered vehicles.

- * Keep the complaints made against your registered vehicles confidential
subject to our Terms and Conditions
- * Attach a dispute to any complaints made against your registered vehicles
- * Check any plate for violations.

This sounds an awful lot like that scam that was going around a couple of years ago...Word-of-Mouth.org, right?

I haven't dug deeply into this, but Yahoo reports that the unsafedriver.com site was started by Lt. Mark Hafkey of the Phoenix Police Department (though it's a "private business", not affiliated with the police department).

I have successfully registered at this site, using, let's just say sketchy data. I have verified that this permits me to enter a report about an "incident". It gives me a choice, as an incident reporter to "remain anonymous" or "I am willing to be contacted by Law Enforcement or an Insurance Carrier via e-mail for clarification and/or further investigation if necessary."

This smells like a scam to me, but I'm surprised that it would be perpetuated by a source as reputable as USA Today. If it's not a scam, it's an outrage.

⚡ Most identity theft occurs offline

<"NewsScan" <newsscan@newsscan.com>>

Thu, 27 Jan 2005 10:44:39 -0700

Despite growing concerns over online fraud, a new study conducted by the Better Business Bureau and Javelin Research finds that most cases of identity theft can be traced to a lost or stolen wallet or checkbook, rather than vulnerable online financial data. Computer crimes make up just 12% of all ID fraud cases in which the origin is known, and half of those are attributed to spyware that sneaks onto computers and steals private information. [AP, 27 Jan 2005; NewsScan Daily, 27 Jan 2005]
<http://apnews.excite.com/article/20050127/D87SE8NO0.html>

✂ Grocery store robot scanner a royal pain

<"Mark Rockman" <mrockman@acm.org>>
Thu, 27 Jan 2005 03:57:36 -0500

The local chain grocery store recently got rid of its personnel problem by hiring a customer-operated robot scanner. The scanner comes with a series of metal bridges that overarch the conveyor belt. The store had removed the arches from the machines because the arches prevent large items from proceeding to the item storage area at the end of the belt. I bought a large, economy size package of paper towels. It would be stopped by the arches, were they in place. The software "knows" about the arches and stopped my checkout process cold while it called a store employee to manually move the package to the end of belt, a process that had

already
completed.

The robot scanner "weighs" items as they travel along the belt, a security measure to ensure the customer placed the scanned item on the belt. I watched the customer in front of me try to buy the candy bar she had eaten, while shopping, by placing the scanned wrapper on the belt. No soap. The wrapper didn't weigh enough. She tried three times to buy the candy bar. Her solution: get another candy bar from the handy display in the checkout aisle and buy 1, get 1 free.

The robot scanner refuses to transact business while anything is traveling down the conveyor belt. Its mechanical voice instructed me to "wait" while it did its business. I was trying to pay for my order. A human clerk who did that may well lose her job.

Before experience taught what the machine expects from me, I tossed items that I had scanned onto the belt. Sometimes this would put the item too far along to be "weighed." The machine refused to recognize the object, reversed belt motion to return the item, and credited my bill. There was no sufficient explanation for this behavior until a human employee provided insight.

Buying fruits and vegetables with robot is a trip. You press a GUI button and are presented with page upon page of photographs of fruits and vegetables organized I don't know how. People spend a great deal of time

trying to identify the item at hand and do not understand that some fruits and vegetables must be weighed, at the scanning station not the belt, for the cost to be figured.

Bagging groceries with a robot is left to the customer unless some store employee takes pity.

You can be bagging furiously, having paid for your items, while the next customer is sending his items to commingle with yours.

The motivation for these devices is obvious: lower cost to the low margin store. The introductory customer instruction was nil and remains nil. I'm surmise there is a certain acceptable level of loss of goods not paid for because the machine cannot catch everything a customer might do.

American Express or Phishing?

<John Pettitt <jpp@cloudview.com>>
Tue, 01 Feb 2005 09:03:28 -0800

I just got this in my e-mail.

> Dear Cardmember,
>
> Your 2004 Year-End Summary is now ready to view online. To
access your
> Year-End Summary, please log in to
> <http://americanexpress.com/yearendsummary2004>
> <[http://www65.americanexpress.com/clicktrk/Tracking?
mid=IUYES03020050201053636024433&msrc=ENG-YES&url=https://www124.
americanexpress.com/cards/yes/yes_home.jsp?
campaignid=Jan_email_05](http://www65.americanexpress.com/clicktrk/Tracking?mid=IUYES03020050201053636024433&msrc=ENG-YES&url=https://www124.americanexpress.com/cards/yes/yes_home.jsp?campaignid=Jan_email_05)>.

>
> With the online version you can view charges by merchant name,
date,
> or charge amount; view your spending, spending of an
Additional Card,
> or everything at once; and print and save your Year-End
Summary for
> future use. As a *new* feature this year, you can also use
business
> and personal check boxes to sort your annual transactions.
>
> We look forward to serving you.

As far as I can tell it's real - the sites it links to have
certificates
that are issued to Amex. However there is no way to tell
without clicking
the link and checking the certificate (something I teach my
users not to do)
that the mail really came from Amex. Even the message headers
show it
originating from aexp.com which sounds close but then so do the
best
phishing scams.

Given that a large percentage of the world now uses s/mime
capable mailers
(Outlook, Outlook express, Thunderbird, Mozilla, etc.), why is
it that
institutions are still sending unsigned e-mail?

✉ Re: HTTPS .ne. secure (Epstein, [RISKS-23.68](#))

<"Robert Ellis Smith" <ellis84@rcn.com>>

Sun, 30 Jan 2005 18:38:00 -0500

> I went to their web page, and filled out the form using name,
address, SSN,

Why, why WHY is a participant in the RISKS list submitting an SSN on-line and why is he even providing an SSN when making an address change? We gotta resist, this so that organizations are sensitized to the risks of using SSNs.

Robert Ellis Smith, Publisher, Privacy Journal, PO Box 28577, Providence RI 02908 ellis84@rcn.com 1-401/274-7861 <http://www.privacyjournal.net>

[R-23.68](#) 'Hot' URLs in e-mail (Re: PayPal contradicting..., Huckvale, [R-23.68](#))

<"Jay R. Ashworth" <jra@baylink.com>>
Mon, 31 Jan 2005 21:44:34 -0500

In [RISKS-23.68](#), Tim Huckvale bemoans the fact that after giving good advice to it's clients about how to avoid phishing attacks in an e-mail it sent him, PayPal then made the mistake of making the URL in it's message a 'hot' link.

I'm not sure which e-mail program he's using; he doesn't say.

But it's worth noting that that e-mail (and it's sender) may not be at fault. Some *mail programs* heat up those links 'for you'. The RISK? Assuming you know where the RISKS are actually *coming* from.

Mozilla's Thunderbird browser is getting anti-phishing measures even as I type. A bit later than I'd have liked. But at least they're

there.

Jay R. Ashworth, Designer, Ashworth & Associates, St Petersburg
FL USA

<http://baylink.pitas.com> +1 727 647 1274 jra@baylink.com

[We received a slew of e-mail on this subject. I picked just
one
thus far. PGN]

★ REVIEW: "Open Source Security Tools", Tony Howlett

<Rob Slade <rslade@sprint.ca>>

Fri, 28 Jan 2005 08:01:11 -0800

BKOPSOST.RVW 20041203

"Open Source Security Tools", Tony Howlett, 2005, 0-321-19443-8,
U\$49.99/C\$71.99

%A Tony Howlett tony@howlett.org

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

%D 2005

%G 0-321-19443-8

%I Prentice Hall

%O U\$49.99/C\$71.99 +1-201-236-7139 fax: +1-201-236-7131

%O <http://www.amazon.com/exec/obidos/ASIN/0321194438/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0321194438/robsladesinterne)

<http://www.amazon.co.uk/exec/obidos/ASIN/0321194438/>

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0321194438/robsladesinte-21)

%O <http://www.amazon.ca/exec/obidos/ASIN/0321194438/>

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0321194438/robsladesin03-20)

%O t1 a r1 2 tc 3 ta 3 tv 2 wq 2

%P 578 p. + CD-ROM

%T "Open Source Security Tools"

The tools listed in this book are for network security, almost
without

exception. The preface states that the book is intended

primarily for systems administrators, although security professionals may find useful information as well. Howlett makes an effort to include items that have Windows versions, although only about a third do. He has also included tutorial materials on detailed aspects of the TCP/IP protocols that have a bearing on the operation of security software.

Chapter one outlines the open source concept, starting with a fairly idealized scenario, but continuing with some history, advantages (and disadvantages), and a brief look at two of the major open source licences.

The nominal topic of chapter two is operating systems, and so it is rather odd that most of the tools described are network utilities.

However, the descriptions are better than are given in most reviews of software tools, and the details are clear for all who may read them. While chapter three does provide a quick overview of TCP/IP and filtering, it does not cover the full range of firewall types. The programs listed are comprehensively described in terms of installation and administration commands.

Port scanning is covered in chapter four, and, again, while the programs are explained well, other details, such as the services that would need to be turned off to reduce the danger of open ports, are not. Much the same can be said about the discussion of vulnerability scanners, in chapter five.

Chapter six looks at the most widely used network sniffers. The concepts behind, and examples of, both network- and host-based intrusion

detection

systems are given in chapter seven. Logging and audit data can accumulate quickly and overwhelm the administrator, so chapter eight reviews some common tools to present, analyse, and manage the information. Chapter nine lists a variety of encryption tools. Wireless tools, primarily for finding networks, are given in chapter ten. Forensic tools are examined in chapter eleven, but there may not be a sufficient distinction made between the network and data recovery tools. Chapter twelve finishes off with some more general discussion about open source software, and where to find it.

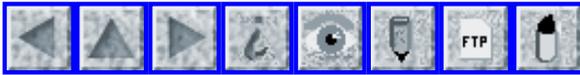
There are some helpful appendices: well-known TCP/IP port numbers, and a large list of plug-ins for Nessus.

The tutorial material could have had more depth and care, but there is no denying the value of the compilation (particularly with all the software included on the CD).

copyright Robert M. Slade, 2004 BKOPSOST.RVW 20041203
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

Volume 23: Issue 70

Weds 9 February 2005

Contents

- [Off-by-one error: Evacuate the entire state!](#)
[Howard M Israel](#)
- [Food via inkjet printer](#)
[Joyce Scrivner](#)
- [An example of vulnerable OS creating havoc in new/unexpected locations](#)
[Karl Klashinsky](#)
- [What's Bugging the High-Tech Car?](#)
[Tim Moran via Howard M Israel](#)
- [Zuerich Main Railway Station Outage](#)
[Peter B. Ladkin](#)
- [Supermarket: Let your fingers do the paying](#)
[Monty Solomon](#)
- [How GPS Is Killing Lighthouses](#)
[sakshale](#)
- [J.K. Rowling denounces Internet fraudsters](#)
[NewsScan](#)
- [Most Dangerous Types Of Spyware Increasing, States SpyAudit Survey](#)
[Monty Solomon](#)
- [Spammers try a new tack](#)
[NewsScan](#)
- [Goofy account identification](#)
[Geoff Kuenning](#)
- [The Land Registry](#)
[Ben Laurie](#)
- [Weak on the concept](#)
[Elias Levy via PGN](#)
- [U of Calgary adding spam and spyware](#)
[Rob Slade](#)
- [Re: Thief-proof car key cracked. What, already?](#)

[Steve Wildstrom](#)

● [Re: It's a feature, not a bug!](#)

[Kees Huyser](#)

● [Re: 'Hot' URLs in e-mail](#)

[William L Anderson](#)

● [Balancing security and our lives](#)

[Jeremy Epstein](#)

● [REVIEW: "Managing Security with Snort and IDS Tools", Cox/Gerg](#)

[Rob Slade](#)

● [COMPSAC 2005: Extended deadline for paper submission](#)

[Yuen Tak YU](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Off-by-one error: Evacuate the entire state!

<Howard M Israel <hisrael@avaya.com>>

Wed, 2 Feb 2005 11:33:13 -0500

Connecticut state emergency management officials said a worker entered the wrong code during the weekly test of the emergency alert system, leading television viewers and radio listeners to believe that the state was being evacuated: "Civil authorities have issued an immediate evacuation order for all of Connecticut, beginning at 2:10 p.m. and ending at 3:10 p.m." The code that was mistakenly entered appeared on a monitor one line above the intended code for the test. As soon as the error was detected, faxes went out to every police department in the state.

Source: Emergency broadcast test mistakenly calls for evacuation, AP item [PGN-ed], The Hartford Courant, 1 Feb 2005, <http://www.ctnow.com/http://www.nynewsday.com/news/local/wire/ny-bc-ct---evacuationerror0201feb01,0,6738941.story>

⚡ Food via inkjet printer

<Joyce Scrivner <kscriv@earthlink.net>>

Fri, 04 Feb 2005 11:24:48 -0600

Moto, a Chicago restaurant, serves "sushi" with maki-like images printed with a Canon i560 inkjet printer using organic food-based inks jetted onto edible "paper" made from soybeans and cornstarch and flavored with powdered soy and seaweed seasonings. Even the menu is edible.

<http://www.nytimes.com/2005/02/03/technology/circuits/03chef.html?>

[ei=5088&en=86bc342e2ce05d47&ex=1265086800&partner=rssnyt&pagewanted=print&position=](http://www.catless.ncl.ac.uk/Risks/23.70.html#ei=5088&en=86bc342e2ce05d47&ex=1265086800&partner=rssnyt&pagewanted=print&position=)

[This article has been severely PGN-ed. Actually, squid ink might be an interesting choice, unless it would clog the jets. Joyce wondered whether a diner could be poisoned by the inkjet food. But perhaps the menu is also printed from the same printers, using the same inks, and not used for other porpoises? You might ask, what do they do for cuttlery? (That's a pun, not a misspelling; a cuttlefish has 10 arms, and is related to the squid. A live one might make an interesting array of chopsticks.) And, if you knew Sushi like I know Sushi, you might want to Moto-r on over. Or maybe not. It might be overpriced, but not overriced. And the chef will maki-a-velli nice presentation. PGN]

✦ An example of vulnerable OS creating havoc in new/unexpected locations

<Karl Klashinsky <klash@cisco.com>>

Wed, 26 Jan 2005 16:02:43 -0800

The topic of software flaws in the embedded systems within modern automobiles has been discussed in RISKS several times. But here's a new twist (to me, at least), a case where the on-vehicle software is corrupted by a virus, inserted into the automobile's computing systems, via a blue-tooth enabled cell-phone:

URL CHANGED FROM

<http://www.infosecnews.com/news/index.cfm?fuseaction=newsDetails&newsUID=bc5789cf-e448-4a6e-bee9-a5dd291405ed&newsType=News>

TO (CORRECTED):

<http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=bc5789cf-e448-4a6e-bee9-a5dd291405ed&newsType=Latest%20News>

[Same article in shorter URL: <http://tinyurl.com/5p3jh>]

There's the obvious risk here... a vehicle can be infected by the cell-phone in the vehicle next to you while stopped in traffic or sitting in a parking lot. As this vulnerability becomes known in the cracker community, how long before someone tailors a virus specific to a vehicular target -- perhaps creating runaway-vehicle scenarios similar to the "faulty cruise control" incidents reported here in RISKS.

✦ What's Bugging the High-Tech Car? (Tim Moran)

<Howard M Israel <hisrael@avaya.com>>

Mon, 7 Feb 2005 09:29:29 -0500

Tim Moran, What's Bugging the High-Tech Car? *The New York Times*, 6 Feb 2005
<http://www.nytimes.com/2005/02/06/automobiles/06AUTO.html?oref=3Dlogin>

On a hot summer trip to Cape Cod, the Mills family minivan did a peculiar thing. After an hour on the road, it began to bake the children. Mom and Dad were cool and comfortable up front, but heat was blasting into the rear of the van and it could not be turned off. Fortunately for the Mills children, their father - W. Nathaniel Mills III, an expert on computer networking at I.B.M. - is persistent. When three dealership visits, days of waiting and the cumbersome replacement of mechanical parts failed to fix the problem, he took the van out and drove it until the oven fired up again. Then he rushed to the mechanic to look for a software error.

"It took two minutes for them to hook up their diagnostic tool and find the fault," said Mr. Mills, senior technical staff member at I.B.M.'s T. J. Watson Research Center in Hawthorne, N.Y. "I can almost see the software code; a sensor was bad."

✈ Zuerich Main Railway Station Outage

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Tue, 08 Feb 2005 11:49:54 +0100

On Monday, 7th February the central computer at the rail control center for Zuerich main station in Switzerland failed. The outage was noticed at 08:40, and had deleterious consequences for further control centers which were dependent on the Zuerich center. It was partially back on-line at 13:40. No cause has yet been announced.

Zuerich is the largest city in Switzerland, and the train lines converging on the main railway station are fairly complicated. Chaos was reported. The Associated Press reported that trains between Zuerich and Pfaffikon, a commuter line on the left bank of Lake Zuerich, were all canceled for nearly four hours. Buses were used to ameliorate the situation, for example for trains in the direction of Chur. The Swiss television SF-DRS was reporting on its WWW site that many commuters were delayed by two and a half hours. Also that the trip between Lachen SZ and Zuerich, normally 45 minutes, took four hours.

The Swiss railway is renowned for its punctuality. They are amongst the foremost, maybe the foremost, in the world in research into railway scheduling and its implementation in the RAIL 2000 program. I heard a talk at the FORMS/FORMAT 2004 conference from Oskar Stalder about experiments in continual punctuality information transfer to drivers, which enabled the equipped trains to maintain a schedule on certain main lines to within a ten-twenty-second margin of error - almost unthinkable. This incident will worsen the stats for 2005 just a little.

The information about the outage came from

<http://www.sfdrs.ch/system/frames/news/sda-news/index.php?/content/news/sda-news/meldung.php?docid=20050207d395595158238553833>

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

✈ Supermarket: Let your fingers do the paying

<Monty Solomon <monty@roscom.com>>

Wed, 2 Feb 2005 02:04:53 -0500

Excerpted from an article by Jo Best, news.com, 1 Feb 2005

A supermarket has given its customers the choice of paying by fingerprint at a store in the state of Washington--and has found them surprisingly willing to use the biometric system. U.S. chain Thriftway introduced the system, which uses technology from Pay By Touch, in its store in the Seattle area in 2002. It said it now sees thousands of transactions a month using the payment method. Once people have enrolled in the Pay By Touch system, they have their fingerprint scanned as verification of identity at the checkout. They then choose which credit card they want to pay the bill with, having already registered the credit cards with the store.

Thriftway President Paul Kapioski said rather than shying away from the technology because of concerns about protecting their privacy, customer demand ensured that the biometric payment system made it past the pilot stage. ...

<http://news.com.com/2100-1029-5559074.html>

✈ How GPS Is Killing Lighthouses

<sakshale@equoria.net>

Tue, 8 Feb 2005 18:08:43 -0500

Spiegel Online has an article about the impact of GPS systems on Lighthouses. They claim that the popularity of the satellite-based global positioning system has led to the closure of lighthouses along the German coast. Critics question whether the new system is reliable and safe enough to warrant the closure of these historical beacons of safety.

<http://service.spiegel.de/cache/international/0,1518,340729,00.html>

✦ J.K. Rowling denounces Internet fraudsters

<"NewsScan" <newsscan@newsscan.com>>

Wed, 02 Feb 2005 12:09:39 -0700

J.K. Rowling, author of the mega-popular Harry Potter series, is warning fans to beware of Internet "phishing" scams claiming to sell electronic copies of her latest book, "Harry Potter and the Half-Blood Prince." "The only genuine copies of Harry Potter remain the authorized traditional book or audio tapes/CDs distributed through my publishers," says Rowling, and her copyright lawyer, Neil Blair, notes that Rowling has never granted licenses for electronic versions of her books. "Please, please protect yourselves, your computers and your credit cards and do not fall for these scams," says Rowling. Police say they suspect organized crime gangs in Eastern Europe are behind the fraudulent e-mail offers. [Reuters/*The Washington Post*, 2 Feb 2005; NewsScan Daily, 2 Feb 2005]

<http://www.washingtonpost.com/wp-dyn/articles/A56379-2005Feb2.html>

✦ Most Dangerous Types Of Spyware Increasing, States SpyAudit Survey

<Monty Solomon <monty@roscom.com>>

Wed, 2 Feb 2005 09:35:22 -0500

The most malicious forms of spyware, system monitors and Trojans, increased in the last three months of 2004, according to the quarterly SpyAudit report, the nation's next-generation Internet Service Provider, and Webroot Software, a producer of award-winning privacy, protection and performance software. The report also documents the complete SpyAudit results for 2004, which tracked the growth of spyware on consumer PCs since the report's inception on January 1, 2004. It shows the instances of system monitors rose 230 percent, while the instances of Trojans rose 114 percent from October 2004 to December 2004. Trojans, keystroke loggers and system monitors are capable of capturing keystrokes, online screenshots, and personally identifiable information like your social security number, bank account numbers, logins and passwords, or credit card numbers.

The number of SpyAudit scans performed during the fourth quarter also rose with an increase of 72 percent from October 2004 through December 2004. In total for 2004, more than 4.6 million scans were performed, discovering approximately 116.5 million instances of spyware, adware or potentially unwanted software. An average of 25 traces were found per SpyAudit scan for 2004. The complete report is available at

<http://www.earthlink.net/spyaudit/press> . . .

PR Newswire, 2 Feb 2005

<http://finance.lycos.com/home/news/story.asp?story=46604321>

✂ Spammers try a new tack

<"NewsScan" <newsscan@newsscan.com>>

Fri, 04 Feb 2005 10:02:08 -0700

Tired of being blocked by "blacklists," spammers are turning to a new technique -- routing it directly through the computers of their Internet service providers, rather than sending it from individual machines. The result poses a dilemma: to block spam coming directly from an ISP's servers would mean blocking all its mail, crippling the system. "From what we've seen, the volumes of this type of spam are going up dramatically," says Steve Linford, who heads up the Spamhaus Project. "We're really looking at a bleak thing" if ISPs don't quickly deploy countermeasures, he adds. Such measures could include more aggressive monitoring and limiting how much mail is being sent from individual machines on their networks. In addition, ISPs should beef up efforts to authenticate mail they pass on through their own computers, says Linford. A study released yesterday estimates that deleting spam costs nearly \$22 billion per year in lost productivity, based on a survey of 1,000 adults who said they spend about three minutes per day trashing spam when they check their e-mail. (*The Washington Post*, 4 Feb 2005; NewsScan Daily, 4 Feb 2005)

<http://www.washingtonpost.com/wp-dyn/articles/A61901-2005Feb3.html>

✂ Goofy account identification

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

01 Feb 2005 23:30:25 +0100

To make a fairly long detective story very short, I have discovered that amazon.com uses not only your e-mail address, but also your password, to uniquely identify your account. It is perfectly possible to have two completely different accounts under the same e-mail address, distinguished only by the password.

Huh?

My guess is that Amazon does this to make it possible for people who share a single e-mail account to have different accounts at Amazon. But it's not documented anywhere, and can lead to great confusion for those who forget that they have an account, create a new one, and later use the original one's password.

And I wonder what happens when you click on the "Forgot your password?" link. Do they reset the passwords on all accounts? When I have a bit more time, I might set up some accounts on a dummy e-mail address to answer to latter question. -- Geoff Kuenning geoff@cs.hmc.edu
<http://www.cs.hmc.edu/~geoff/>

✂ The Land Registry

<Ben Laurie <ben@algroup.co.uk>>
Tue, 01 Feb 2005 22:33:56 +0000

The UK Government has decided to make the Land Registry available online. For those who don't know, this says who owns a property, what the property is (i.e., the boundary), who has charges on the property, similarly whether covenants apply, and so forth.

I suppose this risk isn't new, since this information was available offline, but ... one of the people with a charge on your house is your mortgage lender. This is clearly stated in the Land Registry document. What an excellent resource for phishing and other fraud - both via e-mail and more personal contact.

The relevant Land Registry data is available to all comers for 2 pounds. No restrictions. And now, much easier to get.

<http://www.apache-ssl.org/ben.html> <http://www.thebunker.net/>

✂ Weak on the concept

<"Peter G. Neumann" <neumann@csl.sri.com>>
Tue, 1 Feb 2005 17:15:39 PST

Elias Levy (Symantec) noted a cute illustration of the weakest link in a would-be security system:

<http://www.syslog.com/~jwilson/pics-i-like/kurios119.jpg>

✂ U of Calgary adding spam and spyware

<Rob Slade <rslade@sprint.ca>>
Sun, 6 Feb 2005 16:53:48 -0800

The University of Calgary is back at it again.

<http://www.cbc.ca/story/canada/national/2005/02/05/email-course050205.html>
<http://pages.cpsc.ucalgary.ca/~aycock/>
aycock@cpsc.ucalgary.ca, barker@cpsc.ucalgary.ca

(Interesting that his homepage is entitled "Unfettered by Content." He certainly seems to be unfettered by logic.)

This time they are adding spam and spyware to the curriculum.

I can vaguely see a dim advantage to having students write viruses in order to understand them (rather inefficiently, in terms of time spent), but getting them to write a spamming program in order to understand how to fight spam seems even less effective.

As previously noted, John Aycock doesn't seem to have any credentials in security or malware (no papers published prior to the virus course, nobody in the field seems to know him), so why he, and the university, chose to do this, other than pure self-promotion, is completely beyond me.

I am somewhat relieved by the fact that the paper submitted to EICAR shows that a modicum of thought was given to the security of the laboratory. The irrelevance of the measures undertaken is no great surprise. The bibliography is interesting: Lugwig's second edition is there, along with Mitnick's "19 chapters of gotcha," but on the AV side Cohen's 1994 edition stands alone with Skoudis' rather pathetic work. I would have thought that anyone with even a pretence of academic intentions would have consulted Ferbrache, and possibly Nazario's pompous but flawed attempt at worm analysis. Given Aycock's involvement in a rather banal crypto lab, I'm a bit surprised that he hasn't tried to create Young and Yung's proposed crypto-nasties.

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>

🔥 Re: 'Thief-proof' car key cracked. What, already? (RISKS 23:69)

<"Steve Wildstrom" <steve_wildstrom@businessweek.com>>
Mon, 7 Feb 2005 11:05:27 -0500

I'm late reading and others have probably pointed this out, but Chris Leeson misstates the purpose of the RFID chip in car keys. These are "immobilizer" systems, designed to keep the car from starting, even with a physical key present, unless the RFID tag responds correctly to a crypto challenge.

The full paper, by Steve Bono, Matthew Green, Adam Stubblefield, and Avi Rubin of Johns Hopkins and Ari Juels and Michael Szydlo of RSA, is

available at <http://rfid-analysis.org> <<http://rfid-analysis.org/>> .

Steve Wildstrom, BusinessWeek 1200 G St NW Suite 1100, Washington, DC 20005
www.businessweek.com/technology/

[Also noted by Alexandre Peshansky. PGN]

✈ Re: It's a feature, not a bug! (Weber-Wulff, [RISKS-23.69](#))

<Kees Huyser <kees@huyser.net>>

Wed, 2 Feb 2005 01:28:18 +0100

> a non-printable PDF file

ehhh... non-printable? Hit "print screen"... If you want it to look nicer, OCR the screendump. Even the press should be able to figure this one out. Obviously the Govt. agency responsible for the mess hasn't, which could explain why it is such a mess...

[Dag-Erling Smørgrav says use GNU Ghostscript. PGN]

✈ Re: 'Hot' URLs in e-mail (Ashworth, [RISKS-23.69](#))

<William L Anderson <band@acm.org>>

Wed, 02 Feb 2005 11:16:56 -0500

There's a small fact error in this piece:

Mozilla Thunderbird is an e-mail client.
Mozilla Firebird (and Camino (for the Mac)) are the browsers.

✈ Balancing security and our lives

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

Wed, 2 Feb 2005 11:23:32 -0500

In [RISKS-23.68](#) I wrote about security problems with changing my address online through Bank of New York, and in [23.69](#) Robert Ellis Smith (justifiably) criticized my original action, saying "We gotta resist, this

so that organizations are sensitized to the risks of using SSNs."

After feeling suitably red-faced about my error, I pondered his point. How much can and should we, as the cognoscenti, do in our every day lives to fight silly security? I know full well that most of the airport security is useless (Schneier and others have done a great job pointing this out), but I don't have the luxury of fighting it every time I make a trip. While I might object to showing an ID, unlike John Perry Barlow, I need to earn a living. I don't have the financial or time option of fighting a court case because I think the rule is wrong. I don't even have the time to argue with the underpaid TSA person about the rules, which say you don't have to take off your shoes (but woe be unto you if you refuse).

This was recently driven home to me as I helped my daughter with college applications, which routinely ask for SSNs. We compromised that when the form is asking about financial information, we'd provide the SSN, since they're asking for copies of tax returns which have the SSN anyway, but we wouldn't put the SSN on the general application for admission. Is this the right tradeoff? If she weren't asking for financial aid, I'd probably refuse to provide the SSN at all.

What are some *practical* measures that we can and should be doing as computer security professionals to help further understanding? I agree with Robert Ellis Smith that I shouldn't provide the information I did to change an address, but I need to get the procedure done, and not spend a week arguing that they shouldn't need my SSN to do a change of address.

I suggest that we'd be more effective if we all tried to do *something*, rather than despairing about our inability to accomplish all the changes we'd like to see. Smith's web page has a good list (<http://www.privacyjournal.net/bio.htm>); how many of us have the time & energy to do more than a handful of them? He hits the nail on the head when he says ``Choose your battles. Not every collection of personal information or every intrusion is worth expending your energy. Decide which information is most sensitive to you and which moments in your life are most important to protect.''

Where can and should working security professionals draw the line?

REVIEW: "Managing Security with Snort and IDS Tools", Cox/Gerg

<Rob Slade <rslade@sprint.ca>>
Wed, 9 Feb 2005 08:20:13 -0800

BKMSWSIT.RVW 20041106

"Managing Security with Snort and IDS Tools", Kerry Cox/Christopher Gerg, 2004, 0-596-00661-6, U\$39.95/C\$57.95
%A Kerry Cox

%A Christopher Gerg
%C 103 Morris Street, Suite A, Sebastopol, CA 95472
%D 2004
%G 0-596-00661-6
%I O'Reilly & Associates, Inc.
%O US\$39.95/C\$57.95 800-998-9938 fax: 707-829-0104 nuts@ora.com
%O <http://www.amazon.com/exec/obidos/ASIN/0596006616/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0596006616/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/0596006616/robsladesin03-20>
%O tl a rl 2 tc 3 ta 3 tv 2 wq 2
%P 269 p.
%T "Managing Security with Snort and IDS Tools"

Chapter one explains what Snort, and network intrusion detection, is. The basics of network traffic sniffing and analysis, and the operation of tcpdump and ethereal, are described in chapter two. Installation, options, and the basic operation of Snort are outlined in chapter three. Chapter four details the different types of blackhat and intruder activity in terms of network intrusion. Chapter five details the configuration file and choices. How, and where, to use and set up Snort is the topic of chapter six. Snort rules are explained in chapter seven, which also outlines the system for creating them. Snort can also be used for intrusion prevention, as chapter eight points out. Tuning sensitivity, and establishing thresholds and clipping levels, is discussed in chapter nine. Chapter ten reviews the use of ACID (Analysis Console for Intrusion Detection) as a management console. An alternative program is SnortCenter, described in chapter eleven, and more options are listed in twelve. Chapter thirteen notes possibilities for the use of Snort in high bandwidth situations.

For those interested in the standard intrusion detection program, here is a set of useful explanations for its use and operation.

copyright Robert M. Slade, 2004 BKMSWSIT.RVW 20041106
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>

COMPSAC 2005: Extended deadline for paper submission

<CS Asst Prof Dr Yuen Tak YU <ytyu@cs.cityu.edu.hk>>
Tue, 8 Feb 2005 05:40:18 +0800 (HKT)

The 29th Annual International Computer Software and Applications Conference
COMPSAC 2005

Edinburgh, Scotland, July 25-28, 2005
<http://aquila.nvc.cs.vt.edu/compsac2005>

The major theme will be HIGH ASSURANCE SOFTWARE SYSTEMS.

Please note that the deadlines for submission of both regular and workshop papers to COMPSAC 2005 have recently been extended.

The EXTENDED deadline for paper submission is only three weeks away:

** Extended deadline for conference papers: Feb 28, 2005 **

** Extended deadline for workshop papers: Feb 28, 2005 **

Deadline for fast abstracts (unchanged): Mar 21, 2005

E-mail enquiries

-Program Co-Chairs: irchen@cs.vt.edu rni@inf.ed.ac.uk meih@pku.edu.cn

-Workshop Chair: ewong@utdallas.edu

-Fast Abstract Co-Chairs: xie@cs.pdx.edu ylei@cse.uta.edu

-Steering Committee Chair: yau@asu.edu

Y T Yu, Publicity Chair, COMPSAC 2005

Department of Computer Science, City University of Hong Kong

csytyu@cityu.edu.hk <http://www.cs.cityu.edu.hk/~ytyu>

COMPSAC is a major international forum for researchers, practitioners, managers, and policy makers interested in computer software and applications. It was first held in Chicago in 1977, and since then it has been one of the major forums for academia, industry, and government to discuss the state of art, new advances, and future trends in software technologies and practices. The technical program includes keynote addresses, research papers, industrial case studies, panel discussions and fast abstracts. It also includes a number of workshops on emerging important topics.

For more detailed and updated information, please refer to

<http://aquila.nvc.cs.vt.edu/compsac2005>

For further information, please contact:

Stephen S. Yau, Arizona State University, USA

E-mail: yau@asu.edu



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 71

Saturday 12 February 2005

Contents

- [Australian Frigate reversed onto rocks by computer override](#)
[Anton Lak](#)
- [More uses of satnav/GPS](#)
[David Magda](#)
- [Urology medical student residency "matching" process failure](#)
[Daniel Kahn Gillmor](#)
- [Congressman Ron Paul R-TX Understands Risks and Countermeasures](#)
[Larry Sudduth](#)
- [Flexibility destroys identity uniqueness: Implementing of IDN](#)
[Jon Lingard](#)
- [Exploding cell phone shocks 911 dispatcher](#)
[Keith A Rhodes](#)
- [RFID Tagging Elementary School Children](#)
[Peter H. Coffin](#)
- [The risk of high-speed CD/DVD-rom drives in current-day PCs](#)
[Henk Langeveld](#)
- [You type Zuerich and I type Zurich... A brief note](#)
[David G. Bell](#)
- [Another MS Word info leak](#)
[Richard Akerman](#)

- [High Risk Vulnerabilities in Eudora for Windows](#)
[NGSSoftware via Monty Solomon](#)
 - [Re: U of Calgary adding spam and spyware](#)
[Hendrik Matthew Holmes](#)
 - [Re: Food via inkjet printer](#)
[Brian Reynolds](#)
 - [Minireview: Bill Neugent, No Outward Sign](#)
[PGN](#)
 - [REVIEW: "A History of Computing Technology", Michael R. Williams](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Australian Frigate reversed onto rocks by computer override

<<anton_lak@telstra.com>>

Thu, 10 Feb 2005 11:17:02 +1100

Computer overrides the crew and reverses the Frigate onto rocks,
a classic
risk of such automation.

<http://www.news.com.au/story/0,10117,12204297-26618,00.html>

Frigate on the rocks, By Ian McPhedran, 10 Feb 2005

The [Royal Australian] navy's newest \$500 million warship was driven backwards on to Christmas Island after crew error caused computers to take control of the frigate. A series of errors prompted the computer system to over-ride manual commands and the ship's company had to stand by and watch as HMAS Ballarat backed on to the rocky shoreline. The 3600-tonne high-tech Anzac class frigate, delivered last April, carries a missile-armed

helicopter and has a 127mm gun, torpedoes and missiles.

The 22 Jan incident damaged both propellers and the rudder and left taxpayers with a bill of about \$2 million and the navy with a major headache. The debacle began when the ship was conducting a boat transfer during a planned U-turn manoeuvre. It was operating in "port echo" or economy mode at the time.

The Daily Telegraph has been told the move was supposed to take the warship inside a buoy which had another ship's mooring line attached to it. As the ship approached the buoy it became clear to the crew on the bridge that it would not make it and would pass over the line, so they attempted to make an urgent "three-point" turn. This was when things started to go seriously wrong.

Because the ship had only one of its three engines running, the crew tried and failed to run one propeller forward and one astern to conduct the radical turn. Such a move is impossible with just one engine running. At this point the control system froze, the ship's computer took over and placed both propellers into reverse. It shut down the engine soon afterwards, but by that stage the ship was travelling in reverse at a couple of knots.

[Essentially the same article, with *The Daily Telegraph* replaced with

The Courier-Mail (Brisbane) was submitted by David Tombs. PGN]

<http://www.couriermail.news.com.au/common/>

story_page/0,5936,12199057%255E953,00.html

✶ More uses of satnav/GPS

<David Magda <dmagda@ee.ryerson.ca>>

Sat, 12 Feb 2005 10:05:15 -0500

BBC news is reporting [1] that British Rail is thinking of use sat-nav / GPS to help keep trains running on time.

I hope they realize that GPS may be shut off by the US government during emergencies or terrorist acts (see [RISKS 23.62](#)). Hopefully someone will at least think about using Galileo [2] as a back up, or even better, use inertial guidance [3] as the primary system with satellite navigation as the backup system.

The same concerns are applicable to any transportation system (e. g., cars, boats, airplanes).

[1] <http://news.bbc.co.uk/2/hi/science/nature/4247721.stm>

[2] <http://www.esa.int/export/esaNA/galileo.html>

[3] http://en.wikipedia.org/wiki/Inertial_navigation

✶ Urology medical student residency "matching" process failure

<Daniel Kahn Gillmor <dkg@fifthhorseman.net>>

Tue, 1 Feb 2005 01:52:43 -0500

Source: <http://blogborygmi.blogspot.com/2005/01/selection-dysfunction.html>

Medical students don't just apply for residency positions at graduation -- they "match" into them. The students rank their favorite programs, the hospitals rank their favorite students, and everyone hopes for the best as an algorithm puts them together. This process, more or less unchanged for decades, across many specialties, went terribly wrong last week during the urology match ...

Basically, they had to run the match again (with different outcomes) a few days after announcing the first results. This is huge in the lives of the prospective doctors because a residency determines where you will live and what you will do for many years.

According to the discussion boards, the AUA (American Urology Association?) has blamed the mismatch on a misconfigured computer algorithm, which was only discovered because some top-ranked residency programs were unfilled, which supposedly never happens.

So, why wasn't a human reviewing the results of the match for reasonableness before publication? Why aren't the algorithms used in the match process freely available? What safeguards are there on the data-entry step (since GIGO continues to apply)? Why isn't there an audit process in place?

[It could have been worse. Suppose someone was matched who was reportedly

an expert in Eurology (e.g., an economist in Brussels)... PGN]

✦ Congressman Ron Paul R-TX Understands Risks and Countermeasures

<Larry Sudduth <sudduthlm@securec2.com>>

Thu, 10 Feb 2005 18:42:33 -0500

As early as [RISKS-6.73](#), consequences of automated sharing of driver license information have been discussed. While the appropriateness of countermeasures levied against risks has been a fundamental element of RISKS since its inception, the mention in [RISKS-2.20](#) of Mann's article (<http://www.theatlantic.com/doc/prem/200209/mann>) marked the beginning of a (still nascent) popular tendency to review countermeasures for appropriateness, all the more so since the Patriot Act and successors.

I'm happy to learn that at least one congressman, Dr. Ron Paul, (R) TX, gets it. I'm unhappy that it is not one of my congressmen -- I'm from Virginia -- but maybe mine will learn from their Texas colleague!

H.R. 418, the "Immigrants ID bill" or "REAL ID Act of 2005," is advertised in part as establishing and rapidly implementing "regulations for State driver's license and identification document security standards, to prevent terrorists from abusing the asylum laws of the United States, to unify terrorism-related grounds for inadmissibility and removal." (See <http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00418>.)

The Honorable Dr. Paul characterizes HR 418 as a National ID Card bill masquerading as immigration reform. The clarity and brevity of his comments merit reading, both from an infosec perspective as well as a countermeasures perspective (<http://www.house.gov/paul/congrec/congrec2005/cr020905.htm>), excerpted and LMS-ed below:

" ...this bill will do very little to make us more secure. It will not address our real vulnerabilities. It will, however, make us much less free. In reality, this bill is a Trojan horse. It pretends to offer desperately needed border control in order to stampede Americans into sacrificing what is uniquely American: our constitutionally protected liberty."

"This bill establishes a massive, centrally-coordinated database of highly personal information about American citizens: at a minimum their name, date of birth, place of residence, Social Security number, and physical and possibly other characteristics ... that will be shared with Canada and Mexico!"

"This legislation gives authority to the Secretary of Homeland Security to expand required information on drivers' licenses, potentially including such biometric information as retina scans, finger prints, DNA information, and even Radio Frequency Identification (RFID) radio tracking technology."

"There are no limits on what happens to the database of sensitive

information on Americans once it leaves the United States for Canada and

Mexico - or perhaps other countries. Who is to stop a corrupt foreign

government official from selling or giving this information to human

traffickers or even terrorists? Will this uncertainty make us feel safer?"

Security practitioners know better than most the aptness of the saying, "err

in haste, repent at leisure." I hope Representative Paul's common-sense

proves to be contagious before HR 418 comes to a floor-vote.

Larry Sudduth 703.845-5-eight-33

✶ Flexibility destroys identity uniqueness: Implementing of IDN

<Jon Lingard <j.lingard@sapstrategy.com>>

Thu, 10 Feb 2005 05:39:23 +0000

It is now possible to spoof the URL displayed in the address bar, SSL

certificate, and status bar of a browser, due to the increased flexibility

brought about by the IDN (International Domain Name) implementation, which

allows using international characters in domain names. This can be

exploited by registering domain names with international characters that

resemble commonly used characters.

See security details here: <http://secunia.com/advisories/14163>

<http://www.sapstrategy.com/>

[This is another old topic in RISKS, but as Jon points out, it is

now even easier to fool more people. For example, see Evgeniy Gabrilovich and Alex Gontmakher, The Homograph Attack,

Communications of the ACM, vol 45, no 2, Feb 2002,

netscape <http://www.csl.sri.com/~neumann/insiderisks.html#140>

which has normally been

netscape <http://www.csl.sri.com/neumann/insiderisks.html#140>

but a massive reorganization of the CSL Web structure is underway

at the moment, and the usual URLs and cross-links do not seem to be

working yet today. (If internal links fail, stick in the tilde.)

PGN]

⚡ Exploding cell phone shocks 911 dispatcher

<"Keith A Rhodes" <RhodesK@GAO.GOV>>

Thu, 10 Feb 2005 08:25:16 -0500

http://news.com.com/Exploding+cell+phone+shocks+911+dispatcher/2100-1039_3-5570105.html?tag=nefd.top

How ironic that this would happen to a 911 dispatcher.

http://news.com.com/Symantec+flaw+leaves+opening+for+viruses/2100-1002_3-5569811.html?tag=nefd.top

and the hits just keep on coming.

⚡ RFID Tagging Elementary School Children

<"Peter H. Coffin" <hellsop@ninehells.com>>

Fri, 11 Feb 2005 20:17:05 -0600

<http://www.msnbc.msn.com/id/6448213/did/6942751/>

The only grade school in Sutter, California is requiring students to wear radio frequency identification badges that can track their every move. Some parents are outraged, fearing it will rob their children of privacy. The badges introduced at Brittan Elementary School on 18 Jan 2005 rely on the same radio frequency and scanner technology that companies use to track livestock and product inventory.

While similar devices are being tested at several schools in Japan so parents can know when their children arrive and leave, Brittan appears to be the first U.S. school district to embrace such a monitoring system.

Civil libertarians hope to keep it that way. [PGN-ed]

I trust no one reading RISKS has any troubles imagining many ways to foil this system. "Karen, I wanna ditch. Carry my tag in your backpack?"

[That's why they will be embedded in babies' navels at birth. PGN]

⚡ The risk of high-speed CD/DVD-rom drives in current-day PCs

<Henk Langeveld - risks digest <risks@hlangeveld.mailworks.org>>

Wed, 02 Feb 2005 22:54:00 +0100

I've had the nasty experience to have lost four CD's to newer high-speed CD and DVD-drives within a year.

The current state of technology will run CDs and DVDs at high speeds, and the centrifugal force of the drive increases the risk of any scratch on the media to result in one broken CD, and one ruined drive.

[Drew Dean commented to me on this: ``I believe programs such as Exact

Audio Copy (EAC) do slow down the drive, and most CD/DVD burning software

can write at slower speeds, but I'm not aware of any interface to tell an

OS to always slow down reading.'' PGN]

⚡ You type Zuerich and I type Zurich... A brief note

<dbell@zhochaka.demon.co.uk ("David G. Bell")>

Thu, 10 Feb 2005 09:18:24 +0000 (GMT)

There's been one of those idiosyncratic discussions in rec.arts.sf.fandom on the details of library catalogues and author's names, and the most recent issue of RISKS has sort of bounced off it.

Zuerich is, I understand, a quite correct "english" version of the Swiss placename.

Most english-speakers will type "Zurich", similar to the native version but using an ordinary ASCII "u", just as all sorts of other accent marks get

missed from European-language names.

And now Unicode allows computers to store all the variations as unique codes, which is good for typesetting, but has potential for confusion between visually similar characters. Not everyone will be exploiting that confusion for entertainment, as happened in "Monty Python and the Holy Grail".

But will search engines and indexes get tripped up by the differences, both correct alternatives and mistakes? Google does suggest alternatives to some spelling errors and variants, but how far do you go?

David G. Bell -- SF Fan, Filker, and Punslinger.

[But do American search engines handle Zürich properly? PGN]

Another MS Word info leak

<Richard Akerman <rakerman@chebucto.ns.ca>>
Fri, 4 Feb 2005 14:05:48 -0400 (AST)

Just another example of the risks of Word features. Not quite in the league of the 'dodgy dossier' but still.

'The press release looked pretty unremarkable at first. The McGill University Health Centre announcing an increased risk of heart attack in elderly people with no prior history of heart attack who use the painkiller Vioxx (which is now off the market).

The writing is a bit technical, but pretty clear.

But when press release writers compose these things, they have to run a copy past the scientist involved. His comments in the margin of the final draft were inadvertently sent out to everyone on the mailing list. They're meant to be "blind" -- visible only to a specified reader -- but they were in fact visible on computers with Windows XP and Microsoft Word 2003.'

Fortunately for everyone involved, the scientist didn't say anything particularly controversial.

Source: "Secret comments that everyone can read", Tom Spears, Ottawa Citizen, 3 Feb 2005.

<http://tinyurl.com/43dhg>

<http://www.canada.com/ottawa/ottawacitizen/news/story.html?id=d694b933-e82f-44b9-8732-97ef135d116f>

Richard Akerman <http://www.akerman.ca/>

⚡ High Risk Vulnerabilities in Eudora for Windows

<Monty Solomon <monty@roscom.com>>
Tue, 8 Feb 2005 21:42:44 -0500

<http://www.ngssoftware.com/advisories/eudora-01.txt>

John Heasman of NGSSoftware has discovered multiple high risk vulnerabilities in the Windows version of Eudora.

Versions affected include:

Eudora 6.2.0 and below

The flaws permit execution of arbitrary code via:

- 1) previewing or opening a specially crafted e-mail
- 2) opening specially crafted stationary or mailbox files

These issues have been resolved in Eudora 6.2.1 as detailed at <http://www.eudora.com/security.html>

It can be downloaded from:

<http://www.eudora.com/products/>

NGSSoftware are going to withhold details of this flaw for three months.

Full details will be published on the 2nd of May 2005. This three month window will allow users of Eudora the time needed to apply the patch before the details are released to the general public. This reflects NGSSoftware's approach to responsible disclosure.

NGSSoftware Insight Security Research

<http://www.databasesecurity.com/>

<http://www.nextgenss.com/>

+44(0)208 401 0070

✉ Re: U of Calgary adding spam and spyware (Slade, [RISKS-23.70](#))

<Hendrik <hiz--asa4@islandnet.com>>

Fri, 11 Feb 2005 10:54:34 +0900

The risk of not learning what needs to be learned!

It's about time this was done! :-)

In 1992 I found a small book in a bookstore in Saudi Arabia, that had been published by the German "Kaos Computerclub". In this book the authors explained how viruses worked, from an angle of approach of how to write viruses (at that time we had to deal mostly with DOS boot sector viruses). The authors further described how they had approached major software companies with this information, none of whom was the least bit interested in the information or in any cooperation with people who knew how to write viruses. Some of the approached companies had furthermore warned the authors against publishing the information about viruses they had on hand.

I am not impressed, to say the least, that 13 years after the Kaos Computerclub had the right idea, in a world awash in viruses, worms, and spam, with a world-wide deployed home computer OS that seems to have less security than the front door of my house, we still have not made any progress in regards to how we deal with knowledge about malware.

In the the CBC article that Rob Slade refers to, Aycock (the "virus teacher" at UofC) is quoted as saying "[S]ome companies have said they're not going to hire [our] graduates because they don't like the perception of having someone on board who has written viruses."

Well, I imagine reading the following in Time Magazine: "The White House official said, 'We are not going to hire body guards who have been trained at school X because we don't like the perception of having someone on staff

who has been trained to kill.'" Would you forgive me for laughing?

Rob Slade further writes:

>I can vaguely see a dim advantage to having students write viruses in order
>to understand them (rather inefficiently, in terms of time spent), but
>getting them to write a spamming program in order to understand how to fight
>spam seems even less effective.

Not all approaches to learning something are equally effective, and in an area where something is being pioneered, the first steps may not be quite in the right direction or not as effective as future approaches. But that alone is not a good reason to abolish a certain curriculum. My question would be "What would make this training more effective?"

>As previously noted, John Aycock doesn't seem to have any credentials in
>security or malware [...]

Assuming this is relevant (it may be but need not be - i would suggest that anybody who is a well-trained programmer and has the requisite imagination has in principle the necessary credentials) why not call for a more qualified professor for that course, then, instead of suggesting this training is a bad idea?

I hope one day we will see malware courses in all university computer science programs - then i would have reason to be more optimistic that the "security mess" we are finding ourselves in might be cleaned up. Creativity, more than anything else, is what we need to deal with the

future, and anybody who fosters and harnesses such creativity has my vote.

: -)

[RISKS readers should see George Ledin's article,
Not Teaching Viruses and Worms Is Harmful
in the Inside Risks column space of the January 2005 issue of
the

Communications of the ACM, vol 48, no 1. This article is
also available

online on my Web site

<http://www.csl.sri.com/~neumann/insiderisks05.html#175>

The normal URL has always been

<http://www.csl.sri.com/neumann/insiderisks05.html#175>

PGN]

✶ Re: U of Calgary adding spam and spyware (Slade, [RISKS-23.70](#))

<"Matthew Holmes" <matt@tekassoc.com>>

Sat, 12 Feb 2005 11:23:26 -0500

> ... John Aycock doesn't seem to have any credentials in
> security or
> malware ..., so why he, and the university, chose to do this,
> other than
> pure self-promotion, is completely beyond me.

Hmmmm - who does have "credentials" in these fields? Is there a
"mal-ware"
certification board? I must have missed it.

I did survey Aycock's professional literature, much of which is
available
on-line, and I notice that a great deal of it centers on reverse-
engineering
methodology, compiler/parser theory, etc. These are in fact the
tools of the
virus writer - the real ones, not the script kiddies and buffer-

overflow
people.

Why the snippy tone in a RISKS article?

⚡ **Re: Food via inkjet printer (Re: Scrivner, [RISKS-23.70](#))**

<Brian Reynolds <bfr@murphy.com>>

Thu, 10 Feb 2005 12:07:55 -0500

These setups have been around for years. The last time I saw this was several years ago on the old leben.com epon-inkjet list. The printer was a standard Epson model. There were warnings not to use standard inks in a printer intended for food printing.

One method of doing this involves printing the image onto a potato starch sheet using the food color inks and then affixing the sheet to the food item (e.g., a cake). Here in the USA Baskin & Robbins offers a service to print an image to be put on one of their ice cream cakes.

⚡ **Minireview: Bill Neugent, No Outward Sign**

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

Fri, 11 Feb 2005 20:53:58 PST

Bill Neugent
No Outward Sign
2002

IUniverse.com

ISBN 0-595-25749-6

<http://www.amazon.com/exec/obidos/ASIN/0595257496>

Bill Neugent's web site is at www.TaleCatcher.com.

e-mail: wneugent@mitre.org

Bill (in his work at MITRE) has been on the inside of computer security for many decades. I just finished reading his novel, and found it delightful, and excellent piece of cybersecurity fiction. It is a well-written page-turner. It is soundly based on things that have happened or could easily happen, but threads them all together very nicely through a twisty plot. It twits the oxymoron of computer security, and brings together good-hacker motivations, government bureaucracies, international cyberthreats, short-sighted optimizations, and many other issues familiar to RISKS readers.

The book is now available apparently only on the Internet, so I have included a URL.

★REVIEW: "A History of Computing Technology", Michael R. Williams

<Rob Slade <rslade@sprint.ca>>

Fri, 11 Feb 2005 08:32:32 -0800

BKHSCMTC.RVW 20041018

"A History of Computing Technology", Michael R. Williams, 1997, 0-8186-7739-2, U\$64.95/C\$104.95

%A Michael R. Williams

%C 10662 Vaqueros Circle, Los Alamitos, CA 90720-1314
%D 1997
%G 0-8186-7739-2
%I IEEE Computer Society Press
%O U\$64.95/C\$104.95 714-821-8380, 800-CS-BOOKS c.
baltes@computer.org
%O [http://www.amazon.com/exec/obidos/ASIN/0818677392/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0818677392/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/0818677392/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0818677392/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/0818677392/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0818677392/robsladesin03-20)
%O tl i rl 4 tc 3 ta 4 tv 4 wq 4
%P 426 p.
%T "A History of Computing Technology"

Yet another timeline from the Pascaline to Babbage to ENIAC?
Not so. How
refreshing, and fascinating, to see a history that really tells
us how we
got here.

Chapter one talks about the development of numeration itself,
and the
various forms of representing numbers (as well as a few systems
of
calculation). Early aids to calculation, starting with fingers
and moving
through to slide rules, are described in chapter two.
Throughout the book,
Williams has included frequent references to how calculating
tools and
techniques have given rise to common phrases. The definition of
"point
blank" is particularly fascinating, involving not only a
particular gunnery
instrument, but also the distrust of the Arabic numeral zero,
which paranoia
would have been uniquely strong at that specific time.
Mechanical
calculators are discussed in chapter three, covering much more
than the

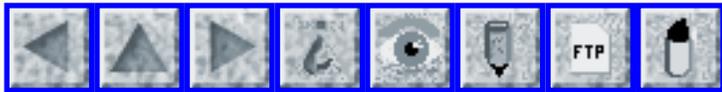
usual reference to the Pascaline. Chapter four outlines Babbage's machine; noting that he was more social than is usually thought, and that he succeeded in a number of fields (inventing, for example, the cow catcher); explains why the Difference Engine is known as such, and further mentions that it was hardly a failure, but spawned a bit of a building spree that lasted over twenty years. Analog, rather than digital, computers are often neglected, but chapter five notes a number of significant devices. The large mechanical or electro-mechanical machines of the 1940s are frequently seen as the beginning of the computer revolution, so it is interesting that the book is half complete before chapter six takes a look at the Zuse machines, the Bell relay machines, and Aiken's line. Chapter seven moves into the electronic world with reviews of the Atanasoff/Berry computer, ENIAC, and the Colossi. Given the importance of the work at Bletchley Park in terms of character manipulation (in cryptanalysis) it is interesting that other forms of text manipulation technology have not been addressed up to this point. The early computers dealing with stored programs are reviewed in chapter eight. As could be expected, the development of memory technologies is a major component of this material. Chapter nine finishes off with a review of some other early mainframe type computers.

We tend to pass over the history of computing with varying degrees of interest. Having a detailed examination of the development of both ideas and technologies of the basics of computing is both fascinating

and helpful.

Those who ignore the history of computing are likely to buy it again, repackaged under a new name. Professionals willing to understand the foundations of the industry and operations of the machinery will be in a much better position to judge what will (and what will not) be of importance in the future.

copyright Robert M. Slade, 2004 BKHSCMTC.RVW 20041018
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

Volume 23: Issue 72

Thursday 17 February 2005

Contents

- [Missile interceptor doesn't even leave its silo -- again](#)
[Jeremy Epstein](#)
- [Report on Patriot missile friendly fire over Iraq](#)
[PGN](#)
- [TCAS RA incident](#)
[Martyn Thomas](#)
- [Scammers access ChoicePoint data on 35,000](#)
[Matt Hines via Monty Solomon](#)
- [Trees with concealed GSM antennas](#)
[Dan Jacobson](#)
- [German TollCollect charges double](#)
[Debora Weber-Wulff](#)
- [Wife broke law in using spyware](#)
[NewsScan](#)
- [Gas stations lose money due inadvertent low pricing](#)
[Arthur T.](#)
- ['Smart' driver's licenses a Trojan horse?](#)
[NewsScan](#)
- ["The Mother is Back!" Announcing "DayThink" Audio Features](#)
[Lauren Weinstein](#)

- [Limits of search-and-replace](#)
[Mike Albaugh](#)
 - [I may know who handles Personal Certs at thawte](#)
[Ed Bruce](#)
 - [Malware and Auto Electronics](#)
[Peter B. Ladkin](#)
 - [Re: More uses of satnav/GPS](#)
[Paul E. Bennett](#)
 - [New copy-proof DVDs on the way?](#)
[John Borland via Monty Solomon](#)
 - [Re: The risk of high-speed CD/DVD-rom drives in PCs](#)
[Eben King](#) [Jonathan Smith](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Missile interceptor doesn't even leave its silo -- again

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

Mon, 14 Feb 2005 21:06:17 -0500

As reported in [RISKS 23.65](#) and 23.66, the Dec 15 test of the missile interceptor system failed when it didn't lift off from the launchpad due to a timing problem.

The 14 Feb test didn't do any better. CNN reports that "a spokesman for the [Missile Defense] agency, Rick Lehner, said the early indications was that there was a malfunction with the ground support equipment at the test range on Kwajalein Island in the Marshall Islands, not with the missile interceptor itself. If verified, that would be a relief for program officials because it would mean no new problems had been discovered with the missile."

That's good news?

In case you're keeping score, that's 6 failures out of 9 attempts since the program started. And the three "successes" have been highly scripted.

Your tax dollars at work (at least for Americans).

✶ Report on Patriot missile friendly fire over Iraq

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

Mon, 14 Feb 2005 11:39:40 PST

Nathan White was piloting a Navy plane at 33,000 feet over Iraq on 2 Apr 2003. He was shot down by a US Patriot missile. The summary of a report released on 10 Dec 2004 concludes that White's plane was mistaken for a nonexistent hostile missile, and that the Patriot's proper launch procedures were violated. However, a redacted version of the report notes the Army's difficulties in using the Patriot system, including gaps in crew training and frequent appearance of false tracks (which in past RISKS items are referred to as ghosts). "The issues show the unintended dangers that computerized weapons systems can pose, and the need for better human oversight." [Source: Palo Alto **Daily News**, 9 Feb 2005, p. 25; PGN-ed]

✶ TCAS RA incident

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

Sun, 13 Feb 2005 16:41:09 -0000

The latest CHIRP Feedback contains an interesting report. Two aircraft crossed with 1000 feet vertical separation in UK airspace. The higher aircraft had a (known) faulty transponder that was reporting 500 ft lower than actual, so the crossing caused a TCAS resolution advisory to descend in the lower aircraft. The crew of the lower aircraft point out that if the faulty transponder had read 1500 feet low, the Advisory would have said "Climb" and they would have climbed into the other aircraft.

✶ Scammers access ChoicePoint data on 35,000 (Matt Hines)

<Monty Solomon <monty@roscom.com>>

Tue, 15 Feb 2005 11:20:34 -0500

[Source: Matt Hines, news.com, 15 Feb 2005]

ChoicePoint confirmed on 15 Feb that criminals recently accessed its database of consumer records, potentially viewing the personal data of about 35,000 Californians and resulting in at least one case of identity fraud.

The unidentified individuals posed as legitimate businesspeople in order to breach its defenses. Chuck Jones, a company spokesman, said that roughly 50 fraudulent accounts were set up by the schemers, through which

they could
view the data of California residents.

News of the crime first surfaced when ChoicePoint sent an e-mail to individuals potentially affected by the attack last week. Among the data available through the company's services, and possibly accessed by the criminals, are consumers' names, addresses, Social Security numbers and credit reports.

<http://news.com.com/2100-1029-5577122.html>

✶ Trees with concealed GSM antennas

<Dan Jacobson <jidanni@jidanni.org>>

Wed, 16 Feb 2005 00:47:06 +0800

"The product used in Palm antennas is formed by the tree itself and the fronds". <http://www.preservedpalm.net/gsm.shtml>

GSM base stations are camouflaged in specially preserved palm trees, with antennas that look like palm fronds with internal steel-bar reinforcements for structural rigidity, and with cable works inside the trunk. [PGN-ed]

I suppose the risk here is assuming the plants aren't doing anything special.

[They won't be doing much by themselves after they've been eviscerated.

But they could serve other purposes as well. This is another variation on

an old theme, so we'll add it to our Fronds List. PGN]

German TollCollect charges double

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

Thu, 17 Feb 2005 18:22:23 +0100

The Berlin daily Newspaper "Berliner Zeitung" keeps beating up on the German TollCollect system.

<http://www.berlinonline.de/berliner-zeitung/berlin/422264.html>

[Note, the author is Peter Neumann, but not PGN!]

On Feb. 16, 2005 they report on a trucking company who was charged for the same truck at the same time for two different pieces of Autobahn, while a short time later they were charged for driving on some street that is not a toll road. The winning charge is for going from Kurt-Schumacher-Damm to Saatwinkler Damm (about 1.5 km as the crow flies) to the tune of 49 kilometers. According to the booking list the truck drove around town twice and used the Avus, apparently turning on the autobahn to continue [Maybe these are the same folks that programmed the MSN map from Haugesund to Trondheim in Norway, via the continent <http://www.englishrules.com/archives/miscellany/index.php> - dww]

On Feb. 17, 2005 they have a nice report about how easy it is to jump paying for the toll.

<http://www.berlinonline.de/berliner-zeitung/politik/422488.html>

It seems that there are just 300 of these bridges that are controlling

bridges, the rest are just for calculating the fare. And the specifications say that a 10% check is done, so there are only ever 30 of them on at a time because the machines do the checking but human intervention is necessary to flag down a toll jumper. In addition to which, the mobile checkers only work day shifts, while a lot of trucking takes place at night. A federal trucking organization took some test drives at night in the East to see if they got hooked - negative. So here we have all this expensive technology and these ugly bridges, and it still doesn't really work.

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

Wife broke law in using spyware

<"NewsScan" <newsscan@newsscan.com>>
Wed, 16 Feb 2005 09:42:15 -0700

A Florida appeals court has ruled that a suspicious wife, who installed spyware on her husband's computer to secretly monitor and record his electronic interactions with another woman, violated Florida's wiretapping law. The law says anyone who "intentionally intercepts" any "electronic communication" commits a criminal act. The wife had argued that her use of Spector spyware should be viewed as similar to reading a stored file on her

husband's computer. But Judge Donald Grincewicz wrote that "because the spyware installed by the wife intercepted the electronic communication contemporaneously with transmission, copied it and routed the copy to a file in the computer's hard drive, the electronic communications were intercepted in violation of the Florida Act." [CNet News.com 15 Feb 2005; NewsScan Daily, 16 Feb 2005]
http://news.com.com/Court+Wife+broke+law+with+spyware/2100-1030_3-5577979.html

✶ Gas stations lose money due inadvertent low pricing

<"Arthur T." <myspamtrap01@yahoo.com>>
Sun, 13 Feb 2005 18:59:06 -0500

A (presumably self-service) gas station went all night with gas priced at \$.19/gallon instead of \$1.83/gallon. The owner didn't know about it until reporters asked him about the low price. He corrected the price only after 1200 gallons had been pumped.

It was blamed on a "computer glitch", but could easily have been a data-entry error. The article mentions another case of a misplaced decimal point in gas pricing.

The Risks are more human than computer. If you're going to leave the gas station unattended, double-check your prices. (Although, I admit, it would be nice to have the computer sanity-check your price.) Note:

The article doesn't say the station was unattended during the time the low price was in effect, but I don't want to believe that any attendant could have let this continue.

URL of story (beware of line-wrap):

http://story.news.yahoo.com/news?tmpl=story&cid=816&ncid=816&e=8&u=/ap/20050211/ap_on_fe_st/really_cheap_gas

'Smart' driver's licenses a Trojan horse?

<"NewsScan" <newsscan@newsscan.com>>

Mon, 14 Feb 2005 10:42:11 -0700

A move by Congress to endorse a Republican-backed measure that would compel states to redesign their driver's licenses by 2008 to comply with standards for making them electronically readable has critics questioning government's motives, saying it gives the Department of Homeland Security carte blanche to do nearly anything "to protect the national security interests of the United States." Rep. Ron Paul (R-Texas) says, "Supporters claim it is not a national ID because it is voluntary. However, any state that opts out will automatically make nonpersons out of its citizens. They will not be able to fly or to take a train." Proponents of the Real ID Act say it reflects the recommendations of the 9/11 Commission and will help in the battle against terrorism and efforts to identify illegal immigrants. But Paul

says, "In reality, this bill is a Trojan horse. It pretends to offer desperately needed border control in order to stampede Americans into sacrificing what is uniquely American: our constitutionally protected liberty." [CNet News.com 14 Feb 2005; NewsScan Daily, 14 Feb 2005]
http://news.com.com/From+high-tech+drivers+licenses+to+national+ID+cards/2100-1028_3-5573414.html

✶ "The Mother is Back!" Announcing "DayThink" Audio Features

<Lauren Weinstein <lauren@vortex.com>>
Tue, 15 Feb 2005 22:49:47 -0800 (PST)

Greetings. I'm pleased to announce "DayThink" -- a new series of very brief (one-minute) MP3 audio features illuminating a wide range of relevant and important topics. Each day's feature will focus on one specific issue affecting our lives -- issues definitely worth thinking about. Many of these segments will deal directly with the impacts of technology on individuals and society.

DayThink features can be accessed via the DayThink main page at:
<http://daythink.vortex.com>

The debut segment is titled:
"The Mother is Back!"

and looks at the current round of telecom mergers and what they may mean for us all.

A notification mailing list has been established that will send out a brief message to subscribers as each new feature becomes available (never more than one per day), including the segment title, a brief description, and a link to the feature audio itself that can be played at one's leisure.

Subscriptions to that list can be established via:

<http://lists.vortex.com/mailman/listinfo/daythink>

or by simply sending a note (no subject or body necessary) to: daythink-subscribe@vortex.com

I hope that these features will be of some value in helping folks wade through the maze of many important issues.

Thanks very much.

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

1 818-225-2800 <http://www.pfir.org/lauren> Fact Squad - <http://www.factsquad.org>

✶ Limits of search-and-replace

<Mike Albaugh <albaugh@perilin.com>>

Mon, 14 Feb 2005 14:33:40 -0700

I dug a few nifty Alphanumeric displays out of the scrap bin, and wanted to use them in a sculpture. A few minutes searching on the web produced a datasheet and application-notes for a plausibly similar device, but were I too literal, I'd be perplexed.

The application-note claims that the sample code scrolls "AGILENT TECHNOLOGIES" across the display, but the 8741 sample source code does not include a general-purpose character generator and literal string. Rather, there is a table of hexadecimal values, each row encoding the pixels of one character. The end-of-line comments confirm the suspicion that a glance at the table raises. Had I actually copied this code, I would see "HEWLETT PACKARD"

The RISK here is only one of embarrassment, but imagine this sort of thing happening in code for a device (e.g. many PC graphics cards) which uses manufacturer's name or model number as a "key" to enable operation.

✶ I may know who handles Personal Certs at thawte

<Ed Bruce <ebruce@hpmich.com>>
Wed, 16 Feb 2005 10:46:01 -0500

My personal e-mail cert from thawte is expiring soon. Thawte sent me an e-mail informing me of this containing "links" to their web page on how to extend it. Problem is I forgot my password and clicked on a link provided to help me recover my password. It didn't work. I'm using Mozilla Thunderbird, which displays the actually link at the bottom of the display. This is what I saw:

```
file:///C:\Documents and Settings\jwolvaardt\Local Settings
```

```
\Temporary
  Internet Files\Local Settings\Temporary Internet Files\OLK3C
\Expiring
  personal Certs March.doc
```

I guess you don't need to just post Word documents to reveal information.

✶ Malware and Auto Electronics (Klashinsky, [Risks 23.370](#))

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Sun, 13 Feb 2005 08:14:49 +0100

Karl Klashinsky reported in [Risks 23.70](#) about:

```
  a case where the on-vehicle software is corrupted by a virus,
inserted
  into the automobile's computing systems, via a blue-tooth
enabled
  cell-phone
```

and suggested the scenario:

```
  As this vulnerability becomes known in the cracker community,
how long
  before someone tailors a virus specific to a vehicular target
-- perhaps
  creating runaway-vehicle scenarios similar to the "faulty
cruise control"
  incidents reported here in RISKS.
```

Interestingly, a day before I had been pointed to an article in a South African newspaper about just such a migration, and there was also something about viruses spreading from cell phones to cars in an article in the **International Herald Tribune**, which I read daily.

There is a wonderful cartoon from the German computer magazine *c't* pinned to my group's noticeboard. A passenger is sitting in an airliner using his laptop, and on the screen appears:

Bluetooth: new device found: Airbus A310

In one journal it's a cartoon, and in the other journal it's news. What's going on? I made some inquiries.

The punch-line first. Ross Anderson pointed me to

<http://www.engadget.com/entry/1234000760029037/>

which reports on someone asking Eugene Kaspersky of Kaspersky Labs about how to cure a virus that ``infected the onboard computers of automobiles Lexus LX470, LS430, Landcruiser 100 via a cell phone.'' Apparently there are some communicating systems on board those cars which use Symbian (one of the mobile-phone OS's) and are bluetooth-enabled, and Kaspersky conjectured that this could be a infection route. The article, from Donald Melanson, suggests that it is not clear whether this has actually happened or not. The South African article, and the other articles besides the IHT mentioned Kaspersky Labs, so this seems to be the source of the "news".

The IHT commented on a document issued Wednesday by IBM Security Intelligence, the Security Threats and Attack Trends Report, which said:

Beware viruses that spread to cellphones, hand-held computers, wireless networks and embedded computers that are increasingly used to run basic automobile functions

<http://www.iht.com/articles/2005/02/09/business/virus.html>

Nothing much there.

Ross also told me of a discussion at the Electronic Security in Cars conference about a (different) major car company which used a T39 mobile phone with a linux card running Apache for managing over-the-air software upgrades in some high-end models.

So it seems as if two car companies use GSM communication over OTS communicators for some on-board systems. Obviously those systems *could* be infected by viruses targeted to those devices, and someone asked Kaspersky about it. That it has actually happened is questionable; that it could happen is not, for those systems, for those cars.

What is there to say about likelihoods? Let me restrict myself to critical systems (chassis, especially brakes and steering; and engine control). Nav systems and in-car entertainment are not critical.

First, the critical on-board systems people (chassis systems, engine systems) build separate systems from others on-board. If they use common busses, those busses (usually CAN, about to become FlexRay or TTP) are hard-real-time and the architectures are explicitly designed to inhibit inter-application interference. The critical systems themselves are hand-designed, often hand-coded, running on small processors built for hard-real-time systems use, although they may migrate to special-purpose OS-based SW in the future. There are many such systems, they are

all
different from each other at present, and they are proprietary.
You can't
easily get a copy to play with, just as you can't easily get a
copy of
Airbus critical-system code to play with. It may be even harder,
since the
companies are all in heavy competition with each other for their
continued
existence (see below) and they are aware of industrial theft and
sabotage
issues.

I don't know of any such system which installs upgrades over
standard mobile
phones. There may be some, but the people I deal with on
critical systems
are all more or less aware of security issues. Furthermore, at
least in
Germany, such systems in the future will have to demonstrate
that they have
been developed according to the precepts of the IEC 61508
standard on
functional safety in E/E/PE systems (roughly, systems which use
programmable
electronic components). That standard explicitly covers
maintenance, and it
does not condone upgrading critical systems using OTS
communication channels
vulnerable to known security problems such as malware
transmission.

Which doesn't mean that no one is going to try it. But it does
suggest that
such an effort would not last long, would end in tears, and
would preclude a
repeat.

Why would it end in tears? Well, few people have remarked it so
far, but
auto manufacturers are at the sharp end of progress in SW safety
and
reliability (components of dependability). A model such as the

Ford Focus

sells a million cars a year. Each of those cars can be expected to drive 300-500 hours a year, and the cars themselves are standardly taken to have a 3-5 year service lifetime. So one model-year alone can be expected to accumulate between 9×10^8 and 2.5×10^9 hours of service. Add to that that systems for such cars are often built by component manufacturers such as Bosch, who install that system or closely similar systems in other cars also, and you are looking at attempting to attain an actual dependability of the order of one critical failure in 10^{10} hours of service.

In aerospace, taken by many to be the industrial pinnacle of critical systems engineering, single-point-of-failure critical systems are built to a nominal standard of one catastrophic failure (loss of the airplane) in 10^9 operational hours. And that is notional; it is intended to be higher than the cumulative service life of the entire model fleet. Whereas the 10^9 to 10^{10} operational hours in automobile electronics is actual.

Now, nobody actually knows how to manufacture SW that is guaranteed to be that dependable (that is, one may achieve it, but one cannot know or prove that one has done it). Current limits (through exhaustive testing of the final product) seem to be about 10^5 operational hours. That is the theoretical limit of certainty through practical testing (Bayesian calculations by Littlewood and Strigini). People are scratching their heads. Heavily. And occasionally asking me and my colleagues to

scratch
ours.

Serious problems are occurring. Each problem will lead to a recall, and I am told that a minimal cost for a recall (SW upgrade, for example) is EUR 50 per auto (Mike Ellims, Pi Technology, personal communication). Mercedes recently had to recall 600K autos for a brake-system SW upgrade (a counter that they thought would not run over between services did, in two instances, and they had to recall all cars with that SW). We could thereby reckon that that cost EUR 30 million, or thereabouts. Given that profit margins amongst those manufacturers that actually do make a real profit are in the low USD 10exp8 region, if that high, a single recall cuts seriously into profit.

(According to the Economist's survey of 4 September 2004, at <http://www.economist.com/surveys/showsurvey.cfm?issue=20040904> which cites a study by Maxton and Wormald for Goldman Sacks entitled "Time for a Model Change", there are only only 8 car companies above the curve of cost-of-capital versus revenue per unit, namely Porsche, Nissan, Honda, Toyota well above, and Mercedes, BMX, PSA and Hyundai barely making it over.)

Recalls are not the only cost. There is also the cost of recompensing the victims of accidents in which system malfunction was a causal factor.

So there is plenty of motivation to make auto critical electronics the most dependable SW-based systems the world has ever seen. We are a long way from

it, but I don't think we are going to be seeing critical systems upgraded through gratuitously insecure channels. Except for the exceptions, of course.

If I were to bet today, I'd bet on the cartoon staying a cartoon.

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

✈ **Re: More uses of satnav/GPS (Magda, [RISKS-23.71](#))**

<"Paul E. Bennett" <peb@amleth.demon.co.uk>>

Sun, 13 Feb 2005 11:20:16 +0000

It seems that some solutions have more "sex appeal" than others and hence get considered for adoption over and above obviously saner solutions.

In respect of trains, as they run on rails, it should be very easy to use the trackside equipment and links to the train to determine that the train is where it should be at that moment in time. It is not as though the trains will be running off the tracks at any time during its journey (unless derailed of course in which case it is definitely going to be late).

Paul E. Bennett <http://www.amleth.demon.co.uk/> peb@amleth.demon.co.uk

Forth based HIDECS Consultancy Mob: +44 (0)7811-639972

✦ **New copy-proof DVDs on the way? (John Borland)**

<Monty Solomon <monty@roscom.com>>

Tue, 15 Feb 2005 11:23:55 -0500

Macrovision is expected to release a new DVD copy-protection technology

Tuesday in hopes of substantially broadening its role in Hollywood's

antipiracy effort. The content-protection company is pointing to the

failure of the copy-proofing on today's DVDs, which was broken in 1999.

Courts have ordered that DVD-copying tools be taken off the market, but

variations of the software remain widely available online.

[Source: John Borland, news.com, 14 Feb 2005]

<http://news.com.com/2100-1026-5576375.html>

✦ **Re: The risk of high-speed CD/DVD-rom drives in PCs ([RISKS-23.71](#))**

<Eben King <eben1@tampabay.rr.com>>

Sun, 13 Feb 2005 11:29:31 -0500 (EST)

You quote Drew Dean as saying: "I believe programs such as Exact Audio Copy

(EAC) do slow down the drive, and most CD/DVD burning software can write at

slower speeds, but I'm not aware of any interface to tell an OS to always

slow down reading."

"Nero CD-DVD Speed" makes the maximum speed of the CD/DVD drive lower. I

use it on my DVR to quiet down (and prevent the "spin up - fill

up cache -

play from cache - spin down" cycle) to slow down my 52x drive to 8x or so.

[Also noted by David DiGiacomo and by Serguei Patchkovskii (who also

provided a URL

<http://www.cdspeed2000.com/go.php3?link=download.html>

and advice for Linux users: you already have the needed tool installed.

At the command line, to get 4x CD-ROM speed,

```
eject -x 4 /dev/cdrom
```

PGN]

⚡ Re: The risk of high-speed CD/DVD-rom drives in PCs ([RISKS-23.71](#))

<Jonathan Smith <josmith7@kant.bubel.net>>

Tue, 15 Feb 2005 12:16:44 -0500 (EST)

I know that for years Plextor CD rom drives have come with a windows taskbar utility that allows the user to force the drive to run at a lower speed along with adjusting other settings.

I ended up needing to use this utility on occasion with the then extremely high-speed 12x CD-Rom drive I owned. CDs built for 1x or 2x drives, including my copy of Windows 95 would vibrate so much in a 12x drive at full speed that the computer case would also vibrate and no data could be read.

Forcing the drive down to 4x would fix the problem.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 73

Sunday 20 February 2005

Contents

- ["High-tech passports are not working"](#)
[Yves Bellefeuille](#)
- [Federal agencies get failing grades on cybersecurity](#)
[NewsScan](#)
- [Break-In At SAIC Risks ID Theft](#)
[Griff Witte via Monty Solomon](#)
- [ChoicePoint warns of ID theft concerns](#)
[NewsScan](#)
- [In the Matter of Component Architecture](#)
[Paul Robinson](#)
- [RSS reader redirect risks](#)
[Monty Solomon](#)
- [eBay redirects to phishers from their own site](#)
[Pete Krawczyk](#)
- [Risks of battery-operated wireless input devices](#)
[Peter Pankonin](#)
- [You There, at the Computer: Pay Attention](#)
[Katie Hafner via Monty Solomon](#)
- [Assuming customers can't spell](#)
[Andrew Malakoff](#)

● [Unintended consequences of automatic abbreviation](#)

[John Pettitt](#)

● [REVIEW: "Modern Cryptography: Theory and Practice", Wenbo Mao](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✶ "High-tech passports are not working"

<Yves Bellefeuille <yan@storm.ca>>

Thu, 17 Feb 2005 21:15:41 -0500

The British weekly magazine `_The Economist_` has an article entitled

`"High-tech passports are not working":`

http://www.economist.com/science/displayStory.cfm?story_id=3666171

The usual arguments are made -- the technology isn't reliable, there will be too many false positives, and so on -- but there's also a new argument I hadn't seem before:

"The data on these chips will be readable remotely, without the bearer knowing. And -- gain at America's insistence -- those data will not be encrypted, so anybody with a suitable reader, be they official, commercial, criminal or terrorist, will be able to check a passport holder's details...

"Passport chips are deliberately designed for clandestine remote reading. The ICAO [International Civil Aviation Organisation, a UN agency] specification refers quite openly to the idea of a "walk-through" inspection

with the person concerned "possibly being unaware of the operation".

Apparently, the only country that's ready for the US requirements is Belgium. It's really the **only** country: the US itself won't be able to deal with the passport requirements it's imposing on others by the November 2005 deadline!

✶ Federal agencies get failing grades on cybersecurity

<"NewsScan" <newsscan@newsscan.com>>

Thu, 17 Feb 2005 15:21:43 -0700

At least half of all federal agencies received a grade of "D" or worse on the House Government Reform Committee's annual cyber-security report card. Agencies that received failing marks include the departments of Agriculture, Commerce, Energy, Health and Human Services, Housing and Urban Development, and Veterans Affairs. A grade of "D" was awarded to the departments of Defense and Treasury, as well as the National Aeronautics and Space Administration and the Small Business Administration. Chairman Tom Davis (R-VA) was encouraged by the fact that the scores of the 10 agencies, as poor as they were, have actually improved since last year, but he warned they must still do better: "I hope it won't take some kind of major cyber-attack to wake everybody up." [**The Washington Post**, 16 Feb 2005; NewsScan Daily, 17 Feb 2005]

<http://www.washingtonpost.com/wp-dyn/articles/A30342-2005Feb16.html>

✶ Break-In At SAIC Risks ID Theft

<Monty Solomon <monty@roscom.com>>

Sun, 13 Feb 2005 23:48:14 -0500

Computers Held Personal Data on Employee-Owners
Griff Witte, *The Washington Post*, 12 Feb 2005, E01

Some of the nation's most influential former military and intelligence officials have been informed in recent days that they are at risk of identity theft after a break-in at a major government contractor netted computers containing the Social Security numbers and other personal information about tens of thousands of past and present company employees.

The contractor, employee-owned Science Applications International Corp. of San Diego, handles sensitive government contracts, including many in information security. It has a reputation for hiring Washington's most powerful figures when they leave the government, and its payroll has been studded with former secretaries of defense, CIA directors and White House counterterrorism advisers.

Those former officials -- along with the rest of a 45,000-person workforce in which a significant percentage of employees hold government security

clearances -- were informed last week that their private information may have been breached and they need to take steps to protect themselves from fraud.

David Kay, who was chief weapons inspector in Iraq after nearly a decade as an executive at SAIC, said he has devoted more than a dozen hours to shutting down accounts and safeguarding his finances. He said the successful theft of personal data, by thieves who smashed windows to gain access, does not speak well of a company that is devoted to keeping the government's secrets secure. ...

<http://www.washingtonpost.com/ac2/wp-dyn/A17506-2005Feb11>

ChoicePoint warns of ID theft concerns

<"NewsScan" <newsscan@newsscan.com>>

Thu, 17 Feb 2005 15:21:43 -0700

ChoicePoint, a Georgia company in the business of selling personal data on consumers, is alerting 145,000 people throughout the nation that a crime ring paid for their credit reports, Social Security numbers and other information. Con artists had posed as owners of debt-collection agencies, insurance agencies and other firms that told ChoicePoint they needed to run background checks on consumers. [*San Jose Mercury News*, 17 Feb 2005; NewsScan Daily, 17 Feb 2005]

<http://www.siliconvalley.com/mld/siliconvalley/10921081.htm>

✶ In the Matter of Component Architecture

<Paul Robinson <paul@paul-robinson.us>>

Sun, 20 Feb 2005 05:27:37 GMT

I had sort of a revelation this afternoon when I think I finally figured what it was that I knew was a missing piece and the explanation.

And it also came to me as to why we have such a horrible problem with software reliability. Let me ask you to take a moment and consider how you started this morning.

Most likely, you crawled out of your cave, went down to the stream to bathe in the ice-cold water, came back and pulled the wheat out of the ground, stripped the chaff, then used either a mortar and pestle or a grindstone to make flour, then pulled some yeast from the pot to mix with it to make bread, then chopped wood, then used the wood to build a fire and baked the bread, then ground peanuts in the same mortar to make peanut butter, then spread it across the bread and ate it, because by now it was lunch, no?

No, most likely you got out of a bed, got up and took a hot shower in your indoor bathroom, poured boxed cereal into a bowl or made breakfast from materials you bought in a store, then cooked it on a range, or went to a

restaurant and bought something to eat, then went on to work,
and probably
in this entire time you did nothing more strenuous than pick up
the morning
paper.

Also, you did not mine the ore for your utensils or forge the
steel for
them, nor did you build the automobile you drove to work. Or a
thousand
other things you used today if you don't drive. You used items
someone else
made. And they used things other people made for them to make
those things.

So what and how does what I just said have anything to do with
the idea of a
means to reduce or eliminate software failure? Because we do not
do the same
thing in the virtual space of software that we do in the real
world.

Every time you use something manufactured, you use a component.
A system as
it were, an object. That component or object is itself built out
of other
components, or subsystems, which are operated upon by various
other objects
through various events. Let me give a simple example.

Using our hypothetical peanut butter sandwich from earlier in
this article,
no, on second thought we'll make it a peanut butter and jelly
sandwich, we
have an object which has three components or subsystems, the
bread object,
the peanut butter object, and the jelly object, which are
manipulated by the
hand and knife objects via the spread event.

Now you may start to see what I'm talking about here. All of the
things we
do or work with are generally made by combining other components

either to produce an object or are used standalone (as when someone eats a sandwich which is finished or was made by someone else). We generally do not build everything from scratch.

But when was the last time you saw this sort of obvious acceptance of previously built components in the software development field? Okay, we will use an operating system and a compiler. That's about it; people will look at you askance if you talk about code reuse and designing applications to be built out of modular pieces and possibly completely built out of components designed by someone else.

For some reason it's perfectly acceptable for a trucking company to build an accounts receivable application from scratch but nobody in their right mind would expect them to build their own trucks.

If you're remodeling a kitchen the nearest Home Depot, Lowes, or a thousand places on the Internet will sell you any of several thousand designs to match your taste, decor and budget. That even though you are constructing a space you can buy all the components pre-built and while some people might be willing to pay extra for custom-built kitchens (and most people won't because the pre-built stuff is absolutely fine for all but the most unusual cases), but even at that nobody makes their own stove, refrigerator or sink.

Go out to a typical shop in a data processing organization and they'll look at you funny as they peer out over the landscape of trees they

plan to mill
for the cabinets, and the stocks of steel and copper tubing they
have to
build the gas powered refrigerators, and the enamel painting
shop they plan
to use to bake the finish onto the custom-built coal-fired stove
they'll
provide you with, to give a mismatched comparison.

They also can't estimate how long it will take to build the
equipment, they
don't know what it will cost, and as for warranty protection
that the stove
won't explode when it's used, a promise that the cabinets will
support the
weight of the dishes and groceries you want to put in them, and
guarantees
that the refrigerator will start when you plug it in and won't
catch fire,
or will even keep food cold, they'll think you're crazy if you
want it
anything but "as is."

Does this make any sense?

And we as software practitioners have been getting away with
this sort of
racket for decades.

The Sears Department stores of K-Mart Corporation will sell you
an
adjustable wrench that not only has a guarantee that it will do
what it is
intended for, and is guaranteed against defects in materials and
workmanship, they will even replace it if you broke it because
you damaged
it on purpose. Forever. And their Craftsman brand is
competitively priced
against tools from competitors. I do note that their more
complicated
appliances don't have this strong a warranty, but in any case
they do have
one on everything they sell.

If you order even the simplest piece of software from anyone they can't even give you the minimum under the Moss-Magnuson Warranty Act: that the product is fit for use for the purpose it is intended to be used. The reasons for this are many, but come down to two things.

Software has neither architectural integrity nor engineering discipline. You buy a house and have knowledge that it was built according to detailed blueprints which an architect knows if it is built according to the specification that it has the characteristics to support the structure. You remodel a kitchen and have knowledge that the cabinets were built according to good engineering practices to support the usual and customary weights and stresses dealing with household goods used in kitchens.

Software developers will promise neither of these in even the simplest pieces of software. Neither will there be a promise of architectural correctness nor even engineering integrity. They can't because they don't have a way to determine what the load factors or stresses on the software are. It's all built by hand, on an ad-hoc basis, usually without any formal disciplines being used, with all new materials milled from scratch. Very little if any predeveloped components are used.

One of the greatest improvements in programmer productivity was the move from using wire boards and toggle switches to being able to write programs in source code, typically assembler. The next boost was the development of

third-generation programming languages such as Fortran, C, Cobol, Basic, Pascal and six thousand others. And I think the next boost was the implementation of object orientation. Of the use of components to build software out of previously constructed pieces. Despite the capacity being there, it's rarely used.

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. But in general, this is not how we are designing software.

The question that should be asked is, "why this is allowed to continue?"

Software as it is currently being developed provides so much value relative to its costs that we as practitioners of this medieval-class craft (in terms of our level of automation and sophistication of production methods) can get away with practices that would not be tolerated by a Taiwanese manufacturer of toasters.

And this is the reason we are seeing programming jobs being outsourced to low wage countries. If you're going to get crappy software there's no reason to pay premium prices for it. It is exactly the sort of situation that befell the American automobile manufacturers back in the 1970s and 1980s. And unless we start to make changes we will see exactly the same

thing happening.

Actually some of the software development places that are used for outsourcing have formal practices in place for reducing defects. So it is entirely possible what we are getting is the exact equivalent of what I stated above. The overseas "manufacturers" produce better quality at a lower cost than we do.

I think that a basis of component architecture is the direction that we need to go in the development of software. That we need to make more software to be designed as a series of reusable components that can be used in other contexts. It also means we need to develop at least an engineering discipline in a way of making software of higher quality and eventually to reduce the risks of development.

And this is why I now understand more clearly why I knew that there was something right about this concept even though I didn't know exactly why at the time. In a book I once wrote, the main character explains about realizing the validity of a concept even if you're not sure why:

I know how that is; more than once I've had gut feelings about things

where I couldn't put my finger on it, but I knew something wasn't right.

Later I would discover why I had that feeling, and, more importantly, why

I was right, but at the time I did not have the evidence or knowledge to

know why I felt that way.

- George Green, "In the Matter of: The Gatekeeper: The Gate

Contracts"

We can continue on the same path of disaster-ridden bugware or we can choose to change. We can change because the current methods do not work very well, they spell disaster in terms of cost, reliability, future employment potential, and the possibility of seeing our craft ruined by heavy-handed government mandates for licensing. We can choose to change because if we do not, the choice on how to make the changes may be made for us, and in a manner we will not appreciate.

The process will not be easy, but the benefits to us will more than outweigh the short-term losses by having to re-learn a new way of working, and thinking. If we want to continue to have fun in this craft without being placed into a bad position because of our own arrogance in failing to acknowledge the incompetence, sloth and waste our current practices contain, we need to change. And we need to do it before we are forced to do so because the customers decide they can't stand it any more, before we do.

✶ RSS reader redirect risks

<Monty Solomon <monty@roscom.com>>

Fri, 18 Feb 2005 02:02:45 -0500

I hooked up my laptop to the network in a hotel room and fired up my browser to connect. The hotel network is set up so that any HTTP

requests redirect
to their registration page before you are registered.

After successfully connecting I noticed that many of my RSS feeds no longer worked in the RSS reader. It turns out that the RSS reader automatically replaces feed addresses with any redirects and it tried to refresh the feeds between the time I connected the laptop and registered to use the network. The URI addresses for many of the RSS feeds were automatically changed to "<http://soln-sr335.solutionip.com/register/>" (the RSS reader was 'active' on the sleeping laptop before it was connected to the network).

This behavior would be repeated when the RSS reader was running when the network performed its automatic daily shutdown. There wasn't any mechanism on the registration page to register for the whole hotel stay instead of on a per diem basis.

At a minimum, the RSS reader should validate the feed at the redirected URI before blindly switching to it.

🔥 eBay redirects to phishers from their own site

<Pete Krawczyk <risks@bsod.net>>
Tue, 15 Feb 2005 09:08:18 -0600 (CST)

eBay fraudsters have a new trick up their sleeve: using eBay's servers to link to a fraudulent web site.

In the past, it was easy to pass a URL through a decoder and find that the actual server hosted behind a URL was not owned by eBay, since phishers would use @, %40, or other domain misdirection tactics. However, I recently received an eBay fraud mail that contained the following URL, which has been edited to point to Google:

```
http://cgi4.ebay.com/ws/eBayISAPI.dll?
MfcISAPICommand=RedirectToDomain&DomainUrl=http://www.google.com/
```

As you can see, that URL will access cgi4.ebay.com, and eBay will gladly hand the browser over to Google for further action. That URL can be trivially changed to any web site.

The RISK is obvious: allowing untrusted URL redirects in this case will fool many more people who may now believe that eBay is truly asking for account details, and may lead to further identity theft.

I contacted eBay, and got nothing but canned responses. I did try the live chat, and after the rep confirmed that I had not given out my account information, he said they would investigate. That was on Saturday.

⚡ Risks of battery-operated wireless input devices

<Peter Pankonin <webtmc@telusplanet.net>>

Thu, 17 Feb 2005 16:44:01 +0000

This week a user complained that his computer system had locked

up. He had typed away on a document for an hour (without saving of course) and couldn't move the mouse. Rebooting didn't fix the problem.

I was summoned to investigate, whereupon I noticed that the mouse pointer was indeed frozen at the center of the screen. Interestingly enough the keyboard still worked. Then I noticed that there was no red light emanating from his wireless optical mouse. After a quick installation of fresh batteries, the system magically recovered. Unfortunately, I was unable to recover the data lost after he rebooted.

Peter Pankonin, digitalcrucible

⚡ You There, at the Computer: Pay Attention (Katie Hafner)

<Monty Solomon <monty@roscom.com>>

Wed, 16 Feb 2005 22:51:24 -0500

Katie Hafner, **The New York Times**, 10 Feb 2005

FIRST, a confession. Since starting to write this article two hours ago, I have left my chair only once. But I have not been entirely present, either. Each time I have encountered a thorny sentence construction or a tough transition, I have heard the siren call of distraction. Shouldn't I fiddle with my Netflix queue, perhaps, or click on the weekend weather forecast? And there must be a friend having a birthday who would love to receive an e-card right now.

I have checked two e-mail accounts at least a dozen times each, and read eight messages. Only two were relevant to my task, but I responded right away to all of them. My sole act of self-discipline: both instant messaging accounts are turned off. For now.

This sorry litany is made only slightly less depressing when I remind myself that I have plenty of company. Humans specialize in distraction, especially when the task at hand requires intellectual heavy lifting. All the usual "Is it lunchtime yet?" inner voices, and external interruptions like incoming phone calls, are alive and well.

But in the era of e-mail, instant messaging, Googling, e-commerce and iTunes, potential distractions while seated at a computer are not only ever-present but very enticing. Distracting oneself used to consist of sharpening a half-dozen pencils or lighting a cigarette. Today, there is a universe of diversions to buy, hear, watch and forward, which makes focusing on a task all the more challenging.

<http://www.nytimes.com/2005/02/10/technology/circuits/10info.html>

✶ Assuming customers can't spell

<"Andrew Malakoff" <ambler@eskimo.com>>
Thu, 17 Feb 2005 12:38:10 -0800

I'm sure this has come up before, but here it is again. I just tried to use the web site of my Very Large mutual fund group to change my address. My new address contains "Greenlake". The c.o.a. form's hidden, unoverridable, spelling checker insists on, mais naturellement, "Green Lake". The risk of assuming your customers can't spell their address properly: misdirected mail and unhappy customers.

A Malakoff, Seattle WA USA <http://www.eskimo.com/~ambler>

✶ Unintended consequences of automatic abbreviation.

<John Pettitt <jpp@cloudview.com>>

Thu, 17 Feb 2005 19:01:02 -0800

I use Thunderbird to read Usenet news - one of the features of this client is that it abbreviates group names automatically when it displays them. It does this using the first letter of each part of the group name but retains the last word- for example comp.protocols.time.ntp becomes c.p.t.ntp. This works fine until you subscribe to ba.jobs.offered which takes on a whole new meaning when abbreviated :)

✶ REVIEW: "Modern Cryptography: Theory and Practice", Wenbo Mao

<Rob Slade <rslade@sprint.ca>>

Mon, 31 Jan 2005 07:46:52 -0800

BKMDNCRP.RVW 20041207

"Modern Cryptography: Theory and Practice", Wenbo Mao, 2004,
0-13-066943-1, U\$54.99/C\$82.99

%A Wenbo Mao

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

%D 2004

%G 0-13-066943-1

%I Prentice Hall

%O U\$54.99/C\$82.99 +1-201-236-7139 fax: +1-201-236-7131

%O [http://www.amazon.com/exec/obidos/ASIN/0130669431/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0130669431/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0130669431/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0130669431/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0130669431/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0130669431/robsladesin03-20)

%O tl s rl 1 tc 3 ta 3 tv 0 wq 1

%P 707 p.

%T "Modern Cryptography: Theory and Practice"

A "Short Description of the Book" states that it is intended to address the issue of whether various crypto algorithms are "practical," as opposed to just theoretically strong. This seems odd, since no algorithm is ready for implementation as such: it must be made part of a full system, and most problems with cryptography come in the implementation. The preface doesn't make things much clearer: it reiterates a "fit-for-application" mantra, but doesn't say clearly, at any point, why existing algorithms are not appropriate for use. The preface also suggests that this book is for advanced study in cryptography, although it states that security engineers and administrators, with special responsibility for developing or

implementing cryptography, are also in the target audience.

Part one is an introduction, consisting of two chapters.

Chapter one

outlines the idea of the first "protocol" of the book: a "fair coin toss"

over the telephone, grounding the book firmly in the camp of cryptography

for the purpose of secure communications. The remainder of the chapter

points out all the requirements to make such an unbiased selector work,

acting as a kind of sales pitch or "come on" to make you want to read the

rest of the book. The promotion is slightly flawed by the fact that there

is very little practical detail in the material (it takes a lot of work on

the part of the reader to figure out that, yes, this system might work),

excessive verbiage, and poor explanations. The stated "objectives" of the

chapter, given at the end, say that you should have a "fundamental

understanding of cryptography": this is true only in the most limited sense.

Chapter two slowly builds a kind of pseudo-Kerberos system.

Part two covers mathematical foundations. Chapter three deals with

probability and information theory, four with Turing Machines and the notion

of computational complexity, five with the algebraic foundations behind the

use of prime numbers and elliptic curves for cryptography, and various

number theory topics are touched on in chapter six.

Part three addresses basic cryptographic techniques. Chapter seven deals

with basic symmetric encryption techniques, touching on substitution and

transposition, as well as reviewing the operations of DES (Data

Encryption

Standard) and AES (Advanced Encryption Standard). The insistence on converting all operations, and giving all explanations, in symbolic logic does not seem to have any utility, does not provide any clarity, and makes the material much more difficult than it could be. Asymmetric techniques, and attacks against them, are outlined in chapter eight. Finding individual bits of the message, a process examined in chapter nine, can, over time, result in an attack on the message or key as a whole. Chapter ten looks at data integrity, hashes, and digital signatures.

Part four deals with authentication. Chapter eleven reviews various conceptual protocols, pointing out (for example) that there is a serious problem of key storage for challenge/response systems. A variety of real applications are considered in chapter twelve, and warnings issued about each. Issues of authentication specific to asymmetric systems are covered in chapter thirteen.

Part five looks at formal approaches to the establishment of security. There is more asymmetric cryptographic theory in chapter fourteen. Chapter fifteen examines a number of provably secure asymmetric cryptosystems, while sixteen does the same for digital signatures. Formal methods of authentication protocol analysis are given in chapter seventeen.

Part six discusses abstract cryptographic protocols. Chapter eighteen reviews a number of zero knowledge protocols, which provide the basis for authentication where the principals are not previously known to

each other.

The coin flipping protocol, initiated in chapter one, is revisited in chapter nineteen. Chapter twenty wraps up with a summary of the author's intentions for the book.

The book is certainly for advanced study, but it is hardly suitable for security administrators, professionals, or even engineers. The mathematical material is quite demanding, and is seldom explained (as opposed to the clear explanations of the implications of the math that is given in, for example, "Applied Cryptography" [cf. BKAPCRYP.RVW], or even the equally advanced but much more comprehensible "Algebraic Aspects of Cryptography" [cf. BKALASCR.RVW]). However, there are points in the material that could be useful for practical cryptographic systems, provided one is dealing primarily with authentication of communications, and the possibility of physical access is ignored. The text would have been much more useful if the author could have been induced to provide some of the basic explanations in English, rather than leaving the reader to work out the math.

copyright Robert M. Slade, 2004 BKMDNCRP.RVW 20041207
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

Volume 23: Issue 74

Weds 23 February 2005

Contents

- [Mobile phone virus infiltrates U.S.](#)
[NewsScan](#)
- [Re: Component Architecture](#)
[Jim Horning](#) [Rick Russell](#) [Kurt Fredriksson](#) [Fred Cohen](#) [Jay R. Ashworth](#) [Ray Blaak](#)
[Richard Karpinski](#) [Geoff Kuenning](#) [Dimitri Maziuk](#) [Stephen Bull](#) [George Jansen](#)
- [Info on RISKS \(comp.risks\)](#)

🔥 Mobile phone virus infiltrates U.S.

<"NewsScan" <newsscan@newsscan.com>>

Tue, 22 Feb 2005 10:02:43 -0700

The world's first mobile phone virus "in the wild," dubbed Cabir, has migrated to the U.S. from its point of origin in the Philippines eight months ago, infecting phones in a dozen countries along the way. Experts say the mobile-phone virus threat will increase as virus-writers

become more sophisticated and phones standardize technologies that will make it easier to for viruses to spread not just across devices, but the whole industry. Up until now, disparate technical standards have worked against fast-moving virus infiltration, but Cabir has now been found in countries ranging from the China to the U.K., spread via Bluetooth wireless technology. The biggest impact of the relatively innocuous virus is that it's designed to drain mobile phone batteries, says Finnish computer security expert Mikko Hypponen. Last November, another virus known as "Skulls" was distributed to security firms as a so-called "proof-of-concept alert, but was not targeted at consumers. [Reuters/New York Times 21 Feb 2005; NewsScan Daily, 22 Feb 2005]

<http://www.nytimes.com/reuters/technology/tech-tech-security.html>

✦ **Re: Component Architecture (Robinson, [RISKS-23.73](#))**

<"Jim Horning" <home@horning.net>>

Sun, 20 Feb 2005 22:15:47 -0800

Excellent points. Made elegantly by Doug McIlroy at the 1968 NATO

Conference on Software Engineering and published in its proceedings

(<http://homepages.cs.ncl.ac.uk/brian.randell/NATO/>) under the title

"'Mass Produced' Software Components."

Nothing new under the sun, as the prophet said.

Jim H. <http://virtualbumperstickers.blogspot.com/>

Software components (routines), to be widely applicable to different machines and users, should be available in families arranged according to precision, robustness, generality and timespace performance. Existing sources of components - manufacturers, software houses, users' groups and algorithm collections - lack the breadth of interest or coherence of purpose to assemble more than one or two members of such families, yet software production in the large would be enormously helped by the availability of spectra of high quality routines, quite as mechanical design is abetted by the existence of families of structural shapes, screws or resistors. The talk will examine the kinds of variability necessary in software components, ways of producing useful inventories, types of components that are ripe for such standardization, and methods of instituting pilot production. The Software Industry is Not Industrialized. We undoubtedly produce software by backward techniques. We undoubtedly get the short end of the stick in confrontations with hardware people because they are the industrialists and we are the crofters. Software production today appears in the scale of industrialization somewhere below the more backward construction industries. I think its proper place is considerably higher, and would like to investigate the prospects for mass-production techniques in software. In the phrase 'mass production techniques,' my emphasis is on 'techniques' and not on mass production plain. Of course mass

production,
in the sense of limitless replication of a prototype, is
trivial for
software. But certain ideas from industrial technique I claim
are
relevant. The idea of subassemblies carries over directly and
is well
exploited. The idea of interchangeable parts corresponds
roughly to our
term 'modularity,' and is fitfully respected. The idea of
machine tools
has an analogue in assembly programs and compilers. Yet this
fragile
analogy is belied when we seek for analogues of other tangible
symbols of
mass production. There do not exist manufacturers of standard
parts, much
less catalogues of standard parts. One may not order parts to
individual
specifications of size, ruggedness, speed, capacity, precision
or
character set... [MDM]

[We received a plethora comments on this, many of which follow.
Although
there is some repetitiveness, it perhaps amplifies points that
need to be
made, REPEATEDLY. PGN]

✶ Re: Component Architecture (Robinson, [RISKS-23.73](#))

<Rick Russell <rickr@rice.edu>>
Sun, 20 Feb 2005 15:15:54 -0600

Although there are many benefits to software components, there
are many
risks as well. Many exploitable failures result from using the
same

component in many different applications. Consider the buffer overflow in the commonly-used JPEG decoding algorithm, for example. Or the innumerable different operating systems that are compromised because of a bug in a popular off-the-shelf component like SSH, SAMBA, or JPEG decoding.

The problem -- and the place where Dr. Robinson's analogy falls down, I think -- is that software is a lot more complicated, in an algorithmic sense, than a pine board or a copper pipe or a steel spring. Even a widely-used software component that is believed to be reliable can have unidentified problems, and when you expand the definition of software components to large-scale systems with tens of thousands of lines of code (database managers are the most glaring example), you end up with lots of otherwise well-written software depending on buggy components.

✶ Re: Component Architecture (Robinson, [RISKS-23.73](#))

<Kurt Fredriksson <kurt.fredriksson@ieee.org>>

Mon, 21 Feb 2005 15:06:49 +0100

Paul Robinson points at an interesting phenomena.

I was, a long time ago, working for a large corporation. I was member of a working group to establish how we should document software properly.

Some background: Every product was assigned a product number in

the form

"ABC 12345". Every document describing the product was assigned a standardised decimal number, for example "1551" was the description of the product. Thus the description of "ABC 12345" was labeled "1551-ABC 12345"

What we discovered for software was, that we never had the product visible.

For hardware you could produce X items and put them labelled on a shelf.

That was impossible for software as the only visible item was a printout of the code, which had its own decimal number, or the code on paper tape (I told you this was a long time ago) which also had its own decimal number.

Thus software was much more intangible than hardware. This makes it hard to describe a software component in a way that makes it easy to find it when you need it. This especially for real-time applications where timing was critical.

I also had an interesting discussion with a project manager who wanted to hurry up the introduction of reusable software. I asked him what he meant by reusable code. I wasn't surprised that he couldn't define what he asked for. This was the time when OO started to come into fashion. For a critical real-time application you had to know the response time. The black box philosophy of OO doesn't work here.

Paul Robinson mentions the development from machine code, through assembler to higher level languages. He then think that OO were the next step in the development because that is when the hyperbole of reusability

became in
fashion.

If we are to use an engineering approach to reusability, it is called experience. An experienced engineer reuses his/her knowledge to create a new product.

What OO has done to the development of software engineering is devastating. Instead of continue to develop more advanced languages we got stuck with half-assembler languages like C and followers. A compiler for a high level language (re-)uses code templates. A compiler for a more advanced language could reuse even larger chunks of code, without any need for a programmer to try to find the code in a catalog.

To my disappointment, I have seen very little progress during the last two decades in the field of software development. The ever increasing speed of the processors and the cheap memory prices has more encouraged fast hacking than a systematic development based on sound engineering principles.

✶ **Re: Component Architecture (Robinson, [RISKS-23.73](#))**

<Fred Cohen>

Sun, 20 Feb 2005 21:22:59 -0800 (PST)

PGN and others have been working on this for some time. The problems are substantial - in particular in specifying interfaces and

properties of
components and forming mathematics required for producing
properties of
composites from the properties of their components and the
topology of their
composition. Unfortunately inadequate funding is behind this
work and too
few researchers are persuing it. The few agencies that fund
that sort of
thing are also funding few real innovators. But like I said -
Peter is
working on it... so there is always hope.

Fred Cohen: <http://all.net/> fred.cohen at all.net tel/fax: 925-454-0171

[Fred, Many thanks for the kind words. See
<http://www.csl.sri.com/neumann/chats4.pdf>
<http://www.csl.sri.com/neumann/chats4.html>

But that report is just a beginning of an ongoing struggle,
seemingly
tilting at the same windmills for a long time. PGN]

✦ **Re: Component Architecture (Robinson, [RISKS-23.73](#))**

<"Jay R. Ashworth" <jra@baylink.com>>
Mon, 21 Feb 2005 13:00:48 -0500

Aren't reusable software components great? Why doesn't anyone
use them?

Well, Paul: they're much more common than you think.

I build a lot of open source and otherwise free software
programs. *Lots*
of them make use of reusable code components, most notably PHP's
PEAR
repository, and the older code repository from which it is still
learning

lessons: perl.org's CPAN -- the Comprehensive Perl Archive Network.

And comprehensive it is: CPAN has modules for damn near everything you might need to to in writing a perl program.

And the code is pretty decent, too.

But here's the rub: it's not free (as in labor).

Even if you depend on code that someone else wrote to do a job, *someone still had to write that code*. And maintain it. And, most importantly, *know how to write reusable modules well*. It's not all that easy.

If you choose poorly the modules written by other people upon which you decide to depend, you (or your users) may find yourselves in Dependency Hell, when you either end up on the pointy end of a cyclic dependency graph between 3 or more of your subordinate modules (A and B both depend on C, but A requires C v2.1 or newer, and B won't work if C is newer than v1.9), or (the degenerate case of that) C gets upgraded before A, and A won't work with the new version -- because the writer of C wasn't careful enough about reverse compatibility.

So, using reusable components doesn't necessarily reduce the amount of work you're going to put into a project -- sometimes it merely redistributes that work from coders to librarians and testers.

The RISK? Not looking deeply enough to find all the RISKS.

As it happens, CPAN, in particular, meets many of the

requirements Paul
places on reusable components: it has a **very** nice test-
harnessing system
built into it (though tracking down why tests **break** may be
problematic for
end-users). And, of course, it's an interpretive language at
heart, so it's
end-sites that have to **do** that tracking. But still, there are
many good
lessons learned from looking at where CPAN is and how it got
there; I
wouldn't want anyone to think I was putting it down.

Jay R. Ashworth, Ashworth & Associates, St Petersburg FL USA
<http://baylink.pitas.com> +1 727 647 1274 jra@baylink.com

✶ Re: Component Architecture (Robinson, [RISKS-23.73](#))

<Ray BlaaK <rAYblaaK@STRIPCAPStelus.net>>

Tue, 22 Feb 2005 05:35:33 GMT

> 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.

✶ Re: Component Architecture (Robinson, [RISKS-23.73](#))

<Richard Karpinski <dick@cfcl.com>>

Mon, 21 Feb 2005 12:32:07 -0800

It's actually worse than you say.

Nobody delivers programs without serious defects built in, bugs as we say.

All programs come with modes which confuse their users and cause them to commit errors.

All operating systems which support applications do so by providing mechanisms to switch between those applications. The applications are separate and again constitute major modes where gestures are interpreted differently. This means that users must learn each application from the beginning. Even text entry, which virtually every application uses, may differ between applications in many ways which cause more confusions and more frustrations.

But help is on the way.

There is exactly one university level text which addresses these matters in a systematic way. The book is "The Humane Interface" by Jef Raskin. He is, incidentally, the creator of the Macintosh project at Apple. He also led the creation of the Canon Cat almost two decades ago. In 1987, the Cat provided a consistent system which had only two modes: programming and using. Most folks used only the latter. Twenty thousand of these machines were sold and
NO USER EVER REPORTED A BUG!

Be that as it may, why should anyone care? Because he's doing it again. In a little while, you will be able to download Archy from the Raskin Center for Humane Interfaces. Archy has bugs now and will still have

some when the Alpha release occurs, soon. The Raskin Center will try very hard to have none left by the time the general release occurs, many months later. You all are invited to help accomplish that difficult but desirable goal.

Archy provides a thorough text handling facility which does not require use of a mouse and does not require documents to be named or filed in folders. Instead of separate applications, Archy accepts collections of commands. Once accepted, every command is available all the time. Such clumsy devices as modal dialog boxes are rigorously avoided in favor of more humane means to accomplish those ends.

Archy is the pronunciation of RCHI and you can find more information about the system and its philosophy at RaskinCenter.org at your leisure.

✶ Re: Component Architecture (Robinson, [RISKS-23.73](#))

<Geoff Kuenning <geoff@cs.hmc.edu>>
21 Feb 2005 09:33:57 +0100

Paul Robinson wrote a lengthy essay asking that we stop building custom software and start assembling it from components.

This is nothing new, of course. People have been calling for component-based software for decades. The usual analogy isn't a peanut-butter sandwich, but rather the electrical components, especially ICs, used to build the computers themselves.

Of course, the problem with this suggestion is that (as far as I know) nobody has been able to tell us exactly what components are needed or how we are going to interconnect them.

Unix made a pretty good start with the pipe model; I have built some very complex applications by combining these basic utilities. Unfortunately, we haven't succeeded in moving beyond the model; in fact, I've observed that many younger Windows-trained programmers have begun to forget the lessons and have stopped writing "pipeable" utilities.

To be fair, we actually have made quite a bit of progress. I don't write in assembly language any more, and I use extensive libraries to build my software. Some of those libraries, though complex, provide very powerful components (e.g., text-entry windows with scrollbars). But compared to the complexity of what we are building, even these components are akin to 7400-series TTL. (And if you look at the systems that were built with early 7400 gates, I think you'll find much the same "build everything from scratch" approach--30 years ago were still creating flip-flops by cross-connecting two NAND gates.)

The other factor is that the deceptively low materials cost of software development--anybody with a computer can get into the field--misleads us into thinking we are qualified to build a large system. Building the first breadboard of a large electronic system would cost thousands or even tens of thousands in parts and labor; that encouraged caution and kept costs down.

Building the first prototype of a software system requires only the time of the coder(s), encouraging much larger designs.

In other words, the problem isn't a lack of components, it's that we're building much larger systems in relation to the power of those components. The software equivalent of a PB&J sandwich is easy and much more powerful:

```
ls -l | grep -v '^d' | awk '{total+=$5}END{print total}'
```

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

✦ **Re: Component Architecture (Robinson, [RISKS-23.73](#))**

<dmaziuk@bmr.wisc.edu (Dimitri Maziuk)>

Mon, 21 Feb 2005 19:20:07 -0600

The problem with analogies is that they never work.

An architect makes a few assumptions: that owner will not move the house and put it down on a bed of quicksand, that surrounding houses will not swell up and lean on his work from all sides. (Some of his assumptions may later prove unwarranted, like that builder won't use substandard materials or that owner won't try to turn the attic into indoor pool, but that's another story.)

Software developers cannot even assume that user's Pentium will return 4 for 8/2. Not to mention "unforeseen interactions between components in a complex

system" -- since they are "unforeseen" we can't foresee them, and if we can't foresee them, all bets are off.

There was an article in an earlier RISKS issue that proposed exactly that:

"all bets are off", or "fault-oblivious" programming -- that's basically what happens if I make the same kind of assumptions in my work as architect does in his. Attractive as it sounds, in real life the result is hordes of angry users demanding that I fix my stuff YESTERDAY! (or else I don't get paid).

Did I mention users? People who don't read the fine manuals? A screwdriver is only guaranteed for life if you don't use it as a cold chisel. Otherwise the handle *will* break and they most likely *won't* replace it on warranty. Unfortunately, software is not nearly as simple as a screwdriver and to find out what it can and cannot do you need to read a few dozen pages of (usually) mind-numbingly boring manual. In spite of Apple Microsoft advertisements that's been telling you "all you need to do is just point and click" for decades.

> But in general, this is not how we are designing software.

Because in real life they aren't. Because in real life partitioning into smaller and smaller components comes with efficiency overhead that nobody wants. Because other people's components will only work for you if those people's domain model is sufficiently close to yours -- otherwise they are be too generic to be of any use to anybody, all they are is

overhead. And
so on and so forth. Sad, but true.

✶ Re: Component Architecture (Robinson, [RISKS-23.73](#))

<Stephen.Bull@invensys.com>

Tue, 22 Feb 2005 08:20:43 +0000

I agree with Paul Robinson that the software industry could do better. You only have to look at recent spectacular failures in computer based systems to confirm this (e.g. Ariane V and the (UK) Child Support Agency).

However, I don't think his article tells the whole story. As any reader of RISKS knows, software is very different from any other product - so any comparisons should be treated with extreme caution. Software is not constrained by the laws of nature (until or unless it comes to controlling a real system) - consider the recent Matrix trilogy of films. Thus while traditional manufacture is bounded by well-established physical parameters which lend themselves to repeatable solutions, requirements for software systems are not so bounded. This tends to mean that the requirements for each system are unique. And because of the perception that software can do anything, the requirements tend to be complex too: arguably excessively so. Working this down into the details of implementation, this means that the components needed tend to be unique for each system - thus

limiting the possibilities of reuse.

The problem is not helped by the perception that software is "easy to change". (I suspect this is because software production does not involve making physical artifacts in the normal way.) As a result, late changes to system requirements tend to get implemented in software, where the far more reliable solution may be to make a small adjustment to the hardware. This usually means "tweaks" throughout the system, bypassing the usual design processes. This can mean that the resulting product is not amenable to reuse - either because the developer did not have time to make the change "properly" or because the associated documentation was not updated in line with the software itself.

Reuse is not always a good thing, either - witness Ariane V, for example. However, I don't think it is fair to claim (nearly) zero reuse within the software industry. On several projects which I am aware of (in the safety critical field) the developers have bent over backwards to reuse legacy code in order to reduce development costs - usually with much more success than Ariane V.

Another facet of the problem is the requirements: problems with requirements have been cited as the major cause of problems in many software systems. Often, the software will meet its requirements - or, at least, the designers' interpretation of the requirements - the problem often lies in

the requirements themselves being inadequate.

All in all, I agree that software reuse could be improved. However, it is not fair to level all the criticism at software development. Good software (well designed, and trouble free) has been produced: some of this software even has significant amount of reused code. Where reuse is low, the lack of reuse is partly due to the different nature of software; it is also partly due to lack of appreciation of the software lifecycle. Several disciplines need to work together if software reuse is to be improved successfully.

Stephen Bull CEng MBCS MIEE AMIRSE Systems Safety Engineer
Westinghouse Rail Systems T: +44 (0)1249 442593 E: stephen.bull@invensys.com

Re: Component Architecture (Robinson, [RISKS-23.73](#))

<"George Jansen" <GJANSEN@aficio.org>>
Tue, 22 Feb 2005 07:52:57 -0500

I question Mr. Robinson's take, both as a programmer and sysadmin and as one who has had a kitchen remodeled.

For the first case, I think that the depiction on the state of do-it-yourselfness borders on caricature, at least for the business as it has been in the last dozen years. The trucking companies may suffer pain implementing Great Plains or Deltek or an ERP system, but they aren't rolling their own accounts receivables systems. An awful lot of

small systems are built in IDEs with lots of dragging & dropping of icons, and little or no hand-coding. Oracle's Jdeveloper, for example, will allow you to generate quite elaborate JSP systems, whether or not you can tell "implements" from "extends" or recall what "private static" adds to "private".

And as this use of components has been increasing, has security and stability increased with it? The obvious example of Microsoft's COM suggests: Not always. Security alerts do appear for the Java VM. I'd be curious to know the consensus of the Risks contributors on this one.

As for kitchens, on some flat earth, in some perfectly plumb and squared room, the component-based model works perfectly every time. Since 1989 I have lived in two houses of very different look and age, and been through renovations of both. Neither house, the one from the 1980s nor the one from the 1930s, was perfectly plumb or square. Neither had everything--electrical outlets, for example--where it should be. The quality of the renovation depended on the care, experience, and common sense of the renovator. Even the house of prefabricated components relies on the existence of subcontractors who know not to saw through joists to run ducts. Christopher Alexander may be a better guide to this world than Eli Whitney.

Finally, building technologies have their lurking flaws. For a simple example, all rowhouses built in the Eastern US from about 1975 to about 1990

used fire-retardant plywood to obviate the need for firewalls protruding beyond the roof. Then it was found that this plywood crumbled away not just at fire temperatures but, more slowly, at normal summer attic temperatures. If you think that the house owners were made whole by the courts, you don't know enough about accountants and lawyers.

Years ago I quoted to an architect Weinberg's line that "If architects built buildings as programmers build programs, the first woodpecker to come along would destroy civilization." "Oh," she said, "but that's just how they do build them."



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 75

Thursday 24 February 2005

Contents

- [Networked homes spell trouble for consumer electronics](#)
[NewsScan](#)
- [Spam-blocker causes missed court date](#)
[Terry Carroll](#)
- [UK gets official virus alert site](#)
[Chris Leeson](#)
- [SPIM](#)
[NewsScan](#)
- [More robot scanner phenomena](#)
[Mark Rockman](#)
- [Re: Component Architecture](#)
[Martyn Thomas](#) [Peter B. Ladkin](#) [Jay R. Ashworth](#) [Mike Ellims](#) [Daniel P. B. Smith](#) [Ben Galehouse](#) [Roderick A. Rees](#) [David G. Bell](#) [Raj Mathur](#)
- [Re: Urology medical student residency "matching" process failure](#)
[Jerry Leichter](#)
- [Re: Assuming customers can't spell](#)
[Tom Russ](#)
- [IWIA 2005 Call for Participation](#)
[Stephen D. B. Wolthusen](#)
- [Info on RISKS \(comp.risks\)](#)

✦ Networked homes spell trouble for consumer electronics

<"NewsScan" <newsscan@newsscan.com>>

Thu, 24 Feb 2005 10:32:31 -0700

The vision of the "networked home" is driving the digitalization of nearly every consumer electronics device, and eventually could lead to the disintegration of the consumer electronics industry as we know it, says Columbia University public policy expert and economist Eli Noam. Caught in the upward spiral of Moore's Law, the chips that run consumer electronics devices will become evermore powerful, and many stand-alone products, such as Blu-Ray Disc players, TVs and PCs, could entirely "disappear," says Noam. In fact, it's already happening: consumer PCs now come with built-in TV and recording functions, and vendors are selling DVD, CD and VHS players packaged as single units with hard disk drives. And while Noam predicts a bonanza for consumer electronics makers in the near term -- the next seven years or so -- ultimately, many of the networked products will be replaced by a single box or hub. "The good news is that this will mean an initial spike in demand for makers. But it also means fewer hardware boxes being sold," says Noam. As the trend continues, and consumers demand easy-to-use and glitch-free home networking, a new breed of specialized services, called CSPs (Consumer Electronics Service Providers), could emerge, who would

integrate home, community and work-based networks, providing services based around content provision, security and assurance.

[*ComputerWorld*, 16 Feb 2005; NewsScan Daily, 24 Feb 2005]

<http://www.computerworld.com/managementtopics/management/itspending/story/0,10801,99821,00.html?source=x10>

✶ Spam-blocker causes missed court date

<Terry Carroll <carroll@tjc.com>>
Wed, 23 Feb 2005 11:54:28 -0800 (PST)

"A plaintiff's attorney in a wrongful-death lawsuit, who missed a court date because his firm's spam blocking software automatically sidetracked the court's e-mail notice, has narrowly escaped being sanctioned for failing to appear at the scheduled status conference...."

<http://news.lp.findlaw.com/andrews/pl/med/20050223/20050223barnes.html>

✶ UK gets official virus alert site (BBC News)

<"LEESON, Chris" <chris.leeson@atosorigin.com>>
Thu, 24 Feb 2005 10:04:22 -0000

The UK government is setting up a Virus Alert site to warn users of viruses, vulnerabilities and so on. It is aimed at home and small business users.

<http://news.bbc.co.uk/1/hi/technology/4291005.stm>

It is expected to issue between six and ten alerts a year, concentrating on the most major problems. It will not provide patches, but will point the user to where the patches can be downloaded. It is also made clear that the site is not a panacea or a substitute for proper AV and Firewall provision.

Similar schemes exist in the USA and Netherlands.

This looks like a very good idea, and I applaud the government for doing it (something that I do not do often). Alas, there remains a number problems:

1. This would be a great site for the Malware Brigade to spoof. I hope that it is more secure than most Web Sites.
2. They are concentrating on the most serious threats. Understandable, but even the "less serious" threats can be trouble.
3. Most PC users are simply not interested in PC Security and won't be convinced that they have to be. The new users may well not realise that they are exposed at all. (I am a little sore about this having just spent three days trying to salvage someone's XP system after the PC had spent two weeks on Broadband without Firewall or AV...)

 **SPIM**

<"NewsScan" <newsscan@newsscan.com>>

Tue, 22 Feb 2005 10:02:43 -0700

Battling the spim-meisters

Almost one in three instant-messaging users in the U.S. have received some kind of "spim" (unsolicited commercial instant messages), according to a survey by the Pew Internet & American Life Project. Results indicate that users age 30 and younger are more likely to get spimmed, compared with the next older age cohort (31-49). Other than the age discrepancy, however, no other demographic trends were discernible, says Pew: "Instant message users in all income brackets and in all racial and ethnic groups are equally likely to receive spim. Somewhat surprisingly, broadband users at home are no more likely than dialup users to receive spim, even though, presumably, those with always-on broadband connections keep their instant message programs running for longer periods of time than dialup users." The survey found that 52 million Americans -- 42% of the online population -- use instant messaging, and among the 30-and-under age group, it's 66%. [Pew Internet & American Life Project, 21 Feb 2005; NewsScan Daily, 22 Feb 2005]

<http://www.pewinternet.org/PPF/p/1052/pipcomments.asp>

First spimmer arrest

An 18-year-old New York teenager has become the first person to be arrested on suspicion of spimming. Anthony Greco allegedly sent 1.5 million messages hawking pornography and mortgages to users of MySpace.com's IM system, and

was arrested in a sting operation in the Los Angeles Airport last Wednesday following an extortion attempt on his part. Greco believed he was flying to LA to seal a deal with the president of MySpace.com, whom Greco had threatened with publicizing his spam techniques if he were not granted an exclusive marketing arrangement that would have legitimized his spamming activities. Assistant U.S. Attorney Brian Hoffstadt says that while Greco's case marks the first criminal prosecution of instant message spamming, there may well be more to come: "We're just beginning to get the tip of the iceberg. This could be a new wave as online communities start up." [CNet News.com 21 Feb 2005; NewsScan Daily, 22 Feb 2005]
http://news.com.com/U.S.+makes+first+arrest+for+spam/2100-7355_3-5584574.html

🔥 More robot scanner phenomena

<"Mark Rockman" <mrockman@acm.org>>
Sat, 12 Feb 2005 21:19:33 -0500

Twice in one week I've tried to use a robot scanner only to find it is stuck at the "FINISH AND PAY" node of the transition diagram. The bagging area has nothing in it. There is no customer around, except me. Conclusion: shopper rang up the goods, bagged them and left. Result: merchant is stiffed for \$17.49, an innocent customer could be accused of having rung up the goods and hid them, and WORST, the lane is out of service

until a manager becomes aware of the situation minutes or hours later and overrides the computer. Does the robot notice time passing at the FINISH AND PAY node? It does not. Shouldn't an alarm go off? I think so.

✦ Re: Component Architecture (Blaak, [RISKS-23.74](#))

<"Martyn Thomas" <martyn@thomas-associates.co.uk>>
Wed, 23 Feb 2005 21:35:30 -0000

Well, I know one company that is willing to offer warranties on its software, free, because it uses a "Correct by Construction" approach that reduces the commercial risks to acceptable levels. They don't charge more for the development, either, because it doesn't cost them any more to work this way than industry norms.

The company is Praxis High Integrity Systems: www.praxis-his.com .

And no - I don't have any financial links with them, although I did co-found a predecessor company.

✦ Re: Component Architecture ([RISKS-23.74](#))

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Thu, 24 Feb 2005 08:15:18 +0100

I was surprised to find little of the extensive commentary on Robinson's essay directed at his premise. (Stephen Bull and George Jansen addressed the premise en passant.)

The premise is obviously false, as points 1-4 below note.

1. I would hazard a guess that most software development in the world (in terms of effort) is directed towards modifying already existing software, and comparatively little of it towards developing source code from scratch in a common programming language.

2. It has been standard knowledge in the industrial SW development world for the two decades I have been working in and around it that between 60% (Putnam, 1978) and 80-90% (Balzer, Cheatham, Green, 1983) of software development lies in "maintenance", that is, modifying already existing SW. (Boehm 1987 put TRW's effort at 67%.) So in simple terms of level of effort, most of the effort even in "from-scratch" SW systems does not go into the initial coding, but into modification of existing systems.

3. The work of many large companies offering SW-based systems is better described as configuring existing systems, or building on a base of existing SW. Air traffic control system providers spend considerable development effort on each new installation. Much of that effort is spend configuring their already-existing SW to the specific ATC center airspace architecture, and modifying it to attain client requirements. The NERC

in Swanwick, U.K., presented as the largest system of its kind, used, roughly, 50% of its code from a common core (~1M LOC) and 50% as local adaptation. (The "common core" ended up not being all that common: the U.S. FAA's AAS, which also was to be based on it, was canceled.) The business of two of the world's largest SW system providers, Oracle and SAP, is better described not as building systems from scratch but as configuring extensive existing SW systems to a client's particular needs.

4. Trucking companies, at least in Europe, buy their enterprise SW from, for example, a SAP-approved company which has adapted SAP's enterprise SW for trucking company business. Or from one of SAP's competitors such as PeopleSoft.

Much of the rest of the commentary points out why configuring existing SW systems to a new application is not that easy. That accounts for why most of SW development effort goes there.

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

✶ Re: Component software edition ([RISKS-23.75](#))

<"Jay R. Ashworth" <jra@baylink.com>>
Wed, 23 Feb 2005 16:10:19 -0500

I found it telling about the RISKS audience that only my submission, and

that of George Jansen, said, in effect, "But we're *doing* that already"; that seemed the fundamental point of Paul's original contribution, and I was surprised that so few of the other categories of responses you selected made the appropriate rebuttal.

Was the percentage of replies that *did* rebut his point proportionately that small, or did you just filter harder there? [YES, NO, respectively. No filtering. I am running almost every reply except for overt dupes. PGN]

Jay R. Ashworth, Ashworth & Associates, St Petersburg FL USA
<http://baylink.pitas.com> +1 727 647 1274 jra@baylink.com
Baylink

✶ Re: Component Architecture (Robinson, [RISKS-23.73](#))

<Mike Ellims <mike.ellims@pитеchnology.com>>
Thu, 24 Feb 2005 16:39:34 -0000

George Jansen introduced the kitchen programming paradigm; the house programming paradigm was introduced in the following paper a couple of years back.

Robert Biddle, Angela Martin, James Noble: No name: just notes on software reuse. OOPSLA Companion 2003: 240-260

It provides an interesting take on the construction parts bin and the literary history of software reuse.

Here's an observation, if the construction/civil engineering industry is so good at reuse. Why is there such a large market for sticky gunk for gluing/filling and otherwise concealing. Where would the construction industry be without "No More Big Holes" (expanding foam in a tube) or PolyFiller?

Mechanical engineering has it's standard components, nuts, bolts, screws, nails etc. Just as we have some as well, languages, editors, protocols etc. The point being missed in arguments like the one Robinson puts forward, is that it ignores the fact that in any system of sufficient complexity - nearly everything else is bespoke design.

How many standard components are there on an F22?

✶ **Re: Component Architecture ([RISKS-23.73](#))**

<"Daniel P. B. Smith" <dpbsmith@verizon.net>>
Wed, 23 Feb 2005 19:34:07 -0500

Who says the parts are interchangeable?

Paul Robinson has the silver bullet, and it is software components. Right.

One of the things I learned from a talk by Tom Love, circa 1991, on software components, was that Eli Whitney's mass-produced parts were not, in fact, interchangeable (even though that was the basis on which he had gotten

Congress to fund his factory).

And so it is with software parts.

Circa 1998, a program I had written, which had been shipping for years, developed a very odd bug.

It turned out to be an error in the vendor's C library implementation of strcmp.

It had some clever-clever optimizations so that it could perform the bulk of the comparison by four bytes at a time. And a number of different logic paths to avoid setting up a zero-count loop if the transfer was less than five bytes long. And some special cases depending on the relative alignment of each of the comparand's addresses with a four-byte boundaries. One of the cases happened to misbehave if a character at one particular position in the string happened to be in the upper byte range (128 to 255, high bit set). (And for the record, yes, the documentation for strcmp does define what the behavior is supposed to be bytes in the upper byte range. And the behavior wasn't consistent; comparing string A with strings B and C, where B and C had identical contents but different placement in RAM, gave different results).

I could have reported the bug to the vendor. As a matter of fact, I did. It hasn't been fixed yet. (The development system was supposedly still being supported but was nearing end-of-life and wasn't a very high priority).

Maybe I could have gotten on my high horse and returned the compiler to the vendor and insisted on our money back. But getting the product to compile and build under another vendor's development system would have taken much, much longer than that.

So I did what I truly believe to be the sensible thing: I wrote my own implementation of strcmp. Wrote it to be as simple as it could possibly be and to hell with efficiency. Unit-tested it. Carefully. With a test-case generator that generated all sixteen cases of relatively alignment of start-of-string to four-byte boundaries, and many combinations of upper- and lower-byte characters. And put it into service.

strcmp is one of the most simple, basic, fully-documented, and frequently-used "components" there is.

strcmp isn't an interchangeable part.

✦ **Re: Component Architecture (Robinson, [RISKS-23.73](#))**

<Ben Galehouse <bgalehouse@spamcop.net>>

Wed, 23 Feb 2005 10:56:42 -0500

I agree in many ways with Paul Robinson's comments. However, I think that it is easy to underestimate the challenges involved. Mechanical engineers have been held accountable (at least in a sense) for their engineering failures since Hammurabi. Almost certainly, this cultural norm makes buildings

safer. However, it certainly doesn't make them perfectly safe.

Standardization and modularization is encouraged in the physical world because specialized equipment greatly increases the efficiency of construction for many products. The equipment needed to create a transformer is rather different than that required to create a capacitor. Standardization also makes warehousing and logistics easier.

These particular advantages either don't exist or aren't so obvious in the computer realm. For these reasons, as well as for all of the reasons typically mentioned for software, there are many standards for nuts, bolts, steel, concrete, and so on.

As a result of this, nuts and bolts are rather standard. Or rather, nearly all of them follow some standard or another. I'm told that some automobiles have both metric and SAE bolts in them. You still need to know the model of your automobile in order to order almost any part. Turnkey machine shops are still in business. I've seen transformer companies specifically advertise their willingness to wind custom transformers. Custom chip fabrication is no small market.

Software engineering is a young field, and it shows. Modularization requires interface standards and these are still being developed. Heck, even the standards for presenting said interface standards seem to be under comparatively active development.

It is easy to present modularization and formal methods as holy grail

solutions. To be sure, they can yield big improvements. However, the standards and modularization that we take for granted in the physical world are the product of much evolution and no small amount of experience. Formal methods played a part in this, but only a part.

✈ **Re: Component Architecture (Robinson, [RISKS-23.73](#))**

<"Rees, Roderick A" <roderick.a.rees@boeing.com>>

Wed, 23 Feb 2005 07:44:52 -0800

Paul Robinson ("In the Matter of Component Architecture") makes some proper points, but there is something missing. There actually are software components that could be widely used -- such as those for straightforward mathematics. The reason for this, though, is that mathematics is deliberately stripped of almost all meaning. Bertrand Russell famously said that it is the subject in which we never know what we are talking about nor whether what we are saying is right. The meanings and definitions of mathematics are deliberately so limited, to minimise the possibility of confusion, that in everyday human terms they are meaningless.

The problem with real and meaningful expression is that it is never fully expressed or even fully conscious. We always make a whole series of assumptions, most of which are not explicit. This leads to all the great battles in theology and philosophy, because no two people are ever talking

about exactly the same thing, which is a direct consequence of the fact that we never fully know our own assumptions. All the great engineering failures, where they were not the consequence of simple mistakes, were caused by ignorance or neglect of physical realities.

In software we see this every day. Several times a week I want to strangle a programmer, because of the things he has assumed about the way other people think. He works on a process for months and is familiar with it, so it all seems obvious to him; and then I am presented with a choice of A and B, and have no idea what assumptions and consequences go with either of them. Or I make the right choice, but it does not work because - as I eventually discover - he requires an updated version of one of my support programs, which I can't get because my company did not know it existed.

There was an article in *New Scientist* some years ago called "Why Can't You Program the VCR?" written by a professor of IT, who admitted that he could not program the damned thing. Designers' assumptions again.

If we are to get anywhere near producing useful software components beyond mathematics, there will have to be a determined effort to uncover the assumptions underlying the requirements, the programmers' training and thinking, and the management control. And who is going to pay for that?

⚡ Re: Component Architecture

<dbell@zhochaka.demon.co.uk ("David G. Bell")>

Thu, 24 Feb 2005 09:53:01 +0000 (GMT)

Computers and Standard Components

May I simply say that I fully support the well-deserved derision directed at software producers who keep re-inventing the wheel wasting time, effort, and what is ultimately **my** money as a purchaser.

One of the pioneering standards for interchangeable components, still in use, is the Whitworth thread. It is ironic that Mr. Whitworth was prompted to devise the standard by the experience of working with Charles Babbage, and the many nuts and bolts of his experimental mechanical computing machines.

Some software I've used, the programmer needs something like a 15/16" Whitworth spanner, applied cranially.

⚡ Re: Component Architecture (Kuenning, [RISKS-23.74](#))

<Raj Mathur <raju@linux-delhi.org>>

Thu, 24 Feb 2005 09:59:50 +0530

```
> ls -l | grep -v '^d' | awk '{total+=$5}END{print total}'
```

It works, yes, but not generally reusable. You may be better off with:

```
ls -l | grep -v '^[bcdps]' | awk '{total+=$5}END{print total}'
```

so you don't try to count sizes of devices, pipes and sockets.

Raj Mathur raju@kandalaya.org <http://kandalaya.org/>

✶ Re: Urology medical student residency "matching" process failure

<Jerry Leichter <jerroldleichter@mac.com>>

Sun, 20 Feb 2005 16:26:52 -0500

Daniel Kahn Gillmor ([Risks-23.71](#)) reports on a problem with the urology medical studentmatch. He points to the blog entry describing the problem:

<http://blogborygmi.blogspot.com/2005/01/selection-dysfunction.html>

and quotes from it - leaving out the actual explanation:

Upon careful review, we found that one of the criteria in the match was

not applied correctly, causing some outcomes to be skewed.

While clearly a bug and embarrassment, it's hardly a deep problem with the program. If you optimize along an incorrectly-computed measure, the result won't be right - but that's hardly a basis for criticism of the optimizer.

Mr. Gillmor complains that "the algorithms used in the match process [should be] freely available". They are: A single Google search followed by looking at three pages leads to:

http://www.nrmp.org/res_match/about_res/algorithms.html

(The mathematics of this were published years ago. Basically, given a set of preferences in each direction - application for program and vice versa - there are exactly two "optimal" solutions, in the sense that for anyone to improve his position by moving to lower-numbered position in his own ranking, someone else would have to be moved to a higher-numbered position by at least as much. The two solutions differ in that one is at least as good as the other - but may be better - from the point of view of all applicants, while the other is at least as good from the point of view of all programs.)

As to his other comments:

> So, why wasn't a human reviewing the results of the match for
> reasonableness before publication?

There are hundreds of people matched every year, apparently with little complaint since the program was put in place (at least since my sister entered her residency, which would be around 20 years ago). In this case, the error was blatant - some highly-rated programs weren't matched to anyone - and indeed was caught within 3 days. It's not clear that a subtle error could be spotted by a human being.

> What safeguards are there on the data-entry step (since GIGO continues
> to apply)? Why isn't there an audit process in place?

This doesn't appear to have been a data-entry error. It's not clear what

should have been audited.

We'd all like systems to be perfect. But the reality is that one has to consider both the cost of the error and the cost of preventing it. Both the programs looking for applicants, and the applicants themselves, pay for this service. I can't right now find the cost - it may depend on the particular match - but having watched people go through this process, I would not expect it to be cheap. How much extra would *you* pay to help eliminate what appears to be a very rare error?

You might also want to look at

<http://medicalmatcherrors.blogspot.com/>

(pointed to from the previous blog), and especially the first (well, only as of when I looked) response.

I should point out that I have absolutely no connection with this process, but I've always thought it was one of the more rational and, from what I've seen, better run selection efforts. I would have much preferred this kind of thing to the college application process I went through in the late 60's - a process that, from all reports, has gotten much more complex, difficult, subject to "gaming", expensive, and unpredictable since!

✶ Re: Assuming customers can't spell (Malakoff, [RISKS-23.73](#))

<Tom Russ <tar@ISI.EDU>>

Wed, 23 Feb 2005 11:28:33 -0800

On Change of Address Form Validation

Andrew Malakoff's experience with the change of address form may have had another, and to my mind more likely, explanation than a spelling checker. I suspect that the address was, in fact, run through the US Post Office's address canonicalization process. This would seem to be a quite reasonable validation step, since most businesses that send out mass mail (like newsletters) have such software for checking and grouping mailings. Changing the address to match what the Post Office expects seems to be the right thing to do, even if the "official" spelling of street or place names is not what the local actually use.

One could test this by going to the USPS web site and running the same process on the address and see if the same thing happens:

<http://zip4.usps.com/zip4/welcome.jsp>

For example, "123 west oak avenue" => "123 W OAK AVE"

IWIA 2005 Call for Participation

<wolt@igd.fhg.de (Stephen D. B. Wolthusen)>

Wed, 23 Feb 2005 15:04:56 +0100 (MET)

Third IEEE International Information Assurance Workshop
March 23-24, 2005 --- College Park, MD, USA

<http://iwia.org/2005>

Sponsored by the
IEEE Computer Society Task Force on Information Assurance
in cooperation with the
ACM Special Interest Group on Security, Audit, and Control

This third international workshop on information assurance pursues several goals. One is the dissemination of research across the spectrum of information assurance and the fostering of a scientific community working in this field. Another primary goal is to bring together researchers and practitioners from both governmental, defense, intelligence, and civilian areas and to stimulate discussions on current and future problems as well as solutions. The keynote talk will be given by Dr. Roger Schell. For information on the program, location of the workshop, accommodation and registration please see <http://iwia.org/2005>.

General Chair: Jack Cole, US Army Research Laboratory, USA
Program Chair: Dr. Stephen D. Wolthusen, Fraunhofer-IGD,
Fraunhoferstr. 5,
64283 Darmstadt GERMANY +49 (0) 6151 155 539



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 76

Monday 28 February 2005

Contents

- [BofA loses backup tapes in transit with customer data](#)
[Nicolai E M Plum](#)
 - [Some Sympathy for Paris Hilton](#)
[John Schwartz via Monty Solomon](#)
 - [Sensitive information: lesson learned](#)
[Bill Hopkins](#)
 - [Computerization of the automobile continues apace](#)
[Omri Schwarz](#)
 - [Address coercion](#)
[Paul D. Smith](#)
 - [Re: "Spam-blocker causes missed court date"](#)
[Joseph Brennan](#)
 - [Re: UK gets official virus alert site](#)
[Rob Skedgell](#)
 - [Re: Component Architecture](#)
[Mark Lutton](#) [Steve Taylor](#) [Jan Vorbrüggen](#) [Olivier Dagenais](#) [Paul D. Smith](#) [Steven Hauser](#)
[Dimitri Maziuk](#) [Bill Royds](#) [Tom Swiss](#) [Ross Lonstein](#) [Dave Budd](#) [Geoff Kuenning](#) [Dan Jacobson](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ BofA loses backup tapes in transit with customer data

<Nicolai E M Plum <nicolai@esperi.org>>

Sat, 26 Feb 2005 15:50:34 +0000

Bank of America "lost computer tapes containing account details of more than one million customers who are US federal employees", reported by the BBC at

<http://news.bbc.co.uk/1/hi/business/4300371.stm>

My first question is "Why were the backups not encrypted before leaving a BofA site?". The RISK is obvious - handing unencrypted sensitive data to random third parties significantly increases the chance of them being stolen and misused. Commercial backup software offers encrypted backups these days, even.

There is another more general RISK, since the theft occurred on a commercial airline flight. There is a conflict between wishing to lock your luggage to prevent theft from luggage handlers (a group of people known to steal from luggage) and being told that if you lock your luggage the lock may be forced open and destroyed by the Transport Security Administration searching your bags - you can't win. The "TSA [master] key" lock idea will just mean the thieving baggage handler will acquire one of the master keys beforehand.

I doubt background checks, as suggested by Senator Charles Schumer in this article, are an effective solution. Failure to encrypt these backups before

they went offsite seems negligent of BofA to me.

✦ Some Sympathy for Paris Hilton (John Schwartz)

<Monty Solomon <monty@roscom.com>>

Sun, 27 Feb 2005 21:24:02 -0500

Some Sympathy for Paris Hilton

By JOHN SCHWARTZ, *The New York Times*, 27 Feb 2005

POOR Paris Hilton!

As unlikely as the preceding sentence might seem, there is ample reason to pity Ms. Hilton, the heiress, reality-TV actress, product pitchwoman and accidental porn starlet.

Ms. Hilton just can't seem to get a break in the digital age. She suffered embarrassment back in 2003 when a homemade sex tape hit the Internet, and now her Sidekick - a high-tech toy that combines phone, organizer and camera and also lets users send e-mail and instant messages - has been hacked. Its contents, like her movie, were posted to the Internet for any and all to enjoy.

"She was pretty upset about it," someone told MSNBC. "It's one thing to have people looking at your sex tapes, but having people reading your personal e-mails is a real invasion of privacy." ...

<http://www.nytimes.com/2005/02/27/weekinreview/27paris.html?ex=1267246800&en=72b477ed1c2b85ad&ei=5090>

✦ Sensitive information: lesson learned

<"Bill Hopkins" <whopkins@wmi.com>>

Fri, 25 Feb 2005 18:25:46 -0500

A Delaware blood bank lost a laptop computer containing sensitive information about donors when it fell off a truck (really). It was found and returned by the finder.

Officials say they will now encrypt the information to prevent its unauthorized use or disclosure.

Who knew? Perhaps the publicity will wake up a few others with similar data responsibility.

[Source: WHY-FM, the Philadelphia NPR station, filtered through BH]

✦ Computerization of the automobile continues apace

<"Omri Schwarz" <ocschwar@MIT.EDU>>

Fri, 25 Feb 2005 12:13:51 -0500

<http://www.sun-sentinel.com/news/custom/fringe/sfl-225nissan,0,2964317.story?coll=sfla-news-fringe>

This system takes over the steering in some situations:

"Lane Departure Prevention" combines a camera and computerized devices

that control braking for front and rear wheels, nudging the car in the right direction. The feature disengages when you hit the turn signal, so you can change lanes and make turns.

The RISKS are obvious.

✶ Address coercion

<"Paul D.Smith" <Paul.D.Smith@dataconnection.com>>

Fri, 25 Feb 2005 09:08:12 -0000

A few years ago I was working in the US and applied for a bank account. They insisted on taking my "permanent" address, which was in England. But on entering the town, Enfield, they were then stuck - their software insisted that Enfield was in either Vermont or a couple of other US states. There is indeed an Enfield in Vermont, just not mine. Just another example of the software being made too "clever" by the programmer with "bullet-in-foot" being the result.

✶ Re: "Spam-blocker causes missed court date" (Carroll, [RISKS-23.75](#))

<Joseph Brennan <brennan@columbia.edu>>

Sat, 26 Feb 2005 17:40:03 -0500

According to the reporter, the lawyer said that "his firm's spam

blocking

software automatically sidetracked the court's e-mail notice" and that "his law firm's spam-blocker software set the Internet security level too high, which blocked the e-mail notification from the court. After the security level was reset, the notification came through."

One would conclude from this that the law firm had unmonitored software that was throwing away mail willy-nilly. Or perhaps that the law firm's system administrator configured it to do so. Both are serious charges that are likely to cause fear and doubt among users of email systems. It is unlikely that either is true.

I submit to the court that the most likely facts are that the filter sorted the court notice into a possibly-spam folder and that the lawyer failed to look at the folder regularly.

The next most likely case is the one I find the most disturbing: that the law firm's system refused the message (smtp 550) or accepted it and mailed a bounce notice back. But if this happened, why would the court issue the show-cause order?

This is a vital question, because as an email system administrator, I rely on refusal as a valid way to notify senders that mail was not delivered. I expect the sender's system to generate a bounce and I expect the sender to look at it. I would be very surprised to be held responsible for failing to read a message that was properly refused. The smtp protocol has always

defined the sender system as responsible until the remote side accepts.

By the laws of wishful thinking I assume that the court does not ignore its bounces, and that the law firm's system does not throw away mail without notice. Therefore the court was in error. Unfortunately the filter software is not a person under law and cannot file for damages!

Joseph Brennan, Academic Information Systems
Columbia University in the City of New York

✉ Re: UK gets official virus alert site (Leeson, [RISKS-23.75](#))

<Rob Skedgell <rob@nephelococcygia.demon.co.uk>>

Fri, 25 Feb 2005 03:54:34 +0000

> 1. This would be a great site for the Malware Brigade to spoof. I hope
> that it is more secure than most Web Sites.

Sadly, no:

Signing up for email or SMS alerts does not appear to require any address confirmation, so presumably anyone can sign up anyone else's email address or mobile phone for alerts. Also, no secure (SSL/TLS) form is provided for submission.

I am also dubious about the 'ITsafe Word' scheme to protect from spoofing by the 'Malware Brigade' -- <http://www.itsafe.gov.uk/glossary/itsafeword.html>

definition: A security feature used on the ITsafe website to help reduce the

risk of someone spoofing our e-mails.

When you sign up to our e-mail service you are asked to type in an ITsafe

Word (please keep this clean). This is not a password, so if you forget

it, it is not the end of the world. You just need to be able to recognise

it again in the future.

All e-mails we send to you will use this word in the 'subject' line. In

e-mail programs this is normally displayed just above the e-mail

content. You can quickly check that the e-mail has come from us as someone

else would not know your ITsafe Word.

Until you forward the email, forgetting to remove it (not that it mentions

that people **should** do this on forwarding etc). Or post it to USENET, or...

I wonder if they have heard of S/MIME or PGP signatures?

The problem here is that quite a lot of people will probably receive this as

a forward, all malware would need to do is search mail folders for a

legitimate bulletin (identified from mail headers) with the ITsafe Word in

the subject line and use this to construct a forgery to attach itself to...

ITsafe site URL <http://www.itsafe.gov.uk/index.html>

✉ Re: Component Architecture ([RISKS-23.74](#) and [.75](#))

<Mark.Lutton@thomson.com>

Fri, 25 Feb 2005 13:19:42 -0500

Several replies to Paul Robinson's "In the Matter of Component Architecture" suggest changes to the analogies.

Robinson: "most likely you got out of a bed, got up and took a hot shower in your indoor bathroom...." As many replies pointed out, the components may be applied in new situations: A Linux computer instead of a Windows computer, or a faster or slower computer where the components may or not meet real-time requirements. Another reply told about a bug in the C library. There can also be a bug in the operating system or in the computer's firmware. Remember how some interrupts wouldn't preserve the BX register on the original IBM PC? The firmware may be a component to you but it's part of the environment to me. My program is expected to work in unpredictably buggy environments. So, add to the analogy: "As you were doing this, several other people attempted to take a shower with identical plumbing and heating: an astronaut on the Space Station in zero gravity, a man on Mars where the low atmospheric pressure made the hot water evaporate as soon as it left the showerhead, and a cold-adapted inhabitant of Pluto who found the showerhead couldn't deliver the ice-cube shower he wanted. "Meanwhile on Earth, a bug in your local laws of nature makes water change into sulphuric acid if its temperature is between 119.3 and 119.4 degrees F, so you have to be careful with the temperature setting or risk damage to the

showerhead. You had some difficulty yesterday when the gravity server malfunctioned for a few seconds and all the water fell up to the ceiling."

Mark Lutton, Dialog, a Thomson business. mark.lutton@thomson.com

✶ Re: Component Architecture ([RISKS-23.75](#))

<"Steve Taylor" <steve.taylor@PETARDSCS.CO.UK>>

Fri, 25 Feb 2005 11:40:00 -0000

I am surprised that nobody has remarked on the fundamental fallacy in comparing the "design" of software with the "manufacture" of physical items. If you want to compare software development with other engineering then you must understand the economics of design and manufacture in these two industries. The software manufacturing process typically involves copying of the software onto a CD; this is so fundamentally cheap that the practical cost of software is focused in the design stage. In physical engineering the vast majority of products that people encounter have the opposite relationship - cost is dominated by manufacturing. This doesn't invalidate the comparison but it does mean that it has to be made very carefully. When, for example, a building designer uses of the shelf components do they do it to make the design process simpler or do they do it because the construction is cheaper. All the cases where the decision is made to reduce

construction costs are not applicable for comparison with the software industry. In fact software designers may make an opposite choice for exactly the same reason - in software any standard of the shelf component may bring manufacturing costs (license fees) whereas a home-grown variety is free. I believe this is an important force undermining reuse of components in software.

I am in the business of producing software with a price limit from tens to hundreds of UK pounds per license. If I reuse commercial components with license fees of 20 pounds each then I very quickly destroy the economic viability of what I am doing. In most cases the functionality I am actually using in a software component that costs 20 pounds can be reproduced for a lot less than the license fees I expect to pay on predicted sales. If I were making physical objects then my custom manufactured component would probably have higher manufacturing costs than a bought in item rather than the zero cost that applies in software.

The optimism that typically pervades the software development industry reinforces this process. Managers choose in house development because the initial estimates show it will be cheaper. If they were a little more aware of the typical cost overruns, additional maintenance costs and the like then there would probably be more reuse.

The result of all this is that there is only widespread take up of component reuse where those components are reliable and free. The

dominant source of
these is the tools built into development environments. I have
been in
software for many years and I remember programming with
assemblers and
simple language compilers where at best I got 3 or 4 machine
instructions
for each line of code. These days the number of machine
instructions and
the amount of functionality for each line of code has increased
dramatically. This is unquestionably reuse of components, even
if many of
them are very small ones, and everybody uses these tools.

Steve Taylor, Technical Director, AssetCo Data Solutions 0116
2405755

✶ Re: Component Architecture ([Risks 23.73](#))

<Jan Vorbrüggen <jvorbrueggen-not@mediasec.de>>
Fri, 25 Feb 2005 15:51:11 +0100

During the more than ten years that I worked at an Institute for
Neural
Computation as a researcher, I regularly held a lecture series
for students
on "neural" and "non-neural" computation, their similarities and
differences. One important point about "traditional" software
that
distinguishes it from physical systems -- and that has been a
major part of
my introduction in the lectures -- has been alluded to in this
thread most
clearly by Stephen Bull ([RISKS 23.74](#)) in saying that "[s]oftware
is not
constrained by the laws of nature." Of course, that's not really
true;
probably the best analogy would be to say that software is

always a
(strongly) chaotic system. To a physicist like me, this means
that a small
difference in initial condition -- just a single bit, perhaps --
can introduce
an arbitrary difference in future state in a finite time.

A physical system, for instance, is almost always dampened or
low-pass
filtered, to use another way of viewing it, which restricts a
change in
local state to a small rate of change; but in a computer system,
it is
equally likely for the most- as for the least-significant bit to
change when
something breaks (be it due to physical change such as radiation
or a
software malfunction). A bug such as a buffer overflow or array
bounds
violation can produce a knock-on effect that is unpredictable in
its
time-space distance. This means, to get back to Robinson's
original post (or
should I say diatribe 8-)?), that the component nature of a
software
component cannot (easily) be guaranteed, part of that nature
being that
components should only be loosely coupled among each other in a
well-defined
way. As a counter-example, you don't expect a scratch on the
cabinet in one
corner of your kitchen to lead to a short-circuit of the stove
in the
opposite corner, killing the user in the process, while the same
kitchen
implemented in software might quite conceivably have a bug that
does that to
its virtual (one does hope) user.

Of course, there are physical systems that are chaotic, or where
the
component nature and loose coupling among components are not
true --

well-known examples might be the Tacoma Narrows bridge or the Columbia accident. Such systems still manage to surprise everybody, including the experts in the field. On the other hand, sometimes a software system -- perhaps modelling a physical system -- can exhibit non-chaotic behaviour in the face of errors; I particularly like the example given by Richard Feynman in the first part of his autobiography.

One can clearly derive some recommendations for software development and use from these deliberations, a lot of which have been well-known for a long time. One of the not-so-obvious ones might be taken from looking at "neural" computation, to get back to the introduction: and that is to try to design algorithms that are tolerant of errors, both in their data as in the details of their implementation. That, of course, isn't easy, and I think it likely that it isn't applicable in all too many cases; but if you have a choice, select the algorithm that is perhaps slower or otherwise "worse", but that is more tolerant of errors.

✶ Re: Component Architecture (D.Smith, [RISKS-23.75](#))

<"Olivier Dagenais" <olivierS_dagenaisP@canadaA.comM>>

Thu, 24 Feb 2005 20:01:54 -0500

> strcmp is one of the most simple, basic, fully-documented, and
> frequently-used "components" there is. strcmp isn't an
interchangeable

> part.

Your own story seems to tell us otherwise: because strcmp was "simple, basic and fully-documented", you were able to write a compatible replacement that traded off efficiency for reliability. (as your own unit tests have shown)

Your story was a little vague on the details of switching all uses of strcmp to "smithcmp", but I presume the "fully-documented" part meant you were able to write an interface-compatible method that meant a simple string replace could be used on your source code to switch to the new implementation.

It would thus appear that if one can get "full documentation" on "simple and basic" software components and write [unit] tests proving equivalent behaviour, interchangeability is indeed possible.

✶ **Re: Component Architecture: strcmp (D.Smith, [RISKS-23.75](#))**

<"Paul D.Smith" <paul_d_smith@hotmail.com>>

Fri, 25 Feb 2005 09:04:07 -0000

Daniel Smith gave a great example of the problems of reusable software.

Clearly the bug in strcmp should have been fixed in the library. A single fix, well tested, would have filtered out to all the other products based on this reusable code.

Better still, the odds on this nasty bug being identified were greatly

increased because the code was used by many applications, in many different ways. Single usage code has a nasty history of bugs that are spotted so rarely that the cause and fix may never be identified.

But this falls down if nobody is making money maintaining strcmp. Good-will goes only so far. Thorough design, testing and maintenance costs and someone has to pay. But development teams often fail to correctly compare hidden "do-it-yourself" costs against direct "buy-it-in" costs. So if you want quality, reusable software with timely fixes, get ready to pay. It doesn't have to be "through the nose", but it does need to be a reasonable amount.

✦ Re: Component Architecture (Kuenning, [RISKS-23.74](#))

<Steven Hauser <hause011@tc.umn.edu>>

Mon, 28 Feb 2005 11:23:00 -0600 (CST)

Software patents make component reuse dead.

Reuse a bunch of stuff and pay many fees, royalties, patent searches, lawyers and contract negotiations. So who will try reusing components with very real legal, financial, etc. risks when the risk of consequence for a bug (even resulting in deaths or huge financial losses,) is small?

Steven Hauser <http://www.tc.umn.edu/~hause011/>

[That of course is precisely one of the main arguments for open-source/free software. PGN]

✉ **Re: Component Architecture (Ladkin, [RISKS-23.75](#))**

<dmaziuk@bmr.b.wisc.edu (Dimitri Maziuk)>

Thu, 24 Feb 2005 19:52:42 -0600

In comp.risks, "Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de> wrote:

> I was surprised to find little of the extensive commentary on
> Robinson's
> essay directed at his premise. (Stephen Bull and George Jansen
addressed the
> premise en passant.)
>
> The premise is obviously false, as ... most software
development ...
> is directed towards modifying already existing software ...

Yes, but that's not entirely the same thing as OO dream of everybody assembling applications from ready-made components while everybody else is getting rich selling libraries of said components.

Yes, larger businesses use custom software built from SAP or Oracle components. At the same time, smaller businesses use lowest common denominator off-the-shelf software that doesn't quite do what they want, but it's "close enough" and is something they can actually afford (speaking from experience).

Of course we reuse code. We reuse entire applications all the

time -- nobody
writes their own webserver when they can simply install Apache.
When it
comes to re-using components I prefer to re-use source code.
Because
cheap-not-quite-right off-the-shelf component is as useless to
me as an
overpriced custom component written to my specs which I know are
going to
change as soon as the users see the final product.

We reuse code a lot. But that's not the same thing as building
new systems
out of preexisting OO components. That dream's been exciting a
few decades
ago but by now it's like that crazy uncle living in the attic:
nobody talks
about it anymore. Anybody can list at least half a dozen reasons
off the top
of their head why it doesn't work. As the comments clearly show.

So I was rather surprised to see Robinson's essay published: not
only the
idea is out of date, the analogies are all flawed. I'm sure
anyone who's
ever renovated more than one kitchen or fixed more than one car
knows
exactly what's wrong with those analogies. (As the comments
clearly show.)
Not to mention that reasons why Sears would rather replace an \$5
item no
questions asked and have the customer come back for more don't
have that
much to do with warranty on the item.

✶ Re: Component Architecture

<"Bill Royds" <bill@royds.net>>

Thu, 24 Feb 2005 22:26:26 -0500

In one interesting way, the problem with present software is not lack of components but use of them without adaptation. In modern software exactly the same program is sold to every user. In the Microsoft world, the install procedure hardly ever ask the users for intended uses of the software, level of knowledge of the subject etc. when installing. One size fits all is the norm for software and the standard executable is given to millions of users, completely ignoring any variances in knowledge, ability, interest or configuration. This is one reason why bugs in this software are so devastating. A problem in a component, such as the RPC bug that lead to Blaster, causes a problem with all systems built with that software. It is not the lack of component based development that is the problem, but the complete dependence on components that are used in places where they have not been fully tested.

✶ Re: Component Architecture

<Tom Swiss <tms@infamous.net>>

Fri, 25 Feb 2005 11:58:29 -0500

If RISKS can bear one more comment on Paul Robinson's component architecture essay...

In my experience, one reason why the decision to build new software rather

than use third-party components is one of control. Robinson mentions that "nobody in their right mind would expect [a trucking company] to build their own trucks"; but if the alternative was to buy trucks with the hoods welded shut, and rely on a locked-in (and historically unresponsive) vendor for repair and maintenance of your business's critical infrastructure, that might just be an attractive option.

Fortunately, Free Software ("free as in freedom, not as in price") provides us with the ability to obtain components that we can fix (or hire experts to fix) if they break. Jay R. Ashworth's response notes CPAN and PEAR as examples of reusable components; I think we need to emphasize that these are not just reusable but are software libre.

✶ **Re: Component Architecture (Bell, [RISKS-23.75](#))**

<Ross Lonstein <r lonstein@pobox.com>>

Fri, 25 Feb 2005 10:31:41 -0500

Whitworth is equally good as an example of a failed attempt at standardization. By the 1900s it was just one British "standard" with the British Standard Fine (BSF), the British Association (BA) thread (metric measured in imperial units) and the Cycle Engineers Institute (CEI) threading in use.

It is ironic that WWII forced the British Army to largely abandon Whitworth's standard and adopt the American standard (actually

two: National

Coarse and National Fine) which has threads that are easier to make (60

degree thread pitch, single cut process with flat roots and crests vs. 55

degree thread pitch, multiple cut process, varying threads per inch by

diameter, rounded roots and crests) and more reliable.

Metric, by the way, uses a 60 degree pitch and designates fasteners by their

nominal diameter and thread pitch, both measured in millimeters.

Software doesn't seem to be doing any worse with regard to standardization

than did mechanical engineering.

✉ Re: Component Architecture (Ellims, [RISKS-23.75](#))

<"Dave Budd" <dave.budd@manchester.ac.uk>>

Mon, 28 Feb 2005 09:56:16 -0000

> "Mechanical engineering has it's standard components, nuts, bolts, screws, nails etc. Just as we have some as well, languages, editors, protocols etc."

www.screwfix.co.uk lists 33 separate major categories of screws, many

divided into sub-categories, and then there are the individual sizes...

It's similar for other components, and this is after over a century of

mechanised production. I know I never seem to have quite the right item

ready in stock for whichever DIY job I'm wanting to do.

So, the kitchen-fitting analogy holds quite well - the whole thing's a mess.

✦ **Re: Component Architecture (Mathur, [RISKS-23.75](#))**

<Geoff Kuenning <geoff@cs.hmc.edu>>
25 Feb 2005 16:36:23 +0100

Raj Mathur spotted a bug in my simple pipe. I was hoping somebody would notice that bug! I spotted it only when the digest came out and I (vanity of vanities) reread my posting. Actually, I'd suggest and even better and simpler fix:

```
ls -l | grep '^-' | awk '{total+=$5}END{print total}'
```

which protects against new future file types.

But I think that my original error nicely (if unintentionally) makes the point that plugging components together isn't a cure-all. --
Geoff Kuenning
geoff@cs.hmc.edu <http://www.cs.hmc.edu/~geoff/>

[The identical fix was also noted by Dave Horsfall. PGN]

✦ **Re: Component Architecture (Kuenning, [RISKS-23.74](#))**

<Dan Jacobson <jidanni@jidanni.org>>
Tue, 01 Mar 2005 03:10:49 +0800

```
ls -l | awk '!/^[\bcdps]/{total+=$5}END{print total}'
```

and with perl, one doesn't even need the ls...



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 77

Wednesday 2 March 2005

Contents

- [Wanna be president of Microsoft?](#)
[Geoff Kuenning](#)
 - [Viruses being delivered into mailing lists via BCC:](#)
[Nick Rothwell](#)
 - [Remote physical device fingerprinting](#)
[Tadayoshi Kohno](#)
 - [Re: BofA loses backup tapes in transit ...](#)
[Terry Harris](#) [Keith F. Lynch](#) [Chris Kantarjiev](#)
 - [Re: UK gets official virus alert site](#)
[David Alexander](#)
 - [Re: Spam-blocker causes missed court date](#)
[Keith F. Lynch](#) [Craig A. Finseth](#)
 - [Re: Address coercion](#)
[John Harper](#) [Russell C Page](#)
 - [Re: Component Architecture](#)
[Martin Ward](#) [Mike Ellims](#)
 - [Components, yes; kitchen sinks, no](#)
[Walter Dnes](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Wanna be president of Microsoft?

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

26 Feb 2005 19:21:02 +0100

This is too good to be true, but I'm afraid it is.

I own a tiny (just me) California corporation. Every year, I have to file a form listing my address, the names of the top officers, etc. It turns out that the form can be filed online (though you have to enable Java to do so).

If you go to <https://businessfilings.ss.ca.gov> you can type in the name of any corporation registered in California and be presented with the corporate-info form. If you type "Microsoft", you'll get several with MS in the name, including one that's located at One Microsoft Way, Redmond, WA.

Keep clicking and you can fill out the form with "corrected" information. It costs a \$25 filing fee, which can be paid with a credit card. They also collect an e-mail address, though I don't know why. So if you have a stolen credit card and a throwaway e-mail address (e.g., at mailinator.com or just good ol' hotmail), you can change Microsoft's information.

For MS, it would probably get caught fairly quickly. But you could cause a lot of trouble for a smaller company. For example, maybe you could change their information, then sue them. Not knowing about the suit, they'd default. Then you could change the information back and

institute
proceedings to collect the judgment.

Hmmm, I wonder if I could sue Bill for a couple of billion? --
Geoff
Kuenning geoff@cs.hmc.edu <http://www.cs.hmc.edu/~geoff/>

⚡ Viruses being delivered into mailing lists via BCC:

<Nick Rothwell <nick@cassiel.com>>
27 Feb 2005 18:51:29 -0000

I've just been rather shafted by this one...

I have a publicity mailing list, which I maintain as a local
alias in qmail
on my mail box. I send out periodic mailshots, to myself as main
recipient,
but BCC:'d to the mailing list, for brevity and privacy.

Well, apparently not. Either the EMACS mail system, or the qmail
delivery
system (probably the latter) drops the supposedly private BCC:
address into
a Delivered-To: header, visible to all recipients.

And in a bad-goes-to-worse scenario, this alias address has
found its way
into an e-mail list currently being used by a virus on a
compromised
broadband machine on Bellsouth, so it's managed to send its
payload to my
entire mailing list. (And, of course, the virus does indeed come
through,
and depart from, my mail machine.)

I've now nuked all my supposedly private mailing list names, and
will use

completely transient ones in future, but this is something of a wake-up call to my assumptions about secret mail headers.

nick rothwell -- composition, systems, performance -- <http://www.cassiel.com>

Remote physical device fingerprinting

<Tadayoshi Kohno <tkohno@cs.ucsd.edu>>
Tue, 01 Mar 2005 14:13:51 -0800

Together with Andre Broido and kc claffy from CAIDA, I have been working on methods for remote physical device fingerprinting, or remotely fingerprinting a physical device without any modification to or known cooperation from the fingerprintee. At a high level, our fingerprinting techniques exploit microscopic deviations in device hardware: clock skews. At a low level, our preferred technique exploits the fact that most modern TCP stacks implement the TCP Timestamps Option (RFC 1323). When this option is enabled, outgoing TCPs packets leak information about the sender's clock. This work further supports the following well-known observation: there can be security relevant information in what one might traditionally consider to be noise.

Our paper and abstract available here:

<http://www.cse.ucsd.edu/users/tkohno/papers/PDF/>>

<http://www.caida.org/outreach/papers/2005/fingerprinting/>>

✶ Re: BofA loses backup tapes in transit ... (Plum, [RISKS-23.76](#))

<"Harris, Terry" <terry.harris@eds.com>>

Tue, 1 Mar 2005 14:51:02 -0500

From my reading of the story, Mr. Plum seems to have jumped to some conclusions. One, I didn't see any mention that the data was not encrypted. Two, the tapes seem to have been shipped as cargo, not in someone's baggage. There was a specific statement that the tapes were being shipped to a backup data center. Something normal for disaster recovery planning.

Considering that the tapes contained data about government officials and at least one Congressman the theft may have been part of someone's "Opposition Research".

[But if it was encrypted, why the BofA statement that no misuse of the data is known to have occurred (yet)? Why not say that the data was encrypted, and therefore this was no big deal? PGN]

✶ Re: BofA loses backup tapes in transit ... (Plum, [RISKS-23.76](#))

<"Keith F. Lynch" <kfl@KeithLynch.net>>

Mon, 28 Feb 2005 22:50:47 -0500 (EST)

Why not always have TSA inspect the bags in the presence of the owner, who is then allowed to lock them?

> Failure to encrypt these backups before they went offsite seems
> negligent of BofA to me.

Perhaps. But this is a minor transgression compared to the
ChoicePoint
issue. ChoicePoint deliberately sold personal information that
didn't
belong to them, without the permission of its owners. The fact
that the
buyers weren't who ChoicePoint thought they were is a side issue.

If I somehow learned private information about you, and sold it
without your
permission, you ought to be more upset at me than if you had
given me
private information, a copy of which was then stolen from me.

✶

<Chris Kantarjiev <cak+news@dimebank.com>>

Mon, 28 Feb 2005 17:31:26 -0800

> The "TSA [master] key" lock idea will just mean the thieving
baggage
> handler will acquire one of the master keys beforehand.

Or not even bother. I have already had two TSA master key locks
removed
destructively.

I view the TSA master key idea as nothing more than a scam to
sell new
locks. It has nothing whatsoever to do with security or fighting
terrorism.

Re: UK gets official virus alert site (Skedgell, [RISKS-23.76](#))

<David Alexander <dave_ale@online.rednet.co.uk>>

Tue, 01 Mar 2005 15:01:24 +0000

I would like to comment on the remarks made so far concerning the UK ITsafe web site. It so happens that I know the guy responsible for planning and implementing the site on behalf of HM Government and we had a long conversation about it the week before it went live at the DIPCOG conference in Leeds.

The first and most important thing to note is that this site is aimed at people who have absolutely zero knowledge of technology, risks or security.

At the risk of sounding patronizing, those who are complete IT novices

(e.g. someone who may well have just bought their first ever computer and

plugged it into the phone line) are the ones the site is set up to benefit.

It is, IMHO, important to view the message that the site carries and the way

in which it does so from the viewpoint of those people, not the informed

position we have as Infosec/IT/risk management/whatever professionals. Those

with knowledge look at bugtraq, CERT, WARPs, a/v provider alerts, etc, the

general public does not - and most probably wouldn't understand the output

and what to do with it if they had it.

The designer had to balance a whole set of risks - if it's too secure or

complex the target audience either won't be able to access it or won't

understand it and will just go away again. If you know how to

use S/MIME or PGP signatures you are too knowledgeable to benefit from the ITsafe site.

The issue of hacking/spoofing has been considered and they have some plans.

My friend was, quite rightly, somewhat reticent to reveal them...

>> 1. This would be a great site for the Malware Brigade to spoof. I hope

>> that it is more secure than most Web Sites.

>

>Sadly, no:

>

>Signing up for e-mail or SMS alerts does not appear to require any

>address confirmation, so presumably anyone can sign up anyone else's

>e-mail address or mobile phone for alerts. Also, no secure (SSL/TLS)

>form is provided for submission.

>

>I am also dubious about the 'ITsafe Word' scheme to protect from spoofing by

>the 'Malware Brigade' -- <http://www.itsafe.gov.uk/glossary/itsafeword.html>

>definition: A security feature used on the ITsafe website to help reduce the

>risk of someone spoofing our e-mails.

>

> When you sign up to our e-mail service you are asked to type in an ITsafe

> Word (please keep this clean). This is not a password, so if you forget

> it, it is not the end of the world. You just need to be able to recognise

> it again in the future.

>

> All e-mails we send to you will use this word in the 'subject' line. In

> e-mail programs this is normally displayed just above the e-mail

> content. You can quickly check that the e-mail has come from

us as someone

> else would not know your ITsafe Word.

>

> Until you forward the e-mail, forgetting to remove it (not that it mentions

> that people *should* do this on forwarding etc). Or post it to USENET, or...

>

> I wonder if they have heard of S/MIME or PGP signatures?

>

> The problem here is that quite a lot of people will probably receive this as

> a forward, all malware would need to do is search mail folders for a

> legitimate bulletin (identified from mail headers) with the ITsafe Word in

> the subject line and use this to construct a forgery to attach itself to...

>

> ITsafe site URL <http://www.itsafe.gov.uk/index.html>

David Alexander, Towcester, Northamptonshire, England

http://home.rednet.co.uk/homepages/dave_ale/dave_ale.html

✉ Re: Spam-blocker causes missed court date (Brennan, [RISKS-23.76](#))

<"Keith F. Lynch" <kfl@KeithLynch.net>>

Mon, 28 Feb 2005 23:07:58 -0500 (EST)

> ... I would be very surprised to be held responsible for failing to read a

> message that was properly refused.

Really? I had thought that bounce messages were pretty much obsolete. I am

forced to killfile all bounce messages directed at me, since the vast

majority of them report bounces of spams forged to be from me.

Not only has it long been the cast that the vast majority of e-mail directed at me is spam (or viruses, worms, bogus bounces, and other junk), but it's also long been the case that the vast majority of e-mail that appears to be *from* me is spam. I believe that same is true of most people with non-secret e-mail addresses. Spammers harvest addresses for *two* reasons -- to get addresses to spam, and to get addresses to forge.

Over a year ago I gave up on filtering, and started whitelisting. Everyone with whom I've exchanged e-mail or newsgroup postings is on my whitelist, as are all the regular RISKS posters, and about eleven thousand other people. I also have a disposable e-mail address on my web page which anyone can send to. And I've borrowed PGN's trick of accepting anything with "notsp" (or any of a few hundred other key words and phrases) on the subject line. This has reduced the volume of spam to a tolerable level, but it *still* exceeds all legitimate e-mail.

The real RISK here is assuming that e-mail is reliable. I never assume anyone has received my e-mail unless they tell me they have. Why are courts relying on it? I thought they didn't even rely on snail mail, other than *registered* snail mail.

Also, the lawyer in question should have whitelisted the court, and anyone else he had business dealings with. There's plenty of blame to go around.

What next? Being served papers, not by a process server, but by e-mail? "If you do not reply to this e-mail, we will assume you have no objection to the court awarding the plaintiff everything you own and everything you will ever earn". Sigh.

✦ Re: Spam-blocker causes missed court date (Brennan, [RISKS-23.76](#))

<"Craig A. Finseth" <news@finseth.com>>
01 Mar 2005 14:54:14 GMT

>One would conclude from this that the law firm had unmonitored software that
>was throwing away mail willy-nilly. Or perhaps that the law firm's system
>administrator configured it to do so. Both are serious charges that are
>likely to cause fear and doubt among users of e-mail systems. It is unlikely
>that either is true.

On the contrary, both possibilities are quite likely.

>I submit to the court that the most likely facts are that the filter sorted
>the court notice into a possibly-spam folder and that the lawyer failed to
>look at the folder regularly.

This is certainly a possibility. However, anti-spam software has improved to the point where there are very few false positives and so many users don't even bother to review their "possible spam" folders.

>The next most likely case is the one I find the most
disturbing: that the
>law firm's system refused the message (smtp 550) or accepted it
and mailed a
>bounce notice back. But if this happened, why would the court
issue the
>show-cause order?

In my experience (operating an anti-spam system with over 50,000
users), the
most likely causes are mis-configured sending mail systems and
accidental
problems.

Many sending mail systems do not follow modern standards
regarding things
like being properly configured in the DNS, having the "From"
address match
the sending system, or even following the RFCs that specify how
to format
messages. If I were investigating the problem, I would look
closely at how
the court system's mail server was configured.

Accidental problems include things like having a document
include innocent
words or abbreviations that trigger spam scores. For example,
reports
including "cumulative grade point averages" which abbreviate
words to, say,
their first three letters. If I were investigating the problem,
I would
also look for problems of that sort.

[...] I suggest that you may need to revise your expectations
about e-mail.
Roughly 2/3 of all incoming messages to our system are spam or
viruses and
neither should receive bounce messages. In fact, if we were to
send bounce
messages about viruses, we would be soundly trounced for the
practice.

And, as you should be well aware, sending bounce messages to spammers simply causes them to send you more spam.

Finally, even if I were to send a bounce message, the court's system would probably classify it as spam and the judge would never see the bounce.

The only reasonable assumption these days is that the message did not make it unless you have received confirmation that it did.

>By the laws of wishful thinking I assume that the court does not ignore its >bounces, and that the law firm's system does not throw away mail without >notice. Therefore the court was in error. Unfortunately the filter >software is not a person under law and cannot file for damages!

Both laws are indeed wishful thinking. The court's e-mail system probably classifies bounces as spam and discards them. The law firm's system throws away lots of mail without notice.

The error is the court's in assuming that sending an e-mail message and not receiving a failure notice means that the message has been delivered. That assumption is not a reasonable or valid one in today's world. Unfortunately.

Craig A. Finseth, Firwood Consulting, Inc., 1343 Lafond, St Paul MN 55104

<http://www.firwood.net> +1 651 644 4027

✉ Re: Address coercion (P.D.Smith, [RISKS-23.76](#))

<John Harper <John.Harper@mcs.vuw.ac.nz>>

Wed, 2 Mar 2005 09:56:09 +1300 (NZDT)

Paul Smith reported a US bank refusing to believe an address in Enfield, UK. I used to have a US bank account; its web page was useless because it insisted that one give a 5-digit zip code. New Zealand and Australia have 4-digit ones, Canada and UK have 6 or more characters in a mixture of letters and digits, ...

John Harper, School of Mathematics, Statistics and Computer Science,
Victoria University, PO Box 600, Wellington 6001, New Zealand
(+64)(4)463 5341

✦ Re: Address coercion (P.D.Smith, [RISKS-23.76](#))

<Russell_C_Page@national.com.au>

Tue, 1 Mar 2005 16:20:15 +1100

A few years back I tried to buy something from a website in the USA from New Zealand. New Zealand has a population of 4 million, and is about the same size as the UK. There are no Post Codes, zip codes, provinces, or states. Presumably the situation is similar in other small countries.

The website refused to recognize an address without a zip code and state, although it did allow me to live in another country. I sent an e-mail to the webmaster and the problem was fixed the next day.

Our nations with their boundaries, laws, and armies are legacies of the kingdoms of medieval Europe. Credit cards, global corporations, and the Internet are making them more and more irrelevant. If you want to do business on the Internet, you have to be able to cater for all your customers.

Security Services National Australia Bank Limited +61 3 9886 2401

⚡ Re: Component Architecture (Taylor, [RISKS-23.76](#))

<Martin Ward <Martin.Ward@durham.ac.uk>>

Tue, 1 Mar 2005 10:42:25 +0000

[This thread is now running thin, so this issue may end it for now.

But it is a very important topic, and for that reason I let it run

a little longer than usual. PGN]

Steve Taylor <steve.taylor@PETARDSCS.CO.UK> notes the fundamental fallacy in comparing the "design" of software with the "manufacture" of physical items. Software "manufacture" is practically cost free, while in physical engineering cost is dominated by manufacturing.

So the real comparison is between *design* of software and the *design* of complex physical artifacts: such as a suspension bridge, a CPU or a kitchen. When I design a kitchen I draw out the room to scale on a piece of

paper, make cardboard cutouts of the various items, and then try out various arrangements. I abstract away almost everything about a cooker, say, apart from its (scale) size and power requirements. By using a language at the appropriate level of abstraction (cardboard cutouts and paper), the design process is simple and effective.

The CPU designer doesn't personally lay out the location of every gate and wire: he uses the appropriate high level abstractions and the CAD software fills in all the details: ensuring that all the constraints on wire separation and length are preserved automatically.

The suspension bridge designer uses the appropriate mathematics to **prove** that her bridge will stay up and carry the required load before construction is started. Jan Vorbrüggen points out that physical systems are dampened, or can be designed to be dampened, so that a small change in initial state results in a small change in output: while computer systems are strongly chaotic. On the other hand, the mathematics required to design physical systems (differential equations, nonlinear fluid dynamics etc. etc.) is fairly heavy going, while the mathematics required to **prove** the correctness of a computer program (basic set theory and logic) is comparatively straightforward. Proofs of correctness of programs are possible when the programs are small enough and written at an appropriate level of abstraction.

The biggest advances in programmer productivity (discounting advances in hardware due to Moore's Law) came with the switch from machine

code to assembler language and again with the switch from assembler to high level languages. The next order of magnitude advance will **not** come from using component libraries in existing OO languages, such as C++ or Java. Instead, what is required are languages at a higher level of abstraction, and this necessarily implies domain-specific languages, which have been designed and implemented with the appropriate formal methods, with the primary aim of enabling correctness proofs to be carried out. Why do we still have buffer overflows and dangling pointers when languages exist in which it is impossible to implement a buffer overflow or a dangling pointer?

Unfortunately, there has been very little work over the last 20 years on the design and implementation of very high level domain specific language based on formal methods and correctness proofs.

I believe that the way to gain higher productivity and reliability in large software development projects is to turn the large development project into two much smaller development projects:

- (1) Design and implementation of a domain specific language in which it is easy to develop the required system; and
- (2) Develop the system in the language designed in step (1).

If the language is released as free software, then the work involved in project (1) can be shared among all the designers working in a particular domain: and the cost savings are even greater!

The design and development of the FermaT program transformation

system

follows this approach. FermaT is implemented in MetaWSL, a language for writing program transformations. 54,000 lines of MetaWSL compiles into nearly 200,000 lines of C: but the MetaWSL is easy to understand (for one familiar with the domain), while the C is impenetrable!

These ideas are explored in more detail in my paper "Language Oriented Programming", Software---Concepts and Tools Vol 15, pp 147-162, 1994
<http://www.dur.ac.uk/martin.ward/martin/papers/middle-out-t.ps.gz>

Martin.Ward@durham.ac.uk <http://www.cse.dmu.ac.uk/~mward/> Erdos number: 4

Re: Component Architecture

<Mike Ellims <mike.ellims@pитеchnology.com>>

Tue, 1 Mar 2005 15:25:22 -0000

The reliability of components has always been somewhat suspect, for example the Basilica project [1] tested various POSIX compliant O/S and found that large numbers of the system calls and library routines contained bugs that would cause core dumps. The faults being mostly connected null pointers being passed as parameters etc.

Things don't seem to be that much better in the open source world either, Torkar et al. [2] performed unit testing on a number of open source classes and found that they could trigger errors with minimal effort.

The situation doesn't seem to be any better with other sources, Kuhn [3] surveyed results for the number of variables required to trigger a failure and found that for medical devices approx. 70% of failures involved only one variable, NASA's Deep Space One craft did little better but the Mozilla and Apache open source projects came in at 30-40%. Of course that could be because of inadequate error reporting.

This is of course slightly annoying given that Duran and Ntafos [4] observed nearly 20 years ago that the bugs they were finding could have been found with *any* sort of reasonable test process.

Of course the problems is worse that this because the majority of the studies cited above examined functions more or less in isolation and as Peter Ladkin is fond of pointing out safety is not composable, and I suspect neither is the use of components in a software systems. That is, just because the components all work perfectly on there own I'm not sure that it is realistic to assume that this will produce a reliable system though I suspect that it may help.

However it does seem to be possible to build reliable software, as noted by Ladkin ([RISKS-23.37](#) after [5]) automotive software seems to be highly reliable a similar conclusions are reached by Littlewood [6] and McDermid [7] at lower levels using the same data. However it should be noted that the data is from the 1998-2001 period and the analysis has not yet been repeated

for newer vehicles.

- [1] Koopman, DeVale : Comparing the Robustness of POSIX Operating Systems, FTCS 1999
- [2] Torkar et al. : An exploratory study of component reliability using unit testing. Proc. ISSRE'03.
- [3] Kuhn et al. : Software fault interactions and implications for software testing, IEEE TSE Vol. 30 No. 6, June 2004
- [4] Duran, Ntafos : An evaluation of random testing IEEE TSE Vol. 10 No. 4 July 1986
- [5] Ellims : On Wheels, Nuts and Software, 9th Australian Workshop on Safety Related Programmable Systems SCS'04
- [6] Littlewood, Assessing the dependability of software based systems: the important role of confidence, KKIO2004, Gdansk, Poland.
- [7] McDermid, Kelly : Software in Safety Critical Systems: Achievement and Prediction, Proc. Institution of Nuclear Engineers Conference, 2004 (to appear)

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

✶ Components, yes; kitchen sinks, no

<"Walter Dnes" <waltdnes@waltdnes.org>>
Tue, 1 Mar 2005 18:21:04 -0500

The theory of component re-use is great. The implementation often stinks to the point where roll-your-own is the superior alternative. My pet peeve is

the combination of...

a) you can't get individual components, you can only get a huge library with zillions of components, even though you need just one or two of the routines in the library

b) There isn't just one humungous library. Every developer and his dog is bringing out their own "superior" library.

perl used to be a "Practical Extraction and Reporting Language". Now it's ballooned into something huge, requiring support libraries of its own.

Don't get me wrong, perl is an OK operating system, but it lacks a lightweight scripting language.

On linux, some programs require perl. Other programs require python. Other programs require PHP. Some require Gtk 1.x series, while others require Gtk 2.x. Etc, etc. So in order to get a full system, you end up loading a ton of libraries, each of which is huge in its own right. I started using linux 5 years ago on a beat-up old Pentium Pro with 16 megs of RAM, which had originally come with Windows95. Today's full versions of Windows and linux aren't really comfortable in less than 512 megs, although linux allows one to drop the GNOME/KDE "Desktop" eye-candy and run with a lightweight window manager. How long will it be before we start reminiscing fondly of the days when "640 megs of RAM was enough for anybody"?

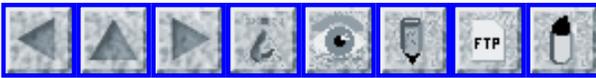
A risk of "component monoculture" is that if a widely used component has a flaw, everybody's vulnerable, especially if the component handles e-mail for

websites. This isn't just a Windows problem. A few years ago it was Matt Wright's (in)famous formmail perl script that was a spammer's delight. More recently, PHP-Nuke has been abused by spammers to flood my inbox.

Walter Dnes <waltdnes@waltdnes.org>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 78

Thursday 10 March 2005

Contents

- [Security? Nuclear plants don't need no stinkin' security!](#)
[Jim Horning](#)
- [Drug-error risk at hospitals tied to computers](#)
[Scott Allen via Monty Solomon](#)
- [Hospital computers make things worse](#)
[Richard Akerman](#)
- [Richard Clarke: Real ID's, Real Dangers](#)
[John F. McMullen](#)
- [MIT says it won't admit hackers](#)
[Robert Weisman via Monty Solomon](#)
- [Website hijackings, 302 redirects, and security issues](#)
[Tim Chmielewski](#)
- [Credit Information Stolen From DSW Stores](#)
[AP via Monty Solomon](#)
- [Garbage Out, Garbage In?](#)
[Adam Shostack](#)
- [More BofA problems](#)
[Tom Watson](#)

- [Re: More uses of satnav/GPS](#)
[Michael Bacon](#)
 - [REVIEW: "Windows Forensics and Incident Recovery", Harlan Carvey](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Security? Nuclear plants don't need no stinkin' security!

<"Jim Horning" <home@horning.net>>
Fri, 4 Mar 2005 17:36:41 -0800

A SecurityFocus post

<<http://www.securityfocus.com/news/10618?ref=rss>>

discusses the nuclear industry's reaction to a proposed voluntary standard
<<http://horning.blogspot.com/2005/01/us-to-tighten-nuclear-cyber-security.html>>
for security of digital systems controlling nuclear power plants.

"Two companies that make digital systems for nuclear power plants have come out against a government proposal that would attach cyber security standards to plant safety systems. The 15-page proposal, introduced last December by the U.S. Nuclear Regulatory Commission (NRC), would rewrite the commission's 'Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.' The current version, written in 1996, is three pages long and makes no mention of security. The plan expands existing reliability requirements for digital safety systems, and infuses security standards into every stage of a system's lifecycle, from drawing board to retirement. Last month the NRC extended a public comment period on the proposal until March 14th to give plant operators and vendors more time to respond. So far, industry reaction has been less than glowing."

"The NRC tries to promote the use of digital technology in the nuclear power industry on the one hand, but then over-prescribes what is needed when a digital safety system is proposed," wrote one company president.

"The entire cyber security section should be deleted and only a passing reference to the subject retained," another company wrote.

More information at <http://www.securityfocus.com/news/10618?ref=rss>
and
<http://horning.blogspot.com/2005/03/security-nuclear-plants-dont-need-no.html>

⚡ Drug-error risk at hospitals tied to computers (Scott Allen)

<Monty Solomon <monty@roscom.com>>
Thu, 10 Mar 2005 07:28:47 -0500

Hospital computer systems widely touted as the best way to eliminate dangerous medication mix-ups can actually introduce many errors, according to the most comprehensive study of hazards of the new technology. The researchers, who shadowed doctors and nurses in the University of Pennsylvania hospital for four months, found that some patients were put at risk of getting double doses of their medicine while others get none at all. 22 types of mistakes were identified, such as failing to stop old medications when adding new ones or forgetting that the computer automatically suspended medications after surgery. The findings underscore the complexity of improving safety in US hospitals, where the Institute of Medicine estimates that errors of all kinds kill 44,000 to 98,000 patients a year. [PGN-ed]

Scott Allen, *The Boston Globe*, 9 Mar 2005
http://www.boston.com/yourlife/health/other/articles/2005/03/09/drug_error_risk_at_hospitals_tied_to_computers/

⚡ Hospital computers make things worse

<Richard Akerman <rakerman@chebucto.ns.ca>>
Thu, 10 Mar 2005 08:36:05 -0400 (AST)

Reports over the past few years of increasing numbers of patient injuries and deaths due to medical errors sent hospital administrators scrambling for computerized solutions. But two new studies suggest that, in many cases, these high-tech systems have left doctors and nurses increasingly frustrated while providing little evidence of real benefit to patients. In fact, one widely used system actually helped foster medication errors, researchers found. See the 9 Mar 2005 issue of the Journal of the American Medical Association.

Sympatico News, Hospital Computers Fail to Deliver: study finds they facilitated errors

<http://healthandfitness.sympatico.msn.ca/News/ContentPosting.aspx?contentid=cd4d283138844d228f2e7a99ff326350&show=True&number=5&showbyline=False&subtitle=&detect=&abc=abc>

Richard Akerman rakerman@chebucto.ns.ca <http://www.akerman.ca/>

Richard Clarke: Real ID's, Real Dangers

<"John F. McMullen" <observer@westnet.com>>

Mon, 7 Mar 2005 17:24:40 -0500 (EST)

Richard A. Clarke, The Security Adviser, Real ID's, Real Dangers,
The New York Times, 6 Mar 2005

<http://www.nytimes.com/2005/03/06/magazine/06ADVISER.html>

Have you ever wondered what good it does when they look at your driver's license at the airport? Let me assure you, as a former bureaucrat partly responsible for the 1996 decision to create a photo-ID requirement, it no longer does any good whatsoever. The ID check is not done by federal officers but by the same kind of minimum-wage rent-a-cops who were doing the inspection of carry-on luggage before 9/11. They do nothing to verify that your license is real. For \$48 you can buy a phony license on the Internet (ask any 18-year-old) and fool most airport ID checkers. Airport personnel could be equipped with scanners to look for the hidden security features incorporated into most states' driver's licenses, but although some bars use

this technology to spot under-age drinkers, airports do not. The photo-ID requirement provides only a false sense of security. [Excellent article abstracted for RISKS. PGN]

✶ MIT says it won't admit hackers (Robert Weisman)

<Monty Solomon <monty@roscom.com>>

Wed, 9 Mar 2005 16:27:41 -0500

Sloan School of Management has joined Carnegie-Mellon and Harvard in rejecting applications from prospective students who hacked into a website to learn whether they had been admitted before they were formally notified. 32 MIT applicants reportedly took a peek, along with 1 at CMU, 119 at Harvard, and 41 at Stanford. The Web site is run by ApplyYourself, and also used by other business schools. Its access was compromised by a posting on a BusinessWeek Online forum. [PGN-ed from Robert Weisman, *The Boston Globe*, 8 and 9 Mar 2005]

http://www.boston.com/business/articles/2005/03/08/harvard_rejects_119_accused_of_hacking_1110274403/

http://www.boston.com/business/articles/2005/03/09/mit_says_it_wont_admit_hackers/

[Dave Farber's IP list had several responses. Rejected applicants considered their treatment excessive. One candidate saw only a blank page at ApplyYourself, but was rejected for having accessed the site. Dave Leshner wrote

What's the B-schools' culpability in contracting out a process to a company with inadequate security? [Presumably] the schools demanded SSN's and other financial data from the applicants. Was there informed consent by the applicants to have their data shared with, in effect, a data broker? Could they apply WITHOUT so agreeing?

Joe Hall wrote

What strikes me is how constructing a URL that is available to students without any further authentication or protection is considered "hacking". That's inevitably diluting any geek cred. held by any of us who are even crappy hackers!

Joe also noted Ed Felten's post on this subject at

<http://www.freedom-to-tinker.com/archives/000780.html>

PGN wonders what if a competing candidate had masqueraded as other candidates to see if others had been accepted, and thereby wound up getting them all rejected! Could that be a suitable defense for the rejected students? PGN]

Website hijackings, 302 redirects, and security issues

<"Tim Chmielewski" <tim@humanedge.biz>>

Thu, 10 Mar 2005 15:36:34 +1100

I have been reading about the problems with the lbu.com site on the forum Webmaster World and decided to try it myself.

Basically what it is that if you type in any site with the format:
<http://www.sitename.com.lbu.com> you will get redirected to another site (actually a proxy server in China) that looks exactly like your site, but none of your pages that use scripting will work.

Using the same technique other sites could hijack banking or online shopping sites and redirect input so they collect your credit card and other information.

While this has been a popular topic of discussion in the webmaster forums, Google itself is silent on the issue.

Tim Chmielewski, Webmaster, Human Edge Software

<http://www.humanedge.biz>

Credit Information Stolen From DSW Stores

<Monty Solomon <monty@roscom.com>>

Tue, 8 Mar 2005 22:13:23 -0500

AP, 8 Mar 2005

Credit card information from customers of more than 100 DSW Shoe Warehouse stores was stolen from a company computer's database over the last three months, a lawyer for the national chain said Tuesday. The company discovered the theft of credit card and personal shopping information on Friday and reported it to federal authorities, said Julie Davis, general counsel for the chain's parent, Retail Ventures Inc. The Secret Service is investigating, she said. DSW was alerted by a credit card company that noticed suspicious activity, she said.

<http://finance.lycos.com/home/news/story.asp?story=47512557>

✶ Garbage Out, Garbage In?

<Adam Shostack <adam@homeport.org>>

Thu, 10 Mar 2005 13:45:50 -0500

An article in the Guardian,

<http://www.guardian.co.uk/online/story/0,3605,1410921,00.html>

discusses a plan to implant chips in garbage bins covers some risks:

"If, for example, computer hackers broke in to the system, they could see sudden reductions in waste in specific households, suggesting the owners were on holiday and the house vacant."

But the tendency to believe anything written on a computer screen continues unabated: "He said the microchips would help the council fend off unwarranted criticism. "We will have a confident response to customers who claim their bin may not have been emptied," he added. "

✶ More BofA problems

<Tom Watson <tsw@johana.com>>

Mon, 28 Feb 2005 20:03:51 -0800

My recent encounters with BofA include attempting to setup an "out of branch" transfer. The thought seems wonderful, and then I try to do it. Navigating the web site (https, thankfully) gets me to a page that asks me to enter a "confirmaiton number" that was sent to my e-mail address. Unfortunately, something doesn't comeplete the sending of this message, and I never get it. Of course no error message appears and I'm left without the ability to transfer. I call the bank (or send internal [secure] messages and the response is "get another e-mail address" or some such. The risks: I'm told some tale that it is really "my problem" (it isn't!), and the bank's web service is sending messages into wierd places. I guess I really can't trust them until they "get it right". On the other hand, my other bank is perfectly able to send e-mail to the address is question. You think they would read their logs and wonder (do they?).

✶ Re: More uses of satnav/GPS

<"Michael \((Streaky\) Bacon" <himself@streaky-bacon.co.uk>>

Wed, 9 Mar 2005 15:25:30 -0000

In [RISKS-23.71](#), David Magda pointed to the suggested use of GPS on trains in the UK. In [RISKS 23.52](#) (Shutting the train door before the commuter has bolted?) I drew attention to existing problems with one such system already operational on some UK trains.

DM highlighted the potential issue of the GPS system being "shut off" by the US government during emergencies and suggests Galileo (or inertial guidance) as a back-up.

The threat of the existing GPS system being 'switched off' has been touted on many occasions, but, given its incorporation into so many systems (public

use as well as military) in the USA and world-wide, it is doubtful that anything more extreme than a 'detuning' of the system would ever be contemplated. This could well be effected via an existing option which would allow the military to continue using GPS at a necessary high degree of accuracy while still providing private users with a service - albeit with lesser accuracy. Whilst the effects of such a lesser accuracy are 'undefined' and could lead to severe consequences - including death - GPS-based systems would continue to operate.

Further, using Galileo as a back-up may be contentious for the reason that the US government has previously expressed grave concerns about its up-coming loss of exclusivity over the provision of such positioning technology and about the nationality of some of the participants in the Galileo scheme. This gives rise to a dilemma. Either the existence of Galileo provides a reason for not 'turning off' (or 'detuning') the existing GPS system; or Galileo itself must be similarly 'turned off' (or 'detuned') in parallel. If we assume the latter, this would have to be effected by one of three means: US governmental pressure on the Galileo operators, external (and unauthorised?) override of the satellites' software, or physical interference with the satellites (up to and including destruction). Any ground-based 'satellites' would (probably) have to be similarly affected.

Thus, if we assume that GPS might be 'turned off' (or 'detuned'), we must assume the same of Galileo. This would leave inertial guidance as the only viable back up system - were such accuracy actually required.

But, let us examine what benefits are sought from using a precise positioning technology. The articles quoted skillfully (and typically) interweave the 'safety' issue - trading on terms such as "A number of devastating crashes over the last 10 years have pushed rail safety to the top of the national agenda." - with that of operational convenience. Trains are currently located somewhere in (say) one kilometre 'blocks' protected to the rear by a red signal. On the UK's railways there have been a number of recent incidents of SDAP - Signal Passed At Danger - some of which have led to fatalities. However, other recent fatalities have had causes that would not be well-militated against through exact positioning technology (e.g. derailment caused by a broken rail and collision with a car at a crossing). The lumping of accidents together - regardless of cause - to justify spending on a system which might address only one of them is all too common.

Whilst it is possible that a GPS-type system could enable signallers to more accurately locate trains and know their speed too and it is possible that this could enhance safety, I fear that the prime driver for the installation of positioning technology is actually intended to enable an increase in train density on the existing rail infrastructure. Such a move would likely increase risk rather than reduce it. The rationale for my fear is that the pressures to increase density exist, are increasing and will continue to increase. Building additional track capacity is not a viable option and lengthening trains themselves is highly problematic - because of restrictions on platform length at termini and intermediate stations. The only option is to increase track usage (more trains per mile of track) - and this cannot be done with the existing signalling systems and block working.

But, is the technology up to it? Railways in the UK provide special challenges for the designers of equipment. The recent history of equipment on new trains such as remotely released doors, automatic announcements, new-style pantograph and third-rail pickups, tilting carriages, etc. has been fraught. Seemingly, designers had no real concept of the challenges provided by the environment. Reliability in an environment that is subject to continual and continually variable vibration and oscillation; intermittent but frequent harsh shocks of variable intensity; rough handling; infrequent, sometimes poor and occasionally non-existent maintenance, and the necessary 'building down to a price' demanded by a cash-strapped industry is demonstrably hard to achieve.

Therefore a primary question must be: "What happens when an on-board positioning system fails (either the computer or the transmitter)?" The train might simply vanish off the display and possibly out of the system. Signallers and drivers of following trains would not know whether there was a train ahead (or behind), nor exactly where that train was. So, if train separations were reduced through the introduction of such a system, catastrophe could easily and quickly result. Even if the system 'fails-safe', problems would still result from any reduction in train separation.

Then there is the human factor. Common issues here include the operator's implicit trust in the automated system, their inability to recognise, assimilate and react to emergency situations, poor MMI and clashes between the system's and the users actions (vis. the Australian Naval ship referred to in [RISKS 23.71](#)).

We have existing examples in air traffic control and aircraft flight systems. These are formed of far-longer established protocols; but we still have (brand new) systems that fail, either inherently or at the man-machine interface, and clashes between pilots and 'George'. When it comes to implementing remote or automated control in mass-transport systems, the record is not good.

When we couple commercial greed - especially when argued in the grounds of 'safety' - with the continuing failure of designers to construct reliable and reliably fail-safe systems the RISKS are manifest and manifold.

🔥 REVIEW: "Windows Forensics and Incident Recovery", Harlan Carvey

<Rob Slade <rslade@sprint.ca>>
Mon, 7 Mar 2005 08:28:59 -0800

BKWNFOIR.RVW 20041224

"Windows Forensics and Incident Recovery", Harlan Carvey, 2005,
0-321-20098-5, U\$49.99/C\$71.99
%A Harlan Carvey
%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario M3C 2T8
%D 2005
%G 0-321-20098-5
%I Addison-Wesley Publishing Co.
%O U\$49.99/C\$71.99 416-447-5101 fax: 416-443-0948 bkexpress@aw.com
%O <http://www.amazon.com/exec/obidos/ASIN/0321200985/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0321200985/robsladesinte-21>
<http://www.amazon.ca/exec/obidos/ASIN/0321200985/robsladesin03-20>
%O tl a rl 1 tc 2 ta 2 tv 1 wq 2
%P 460 p. + CD-ROM
%T "Windows Forensics and Incident Recovery"

Chapter one is an introduction, both to the book and to the ideas behind it. For once, the author does, indeed, try to define what an incident is. The definition is broad, but so are the possibilities. The intended audience is

stated to be anyone interested in the security of Microsoft Windows, but it is instructive that, in listing specific groups, forensic specialists and security professionals are *not* mentioned. Carvey notes that a great many people would like to know the information that Windows forensics can provide, since the platform is nearly ubiquitous, but few have the knowledge of system internals that is necessary to find the relevant bits. Based on the definition of an incident as an event that violates security policy, chapter two demonstrates some of the ways that policy failures, and therefore attacks, can occur. (The rationale behind the inclusion of eleven pages of Perl source for a program to detect null sessions escapes me.)

Chapter three reviews a number of places to hide data, but all of these are at the user interface level, such as setting hidden file attributes, placing data in unused keys in the Registry, NTFS (NT File System) alternate data streams (ADS), and the extra information stored in data files by applications like Microsoft Word. There is no mention of the lower level caches: slack space (whether in terms of zero padding, extra space in sectors, or the timing margins on hard disks) or page files. In addition, for those locations that are mentioned, specific programs for extracting particular data are listed, but no details of structural internals (for example formats for NTFS, OLE/COM, or Word) are provided for analysis with more general utilities. This is not to say that Carvey does not do a good job of explaining what he does cover: the tutorial on NTFS ADS is clear and complete. The material in chapter four addresses the issue of preparation by suggesting various means of hardening systems and networks against attack. The content is unusual, and deals with functions and activities that are frequently left out of security texts. At the same time, it does not touch on some common suggestions for system security: this should be seen as a complement to, rather than a replacement for, other Windows security works. A wealth of utilities for deriving all manner of information from Windows systems are listed and described in chapter five.

Chapter six presents suggestions for the methods and procedures to be used in responding to a potential incident, but it does so in the form of a number of fictional examples. The stories can be instructive, but it does take a long time to sort through the material to find the relevant points to use. Various indications that can be evidence of the existence of malware (particularly network-based remote access trojans) are examined in chapter seven. The author's Forensic Server Project, a tool for managing forensic data collection, is presented in chapter eight. Chapter nine describes an assortment of network scanning and data capture tools.

Although a number of areas are addressed, the text will be of greatest use to those who are concerned about network malware, especially of the remote access type. The intended audience, of experienced but non-specialist Windows administrators and law enforcement professionals with some technical background, will find a number of valuable indicators that will point out whether a system will reward further scrutiny. The professional, and particularly one with experience in forensic analysis, will find some very useful information on newer operations of Windows, but may be frustrated at the lack of detail. (I'm still not sure who is going to get a lot out of all the Perl source code ...)

copyright Robert M. Slade, 2004 BKWNFOIR.RVW 20041224
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

Volume 23: Issue 79

Thursday 17 March 2005

Contents

- [Professional Risk Assessment](#)
[Jack Goldberg](#)
- [Fallbacks that cry wolf](#)
[Steve Summit](#)
- [Airbus A300/310 rudder problems](#)
[David Rose via Harry Crowther](#)
- [Oyster card fault causes problems on London Underground](#)
[Daniel Thomas via Paul Rummell](#)
- [Computerized Physician Order Entry Systems](#)
[Charles J. Wertz](#)
- [Computerized medical mistakes](#)
[Bob Morrell](#)
- [Ballots "enhanced" by City Clerk](#)
[Arthur Kimes](#)
- [Centralized Privacy Rights Mechanism](#)
[Curt Sampson](#)
- [Man in the middle attack on SSL?](#)
[Russell Page](#)
- [Payment via MSN and related news](#)
[Koos van den Hout](#)

- [Microsoft antivirus - is it beta?](#)
[Rob Slade](#)
 - [Re: Viruses being delivered into mailing lists via BCC:](#)
[Dave Sill](#)
 - [Re: Richard Clarke: Real ID's, Real Dangers](#)
[Marc Auslander](#) [Mike Pritchard](#)
 - [Users of AOL Instant Messenger and other services beware!](#)
[Alistair McDonald](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Professional Risk Assessment

<Jack Goldberg <jackgoldberg@earthlink.net>>
Sat, 12 Mar 2005 10:30:00 -0800

Risks associated with developing and using computer systems have been documented widely (e.g., by PGN) and have become part of popular awareness. Economic costs resulting from these risks are huge, though presently unquantified. They include the costs of system failures, abandoned system developments, and lost opportunities to build valuable systems whose complexity is deemed beyond present art.

Despite the widespread awareness of this situation, nothing fundamental has been done to change it. New system technologies attempt to improve matters by giving system builders better tools. Large corporate and government initiatives to improve system trustworthiness have been announced. Despite many advances, system development risks have not abated. New systems keep getting developed whose defects are discovered too late to be

repaired economically. Repairs become patches and basic defects remain embedded in the system. These problems are pervasive, both in safety and infrastructure-critical applications and in the mundane data-processing applications that support the national economy.

With all the awareness of the hazards of system building, why does this bad situation continue? We suggest that the reason is the weakness of current risk assessment for new systems. Warnings about computer system risks that are given in an early stage do not have the force of warnings in other disciplines such as medicine and civil engineering and so they are ignored or discounted.

What can be done to improve the believability of warnings about development hazards? We do not envision a super-powerful tool that can generate a high-confidence hazard assessment for all situations. Rather we see the need for a profession of hazard auditors who have earned acceptance based on their scientific skills and experience. The need for their skills should be assumed and demanded in all system development efforts. Their observations (and if necessary, testimonies) should be communicated to purchasers, builders and users. Tools should be developed to support their analyses.

Building such a profession would be a substantial effort but the effort would surely be justified by the enormous cost of current development deficiencies. Government agencies, corporations, universities and

professional associations all have clear roles to perform.

✶ Fallbacks that cry wolf

<Steve Summit <scs@eskimo.com>>

Wed, 16 Mar 2005 22:55:31 -0500

It's said that every new technology carries with it the possibility of a new crime, and in a similar way, every new safety feature has some possibility of actually causing more problems than it's supposed to solve. This was brought home to me the other night at Logan airport where I noticed a shuttle bus whose destination sign persisted in showing the special legend "Call 911", despite the best efforts of the driver and several dispatchers whose conversations I was able to listen in on from the driver's radio of the bus I was on. I don't know if they eventually got the sign turned off or had to take the bus out of service, nor do I know how many calls to 911 that night there were about it.

✶ Airbus A300/310 rudder problems

<"Harry Crowther" <crowther@ziplink.net>>

Sun, 13 Mar 2005 07:36:22 -0500

What made an Airbus rudder snap in mid-air?

David Rose - **The Guardian** (UK), *The Observer*, 13 March 2005

<http://observer.guardian.co.uk/international/story/0,6903,1436374,00.html>

When Flight 961 literally began to fall apart at 35,000 feet, it increased fears of a fatal design flaw in the world's most popular passenger jet.

At 35,000 feet above the Caribbean, Air Transat flight 961 was heading home to Quebec with 270 passengers and crew. At 3.45 pm last Sunday, the pilot noticed something very unusual. His Airbus A310's rudder - a structure 28 feet high - had fallen off and tumbled into the sea. In the world of aviation, the shock waves have yet to subside. ...

In November 2001, 265 people died when American Airlines flight 587, an Airbus A300 model which is almost identical to the A310, crashed shortly after take-off from JFK airport in New York. According to the official report into the crash, the immediate cause was the loss of the plane's rudder and tailfin, though this was blamed on an error by the pilots. ...

There have been other non-fatal incidents. One came in 2002 when a FedEx A300 freight pilot complained about strange 'uncommanded inputs' - rudder movements which the plane was making without his moving his control pedals. In FedEx's own test on the rudder on the ground, engineers claimed its actuators - the hydraulic system which causes the rudder to move - tore a large hole around its hinges...

The Observer has learnt that after (an earlier) disaster, more than 20

American Airlines A300 pilots asked to be transferred to Boeings, although this meant months of retraining and loss of earnings. Some of those who contributed to pilots' bulletin boards last week expressed anger at the European manufacturer in vehement terms. One wrote that having attended an Airbus briefing..., he had refused to let any of his family take an A300 or A310 and had paid extra to take a circuitous route on holiday purely to avoid them: 'That is how convinced I am that there are significant problems associated with these aircraft.'

✈ Oyster card fault causes problems on London Underground

<"Paul Rummell" <rummell@myprivacy.ca>>

Thu, 10 Mar 2005 21:44:49 -0500

"Oyster card fault causes problems on London Underground"

"Automatic updates cause journey renewal problems"

Daniel Thomas, *Computing*, 10 Mar 2005

Londoners were faced with travel problems this morning after an IT error meant hundreds of commuters could not renew journeys on their Oyster card.

The error, which affected the whole of the London Underground (LU) and Docklands Light Railway (DLR), was caused when an overnight electronic updating process went wrong.

Transport for London (TfL) and TranSys - the consortium that operates the Oyster card scheme - automatically updates the system each night

to add new records and block stolen and canceled cards.

But a glitch in the system early this morning means commuters are unable to use machines at Underground or DLR station this morning to add new journeys onto the smart cards.

'Every morning information goes out about stopped cards and it was an error in the data that caused the problem,' said a spokeswoman for TransSys.

Passengers that have already paid for their journey or using prepay can still use the system as normal.

TfL and TransSys identified the error at 4am this morning and starting issuing a fix to the problem by 8.30am.

'We hope everything to be up and running again by the end of the morning,' said the TransSys spokeswoman. 'We are now looking into what actually caused the error and ways of ensuring this doesn't happen again.'

✶ Computerized Physician Order Entry Systems

<"Charles J. Wertz" <wertzcj@buffnet.net>>
Fri, 11 Mar 2005 14:47:44 -0500

The 9 Mar 2005 issue of the *Journal of the American Medical Association* contains two articles and an editorial that should be of interest to Risks readers.

ROLE OF COMPUTERIZED ORDER ENTRY SYSTEMS IN FACILITATING MEDICATION ERRORS

discusses a variety of issues including poor interface design requiring a physician to look at as many as 20 screens to see all the information about a patient, misleading and frequently misinterpreted dosage information, dosage change requires adding the new and deleting the old, poor integration of multiple systems, poor handling of discontinuation and resumption of medications, loss of orders and others. This article appears to be the result of a well done comprehensive study at one specific hospital.

The Editorial, COMPUTER TECHNOLOGY AND CLINICAL WORK: STILL WAITING FOR

GODOT makes a number of good points such as, "The misleading theory about technology is that technical problems require technical solutions; ie, a narrowly technical view that leads to a focus on optimizing the technology.

In contrast, a more useful approach views the clinical workplace as a complex system in which technologies, people, and organizational routines dynamically interact." Anyone interested in systems design will find this interesting.

The other Article, EFFECTS OF COMPUTERIZED CLINICAL DECISION SUPPORT SYSTEMS ON PRACTITIONER PERFORMANCE AND PATIENT OUTCOMES: A SYSTEMATIC REVIEW

provides a comprehensive review of the topic.

If you have access to this journal and the time to read these articles, you will find them interesting.

✈ Computerized medical mistakes

<Bob Morrell <bmorrell@triad.rr.com>>

Sat, 12 Mar 2005 09:21:28 -0500

Recent coverage of a JAMA article on the patient errors (cited by R. Akerman in [RISKS-23.78](#)) caused by computers will likely be cited by those who resist the movement towards an electronic medical record. This despite the fact that all acknowledge that the current mixed state of computerized and non-computerized medical systems is abysmal. My perspective on this is that we often miss the core truth of most medical mistakes: they are caused by humans, not computers. In the 1990's I developed several programs designed to find medical mistakes. As such, I spent a lot of time analyzing mistakes, and dealing with defensive reactions by physicians and nurses to the mistakes found. The most common mistake, at its core, was raw human misunderstanding: conceptual misunderstanding leading to misinterpretation of medical data (surgeons who thought the higher the bacterial MIC number, the better the antibiotic, when the reverse is true, and therefore put the patient on an antibiotic guaranteed to be ineffective). A close second was communication failures, where a key report was pocketed, lost or otherwise not communicated to others who would understand its importance.

However, in all these cases, the typical hospital political hierarchy sought to turn each of these medical errors into a computer error, lest a human (particularly a Doctor human) be found at fault. While I was grumpy about this at first, I soon realized that there was at least some truth in it, in that more easily understood medical reports, that highlighted and provided some interpretation to key information, and were more widely distributed were in fact improvements worth making to medical systems, and certainly would prevent far more errors than my mistake finding programs would ever find. The problem was however, that as the concept of the electronic medical record began taking shape, resistance to it often cited the end of incident analysis that blamed the computer, rather than the physician or nurse who was primarily at fault. The JAMA cases certainly sound like real problems with the human/computer interface, but they sound suspiciously like the final reports we used to end up on real mistakes made by real humans.

The medical environment is extremely complex, understaffed and wrought with automated and semi automated systems that all can fail or conflict whether they are computerized or not. I routinely saw problems with continuation of standing order dosing long before those standing orders were computerized. Blaming the computer misses the point, even if it does point out how the computer system could be made better.

The risk is one I often see in The Risks Digest: problems with computerized

systems seem to get more attention than the usually much greater problems in the existing non-computerized systems.

[Bob, Remember the full name of the Risks Forum! Actually, I get scolded now and then for running noncomputer-related items, but I try to keep noting how the noncomputer computer are also illustrative. PGN]

✶ Ballots "enhanced" by City Clerk

<Arthur Kimes <artki@sbcglobal.net>>

Sat, 12 Mar 2005 07:09:25 -0800

<http://www.dailynews.com/Stories/0,1413,200~20954~2758409,00.html>

> Los Angeles City Clerk Frank Martinez ordered election workers Tuesday night to use blue highlighter pens to re-ink thousands of voters' ballots that had "bubbles" partially or faintly filled in, ...

Los Angeles is using the Inkavote system. The voting machines and ballots look like the punchcard system (as in Florida 2000) but the ballot is poked by a special marker that puts a nice round ink blot in the round hole.

The company that makes the counting equipment says that this highlighting step isn't needed since their machines are supposed to be able to count ballots that have even a small amount of ink in the right place.

There were only a few thousand votes between the 2nd and 3rd

place finishers

in this election - the top two are headed for a runoff in May.

✶ Centralized Privacy Rights Mechanism

<Curt Sampson <cjs@cynic.net>>

Tue, 15 Mar 2005 14:11:27 +0900 (JST)

Bruce Schneier, on his blog recently, mentioned the paper "A Model Regime of Privacy Protection" by Daniel J. Solove & Chris Jay Hoofnagle. His link and discussion is at

http://www.schneier.com/blog/archives/2005/03/ideas_for_privacy.html

The paper's abstract and a link to download it can be found at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=681902

There are a lot of good ideas in this paper, but one in particular struck me as potentially unwise, and certainly underdeveloped:

In conjunction with the universal notice, the FTC shall develop a centralized mechanism for people to exercise their rights with respect to their personal information. Such a mechanism would mimic the Do Not Call website, which allows individuals to opt-out of telemarketing and verify their enrollment by visiting a single website.

Many interesting RISKS are raised by this. How do you identify the people in the opt-out registry? How do you authenticate requests to deny distribution of certain information? (A malicious person might try to cause

difficulties

for someone by forging a request to deny all credit data to potential lenders.) How do you determine who may or may not search the registry or read information in it? How do you keep this from acting as the "central key" to all the information on a person, effectively moving us closer to having One Central Database, with all of the problems that brings?

There's a huge can of worms here waiting to be opened.

Personally, my first instinct would be to avoid such a central registry and instead make it the responsibility of the data collectors to contact each individual with information about what they're collecting and how they're using it, and solicit permission to do so, as well as offer the ability to review the information. This avoids any centralized system, and also avoids certain types of error. For example, if I'm contact regarding a file that appears to have nothing to do with me, I can point that out, rather than have a company mistakenly believe that this file does correspond with my life. (Or I might just say it does, and use the information for identity theft. Who knows?)

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

⚡ Man in the middle attack on SSL?

<"Russell Page" <russellpage@hotmail.com>>

Fri, 11 Mar 2005 12:05:03 +1100

Marketscore (www.marketscore.com) offer a free proxy service web users. They offer accelerated downloads and e-mail virus scanning. To use their service users download and install software onto their PCs. Marketscore are quite explicit that they collect a wide range of information about their subscribers, and make information available to web site owners on usage patterns - a sort of "Neilson" for the net.

Unfortunately, they also impersonate SSL sites. If a subscriber attempts to set up an SSL connection to say, her bank, the Marketscore proxy sends back it's certificate, and then establishes an SSL connection to the destination. Clearly for this to work, the servers have to decrypt then re-encrypt all of the traffic. Equally clearly, large numbers of credit card numbers, account names, passwords etc are passing through the Marketscore systems in the clear.

There is a very good explanation of the problem here:

<http://www.shellnofcu.com/site/scams.html>

⚡ Payment via MSN and related news

<Koos van den Hout <koos@kzdoos.xs4all.nl>>

Fri, 11 Mar 2005 10:53:57 +0100

Nu.nl Internet <url:<http://www.nu.nl/rubriek.jsp?n=224&c=50>>, a current news website (in Dutch) had the following two headlines following each other this morning (my translation):

* MSN as form of payment

<http://www.nu.nl/news/495376/57/art.html>

* Viruses in chat programs increasing in popularity

<http://www.nu.nl/news/494989/50/art.html>

The first article is about the SNS bank in the Netherlands introducing a service for small payments via Microsoft's MSN Messenger.

The second article is about chat programs like MSN Messenger being used increasingly for spreading viruses.

With all the phishers and some of the virus-writers targeting online banks and sites such as Pay-pal, guess where this will be going.

Microsoft antivirus - is it beta?

<Rob Slade <rslade@sprint.ca>>

Wed, 16 Mar 2005 10:03:40 -0800

Some months back, Microsoft announced the purchase of an antivirus company.

For those in malware research, this appeared to be an indicator that

Microsoft would be getting back into the field. Apparently, very few of us

are old enough to recall the first time Microsoft "produced" an antivirus

product, but those who are remember that the kindest way to

describe the attempt would be "not fully thought through." Therefore, we did not look forward to this event with any great enthusiasm.

Subsequently, Microsoft announced it had acquired an anti-spyware company.

Then it announced a beta test version of an anti-spyware product. Then there was a flurry of announcements about legalities, copyright infringements, products that would be free, settlements of copyright infringement suits, products that would be charged for, and so forth, so I hope I can be forgiven for not recalling exactly where in that timeline came the announcement of a beta version of an antivirus product.

I viewed the antivirus beta with some trepidation. The announcement was not particularly clear about the capabilities of the product. It did indicate that the antivirus would be a) limited to specific malware programs, b) concentrate on "worms," and c) there seemed to be hints that the program would run in the background. With apprehension I downloaded the beta antivirus and installed it on one machine.

Nothing happened.

Nothing appeared in the Start menu programs list. Nothing appeared in the "Program Files" directory. Nothing appeared in the "Remove Programs" list. Nothing disappeared from my malware samples directory.

Subsequently, I have been receiving announcements from "Auto Update" that the "Windows Malicious Software Removal Tool" was ready for installation.

Previously I found this completely bewildering. In the latest

instance, if you choose "Custom Install," it does inform you that the tool will run once, and then be deleted from your computer. This makes a bit more sense.

According to Microsoft, more information for this update can be found at <http://www.microsoft.com/malwareremove>. This page states the same "run and then disappear" process, along with the assertion that the program will generate a report on the status of your computer. (So far, in my experience, this hasn't happened.)

The page lists seventeen pieces of malware that the program "cleans." The mention of "background" operation now seems to be tied to the Auto Update process, although it isn't completely clear that the antivirus itself doesn't run in the background. (The "run and delete" description would seem to indicate that the antivirus doesn't run in the background.)

I am interested in results from any others who have studied the program in more detail, including issues related to where the program looks for infections, what is cleaned, removal of malware from memory, cleanup of the Registry, scanning of mail files (many of the malware items listed are spread via e-mail attachments), and so forth.

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>

✶ Re: Viruses being delivered into mailing lists via BCC:

<Dave Sill <de5-dated-1111440414.241b1c@sws5.ornl.gov>>

Wed, 16 Mar 2005 16:26:53 -0500

(Rothwell, [RISKS-23.77](#))

The Delivered-To field is added by gmail (and other MTAs) when the message is delivered, so it's only visible to the recipient named in the field.

For example, if I send a message to joe@example.com and BCC dave@sill.org, the copy of the message that Joe receives might get a Delivered-To field like:

```
Delivered-To: joe@example.com
```

And I'll get one like:

```
Delivered-To: dave@sill.org
```

But since these are completely different copies of the message residing on different servers, Joe won't be able to see that I received a copy of the message.

Of course if I were to forward my copy of the message to Joe with its Delivered-To fields intact, that would expose the blind copy.

Dave Sill, Author, The gmail Handbook

✶ Re: Richard Clarke: Real ID's, Real Dangers (McMullen, [RISKS-23.78](#))

<Marc Auslander <marcausl@optonline.net>>

Wed, 16 Mar 2005 20:58:16 -0500

Actually, it has always seemed obvious to me that the real purpose of the photo ID check, and the reason the airlines cooperate, is that it interferes with a secondary market in non-refundable tickets.

✈ Re: Richard Clarke: Real ID's, Real Dangers (McMullen, [RISKS-23.78](#))

<Mike Pritchard <mpp@mppsistemas.com>>

Fri, 11 Mar 2005 05:11:38 -0600

Having worked in the bar and liquor store industry for the last 6 years, I can tell you the scanners are not the end all solution either. At my work we have a large collection of fake ID's that scan just fine. All the info matches what is printed on the ID, but the ID was still fake. You can buy a mag strip writer for a few hundred dollars off the Internet and write whatever info you want on there. If you are smart enough, you can generate the correct 3-D barcode, and print that on the ID, too, and all the high priced scanners will tell you the ID is fine, even when it is a fake. The fake ID people even can get the UV light seals nearly 100% correct.

The other risk here is not checking what the scanner says. A large number of the fake IDs I've confiscated scan (reports the person is 21 or older), but the info doesn't match. The person producing the fake used a real ID to

generate the barcode info. Some of our scanners just check age, and don't display the actual data. And some states encrypt that data, so the scanner is useless on those.

At my previous job, we had no scanners, so detecting fakes was all visual inspection (or by touch, a lot of fakes just don't feel right). On a number of fakes I confiscated, I had people insist I scan it! Told them I had no scanner, and I knew it was fake, and the only way they were going to gain entrance was for a police officer to verify the ID. Had a few call my bluff, and the cops came and wound up giving them a ticket. I took some of those ID's over to another location that had a scanner, and sure enough the scanner said they were 21!

The place I'm at now has scanners, and some of the staff rely too much on them. I've grabbed ID's out of other clerks hands to inspect them when they ran them through the scanner and it said it was ok, and a lot of times it does turn out to be fake.

⚡ Users of AOL Instant Messenger and other services beware!

<"Alistair McDonald" <alistair@inrevo.com>>
Sat, 12 Mar 2005 23:16:27 -0000 (GMT)

AOL has changed their Terms of Service for users of their services - see <http://www.aim.com/tos/tos.adp>.

Users of their services, for example AOL Instant Messenger (AIM) in particular should note the details, including: "by posting Content on an AIM Product, you grant AOL, its parent, affiliates, subsidiaries, assigns, agents and licensees the irrevocable, perpetual, worldwide right to reproduce, display, perform, distribute, adapt and promote this Content in any medium".

Nice one!

A few points:

- 1: We've seen this before: a company makes a niche, gains userbase, then turns bad in some way and shafts the user.
- 2: I've often used IM services to send beta software, specs, and so on to clients, using the "send file" option. By transferring them via AIM, I've allowed them to be reproduced in any form. There goes client confidentiality.
- 3: Big companies use AOL - one of my clients is one of the largest investment banks in the world. Their desktop IM client includes an AIM bridge, I guess that some traders use it to communicate with clients (by using the bridge, the bank can log everything and keep regulators happy).
What does this mean to the bank, or another large company?
- 4: What if some voice over IP (VoIP) provider pulls this one. Or even an e-mail provider?

Jabber and ICQ are free (as in beer) IM services. I've used ICQ, but have no experience of Jabber <<http://www.jabber.org/>> and <<http://www.icq.com/>>.

Added note, 14 Mar 2005 13:51:55 -0000 (GMT)

AOL has subsequently clarified its ToS. This has been reported in a

blog:<<http://www.chron.com/cs/CDA/ssistory.mpl/tech/blog/3082956>>, which

itself reports on e-mail and telephone conversations with AOL spokesman

Andrew Weinstein.

However, the ToS still read as they did yesterday (I doubt AOL are going

to modify them without a lawyer casting an eye on them, and this story

broke over the weekend). The terms are still ambiguous and everyone should

be careful!

Alistair McDonald, InRevo Ltd (<http://www.inrevo.com>) 07017 467 396

Author of the SpamAssassin book: <http://www.spamassassinbook.com/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 80

Wednesday 23 March 2005

Contents

- [Procurement risks and nonverifiable code](#)
[Tim Panton](#)
- [DEA agent shoots self while demonstrating gun safety](#)
[Arthur T.](#)
- [Boston College loses thousands of SSNs](#)
[Geoff Kuenning](#)
- [Yes, we know what that means!](#)
[Tim Connors](#)
- [Risks of long and short URLs](#)
[Arthur T.](#)
- [GPS](#)
[Martyn Thomas](#)
- [Snowplow fraud and GPS devices](#)
[David Tarabar](#)
- [Re: More uses of satnav/GPS](#)
[Roland Giersig](#)
- [Re: Website hijackings, 302 redirects, and security issues](#)
[Drew Dean](#)
- [Re: Remote physical device fingerprinting](#)
[Markus Roth](#)

● [REVIEW: "The Information Security Dictionary", Urs E. Gattiker](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Procurement risks and nonverifiable code

<Tim Panton <thp@westhawk.co.uk>>

Fri, 18 Mar 2005 13:54:35 +0000

In today's *Independent* newspaper:

[<http://news.independent.co.uk/business/news/story.jsp?story=621293>]

> Edward Leigh, the Conservative chairman of the committee,
> said: "It is
> simply disgraceful that the MoD has spent a quarter of a
> billion of
> taxpayers' money on the botched procurement of eight Chinook
> helicopters that cannot be flown because the MoD can't
> determine if
> they're safe."
>
> The problem has arisen because the MoD cannot validate the
> software
> codes used by Boeing in the helicopters' avionics system and
> flight
> controls. The US company is not prepared to release these for
> security
> reasons.

Apparently the contract doesn't specify that the MoD has the
right to
see the code.

Open-source avionics anyone ?

✶ DEA agent shoots self while demonstrating gun safety

<"Arthur T." <myspamtrap01@yahoo.com>>

Wed, 23 Mar 2005 10:34:18 -0500

The subject doesn't sound like a computer-related risk? The follow-up may be.

A year after the incident, home video of the incident is on various web sites. From Snopes:

Experts in the field said that the undercover agent should never have been

videotaped because it could put the agent's life at risk.

"It puts a lot of undercover agents in jeopardy if their faces are

videotaped," a masked agent told Local 6 News. "His identity is

burned. His identity is known as a police officer and its a potential

personal safety hazard to himself as well as his family members."

As is often the case with "computer error", this is actually human error.

Even if not being videotaped, why was an undercover agent appearing in

public as himself? Admittedly, computers may have exacerbated the problem.

[Source: <http://www.snopes.com/photos/accident/gunsafety.asp>]

✶ Boston College loses thousands of SSNs

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

19 Mar 2005 00:37:16 +0100

Hackers have invaded a Boston College database of alumni, compromising

data on up to 100,000 people. The data includes Social Security Numbers.

In a choice quote, Jack Dunn of BC ``noted that Boston College will

hereafter delete Social Security numbers from its records, despite their

usefulness in maintaining accurate records.''

Question: If every organization that currently stores SSNs waits until

after they are hacked before they decide that maybe it's not smart to

expose sensitive data, how many Americans will be left with uncompromised

SSNs?

Liability laws are desperately needed.

More information at:

http://news.zdnet.com/2100-1009_22-5623084.html

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

⚡ Yes, we know what that means!

<Tim Connors <tconnors+risks@astro.swin.edu.au>>

Wed, 16 Mar 2005 17:44:46 +1100 (EST)

Whilst booking a ticket for an event in the Food and Wine Festival, I came

across this: <http://www.ticketmaster7.com/help/privacy.asp>

4: Data Security Ticketmaster7 will endeavour to take all

reasonable steps

to keep secure any information that we hold about you.

Ticketmaster7 has

security measures, proprietary secure algorithms, in place to protect the

loss, misuse and alteration of the information under our control. Our

secure server software is the industry standard and among the best

software available today for secure commerce transactions.

Am I too cynical? Why do people always thing "proprietary" means "best"?

Am I just meant to say "I don't think that word means what you think it

means"? Oh, and "industry standard". You mean, run by microsoft, insecure,

buggy, and plain does not do its job, but it's at least the normal state of affairs!

TimC -- <http://astronomy.swin.edu.au/staff/tconnors/>

✶ Risks of long and short URLs

<"Arthur T." <myspamtrap01@yahoo.com>>

Sun, 13 Mar 2005 10:32:23 -0500

We all know the Risks of long URLs. They include line-wrap problems and trying to find an "@" about 100 characters in.

To combat the line-wrap problem, some sites are providing short URLs for any

arbitrary page. One such is <http://tinyurl.com> . The problem here, though,

is that you can't know where you're going until you get there. This hampers

the anti-phishing advice to type in a URL sent in e-mail. It could be used for a range of nefarious or hoax uses.

I looked at the tinuyrl site and didn't find any way to expand a compressed URL. Since they specifically suggest using their service to hide affiliate URLs, this is probably on purpose.

⚡ GPS

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

Sun, 13 Mar 2005 18:39:44 -0000

Proposals to use GPS for functions that are essential to critical infrastructure (rail, for example) seem to appear every week.

GPS is a system that relies on weak signals detected by aerials that are not focused on the position of the satellites. It is therefore extremely vulnerable to in-channel jamming.

How can we get some reality into these proposals? Or are we destined to be at the mercy of denial of service attacks by anyone who knows enough electronics to be able to generate a few watts of RF noise?

⚡ Snowplow fraud and GPS devices (Re: [RISKS-23.67](#))

<David Tarabar <dtarabar@acm.org>>

Sat, 12 Mar 2005 09:19:15 -0500

As I reported in [RISKS-23.67](#), for the past several years, the Massachusetts Highway Department (MassHighway) has required that private snow-removal contractors carry a GPS equipped mobile phone.

On 11 Mar, the Mass. Attorney General indicted a contractor and an employee on charges that they did privately-paid work during state time and used state road salt on this private work.

The contractor was responsible for a section of state highway. During a heavy snowstorm, the contractor got road salt from a state depot, left his GPS device in a snow bank on the side of the highway, and drove off to do his non-state plowing. Later he gave his GPS device to his employee who was plowing the state highway - so it appeared that two trucks were plowing in tandem. The contractor confessed to double dipping during this winter and the 2003-2004 season.

It should be noted that this scheme was NOT discovered via the GPS device. The State Police got a tip and followed the contractor during a recent storm. When GPS records were examined, they found that the contractor's GPS device showed periods of excessive inactivity during most storms this year. Officials at MassHighway said that it was human error that this fraud was not detected by examining GPS records.

[Source: *The Boston Globe*, 12 Mar 2005, John Element, Mass. charges 2 in alleged snowplow scam]

✈ **Re: More uses of satnav/GPS (Bacon, [RISKS-23.78](#))**

<Roland Giersig <roland+[risks23.78](mailto:risks23.78@giersig.org)@giersig.org>>

Tue, 15 Mar 2005 15:19:41 +0100

In [RISKS-23.78](#), Michael Bacon gave a good discussion about the risks of using GPS in commercial safety-critical applications, namely railroads. I want to answer some open points and discuss them more deeply:

Determining the position of a train is only one point, the second crucial point is communicating this position to other trains. Currently this works via track-side sensors and track-side signalling, where data is exchanged between the on-board unit, the track-side systems and the track operators. Critical failure of some part of this system triggers a set of actions that brings the whole system (i.e. all trains) into a safe state: signals go to red (luckily, trains, unlike airplanes, do have a simple, safe state :-). If the failure is not too severe, e.g. track-side communication to the on-board units fails, then the system falls back to a state where the train pilot has to navigate by sight instead of relying on the electronic systems. And this is perfectly safe, unlike in air-traffic-control.

And this fall-back also would be the case for GPS-based positioning: the danger does not lie in GPS failure (outage), which is detected easily and the same fall-backs are possible as with current systems.

>>> The danger lies in the unknown accuracy of the GPS signal!!

<<<

This is where EGNOS and GALILEO come into play: EGNOS is an additional information system that will provide up-to-date accuracy information about the GPS signal. This enables safety-critical systems to react to increased error in the GPS signal. GALILEO on the other hand, being a commercial, multi-national system, is supposed to be completely independent of the GPS system (and of foreign influence, hostile actions notwithstanding).

My conclusion: from a technological point of view, the use of GPS-based positioning systems does not produce an additional risk that cannot be handled.

Still, most criticism from the former article holds: increasing traffic density via new technology is a trade-off: if the new high-tech system (GPS-based) has to fall back to a technologically lower state (line-of-sight navigation), all of a sudden the whole infrastructure is overloaded, which will result in a severe break-down or even deadlock.

If this trade-off is worthwhile should be closely examined. But I have a hunch that the decision to install such a system will not be based on such elaborations...

✶ Re: Website hijackings, 302 redirects, and security issues

<Drew Dean <ddean@csl.sri.com>>

Mon, 14 Mar 2005 12:09:04 -0800

(Chmielewski, [RISKS-23.78](#))

I co-wrote an early paper on related to Tim's RISKS posting: see <http://www.cs.princeton.edu/sip/pub/spoofing.php3>

✶ Re: Remote physical device fingerprinting (Kohno, [RISKS-23.77](#))

<Markus Roth <atempest@bigfoot.com>>

Sun, 13 Mar 2005 00:32:05 -0500

> Together with Andre Broido and kc claffy from CAIDA, I have
> been working
> on methods for remote physical device fingerprinting, or
> remotely
> fingerprinting a physical device without any modification to
> or known
> cooperation from the fingerprintee.

I'd like to summarize the meat of the paper and point out that
this is not
as big a privacy RISK as one might initially assume. Remember,
this is just
the gist of the paper; I have simplified many things.

First, a definition of "clock skew": A clock with skew is
gaining or losing
time. For example, a wall clock with a 2-minute skew that
correctly shows
12:00 at noon, will show 1:02 when it is one o'clock, then 2:04
when it is
two o'clock, next 3:06 at three, and so on. Similarly, a clock
with a -2
minute skew loses 2 minutes every hour.

This is different from a clock running fast or slow. A clock
running 2

minutes fast would show 12:02 at noon, 1:02 at one o'clock, 2:02, 3:02, etc.

The authors' experiments demonstrate that the various clocks found on a computer have tiny skews. The skews range from roughly -50 to 50 microseconds every second, and they stay constant for a particular computer. The authors say that there is enough statistical variation among skews to tell apart one computer from another if you can somehow watch a targeted computer's system clock.

How do you watch the clock on a remote computer? It turns out that most implementations of TCP/IP put a 32-bit timestamp into each TCP packet. The authors' trick is to monitor thousands of packets from a targeted computer over the course of minutes or hours; then, using some linear algebra, they determine the targeted system's skew.

For example, a laptop accessing the Internet from New York may have its skew measured as 45 microseconds per second. Later, the same laptop connecting to the 'net from Berlin would again show a skew of 45 microseconds per second.

The authors claim that their method will allow you to learn 6 bits of information about a device. Well, 2^6 is only 64 different devices. If there are 200 million computers on the Internet, their method would divide the world into 64 groups of 3 million computers each. Your computer would look identical to 3 million other computers!

This technique would be useful to show negative but not positive results. If

a laptop in Berlin gives a skew value of 26 microseconds, you can conclude that it is a different laptop than the one in New York. But if an arbitrary laptop in Berlin shows a 45 microsecond skew, you can only say that there are 3 million other computers like it. You cannot conclude that it is the same laptop that was once in New York.

⚡REVIEW: "The Information Security Dictionary", Urs E. Gattiker

<Rob Slade <rslade@sprint.ca>>
Mon, 14 Mar 2005 08:08:57 -0800

BKINSCDI.RVW 20041222

"The Information Security Dictionary", Urs E. Gattiker, 2004,
1-4020-7889-7, U\$145.00/C\$203.50

%A Urs E. Gattiker dictionary@weburb.com

%C 233 Spring St., New York, NY 10013

%D 2004

%G 1-4020-7889-7

%I Springer-Verlag/Kluwer

%O U\$145.00/C\$203.50 212-460-1500 800-777-4643

%O [http://www.amazon.com/exec/obidos/ASIN/1402078897/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1402078897/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/1402078897/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1402078897/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1402078897/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1402078897/robsladesin03-20)

%O tl n rl 1 tc 0 ta 2 tv 1 wq 0

%P 411 p.

%T "The Information Security Dictionary"

A good dictionary of information security terms is seriously needed by the security community, and by the computer and communications

industry as a whole. The "Internet Security Dictionary" (cf. BKINSCDC.RVW), by Phoha, was a good start, but needs to be expanded and updated.

I have been working on a security glossary myself, so this might be yet another case of bias or conflict of interest. I should also note that, although it is widely believed that I enjoy trashing books, I am actively looking for works that I can recommend. Oh, it's easier to point out flaws in a work than it is to say why someone writes well. However, I take no particular pleasure in having to savage a work as thoroughly as this one requires.

Far too many of the definitions contain misleading, incomplete, or outright false information. Anomaly-Based Intrusion Detection Systems are said to discover known attacks, which might be true, but signature-based systems would normally be considered better for that purpose: you want anomaly-based detection to discover previously unknown attacks. The entry for Authentication does not list the standard factors of something you know, have, or are. The definition for the Bell-La Padula security model doesn't provide any details of the pattern itself, does not mention confidentiality (a central concept), and does not refer to the Trusted Computer System Evaluation Criteria and other outcomes of the paradigm. The Biba integrity model is listed as "Bibra."

Patent mentions the ability of the patent holder to restrict use, but doesn't mention that patent is only applicable to devices and that the

device must be novel, useful, and non-obvious. Reference is made to copyright (the definition of which is equally flawed) and to Tables 16A and B, neither of which alludes to intellectual property laws. No listing is given for trade secrets or trade marks. Both the entry for patent and the account of copyright state that patents protect ideas, which is specifically untrue.

There is a listing for Illegal Software (software used without a licence), although there isn't one for piracy. There is one for Software Piracy, but neither of the two cross-references points to Illegal Software. There is an entry for Cable, as in cable TV, but nothing for cabling as in network media, which has much greater importance in terms of information security. Challenge Handshake points to Handshake (there is no listing for challenge/response) and, for some completely inexplicable reason, also to Circuit-Level Gateway.

The sub-listing for Content Filtering (which comes under filtering, rather than content) makes no mention of the origin of the practice in restricting access to objectionable material.

"DoS on the 13 Internet Root Servers" is not the title of a famous Cultural Revolution artwork, but a reference to the October, 2002 attack against the top-level DNS servers. Almost no details of the event are provided (and this was actually a *distributed* denial of service attack).

Digital Versatile Disk (generally used as an update to Digital Video Disk, the original expansion of the DVD acronym) is defined as

using
both sides of the disk (almost unknown in commercial DVDs) and
also
notes a capacity of 17 gigabytes, which would actually require
both
sides and both depths.

One of the sub-entries under Disinfection is Generic Scan String,
which has nothing to do with disinfection of computer viruses.

"Activity monitor" is defined solely in terms of employee
surveillance, and ignores the specialized use in malware
detection.

The entry for Cookies states (incorrectly) that they can only be
used
by the originating site. However, there is a cross-reference to
table
18A (a mere 140 pages from the entry). Table 18A has no mention
of
the term. Table 18B does have a listing for Java Cookies--which
contradicts the earlier assertion, and says that other parties
can
read cookies. Defence-In-Depth has a reference to Table 6A.
There is
no 6A, although there is a 6. Table 6 contains no reference to
defence-in-depth.

Urs isn't always certain of his definitions: an Application Level
Gateway "could" be a type of firewall. However, in that case,
he is
certain that it re-addresses traffic--which is actually the
function
of network address translation (NAT), generally considered a
type of
circuit-level proxy firewall. Phishing is equated with "carding"
(obtaining or trading in credit card numbers for fraudulent use)
while
the more definitive practice of obtaining banking information is
ignored. (We are told that avoiding the running of attachments
prevents phishing. Phishing scams seldom make use of
attachments or
executable code.)

Cross references are not always accurate. On page 12 the listing for "Anti-Virus Researcher" points to the entry for "Research." There is no material for Anti-Virus Researcher in that entry, but there is in the later entry for "Researcher." Ethics points to Justice, which doesn't say anything about ethics.

Some of the terms included are rather odd. "Binders" are supposed to be utilities that bind multiple code modules together. Most people refer to these utilities as linkers. "Derf" was used as a term for hijacking sessions on logged in terminals, but in a limited setting and quite a while back: the term is pretty much unknown today.

The definitions given for some entries don't seem to have any real meaning. For example, "Virus Algorithm means a set of operations or a procedure designed to create a virus problem." Many long definitions appear to have been patched together from disparate and unrelated sources, not listing additional meanings, just appending disjointed verbiage.

Some of the definitions given are correct. Heck, some are copied straight out of government documents. But Gattiker has included a number of terms which are either generic, or have only the most tenuous of connections to security. There is an entry for Computer Mouse. There is a listing for the fictional cyberpunks, but no mention of the real-world cypherpunk community. The definition for Virology deals only with biology. The entry for Virus is only relevant to (pretty much obsolete) file infectors.

As could be expected with a work of this calibre, a number of terms are simply missing. There are entries for false positive and false negative, but none for false acceptance or false rejection (the more widely known terms for similar concepts).

It is difficult to give a complete picture of the unreliability of this text. It would be easy for me to simply do an exhaustive search of every minor error, and in a few pages collect all that might be wrong with an otherwise great work. But in this volume we have spurious listings, missing entries, definitions that make no sense to the reader, explanations that are erroneous, and even opinion stated as fact. (The man, or manual, pages of the UNIX system, incorrectly identified as "main" pages, are said to be technobabble, presumably because Urs doesn't understand their cryptic nature.) Slang is included and technical terms are left out.

Probably the best way to give a flavour of the quality of this work is to reproduce some listings. (I have tried to be as careful as possible in copying the exact writing and punctuation of the entries as they appear in the book.)

A listing that sounds good but makes no sense (as well as being a non-sequitur) provides a good feel for the quality of language and logic representative of the work as a whole:

Homomorphic Encryption is a cryptographic technique in which the sum of two encrypted values is equal to the encrypted sum of the values. The signature operation in public key

cryptography is an exponentiation operation using the private key as the exponent.

According to "Algebraic Aspects of Cryptography" by Neal Koblitz (cf. BKALASCR.RVW), and a number of other references, homomorphism refers to groups or sets rather than express algorithms or techniques. Homomorphic encryption can be useful for signature or authentication systems where anonymity is important (such as in voting procedures) but it probably isn't necessary to specify exponentiation.

The sub-entry for "Anti-Virus Researcher or Security Assurance Researcher" on page 270 is lengthier, and requires a bit more dissection:

Anti-Virus Researcher or Security Assurance Researcher may conduct his or her research in many ways. An example might be a lawyer searching among old court cases for legal precedents regarding Privacy and Hacking.

An epidemiologist studying age groups or cohorts and hip-fracture incidents to an Anti-Virus Researcher studying malicious code to discover programming patterns and characteristics (see Theory).

Often Anti-Virus Researcher is used synonymously with "product development." Sometimes, a "bonafide antivirus researcher's" role within his or her organization might be documented by independent examination (see also Appendix 3 and badguys website).

It should be reasonably obvious that the specialized activity of antivirus research and the more general undertaking of security assurance research are not exactly synonymous. In addition, very little antivirus research involves case law. If you are confused by the meaning of the sentence about an epidemiologist, you are not alone. Again, very little antivirus research involves hip-

fractures.

Some AV researchers are also product developers, but the two activities are hardly identical. The reference to "badguys website"

is to the "Bad Guys" Website (www.badguys.org) run by Sarah Gordon,

which does have some information about legitimate virus research, in

opposition to the blackhats who write viruses and call themselves researchers.

If, following the cross reference to Theory, we flip to page 324, we

find a sub-entry for "Anti-Virus Theory":

Anti-Virus Theory if it would exist would be based on Inductive or Deductive Research outline phenomena and their relationship to other issues. Hence, investigation of the subject aimed at uncovering new information in a systematic way, while permitting a group of statements about how some part of the world works, in this case Computer Viruses. A good Anti-Virus Theory would allow us to generalize from one virus to the next (see Tables 19A and 19B).

The wording here would seem to imply that Anti-Virus Theory does not

exist, which raises the immediate question of why you would include an

entry for a non-existent entity. Induction and deduction are fairly

broad tools: the first sentence doesn't really appear to say anything

useful about the type of theory or research. Tables 19A and B are

nowhere near that entry. In fact, you will find them on pages 207 and

209-11. Neither do the tables have anything to do with viruses: they

talk about the costs and prevalence of various forms of Internet access. In any case, that entry doesn't appear to say anything about

any theory to do with computer viruses, beyond the definition of a

theory in general.

(If we follow the further cross-reference to "Methodology," we find no allusion to antivirus research at all.)

Errors in formatting (particularly indenting) are rife, and make it difficult to follow the structure of entries, or the book as a whole.

Bold text sometimes means that the term is another entry, but sometimes it doesn't seem to mean anything. Sometimes the formatting

problem might explain entries that appear to be out of place, but I'm

not sure that they explain the sequential listings of Autopsy, Authorization, and Auto Dial-Back.

There are numerous typographical errors, mistakes in spelling and grammar, and tremendous inconsistencies in capitalization. Even the

most cursory copy and style edit would have improved things enormously.

The security community and industry deserves better than this. Students of security need more accurate information than is provided

in this work. Society as a whole is relying on information security

and requires more credible content than this book contains.

copyright Robert M. Slade, 2004 BKINSCDI.RVW 20041222
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

Volume 23: Issue 81

Monday 28 March 2005

Contents

- [Essex County NJ Jail locking-system failure](#)
[Charles Lamb](#)
- [Cruise-control failures?](#)
[Robert Scheidt](#)
- [TSA Finds Data On Air Passengers Lacked Protection](#)
[Amy Schatz via Richard M. Smith](#)
- [RSA Finds More Flaws in RFID](#)
[Stephen D. Poe via Dave Farber](#)
- [Sumitomo cyberattack](#)
[Tom Van Vleck](#)
- [Clinical Healthcare IT, 'error', and safety](#)
[Richard Cook](#)
- [Human error and computerized medical systems](#)
[Don Norman](#)
- [Why IE is insecure: flawed logical thinking...](#)
[Craig DeForest](#)
- [Re: Risks of long and short URLs](#)
[D.F. Manno](#)
- [Risky US Bank Visa product](#)
[John Meissen](#)

● [Important PITAC Cybersecurity report released](#)

[Gene Spafford](#)

● [EEPI - Electronic Entertainment Policy Initiative](#)

[Lauren Weinstein](#)

⚡ **Essex County NJ Jail locking-system failure**

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

Thu, 24 Mar 2005 01:17:08 -0500

According to an article in the 20 Mar 2005 issue of *The Star-Ledger*

(Newark NJ), New Jersey's Essex County Jail has experienced another failure

of its touchscreen based physical access control system.

<http://www.nj.com/news/ledger/essex/index.ssf?/base/news-6/1111297930265190.xml>

Essex County Executive Joseph DiVincenzo sounds like he's never encountered

a competent systems engineer. "These things happen. This is not the first

time it's happened. ... It's happened a couple of times already, and it's

not going to be the last time either." Police Benevolent Association Local

157 president Joe Amato has a more practical view, "Modern technology at its

finest. Who needs it? ... An old-fashioned turnkey operation would have just

been fine, but we spent millions for a high-tech computer-controlled jail

that isn't worth the contaminated dirt that it's built on." One wonders how

well the system will function once the inmates get their hands on it.

✈ Cruise-control failures?

<"Robert Scheidt" <robertscheidt@tiscali.be>>

Wed, 23 Mar 2005 11:31:45 +0100

Recently in France a number of failures of "cruise control" systems especially on recent models of Renault made cars have been reported, some creating serious accidents (including a deadly one). In general it is reported that the car stays at his set speed and no matter what the driver does, including cutting the ignition and breaking, the car continues at that speed.

What's more surprising is that it is also reported that brakes become ineffective (the brake pedal resists pressure).

I could imagine that the cruise control being probably under control of some microprocessor, this microprocessor could "hang" due to some software problem and therefore that everything it controls just stays as it is. Especially in newer cars where fuel injection is completely electronically controlled (no mechanical link between the gas pedal and the fuel injection controls).

However, I have difficulties believing that the same microprocessor would control the brakes and make them ineffective. I wonder if somebody on this board has some insight on how the electronic controls of modern cars are designed and especially if a single component's failure (such as

a common
microprocessor) could affect multiple functions (e.g.,
acceleration and
brakes).

✶ TSA Finds Data On Air Passengers Lacked Protection

<"Richard M. Smith" <rms@computerbytesman.com>>

Fri, 25 Mar 2005 07:09:40 -0500

[Source: Amy Schatz <Amy.Schatz@wsj.com>, *Wall Street Journal*,
25 Mar

2005, A4; PGN-ed]

[http://online.wsj.com/article/0,,SB111172077661889592,00.html?
mod=todays_us_page_one](http://online.wsj.com/article/0,,SB111172077661889592,00.html?mod=todays_us_page_one)

A new government report says officials in the Department of
Homeland
Security didn't do enough to keep airline-passenger data secure
when using
it to test a traveler-screening program. DHS's Inspector
General says the
Transportation Security Administration gathered 12 million
passenger records
from February 2002 to June 2003 and used most of them to test
the Computer
Assisted Passenger Prescreening System, or CAPPS 2, which was
designed to
check passenger names against government watch lists. Passengers
weren't
told their information was being used for testing. TSA
officials shelved
CAPPS 2 last year amid complaints it was an invasion of passenger
privacy. The agency has replaced it with a similar system,
called Secure
Flight, which is being tested and is expected to debut in August.

The report raises concerns because Secure Flight ultimately will

gather private information, such as names, addresses, travel itineraries and credit-card information, on anyone who takes a domestic flight. That effort could be slowed by a Government Accountability Office study due Monday which is expected to be critical of TSA's efforts to develop passenger-privacy protections.

The report said TSA "did not ensure that privacy protections were in place for all of the passenger data transfers" and noted that "early TSA and [CAPPS 2] efforts were pursued in an environment of controlled chaos and crisis mode after the Sept. 11 attacks."

Investigators also found TSA provided inaccurate information to the media about the agency's use of real passenger records for CAPPS 2 testing and wasn't "fully forthcoming" to the agency's own internal privacy officer during an investigation into the matter. "Although we found no evidence of deliberate deception, the evidence of faulty processes is substantial," investigators said.

✶ RSA Finds More Flaws in RFID (via Dave Farber's IP)

<Stephen D. Poe <sdpoe@acm.org>>
Thu, 24 Mar 2005 10:56:00 -0500

By Jacqueline Emigh, eweek.com, 23 Mar 2005

After uncovering a security weakness in a radio-frequency

identification tag
from Texas Instruments Inc., researchers from RSA Security
Inc.'s RSA
Laboratories and The Johns Hopkins University are now eyeing
future exploits
against other RFID products in the interests of better security,
one of the
researchers said this week. Meanwhile, TI will keep making the
compromised
RFID tag in order to meet the needs of applications more
sensitive to speed
and pricing than to privacy, according to a TI official.

The Johns Hopkins University Information Security Institute and
RSA first
publicized their findings about the RFID security hole in
January. In a
paper posted at www.rfidanalysis.org, the researchers claim that
by cracking
a proprietary cipher, or encryption algorithm in one of TI's DST
(digital
signature transponder) RFID tags, they were able to circumvent
the tags'
built-in security enough to buy gasoline and turn on a car's
ignition. The
researchers from Johns Hopkins and RSA reverse-engineered and
emulated the
40-bit encryption over two months.

[The full article is on IP:]

IP Archives at: [http://www.interesting-people.org/archives/
interesting-people/](http://www.interesting-people.org/archives/interesting-people/)

Sumitomo cyberattack

<Tom Van Vleck <thvv@multicians.org>>

Thu, 24 Mar 2005 16:22:07 -0500

Police foil 220-million-pound 'keyboard hacker' raid on bank,
TimesOnline, 17 Mar 2005

<http://www.timesonline.co.uk/article/0,,2-1529429,00.html>

★ Clinical Healthcare IT, 'error', and safety (Re: Morrell, [RISKS-23.79](#))

<Richard Cook <topquarkguy@sbcglobal.net>>

Thu, 17 Mar 2005 21:24:18 -0600

The note in [RISKS-23.79](#) regarding COPE [Computerized Physician Order Entry Systems] prompts me to point to our website, www.clab.org, where some of the papers cited by the JAMA articles by Koppel et al., Garg et al., and editorial maybe found. The finding that CPOE is a source of new forms of failure is not surprising. We have, indeed, predicted this for at least a decade, as the editorial by Wears & Berg points out. It is not surprising, either, that some continue to claim that most medical "mistakes" are "caused by humans". Although this notion of error has been thoroughly debunked over the past twenty-five years, the idea is deeply ingrained.

The scientific understanding of the nature of human performance, technology, and complex systems and their failures traces back to the aftermath of the Three Mile Island nuclear event in 1979. Woods, Norman, Rasmussen, Hollnagel, Senders, Moray, Wreathall, and many others spent fifteen years understanding the relationships between failure and success in

domains including aviation, nuclear power generation, and, more recently, in healthcare. [There is a useful bibliography in the short paper "A Brief Look at the New Look in Complex SYSTEM Failure, Error, and Safety" that can be found at www.ctlab.org .] When the patient safety movement began in the 1990's, our hope was that healthcare could avoid getting caught up in the sterile business of error attribution and counting and quickly move to the modern view of failure and success. Several scientists, notably David Woods, spent a great deal of time and effort with groups like the National Patient Safety Foundation in an effort to 'jump start' healthcare's work on safety. We achieved only a partial success --- the healthcare world did 'discover' error and become fascinated by it but, after a decade, most of the leadership now understands that the pursuit of 'error' is unproductive and a mistaken goal.

The JAMA papers and editorial are correct in their assessment of the current state of Clinical Healthcare Information Technology (CHIT). What is missing from the JAMA paper on CPOE and also from the editorial by Wears and Berg is a clear understanding of why current CPOE is so badly suited to the task of improving safety. Neither the paper authors nor the editorial writers are able to look deeply into the design features of these systems or the work that they are supposed to support. Such close examination reveal, as RISKS readers will already have anticipated, that it is the failure to produce

USER centered design that is the root cause of the poor performance of CHIT. The complex activity network that produces patient care is perhaps the most difficult place to insert interactive computing aids and the designers of these systems have done little to understand the patterns of work that occur there or the kinds of support that would be helpful; the paper by Patterson et al. in J Am Med Informatics Assn 2002:9;540-53 provides a detailed study. The result is TECHNOLOGY centered systems that generate failures because they are so ill-suited to the work at hand. Of course the designers of these things were certain that they were making user centered designs but the actual results are thoroughly technology centered. As David Woods said, "the road to technology centered systems is paved with user centered intentions."

We know, in principle and through demonstration, what it takes to make good CHIT. As Nemeth, et al., point out in a recent issue of IEEE Systems Man and Cybernetics (part A, vol 34, 2004), what is needed is detailed, calibrated understanding of the actual task requirements of the work domain and the tradeoffs and strategies that workers use to meet these demands. There are excellent examples of this sort of approach available but , like all good design, it takes time, money, and more than a little sophistication to do it. The rush to eliminate "human error" from medicine has led an eager and somewhat naive group to insist that new CHIT be put in place to forestall error by practitioners. Fueled by folk models of human error,

this
insistence has produced a whole lot of CHIT that will be the
source of a
steady stream of interesting failures over the next decade.

It is unsettling and disappointing to realize that the efforts
to produce
really good CHIT are going to require a great deal more time,
effort, and
money than has been budgeted. But RISKS readers will recognize
that this too
is a common experience with large systems. Many hospitals are
already deeply
involved in buying and installing new CHIT and the strong
government
pressure to continue this effort is likely to continue. We can
only hope
that a parallel effort to understand the technical work of
healthcare will
be undertaken so that, in time, it will be possible to make
better, more
useful, more user centered technology.

Richard Cook, MD, Cognitive Technologies Laboratory, University
of Chicago

[RISKS-23.79](#) Human error and computerized medical systems (Re: Morrell, [RISKS-23.79](#))

<"Don Norman" <norman@nngroup.com>>

Fri, 18 Mar 2005 09:12:58 -0800

In [RISKS-23.79](#), Bob Morrell once again wants to blame the human
for error in
complex medical systems. Geesh, I thought that RISKS readers
knew better.

Yes, people do make mistakes, but as I and many others have

repeatedly pointed out, in complex systems, there is seldom a single point of failure, so to trying to assess "the" cause of an error is counterproductive. Yes, it feels good to be able to blame some person or thing, but this is what I have called the "blame and train" philosophy. It fails to fix the complex underlying causes.

If there really is a single point of failure, especially one that repeats over time, the proper response is to make the system insensitive to this problem. If we know that a system component is noisy or error-prone (a transducer, say, or a noisy transmission line), we take care to design the system so as to be tolerant of those problems. We use error-correcting codes, or redundancy or we change the procedures. This is frequent with mechanical and electronic components, but almost never with people. When people err in this fashion, we punish them, which does nothing to get at the real cause. We know people transpose digits, confuse complex directions, and make other well-known and simple errors. Therefore it is a system error not to have designed the system to be tolerant of these problems.

Morrell gives the following example: "The most common mistake, at its core, was raw human misunderstanding: conceptual misunderstanding leading to misinterpretation of medical data (surgeons who thought the higher the bacterial MIC number, the better the antibiotic, when the reverse is true...)"

Gee, what stupid surgeons -- at least that is what we are supposed to believe. Even this simple example is open to question. These surgeons sound incompetent: why couldn't they remember that higher MIC numbers are bad?

Well, how many arbitrary little rules do surgeons have to remember? Note that the human default is that high numbers are good (and that "up" maps to "higher," "more," "larger," "louder," etc. - all of which usually are interpreted as "good." In general, larger numbers mean better (hence all the jokes about excellent golf and bowling scores). So assuming that high MIC is better makes sense.

For me to understand whether this was surgeon stupidity or a system problem, I would ask how many such rules had to be learned, how consistent where they, and how frequently did this one come into play. Indeed, what is the meaning of an MIC number? A quick Internet search reveals these two definitions of MIC (from very different sources):

Definition 1: "The MIC of a drug is defined in broth as the lowest concentration that prevents visible turbidity of the broth following the overnight incubation of 10^5 - 10^6 colony forming units (CFU)/ml (obtained during the log phase of growth)."

Definition 2: "The lowest concentration of antimicrobial agent that inhibits the growth of the microorganism is the minimal inhibitory concentration (MIC). The MIC and the zone diameter of inhibition are inversely correlated (Fig. 10-5). In other words, the more susceptible the

microorganism is to the antimicrobial agent, the lower the MIC and the larger the zone of inhibition. Conversely, the more resistant the microorganism, the higher the MIC and the smaller the zone of inhibition."

(I am tempted to say: case closed. Quick: is high MIC good or bad? Rule of thumb: Any definition that has to contain the phrase "in other words" is a definition in trouble. In this case, after reading the "in other words" phrase, I still don't know. I think this means that a High MIC number is good for the organism, but bad for the physician trying to kill it. I still have no idea of how this translates into the MIC rating for an antibiotic.)

Folks, there are major system errors here. Don't be so quick to blame the people, even if surface evidence indicts them. The problems are rich, complex, and deep. MIC is perhaps a wonderful term for scientists, but it is a bad term to be used by practitioners. I sympathize with the surgeons. We need system thinking, and a deep understanding of the complex context in which medicine is practiced before we can assess blame and before we can start to fix the problem, whether with technology or not.

The RISK here is enormous. Well-meaning people claim that technology will fix the problem of medical errors. Nonsense. Technology is a tool, and whether it is effective or even more damaging depends upon how it is deployed. Thinking there is a single source of error - and therefore a single problem to be solved -- will lead us to even worse problems.

Don Norman, Nielsen Norman Group
Northwestern University norman@nngroup.com www.jnd.org

⚡ Why IE is insecure: flawed logical thinking...

<Craig DeForest <deforest@boulder.swri.edu>>

Thu, 24 Mar 2005 09:29:34 -0700

IE appears to be insecure in part because of flawed logical thinking by its development team.

There is currently a debate of sorts in the news between Mitchell Baker ("chief lizard wrangler" of the Mozilla Foundation) and Dave Massy (head developer of Internet Explorer) over which web browser is more secure. In a recent ZDNET article (also covered on Slashdot; see links at end), Baker points out that, since IE is tightly coupled to the Microsoft Windows operating system, it is bound to be less secure than Mozilla, which is well separated from its host OS.

Dave Massy's reply is very interesting (link at bottom):

>The issue of not being part of the OS is an interesting one though that

>is frequently the subject of misunderstanding. IE is part of [Microsoft

>Windows] so that parts of the SO and other applicaaitons [sic] can rely on

>the functionality and APIs being present. IE in turn relies on OS

>functionality to do it's [sic] job. To be clear there are no OS APIs that

>IE uses that are not documented on MSDN as part of the

platform SDK and

>available to other browsers and any other software that runs on Windows.

Dave is making a flawed argument:

Premises:

- IE uses a documented interface to the OS
- The OS interface is available to other software on the OS

Conclusion:

- The complexity of our interface is irrelevant to security

The argument is wrong for two reasons: there is a false hidden premise (that the OS is bulletproof); and the argument itself is invalid (even if the hidden premise were true, the conclusion would not follow).

One only need read back-issues of RISKS to find case after case of complex, unanticipated failure modes in complicated interfaces, each element of which is thought to be secure. That lesson is at least 30 years old -- I am thinking of the stories about hidden data channels in Multics.

This is of interest to RISKS readers because it is a stunning example of poor design by flawed logic: even if the IE coding were flawless at the subroutine level (we can bet that it isn't), Dave's stated attitude toward interface security would doom it to be susceptible to attack.

References:

http://news.zdnet.com/2100-9588_22-5630529.html

<http://blogs.msdn.com/dmassy/archive/2005/03/22/400689.aspx>

<http://slashdot.org/article.pl?>

[sid=05/03/24/1352211&tid=113&tid=154](http://slashdot.org/article.pl?sid=05/03/24/1352211&tid=113&tid=154)

✦ Re: Risks of long and short URLs ([RISKS-23.80](#))

<"D.F. Manno" <dfm2a3l0t2@spymac.com>>

Thu, 24 Mar 2005 21:32:32 -0500

In [RISKS-23.80](#), Arthur T. writes of a shortcoming with using tinyurl.com as a substitute for typing long URLs, that being that you do not know where a tinyurl will take you.

The links created by Makeashorterlink <<http://www.makeashorterlink.com>>

first take you to a page displaying the URL that you are to be redirected to, giving you the opportunity to bail out if you don't want to go there.

D.F. Manno dfm2a3l0t2@spymac.com

✦ Risky US Bank Visa product

<"John Meissen" <john@meissen.org>>

Thu, 24 Mar 2005 01:14:00 -0800

US Bank has a Visa product targeted at teens (or rather, their parents), called VisaBuxx. It looks and acts like a standard Visa-logo debit card, but is more like a prepaid phone card - you pre-load it with value, and it's not directly tied to any bank account.

Their web site and marketing literature talk about being able to easily add value to the card by transferring money online from an existing US Bank

checking account. Unfortunately, the system leaves a lot to be desired.

The usbank.com website has a link for the VisaBuxx program. When you click on it you're redirected to another site, called visabuxx.com. This site is apparently run by someone called "WildCard Systems". In order to transfer money from your US Bank checking account to the card you have to provide WildCard Systems with your checking account number and routing information and authorization to pull funds from the account, or give them your own debit card number. While WildCard Systems may be honorable and trustworthy, the risks in this are so obvious that it's painful. Meanwhile, the Terms Of Service published on the site go to great lengths to explicitly disavow any responsibility for anything bad that might result from the use of the site.

The correct way for the bank to have implemented this would have been to provide the ability to associate the card with your existing Internet banking identity, and then let you log in through the bank's website and tell them to send money from an account to the card rather than allowing the card operators to pull money from your account. Having the ability to provide account data to the VisaBuxx website is useful for non-US Bank customers, but a legitimate US Bank customer I shouldn't be forced to do it.

I find it mind-boggling that financial corporations still can't see the obvious when it comes to protecting customer account data. When dealing with

an official bank product I should NEVER have to tell the application anything about my accounts.

⚡ Important PITAC Cybersecurity report released

<Gene Spafford <spaf@cerias.purdue.edu>>

Fri, 18 Mar 2005 12:29:22 -0500

[As a member of the PITAC and a co-author of the report, I strongly encourage people will take time to read this and think about how to help carry out the recommendations. --spaf]

PRESIDENT'S INFORMATION TECHNOLOGY ADVISORY COMMITTEE RELEASES
NEW REPORT
CYBER SECURITY: A CRISIS OF PRIORITIZATION

Vital to the Nation's security and everyday life, the information technology (IT) infrastructure of the United States is highly vulnerable to disruptive domestic and international attacks, the President's Information Technology Advisory Committee (PITAC) argues in a new report. While existing technologies can address some IT security vulnerabilities, fundamentally new approaches are needed to address the more serious structural weaknesses of the IT infrastructure.

In *Cyber Security: A Crisis of Prioritization*, PITAC presents four key findings and recommendations on how the Federal government can foster new architectures and technologies to secure the Nation's IT infrastructure.

PITAC urges the Government to significantly increase support for fundamental research in civilian cyber security in 10 priority areas; intensify Federal efforts to promote the recruitment and retention of cyber security researchers and students at research universities; increase support for the rapid transfer of Federally developed cyber security technologies to the private sector; and strengthen the coordination of Federal cyber security R&D activities.

To request a copy of this report, please complete the form at <http://www.nitrd.gov/pubs/>, send an e-mail to nco@nitrd.gov, or call the National Coordination Office for Information Technology Research and Development at (703) 292-4873. Cyber Security: A Crisis of Prioritization can also be downloaded as a PDF file by accessing the link at <http://www.nitrd.gov/pubs/>.

About PITAC

The President's Information Technology Advisory Committee (PITAC) is appointed by the President to provide independent expert advice on maintaining America's preeminence in advanced information technology. PITAC members are IT leaders in industry and academia representing the research, education, and library communities, network providers, and critical industries, with expertise relevant to critical elements of the national IT infrastructure such as high-performance computing, large-scale networking, and high-assurance software and systems design. The Committee's studies help guide the Administration's efforts to

accelerate the development and adoption of information technologies vital for American prosperity in the 21st century.

Contact: "Alan S. Inouye 1-703-292-4540" <inouye@nitrd.gov>

✶ EEPI - Electronic Entertainment Policy Initiative

<Lauren Weinstein <lauren@eepi.org>>

Fri, 25 Mar 2005 12:38:04 -0800 (PST)

I'm pleased to announce "EEPI" (<http://www.eepi.org>), a new initiative aimed at fostering cooperation in the areas of electronic entertainment and its many related issues, problems, and impacts.

I've teamed with 30+ year recording industry veteran Thane Tierney in this effort to find cooperative solutions to technical, legal, policy, and other issues relating to the vast and growing range of electronic technologies that are crucial to the entertainment industry, but that also impact other industries, interest groups, individuals, and society in major ways.

There are many interested parties, including record labels, film studios, the RIAA, the MPAA, artists, consumers, intellectual freedom advocates, broadcasters, manufacturers, legislators, regulators, and a multitude of others.

The issues cover an enormous gamut from DVDs, CDs, and piracy issues to

multimedia cell phones, from digital video recorders to Internet file sharing/P2P, from digital TV and the "broadcast flag" to the Digital Millennium Copyright Act (DMCA) and "fair use" controversies.

Working together, rather than fighting each other, perhaps we can all find some broadly acceptable paths that will be of benefit to everyone.

For more information, please see the EEPI Web site at:

<http://www.eepi.org>

A moderated public discussion list and an EEPI announcement list are now available at the site.

Public participation is cordially invited. Thank you very much.

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

+1 (818) 225-2800 <http://www.eepi.org> <http://www.pfir.org/lauren>

<http://lauren.vortex.com> <http://www.pfir.org> <http://www.vortex.com>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 82

Tuesday 29 March 2005

Contents

- [Times change ... problems don't](#)
[Michael Bacon](#)
 - [Unintended consequences: CA data theft reporting](#)
[Steve Summit](#)
 - [Even some major corporations don't understand domain names](#)
[Jonathan Leffler](#)
 - [Re: Cruise-control failures?](#)
[Stanislav Meduna](#) [Steve Loughran](#) [Nick Brown](#) [Robert Scheidt](#) [Ray Todd Stevens](#) [Mark Brader](#)
 - [Re: Don Norman: High is good?](#)
[Ken Knowlton](#)
 - [Re: Computerized medical mistakes](#)
[Dave Brunberg](#) [Bob Morrell](#) [Richard Cook](#)
 - [Re: More uses of satnav/GPS](#)
[Chris Smith](#)
 - [Re: Remote physical device fingerprinting](#)
[David E. Ross](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Times change ... problems don't

<"Michael \ (Streaky\) Bacon" <himself@streaky-bacon.co.uk>>

Mon, 28 Mar 2005 10:49:11 +0100

On 27 Mar 2005, the UK put its clocks forward one hour. This apparently caused problems for Barclays Bank - one of the UK's leading banks - with ATMs and other online services unavailable to customers in the South of the country. The text of the Daily Telegraph's report on the failure is reproduced below.

<http://www.telegraph.co.uk/news/main.jhtml;sessionid=3D4HHCXBASXCNU5QFIQMGC5WAVCBQUJVC?xml=3D/news/2005/03/28/nbarc28.xml&sSheet=3D/portal/2005/03/28/ixportal.html>

I would be surprised if the bank relied upon the actions of a human to change the time on its servers. For example, if the servers are not time synchronised through an atomic clock receiver or from an NTP Time Server, it begs serious questions regarding the time-standing of transactions.

Bi-annual time changes have been a part of computing at least since the first commercial systems began processing. Surely 54 years is not too short a time to have worked out the risks and put in place procedures to deal with them.

If it was indeed a human error, perhaps the heading on the relevant page should read: "Spring forward, fall back".

Another puzzling factor is that it apparently took 11 hours (4 am to 5 pm) to determine and correct the problem. In my experience, the first thing to be blamed is the last thing that was changed.

Michael 'Streaky' Bacon

Summer Time slip-up forces Barclays' cashpoints to close
The Daily Telegraph, 28 March 2005

Millions of Barclays customers were unable to withdraw money yesterday after the bank's cashpoint network crashed amid claims that a duty manager had accidentally put the clocks back instead of forward. More than 1,400 auto-tellers in the south of England and some on-line services were out of order. Barclays customers were unable to withdraw money from any bank, while cardholders with other banks were unable to use Barclays cash machines.

The error came to light at 4am on 27 Mar 2005 when technicians noticed that customers' personal details were not being forwarded to the computers that control much of the bank's infrastructure. The problem was eventually resolved at 5pm. Executives trying to determine the cause of the problem admitted that a mistake during the switch to British Summer Time could have been to blame. Customer services staff were less ambiguous. One admitted: "A manager put the clocks back instead of forward and that has caused enormous problems."

The bank's British network uses two servers based in Gloucestershire: one

for operations north of the Wash and the other to control operations in the South. The Gloucester South server is understood to have been set one hour back instead of forward. The bank conceded that an error over the time change was to blame but denied that an individual manager made the mistake. Alistair Smith, a spokesman for the bank, said: "It seems that this problem may somehow be related to the time change, although I am told it was not to do with someone making a mistake while manually changing the time."

✶ Unintended consequences: CA data theft reporting

<Steve Summit <scs@eskimo.com>>

Tue, 29 Mar 2005 12:27:39 -0500

A laptop computer containing names, SSNs, and some addresses and birthdates for 98,369 alumni, grad students and applicants was stolen from an office at UC Berkeley. In compliance with California's new data-theft reporting law, the breach was reported and has now been widely publicized -- although ironically, as a writeup on slashdot points out, this publicity may have alerted the thief, who was probably only interested in the hardware, to the true value of his find.

Links:

<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2005/03/28/financial/f151143S80.DTL>

<http://yro.slashdot.org/article.pl?sid=05/03/29/036237>

✦ Even some major corporations don't understand domain names

<Jonathan Leffler <jleffler@earthlink.net>>

Wed, 23 Mar 2005 23:17:49 -0800

Case in point, the agreement (Enrollment E-Consent) you are asked to accept when you sign up for Hertz #1 Gold membership - at

<https://www.hertz.com/servlet/JoinProfileServlet?club=G>

Right at the bottom, where your consent is sought, there's a footnote that says:

* "Any Hertz rental website" or "the Hertz rental website" means any Hertz website relating to vehicle rentals including, without limitation, all websites with addresses which begin "www.hertz".

The relevant text, much further up the document, is:

Disclosures to You by Hertz

1. Summary of Your Consent. At the bottom of this page, after you have reviewed these disclosures, you will be asked to give your consent (your "Consent") to Hertz's use of an electronic record rather than paper format to provide or make available to you the following information (the "Information") via any Hertz rental website* or by e-mail (collectively "Electronic Record(s)"), subject to the conditions

and other requirements discussed below:

I first noticed this several years ago - and reported it to the web master.

I don't recall getting any response, and the web site today shows that I didn't get the message through to anyone.

Clearly, if I own a domain bogus.tld, I can create a www.hertz.bogus.tld

site and there's nothing to stop Hertz using any information submitted

there - I'm not sure how they'd get hold of information submitted to my

hypothetical web site. It'd be cute mistake for a Mom'n'Pop outfit to

make; it is more serious when it's a major international corporation that

is suffering from technical myopia.

Jonathan Leffler Guardian of DBD::Informix v2005.01 -- <http://dbi.perl.org/>
jleffler@earthlink.net, jleffler@us.ibm.com

✶ Re: Cruise-control failures? (Scheidt, [RISKS-23.81](#))

<Stanislav Meduna <stano@meduna.org>>

Mon, 28 Mar 2005 22:40:55 +0200

> I wonder if somebody on this board has some insight on how the electronic

> controls of modern cars are designed

AFAIK technically it is a distributed control system with quite many

relatively independent units communicating through a bus (typically CANbus).

> and especially if a single component's failure (such as a
common
> microprocessor) could affect multiple functions (e.g.,
acceleration and
> brakes).

The various ESPs (electronic stability programs) are able to
reduce engine
power and apply selective braking on some wheels in order to
stabilize the
vehicle. So there already is something that can give commands to
both the
brakes and the engine. I have no idea how (im-)probable is that
kind of
failure mode, though.

Re: Cruise-control failures? (Scheidt, [RISKS-23.81](#))

<Steve Loughran <steve.loughran@gmail.com>>

Tue, 29 Mar 2005 20:34:49 +0100

In [RISKS-23.81](#), Robert Scheidt expresses doubt that a hung cruise
control system would stop braking, in "Cruise-control failures"

I can't assess that, but I do know that the handbrake/parking
brake on a
2004 Renault Scenic is CPU controlled, by the system that
manages the
ignition.

When you pull out the 'ignition card", the parking brake engages
automatically. There is also a handle you can pull below/left of
the
steering wheel, which sends a request to turn parking on. There
was a bit of
a lag engaging, as I recall from my weeks rental, say 0.5s or so.

How does it disengage? Well, there is the fun part. The parking

brake

disengages when you drive off. This seems like a convenient feature, but was certainly a disadvantage when I rented the car in the Alps for a week -even without any of these 'cruise control failure' disasters.

The problem was simple: how do you turn round on a sloping mountain road near grenoble, when the snow has got too deep for you to continue.

In a conventional car, the solution is the three-point turn, executed with maximum care. You back up and turn, then go forwards, completing the turn.

This is actually a manoeuvre which is part of the UK driving test, albeit on a flat road. To do it safely on a mountain road you need to

1. Make sure you are in a gear that is going in the correct direction, so as not to drive off the edge of the (steep, unprotected) drop.
2. With a manual transmission, bring up the clutch slowly until the transmission is engaged. This stops you slipping (the hill start), and provides an extra cue that you have (#1) right.
3. Move off very gently as you release the handbrake. This is your final sanity check.

The key point here is the failure mode "driving off the edge of the road" is not something you want to encounter, nor is "sliding down the hill as you set off".

Unfortunately, the Renault Scenic, with its automatic handbrake, doesn't let you do any of these. You cant bring up the clutch under gentle

acceleration

(check 2), as the handbrake comes off too early. The only way to do a hill start is put your foot down enough to be sure that when the handbrake comes off, you aren't go slide backwards. This eliminates any chance of making sure that you are in the right gear through tentative car motions.

Let's just say I wasn't happy with the whole process. We did turn round safely; I am writing this email. But I had to check and doublecheck the gear lever settings before each step in the process, and it was no fun at all.

An interesting footnote is what would have happened if I'd got it wrong? I'd have driven off a cliff and not been found until later in the spring. At that time, I am sure the cause of the crash would have been attributed to "driver error", and not system failure. This is so reminiscent of assigning "pilot error" to any crash of an airplane with no obvious mechanical cause. This is something that should be so familiar to RISKS readers, be it related to A320 flight control systems. Chinook fog navigation, etc, etc. Are we going to replicate these incidents with drive-by-wire car control systems?

✶ Re: Cruise-control failures? (Scheidt, [RISKS-23.81](#))

<"BROWN Nick" <Nick.BROWN@coe.int>>

Tue, 29 Mar 2005 15:13:56 +0200

In any car that I have ever seen, cruise control has been an option installed late in the assembly process. In some cases, the marketing department has decreed that you can't buy the car without cruise control, but it's not something that is generally built in "deep down" in the system. Cruise control is typically a fairly dumb system - "all" you have to do is to detect the current road speed and apply more or less pull on the throttle cable to compensate. In all the cars which I have driven with cruise control, you can feel the accelerator pedal drop slightly when you hit an uphill climb. And cruise control after-market modules are widely available.

The basic brake system of "most" (all?) modern cars - certainly including the Renault "Vel Satis" and "Laguna" models allegedly involved in the widely-publicised cruise control issues - is essentially a very simple hydraulic circuit. ABS, EBD, etc modules may be able to cut in and remove pressure from the circuit momentarily, but you'll generally know about that (at least in the case of ABS) from the noise. Aside from that, there's a direct mechanical/hydraulic, cause-and-effect relationship between the brake pedal and the wheels. Additionally, braking systems are designed so that the force which can be applied exceeds the force which the engine can provide by a substantial factor.

So in the Renault cases, while it's entirely possible that a number of independently-designed and unconnected mechanical systems

(brakes, throttle, gear lever, ignition key or card) failed simultaneously, it's also possible that the driver made a mistake (honest or otherwise). It has been reported that the driver in the first incident (October 2004) had just had his driver's license restored after a four-year ban for various speeding and alcohol-related offences; perhaps he thought he'd been "flashed" by a speed trap and needed an excuse? And after that, anyone who wants to get on TV can just call and say their Renault's cruise control blocked; it's "another claimed incident", and why should anyone check if it really happened, if it makes a good story?

When the first incident occurred, it became an excuse for every columnist who has ever had an expensive electronic module replaced in their car, to get on their high horse about "how there's too much electronics and software in cars these days". This ignores the generally superior reliability of electronics - although it's maybe not much comfort if you have a \$600 part to replace, that 10 other people have been saved \$80 each - and also the fact that without electronics, car manufacturers would be unable to meet emissions standards, thereby incurring the wrath of much the same group of journalists.

A few years ago in the UK, there was a related incident when a trucker claimed that a stuck throttle cause him to be unable to stop his truck on a busy highway. It was later revealed (but not on the front page) that he was

undergoing psychiatric treatment for an attention-seeking disorder...

✶ Re: Cruise-control failures? (Scheidt, [RISKS-23.81](#))

<"Robert Scheidt" <robertscheidt@tiscali.be>>

Tue, 29 Mar 2005 16:07:03 +0200

Nick, Thanks for your reply. Please note that I am not taking sides on this, just being curious, and I am not an owner of one of those renault cars. I also had no accident recently where I need this as an excuse and don't plan any.

Regarding your first remark I would like to mention that cruise control is in my opinion now part of the system in newer cars. The gas pedal does not move as part of speeding up or going up a hill. In fact the gas pedal just gives an electric signal to the electronic injection system and there is no mechanical connection. This is true for my current car (Honda accord 2004) and was true in my previous car (bmw 530d 2000) and to the best of my knowledge it is implemented in such a way also in the Renault cars involved.

Regarding the brakes I hope of course that there is no relation with the cruise control. However many cars (including some of the renault models) have now more dynamic controls, like for anti-skidding where brakes on one of the rear wheels is activated when some detection that the car

skids in
one or the other directions is detected. And this happens
without having to
press the brake pedal. Mercedes started this a few years ago and
it is now
widely used (including in my Honda)

The other possibility I could think about, it that if the cruise
control
goes indeed get stuck or blocked (for whatever reason) and does
not
deactivate when pressing the brake pedal, the driver may have
the impression
that the brakes are ineffective since the cruise control will
counteract
with the brakes by speeding up the car whilst the brake pedal is
being
pressed.

See that you are living in Strasbourg. I was born in a village
not far away
(Mundolsheim) and lived there until I started traveling as a
computer
specialist in the 1970's. Now living in Brussels.

✶ Re: Cruise-control failures?

<"Ray Todd Stevens" <raytodd@kiva.net>>
Tue, 29 Mar 2005 08:12:03 -5

This would not take a common microprocessor. It would not even
take a
microprocessor although there might be one for the anti-lock
brakes which
are common on today's cars. Brakes when they operate turn
forward motion
and turn it into heat. In doing so the brakes themselves heat
up --- a lot.

Now in normal use they can quickly cool down because you reach a speed of zero, and either wait for a bit, or stop braking and start going again. Either way they can cool down. However, if they are used enough they don't get a chance to cool. This is a problem in race cars and they use special brake pads because of this. It is not normally a problem in street cars. However, if you are trying to override the accelerator with the brakes the brakes will in fact overheat. This can cause the brakes to work less well. Eventually if you get them hot enough the fluid can boil, and cause the feedback issue that has been mentioned.

The real question is why do they make cars where the computer also controls turning the engine off and on?

✶ **Re: Cruise-control failures? (Scheidt, [RISKS-23.81](#))**

<msb@vex.net (Mark Brader)>

Tue, 29 Mar 2005 13:05:15 -0500 (EST)

Perhaps the loss of braking is really a loss of power braking due to the ignition switch being off? Then the brake pedal still works, but requires more pressure, so it seems to be resisting.

Mark Brader, Toronto, msb@vex.net

⚡ Re: Don Norman: High is good?

<KCKnowlton@aol.com>

Mon, 28 Mar 2005 18:20:33 EST

In his otherwise well reasoned mini-essay, I take issue with Don Norman's statement ([RISKS-23.81](#)) regarding what is interpreted as "good".

My own recent blood work report gives the measured concentrations, counts, etc., along with "reference ranges" of acceptable values:

34 instances of the form	m < acceptable < n	i.e., higher or lower are bad
6 instances of the form	acceptable < n	i.e., low is good
1 instance of the form	m < acceptable	i.e. high is good

This suggests that doctors, in particular, are in general not likely to assume that "high numbers are good."

⚡ Re: Human error and computerized medical systems (Norman, [RISKS-23.81](#))

<"Dave Brunberg" <DBrunber@FBLEOPOLD.com>>

Mon, 28 Mar 2005 16:31:07 -0500

(I am tempted to say: case closed. Quick: is high MIC good or bad? Rule of thumb: Any definition that has to contain the phrase "in other words" is a definition in trouble. In this case, after reading the "in other words" phrase, I still don't know. I think this means that a High MIC number is good for the organism, but bad for the physician trying to kill

it. I still
have no idea of how this translates into the MIC rating for an
antibiotic.)

The definition is quite clear, in fact I (not a medical doctor)
understood
why a low MIC indicates acceptable antibiotic performance of a
drug upon
reading the original article (Morrell, [RISKS-23.79](#)).

The definition makes clear that the MIC refers to the minimum
dose that
provides suitable antibiotic performance. The text, "The MIC of
a drug is
defined in broth as the lowest concentration that prevents
visible turbidity
of the broth following the overnight incubation of 10⁵-6 colony
forming
units (CFU)/ml (obtained during the log phase of growth),"
cannot get more
clear on this. All that is required for a complete
understanding is
knowledge of the word "turbidity" and why measured turbidity in
a previously
clear solution indicates pathogenic growth.

In this respect I must disagree with Mr. Norman, and submit that
a surgeon
who can't be bothered to remember (or figure out as quickly as I
did) the
more desirable relative magnitude of a MIC, should be giving his
work
considerably more thought.

David W. Brunberg, Engineering Supervisor, The F.B. Leopold
Company, Inc.

✦ Re: Computerized medical mistakes (Cook & Norman, [RISKS-23.81](#))

<"Bob Morrell/Cancer Center" <bmorrell@wfubmc.edu>>

Mon, 28 Mar 2005 18:16:18 -0500

The responses to my note concerning the original *JAMA* article on computer assisted mistakes miss my point entirely. Richard Cook discusses at length the problems of complex mistakes and cites Three Mile Island and other complex systems. Don Norman googles himself into trouble by trying to figure out what an MIC is. Like many a googler, he got the definition right, but lost on context. Meanwhile, off thread I discussed the nature of mistakes in the medical environment. Several people sought information on detected medical mistakes. I cautioned against looking for the complex, obscure mistake and instead suggested they target "simple" problems in an overworked, high volume system. "Aim low" I suggested, having observed that most mistakes that I found were simple mistakes dealing with basic medical ideas that preceded computers, computerized systems and were taught to first year medical school students, but forgotten, ignored or overlooked by overworked staff. The fact that computerized systems did nothing to help alleviate these errors is lamentable, but has nothing to do with the mistake, and in fact the error, conceptually preceded computers. Amputating the wrong limb is not a computerized mistake, an adult dose to a pediatric patient is not convergence of multiple errors. Picking the wrong antibiotic based on a confused memory of which is best (high or low) is more understandable to layman, but to the physician proud of how many undergrad

and others he had to be better than to become a doctor, it is insulting. When an in-house reviewer reviewed an appendix of mistakes on our first publication, he scribbled in the margins: "this is going to make some of our doctors look like blockheads". This doctor did not consider these mistakes the product of a complex interaction of events, but something that could have been avoided with simple thought and professionalism.

I have no real disagreement with either responder on the problems with the complexity of current medical systems, and the need for expensive and comprehensive reform. What I disagree with, as someone who watched real mistakes being made is the idea that that the bulk of mistakes being made in a hospital environment resemble the complex chain of events that occur in airline crashes or nuclear reactor accidents. I am sorry, I have worked my entire professional life in a hospital, and it is far less regulated and far more human, and has far fewer layers of protection between the patient and a serious mistake. Are complex systems introducing new mistakes? No doubt. But the mistakes my system found routinely were simple, and embarrassing to those that made them.

My point was that before we chase the complex mistakes, we need to first deal with the simple ones.

✶ Re: Computerized medical mistakes (Morrell, [RISKS-23.82](#))

<Richard Cook <topquarkguy@sbcglobal.net>>

Mon, 28 Mar 2005 17:49:20 -0600

Bob, Thanks for your note. It was charitable of you to send it. I am afraid that we are in rather serious disagreement here. There is no misunderstanding on my part or on Don Norman's. We understood you perfectly. What you wrote was simply wrong. The 'aim low' argument is nonsense as is the contention that these are 'simple' mistakes. Don and I have written enough to make all this clear.

[This has been a very interesting discussion. However, I think the basic

points have now been adequately made. As I noted in [RISKS-23.81](#), the

bottom line is that blame can often be distributed variously and

generously! Thanks to the contributors (who have serious credentials) and

to the RISKS readers for staying with us! PGN]

Re: More uses of satnav/GPS ([RISKS-23.80](#))

<Chris Smith <smith@interlog.com>>

Thu, 24 Mar 2005 01:39:31 -0500 (Eastern Standard Time)

In [RISKS-23.80](#), Roland Giersig makes two assertions that I do not believe to be correct.

While discussing railroad safety and communication, he states that, for

example, if "track-side communication to the on-board units fails, then the

system falls back to a state where the train pilot has to

navigate by sight
instead of relying on the electronic systems. And this is
perfectly safe,
unlike in air-traffic-control."

Every system will have its limitations. Even navigation by sight
is not
perfectly safe. I refer you to the Canadian Transportation
Safety Board
Investigation Report on the derailment and collision at
Thamesville,
Ontario, 1999 April 23, at
<http://www.tsb.gc.ca/en/reports/rail/1999/r99h0007/r99h0007.asp>

The train involved was navigating by sight, in midday, under
reasonable
conditions. After noting a switch target indicating an
incorrectly
positioned crossover, the crew did not have sufficient time to
prevent the
subsequent derailment and collision with parked and loaded cars
on a siding.

Many times, your most reliable safety measure is an alert and
informed human
somewhere in the system. In the 10 seconds between observing the
switch
target and the derailment, the crew fully applied emergency
braking, shut
down the main diesel engine, and transmitted and then repeated
an emergency
stop message to a train approaching within two minutes in the
opposite
direction, successfully preventing a far greater tragedy than
did occur.
Both of the train crew in the engine were killed - the only
deaths in the
accident. For their actions, both were posthumously awarded the
Meritorious
Service Medal by the Governor General of Canada.

Second, he highlights the statement that "The danger lies in the
unknown

accuracy of the GPS signal!!" I do not believe the accuracy of the GPS signal is unknown. Many GPS units report EPE - Estimated Position Error, which is an estimate of the accuracy of the GPS signal. It is the estimated error for a 1-sigma level of confidence. A 3-sigma, 95% confidence level, error measure can be calculated by multiplying the given EPE by 3. (Some low-end handheld units are reported to stray from this definition.)

With many GPS units delivering 3 metre accuracy, a 95% confidence level with an accuracy of 9 metres would be possible under many conditions. With a GP40 engine measuring 18 metres overall, accuracy comparable to the size of the engine should be possible, and verifiable, in many cases. Of course, it is still necessary to actually design the control system to take advantage of this information.

Ultimately, it appears that developers of such systems can fail twice - once by not leveraging all the information provided by the positioning system, and again by not providing useful human interfaces (both informational and control) in the event of either positioning failures or degraded accuracy.

⚡ Re: Remote physical device fingerprinting (Roth, [RISKS-23.80](#))

<"David E. Ross" <david@rossde.com>>
Wed, 23 Mar 2005 17:09:33 -0800

Clock Skew

I have an NTP (Network Time Protocol) client installed on my PC. Every hour (and additionally when I manually request), it resynchronizes my clock to NTP servers around the world. Querying five servers (from a list of 164 servers), it uses results from the "best" based on a scoring algorithm. Since different scores might result at different querying events, I keep resynchronizing to different NTP servers with differing skews. If any of the five servers gets a really poor score, it drops out of the chosen five; and another server from the list of 164 joins the five.

To defeat fingerprinting based on clock skew, all I have to do is change the option for the resynchronization period to a shorter interval.

David E. Ross <URL:<http://www.rossde.com/>>

I use Mozilla as my Web browser because I want a browser that complies with Web standards. See <URL:<http://www.mozilla.org/>>.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 23: Issue 83

Wednesday 6 April 2005

Contents

- [Cancer patients exposed to high radiation](#)
[Monty Solomon](#)
- [Carjackers swipe biometric Mercedes, plus owner's finger](#)
[John Lettice via Alpha Lau](#)
- [Air disasters: A crisis of confidence?](#)
[Michael Bacon](#)
- [Secret Service DNA - "Distributed Networking Attack"](#)
[Brian Krebs via Monty Solomon](#)
- [Yet another phishing scam](#)
[Michael Bacon](#)
- [Times change ... problems don't](#)
[Louise Pryor](#)
- [Re: Why IE is insecure ...](#)
[Steve Taylor](#) [Simon Zuckerbraun](#) [Craig DeForest](#)
- [Re: Remote physical device fingerprinting](#)
[Jerry Leichter](#)
- [Re: Cruise Control failures](#)
[Jay R. Ashworth](#) [John Sawyer](#) [Neil Maller](#) [Markus Peuhkuri](#) [David G. Bell](#) [Amos Shapir](#)
[David R Brooks](#)
- [New Security Paradigms Workshop submission deadline approaching](#)

[George Robert Blakley III](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Cancer patients exposed to high radiation

<Monty Solomon <monty@roscom.com>>

Sun, 3 Apr 2005 22:37:38 -0400

77 patients at the H. Lee Moffitt Cancer Center and Research Institute cancer treatment center were exposed to radiation levels 50% stronger than they were supposed to receive because a radiation machine was improperly installed. Physicists from the federal Radiological Physics Center detected the error on 7 Mar, but it was not acknowledged until 1 Apr. According to a report by the Florida Bureau of Radiation Control, a physicist calibrating the machine used an incorrect formula. Certain side-effects (headaches and speech and memory loss) reportedly can take from 3 to 12 months to develop. Twelve patients subsequently died (although the article did not indicate whether it was as an iatrogenic result of the overdosing or just progressed cancer). [Source: AP item in *The Boston Globe*, 2 Apr 2005; PGN-ed]

http://www.boston.com/yourlife/health/diseases/articles/2005/04/02/cancer_patients_exposed_to_high_radiation/

✶ Carjackers swipe biometric Mercedes, plus owner's finger

<Alpha Lau <avlxyz@yahoo.com>>

Mon, 4 Apr 2005 23:26:01 -0700 (PDT)

Carjackers swipe biometric Merc, plus owner's finger

By John Lettice - 4 Apr 2005

A Malaysian businessman has lost a finger to car thieves impatient to get around his Mercedes' fingerprint security system. Accountant K Kumaran, the BBC reports, had at first been forced to start the S-class Merc, but when the carjackers wanted to start it again without having him along, they chopped off the end of his index finger with a machete.

The fingerprint readers themselves will, like similar devices aimed at the computer or electronic device markets, have a fairly broad tolerance, on the basis that products that stop people using their own cars, computers or whatever because their fingers are a bit sweaty won't turn out to be very popular.

They slow thieves up a tad, many people will find them more convenient than passwords or pin numbers, and as they're apparently 'cutting edge' and biometric technology is allegedly 'foolproof', they allow their owners to swank around in a false aura of high tech.

http://www.theregister.co.uk/2005/04/04/fingerprint_merc_chop/

And that is exactly where the risks lie, high-tech does not necessarily mean high-security!

At least in sci-fi, fingerprint systems check for a heartbeat or pulse!!!

[`Cutting edge', eh? Wow! Incidentally, for many years I've been citing the concept of an amputated finger as a hypothetical way of defeating a poorly designed fingerprint analyzer. It's no longer hypothetical. PGN]

✈️ Air disasters: A crisis of confidence?

<"Michael \ (Streaky\) Bacon" <himself@streaky-bacon.co.uk>>
Tue, 5 Apr 2005 10:42:47 +0100

Air disasters receive widespread press coverage. Crashes often cause people to cancel bookings with the affected airline. The share price often dips, sometimes severely, in the aftermath of an air accident.

This is also true for many other major incidents involving corporations (i.e., not 'natural' causes).

One thing often stands between a 'crisis of confidence' and 'business as usual', and that is the credibility of the organisation's spokespeople.

On 3 April, a Phuket Air 747 was twice forced by passenger action to abort a take-off from the UAE when fuel was seen flowing from the wing over an engine as the plane accelerated down the runway. A UK-based spokesman for the airline told the media that no-one had been in any danger and claimed that passengers had "panicked". He is also reported to have said that passengers were not qualified to judge what was safe or not. He said that

the wing tanks had been "over-filled".

Whilst I do not comment upon the accuracy or otherwise of the spokesman's comments, I will comment on their advisability and I do suggest that this is not a good way to manage risk.

It is reported that many passengers have now refused to fly any further with the airline.

A contrast in risk management is provided by one British airline that suffered two 'incidents' with the same type of aircraft some nine years apart. In the first, the aircraft crashed with tragic loss of life following the (erroneous) shutdown of one engine and loss of power on the other (faulty) engine during an emergency landing. The Chairman of the airline was interviewed at the scene and with tears in his eyes promised to find out what had happened and to take every possible step to prevent its recurrence. The share price was not much affected, neither were bookings. The second incident concerned the loss of oil pressure in both engines shortly after take-off - leading to the shut-down of both engines and a successful 'dead-stick' landing. The loss of oil was caused by a maintenance failure. The airline put the 'Director of Engineering' (or similar title) in front of the media, and he attempted to explain away the incident as a problem with their maintenance company. It was reported at the time that passengers subsequently canceled bookings and the stock price fell.

The 'what', the 'way' and the 'how' of the Chairman were believable,
those of the Director were not.

The RISK is in getting the wrong person to say the wrong thing.
Effective
crisis management involves the right thing by the right person
at the right
time in the right way to the right people.

[The first case is that of a British Midland 737-400 ([RISKS-11.42](#)). PGN]

🔥 Secret Service DNA - "Distributed Networking Attack"

<Monty Solomon <monty@roscom.com>>
Wed, 30 Mar 2005 09:07:19 -0500

DNA Key to Decoding Human Factor: Secret Service's Distributed
Computing
Project Aimed at Decoding Encrypted Evidence
Brian Krebs, **The Washington Post**, 28 Mar 2005 [PGN-ed]

For law enforcement officials charged with busting sophisticated
financial
crime and hacker rings, making arrests and seizing computers
used in the
criminal activity is often the easy part.

More difficult can be making the case in court, where getting a
conviction
often hinges on whether investigators can glean evidence off of
the seized
computer equipment and connect that information to specific
crimes.

The wide availability of powerful encryption software has made
evidence

gathering a significant challenge for investigators. Criminals can use the software to scramble evidence of their activities so thoroughly that even the most powerful supercomputers in the world would never be able to break into their codes. But the U.S. Secret Service believes that combining computing power with gumshoe detective skills can help crack criminals' encrypted data caches.

Taking a cue from scientists searching for signs of extraterrestrial life and mathematicians trying to identify very large prime numbers, the agency best known for protecting presidents and other high officials is tying together its employees' desktop computers in a network designed to crack passwords that alleged criminals have used to scramble evidence of their crimes -- everything from lists of stolen credit card numbers and Social Security numbers to records of bank transfers and e-mail communications with victims and accomplices.

To date, the Secret Service has linked 4,000 of its employees' computers into the "Distributed Networking Attack" program. The effort started nearly three years ago to battle a surge in the number of cases in which savvy computer criminals have used commercial or free encryption software to safeguard stolen financial information, according to DNA program manager Al Lewis. ...

<http://www.washingtonpost.com/wp-dyn/articles/A6098-2005Mar28.html>

✶ Yet another phishing scam

<"Michael \(\Streaky\) Bacon" <himself@streaky-bacon.co.uk>>

Mon, 4 Apr 2005 07:09:26 +0100

The Internet payments company PayPal is a natural target for phishing scams.

The latest has both amusing and serious issues.

Received 3 April it refers to "8 April" as the date on which "unusual activity" was identified ... clearly the phishermen (I do hope that's not non-PC) have conquered time travel (but one therefore queries why they need to phish).

The fonts change throughout the e-mail, in one instance within a sentence.

The formatting is poor too.

There is the usual link to click. This points to an IP address that appears to be hosted in India (I am in UK).

It also refers to (but does not provide a clickable link to) "<https://www.paypal.com/us/>" - an authentic PayPal website and indicates that you should type this into your browser ... which is good practice.

When the false link is clicked, a page loads from the IP address. This page then reports an error and loads another page that shows "https://www.paypal.com/cgi-bin/webscr?cmd=3D_login-run" in the Address box and status line. It does not, however, show a 'locked' icon on the status line. This is, of course, a 'false flag' page ... but it is

good enough to
fool more people than many other phishing scams.

I'm not a techie, so do not purport to understand how this works. For the real experts out there, the clickable phishing address is http://61.95.206.3/.paypal.com/cmdr_login/error.html .

The RISKS? As we get more sophisticated ... so do the crooks.

The 'saving grace'? Most crooks are not that clever.

⚡ Times change ... problems don't ([RISKS-23.82](#))

<Louise Pryor <pryor@pobox.com>>

Thu, 31 Mar 2005 16:24:12 +0100

The clocks changed in the UK at the weekend, as they do twice a year. So you'd think that computer systems would be able to cope, and that there would be no major disruption. And, on the whole, you'd be right, though you wouldn't necessarily know it from the press coverage.

About 1,500 Barclays ATMs (out of a total of about 4,000) were out of action for over 12 hours on Sunday. We were told that a manager put the clocks back rather than forward, and that this mistake had caused the problems. The Daily Telegraph carried a leader opining on the lessons that Barclays could learn from its employee's blunder. <http://makeashorterlink.com/?M170229CA>

But hang on a minute: A real live person, changing the clocks in the data

centre at 01:00 on Sunday morning? It just doesn't make sense. Why on earth wouldn't the time change be automated? After all, it is in just about every other computer in the world. Did you have to change the time on your PC this weekend?

And in fact, Barclays say that it was a hardware fault, and not related to the time change at all. This is much more plausible, and is what I heard a Barclays person say on the radio. But if it's true, where did the story of the error-prone manager come from? The Telegraph said that they had it from customer services staff.

I imagine it happened something like this: The ATMs go down. (And, it appears, the online banking too). Calls pile into the call centre. Nobody at the call centre knows what the problem is. (And why should they know? They are not omniscient, and these things often take time to track down.) They are talking to each other about what is going on. Someone says that it must be something to do with the clocks changing, as that's something that doesn't happen every day. And someone else says "Yeah, I bet that's it. Some stupid person changed them in the wrong direction!" And before you know where you are, an off the cuff remark (probably made in jest) has spread around the call centre and becomes the official version.

People are very unwilling to believe in coincidences. They also have mental models of how things work. And surprisingly often, those mental models boil down to a little man in the box (or, in this case, in the data

centre). So when the journalists were told that the problem arose because a person made a mistake, they didn't stop to think about whether the story really made sense.

Louise Pryor <pryor@pobox.com> www.louisepryor.com

⚡ Re: Why IE is insecure: flawed logical thinking... (DeForest, [R 23 82](#))

<"Taylor, Steve" <Steve.Taylor@assetco.com>>
Wed, 30 Mar 2005 10:04:26 +0100

Craig DeForest has quite correctly raised the issue of logical flaws in the argument presented by Dave Massy (head developer of Internet Explorer), however, the key thing that I read in the argument is that Dave Massy is not interested in whether IE or Mozilla is more secure, he is simply presenting 'rhetoric' in an effort to win the argument. This is a classic situation for not getting at the truth. It is common in this sort of situation that both sides are so preoccupied in winning the argument that the truth becomes irrelevant, after all, rising higher in any organisation is often more about winning arguments than getting at the truth.

The sorriest aspect of this is the clear implication that Dave Massy is not interested in whether IE is secure, he is only interested in its reputation. This matches Microsoft's traditional behaviour of addressing

perception
rather than reality.

This is one of the most serious human risk factors on any project.

Steve Taylor, Technical Director, AssetCo Data Solutions

⚡ Re: Why IE is insecure: flawed logical thinking... (DeForest, [R 23 82](#))

<Simon Zuckerbraun <szucker@sst-pr-1.com>>

Fri, 01 Apr 2005 13:24:46 -0600

Dave Massy never made the colossal mistakes you think he made. All Dave Massy was saying is that IE access the Windows operating system through the same interface that Mozilla does. Therefore a misbehavior of Mozilla has the potential to cause the same amount of damage as a misbehavior of IE has the potential to cause. This would not be the case if, for example, IE were embedded in the Windows kernel, or otherwise had special access to privileged APIs. In that case, IE could cause **far more** damage than a third-party browser could, and this would indeed be a poor security configuration.

People may be led to believe that the latter situation is actually the case, due to the fact that IE is called "part of the Windows OS". Dave Massy wrote to clarify this matter. The truth is that all that the statement "IE is part

of the Windows OS" is meant to imply is that IE is installed automatically on every Windows system, and developers writing for the Windows platform may rely on IE's presence if they so choose.

⚡ Re: Why IE is insecure: flawed logical thinking... (DeForest, [R 23 82](#))

<Craig DeForest <zowie@euterpe.boulder.swri.edu>>

Fri, 01 Apr 2005 12:55:20 -0700

Simon Zuckerbraun wrote:

> All Dave Massy was saying is that IE access the Windows operating system through the same interface that Mozilla does. Therefore a misbehavior of Mozilla has the potential to cause the same amount of damage as a misbehavior of IE has the potential to cause.

Hmmm... I agree that he made that point among others, but he appears to be saying much more than that. It is worth excerpting Dave's blog here, to see exactly how he responds to Mitchell's claims about why Firefox might be more secure than IE.

> [...]

We could spend a long time deconstructing exactly what each of the authors believes and/or says about IE and Firefox; but I find it hard to understand Massy's meaning without including the fallacious argument I mentioned earlier, or (perhaps worse) assuming that he is being

disingenuous. Not being an OS facility is a significant advantage to Firefox, even if only because the Firefox code does not need to have as many entry points.

✦ **Re: Remote physical device fingerprinting (Ross, [RISKS-23.82](#))**

<Jerry Leichter <jerroldleichter@mac.com>>

Wed, 30 Mar 2005 10:06:12 -0500

David Ross responds to the article by Roth in [RISKS-23.80](#) referring to Broido and Claffy's work on identifying physical computers by their clock skew (www.cse.ucsd.edu/users/tkohn/papers/PDF/KoBrCl05PDF-lowres.pdf). In the grand Internet tradition of attacking work without reading it (well, I suppose the tradition is much older than the Internet...) he claims this is easy to defeated by synchronizing with multiple NTP servers, perhaps more frequently than usual.

Quoting from the abstract of the paper:

> Further, one can apply our passive and semi-passive techniques when the
> fingerprinted device is behind a NAT or firewall, and also when the
> device's system time is maintained via NTP or SNTP.

The details are discussed in the paper. (Basically, one measures the skew over multiple short intervals - intervals in the sub-second range. I won't go into details because this is a good paper and worth reading.)

✶ Re: Cruise Control failures (Brown, [RISKS-23.82](#))

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

Mon, 4 Apr 2005 21:33:07 -0400

> ... anyone who wants to get on TV can just call and say their
Renault's
> cruise control blocked; it's "another claimed incident", and
why should
> anyone check if it really happened, if it makes a good story ?

Exactly. This is the same reason, you'll recall, that the Audi
5000 was
taken off the US market: driver error that the driver didn't
want to take
responsibility for. The assertion that the car suddenly took
off by itself
was later discredited by the NHTSA, as reported in the book
_Gallileo's
Revenge: Junk Science in the Courtroom_, but that didn't stop
the incident
from costing Audi and the remains of the car industry in the US
about \$150M,
installing accelerator interlocks.

House (MD) has it right: everybody lies.

Jay R. Ashworth <jra@baylink.com>, Ashworth & Associates, St
Petersburg FL USA

<http://baylink.pitas.com> +1 727 647 1274

✶ Re: Cruise-control failures? (Scheidt, [RISKS-23.81](#))

<John Sawyer <jpgsawyer@btopenworld.com>>

Wed, 30 Mar 2005 08:58:57 +0100 (BST)

In response to the article about Cruise-control failures in [RISKS-23.81](#), my

father (a braking system engineer for over 30 years) wrote the following.

Dr John Sawyer

Well all the ABS systems I know have their own micro processor. Of course that does not mean a Renault has!

Also ABS systems do nothing unless a wheel is detected locking. i.e. no fluid flow is closed off from the brakes. Generally when they do activate they do not shut off the brakes but dump fluid which would tend to make the pedal sink. That is why the brake pedal tends to pulse while in an ABS stop. This is not always the case as there are systems that isolate the apply system to stop the brake pedal pulsing. Not sure what is on a Renault. But anyway, in this case the ABS would not be active so it should have no effect.

However if the cruise control for some reason does not disengage, the brakes could feel ineffective as the brakes fight the engine as the cruise control tries to maintain speed! The brakes would win but it would give you a fright!

On micro processors, generally the systems are designed with multiple check systems and any fault results in a shut down reverting the vehicle to a limp home mode or complete shut down. ABS systems become inoperative such that

the brakes operate normally but have no way of stopping them locking up. Brakes are still hydraulic and do not use micro processors to make them work. (Yet anyway!) Only to stop them locking! This is what is making people going to electric operated brakes nervous! I am not aware of a complete electrically operated brake system going into production as yet.

Patrick Sawyer
(Former Chief Engineer - Braking Systems for a Major Brake Manufacturer)

✶ Re: Cruise-control failures?

<Neil Maller <neil.maller@gte.net>>
Wed, 30 Mar 2005 14:47:26 -0500

Nick Brown point out ([RISKS-23.82](#)) that typical brake designs provide substantially more stopping force than the engine can provide propulsive force. This invariably so: in the case of my own car the brakes are roughly equivalent to 1000 hp, more than four times the power of the engine.

However Mark Brader suggests possible loss of power braking due to the ignition being off. That's not how it works: brake power assist is provided from engine vacuum, or rarely by a hydraulic pump. In either case a vacuum or high pressure reservoir provides more than enough power assist to stop the vehicle, even from high speed, without the engine running.
Ray Todd

Stevens suggests that the braking system's thermal capacity could be exceeded, causing brake fluid to boil and braking effectiveness to be lost.

It's possible to imagine a simultaneous failure condition which would result in a driver's inability to stop the vehicle. First a failure in the cruise control itself or the drive-by-wire throttle results in a WOT (wide-open-throttle) condition. Then the driver brakes, but insufficiently to overcome the engine, resulting in excessive brake heating, boiled brake fluid and resultant complete loss of braking power. And because little engine vacuum is developed at WOT it's also possible that prolonged brake application might exhaust the vacuum reservoir and cause total failure of brake power assist.

Ray Todd Stevens also said that "This [overheating] is a problem in race cars and they use special brake pads because of this." Speaking as one who does drive cars on race tracks I must point out that we use special brake *pads* in order to avoid those brake *bads.*

However I'm not volunteering to put either of the theories to the test!

✶ Re: Cruise-control failures?

<Markus Peuhkuri <puhuri@iki.fi>>

Thu, 31 Mar 2005 09:04:38 +0300

I think it is time to put some real figures for discussion. As Nick Brown stated, force by breaking system exceeds one given by motor. A simple calculation:

Mass of car: 1500 kg. Time to stop from 100 km/h speed: 3 s.

Power

consumed by breaks: $P = 1/2 m v^2 / t = 1/2 * 1500 * 27.8^2 / 3 = 193$

kW. Power output from 2.0 litre machine at 3000 r/min: less than 100 kW.

Somebody more in mechanical engineering may correct, but based on figures above, I would say that it takes less than 6 seconds to stop run-away car using breaks that should not yet cause serious heat problems. Even if motor does not give support for breaking, one can apply a force more than ones weight on breaking pedal. Also, the breaking power is underestimated because the 3 second time-to-stop is limited by tyres, not by breaks on modern cars. Also, there should be at least two independent breaking circuits. I was not able to find current car approval rules, but as far I know, at least steering MUST have mechanical connection from steering wheel to wheels.

This leaves us two possibilities: either something interfered with breaking system (ABS, ESP) or then it was plain user error or action.

✶ **Re: Cruise Control Failures (Stevens, [RISKS-23.8x](#))**

<dbell@zhochaka.demon.co.uk ("David G. Bell")>

Wed, 30 Mar 2005 08:57:37 +0100 (BST)

My guess is that the indirect control of power to the engine ignition and fuel systems is a side effect of anti-theft systems.

But some effective emergency-stop override of the engine control systems ought to be there.

Trouble is, another anti-theft feature is that removing the vehicle key from the main switch will mechanically lock the steering, even if it does cut all the electrical power.

Race-prepared vehicles do have battery isolators, placed for easy operation by the marshals when a vehicle goes off the track. Unfortunately, some early engine control computer systems on cars lost key data when they lost power, even if only for a few seconds.

Unintended consequences strike again.

Re: Cruise-control failures

<"Amos Shapir" <amos083@hotmail.com>>

Sat, 02 Apr 2005 13:48:47 +0300

Back in 1991, I used to own a Renault Clio. One day, the cabin ventilation fan got stuck in the "on" state, not turning off even when the ignition key was out. In the garage, a mechanic checked it, went off to the

store room
to fetch a HUGE box back: there is no fan any more, only a
"climate control
system" which includes a bellows, a fan, its motor, dashboard
switches and
an electronics card, and costs about \$300 to replace.

The mechanics liked the idea of just replacing the unit by
unscrewing 5
screws in less than two minutes, instead of searching for
crossed wires
somewhere in the system; Renault liked selling it; I certainly
did not like
it and never owned a Renault since. It seems that now there is
no way to
escape this forced computerization at any price (which we the
buyers must
pay).

✶ Re: Cruise Control failures

<David R Brooks <davebXXX@inet.net.au>>
Sat, 02 Apr 2005 21:47:29 +0800

I work on engine-control computers for buses. We are required to
have power
for the fuel injectors & for the ignition (these are natural-gas
fueled
engines) run through the ignition switch. That way, the driver
can turn off
the switch (not, of course, far enough to lock the steering),
and the engine
is twice dead: no fuel, no spark. The brakes on these are not
computerised.
I am surprised they aren't required to build cars similarly.
Methinks I
shall try to buy used cars rather than new ones, now.

⚡ New Security Paradigms Workshop submission deadline approaching

<George Robert Blakley III <blakley@us.ibm.com>>

Wed, 6 Apr 2005 11:41:11 -0500

We're accepting papers for this year's ACSA New Security Paradigms Workshop for another two weeks.

The CFP and a link to the mail alias for submissions can be found here:

<http://www.nspw.org/current/cfp.shtml>

Bob Blakley, Chief Scientist, Security and Privacy, IBM
blakley@us.ibm.com +1 512 286-2240 fax: +1 512 286-2057

[This is a rather small but important security workshop. 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 23: Issue 84

Monday 18 April 2005

Contents

- [Ch7 Australia off-air due to multiple system failures](#)
[Andrew Goodman-Jones](#)
- [310,000 Lexis-Nexis records accessed by identity thieves](#)
[PGN](#)
- [Polo Ralph Lauren customer database attacked](#)
[Mohl/Bray via Monty Solomon](#)
- [Tufts alumni data compromised](#)
[Hiawatha Bray via Monty Solomon](#)
- [BofA agent gives out personal information to finder of lost VISA card](#)
[Caskey L. Dickson](#)
- [Computer-generated gibberish conference paper accepted](#)
[PGN](#)
- [Vatican's prescient Web masters](#)
[Diomidis Spinellis](#)
- [Bullet trains with faulty speed controls](#)
[Dennis Mullin](#)
- [Michigan message board says speed limit 100 mph](#)
[Monty Solomon](#)
- [Israeli system for secure e-mail with the government](#)
[Shoshannah Forbes](#)
- [The risks of phone number rollover procedures](#)
[Karl Klashinsky](#)
- ["War" driving a minefield?](#)
[Rob Slade](#)
- [Online security with usability problems](#)
[Ed Taft](#)
- [So is this a phishing attack or not?](#)
[Jim Horning](#)
- [Re: Short links and phishing](#)
[Alan D. Zimmerman](#)

• [Re: Times change ... problems don't](#)

[Michael Bacon](#)

• [Medical errors/usability](#)

[Jim Jewett](#)

• [Comcast cable daylight savings change over problem](#)

[Mark A. Biggar](#)

• [Info on RISKS \(comp.risks\)](#)

✂ Ch7 Australia off-air due to multiple system failures

<"Andrew Goodman-Jones" <goodie@ozemail.com.au>>

Fri, 15 Apr 2005 14:06:47 +1000

Ch7 is one of the three national commercial TV stations in Australia. On the evening of 13 Apr 2005 they had a power failure and a back-up power failure in Melbourne, the automatic cutover to an alternate broadcast center failed, and the national phone system failed. All national transmissions come from a single center. Almost a million viewers had 41 minutes of the blank screen. Lost ad revenues were estimated at AU\$600,000. The cause was apparently not known.

[Source: Australia's Channel 7 loses bucks in blackout,
By Eleanor Sprawson, *The Herald Sun*, 15 Apr 2005; PGN-ed]

Because transmissions for the whole country come from the one broadcasting centre, Seven was unable even to broadcast a message apologising for the situation until power in Melbourne was restored at 9.50pm.

But the glitch did not result in a ratings boost for public broadcaster SBS, with figures showing viewers preferred Seven's blank screen.

To Seven's astonishment more than 900,000 viewers stayed tuned to the network after screens went blank 38 minutes into the nail-biting episode. "Around a million Australians hung in there for us and we thank them for their commitment," Seven Sydney spokesman Simon Francis said last night.

He also apologised to viewers who tried to ring Seven on Wednesday night, as the network's national phones were down too.

Seven will re-screen the episode next Wednesday at 8.30pm, then a new episode in the current serial killer storyline at 9.30pm.

Johnson confirmed the network "lost quite a bit" in advertising from the shutdown. Last night Geoff Clarke, media investment director for MindShare, estimated it had cost the network more than half a million dollars.

The shutdown meant Seven came third in the ratings on Wednesday night.

✂ 310,000 Lexis-Nexis records accessed by identity thieves

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

Thu, 14 Apr 2005 10:15:21 PDT

The saga of hacked personal information continued with a report as we go to press that Lexis-Nexis admitted to having been victimized by the theft of personal records of 310,000 people (10 times more than originally reported), including SSNs and drivers' license numbers. 59 cases were discovered of access by unauthorized persons using legitimate IDs and passwords. 64,145 of those lost records involved California residents. [Source: David Colker and John Spano, *Los Angeles Times*, 13 Apr 2005; PGN-ed]

✦ Polo Ralph Lauren customer database attacked

<Monty Solomon <monty@roscom.com>>

Fri, 15 Apr 2005 22:14:59 -0400

The scope of a computer system breach at a national retailer widened on 13 Apr 2005 to involve the customers of a second major credit card firm, but those companies refused to divulge the name of the retailer. The existence of the security breach first surfaced this week when HSBC North America began notifying 180,000 of its GM MasterCard customers that their credit card information had potentially been compromised. HSBC, which issues the GM cards, urged each customer to replace their card as quickly as possible. [Source: Breach in security reaches 2nd credit firm; MasterCard, Visa refuse to identify retailer whose computer system was hit Bruce Mohl, *The Boston Globe*, 14 Apr 2005; PGN-ed]

http://www.boston.com/business/technology/articles/2005/04/14/breach_in_security_reaches_2d_credit_firm/

A computer security breach at Polo Ralph Lauren Corp. that has recently roiled two major credit card companies actually occurred last fall. But Polo only made the problem public on 14 Apr 2005. [Source: Retailer knew last fall about security breach that recently roiled credit card companies, By Hiawatha Bray, *The Boston Globe*, 15 Apr 2005]

http://www.boston.com/business/globe/articles/2005/04/15/retailer_knew_last_fall_about_security_breach_that_recently_roiled_credit_card_companies/

✦ Tufts alumni data compromised

<Monty Solomon <monty@roscom.com>>

Fri, 15 Apr 2005 22:12:07 -0400

Tufts University began sending letters to 106,000 alumni, warning of "abnormal activity" on their fund-raising computer system that contained names, addresses, phone numbers, and, in some cases, Social Security and credit card numbers.

[Source: Tufts warns alumni on breach; Computer attack exposed names, numbers to theft, By Hiawatha Bray, *The Boston Globe, 12 Apr 2005; PGN-ed]

http://www.boston.com/business/technology/articles/2005/04/12/tufts_warns_alumni_on_breach/

✂ BofA agent gives out personal information to finder of lost VISA card

<"Caskey L. Dickson" <caskey@technocage.com>>

Thu, 07 Apr 2005 14:44:01 -0700

While out shopping, my wife found a credit card dropped in the parking lot. Since the facility was a strip-style mall there wasn't an obvious place it could be left for the owner to pick it up.

She decided to call the 1800 number on the back of the card to find out where she should mail or drop off the card. What happened next was almost surreal.

After much button pressing to get past the automated prompts (my wife didn't want to just enter the card number because then she may hear information like the owner's balance) she finally got in touch with an agent. My wife tells the agent the story of the found card and after giving only the name on the card and the account number, the agent proceeds to tell her three things (completely unbidden):

- 1) The card has not yet been reported stolen
- 2) The cardholder's billing address
- 3) The cardholder's home phone number

Combine this with *physical possession* of the card, you can see the problem.

It was midway through item number 2 that my wife realized that the address wasn't the address of a branch or office and she tried to stop the agent from revealing more information. The agent more or less insisted that this was the best way to get the card back to the owner and when the agent was told that she was in essence enabling identity theft, her reply "oh, that's not a problem".

My wife elected to drop it by a branch she passed en route home. The teller there was at least surprised at the story of the phone agent's activity, commenting that "she must be new".

I can only hope that it is a poorly trained phone agent, however the fact that BofA's training program doesn't condition agents to resist giving out personal information so easily is more than a little disturbing.

✂ Computer-generated gibberish conference paper accepted

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

Fri, 15 Apr 2005 17:12:11 PDT

Three MIT students developed a program to generate papers with more-or-less random text based on a context-free grammar, and submitted it to the World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI) to be held in Orlando in July. Not surprisingly, one of their papers, "Rooter: A Methodology for the Typical Unification of Access Points and Redundancy", was accepted. The paper features such gems as: "the model for our heuristic consists of four independent components: simulated annealing, active networks, flexible modalities, and the study of reinforcement learning" ... "We implemented our scatter/gather I/O server in Simula-67, augmented with opportunistically pipelined extensions." [According to other out-of-band sources, this is reportedly a conference that generally accepts a paper from every would-be author, but charges speakers to attend; perhaps no one else attends other than those gullible speakers?]

According to CNN, the prank was reminiscent of a 1996 hoax in which New York University physicist Alan Sokal succeeded in getting an entire paper with a mix of truths, falsehoods, non sequiturs and otherwise meaningless mumbo-jumbo published in the quarterly journal *Social Text*, published by Duke University Press.

[Source: PGN-ed from a Reuters item]

<http://www.cnn.com/2005/TECH/science/04/14/mit.prank.reut/index.html>

🚀 Vatican's prescient Web masters

<Diomidis Spinellis <dds@aueb.gr>>

Sat, 09 Apr 2005 10:46:39 +0400

The "Vacancy of the Apostolic See" Web page appears to have been prepared one day BEFORE the Pope's death.

The page's <http://www.vatican.va/gpII/documents/index_en.htm>

HTML markup contains the following meta tags:

```
<meta name="title" content="vacancy of the Apostolic See" />
<meta name="creator" content="Vacancy of the Apostolic See" />
<meta name="subject" content="Vacancy of the Apostolic See, death of
John Paul II, Holy Father" />
```

```
<meta name="date.created" content="2005-04-01" />
<meta name="date.issued" content="2005-04-03" />
<meta name="date.expires" content="" />
```

Thus it appears that the web page was created on April 1st, yet the Pope's death certificate clearly indicates that the Pope died on April 2nd.

"His Holiness John Paul II (Karol Wojtyla) born in Wadowice (Crakow, Poland) the 18th of May 1920, resident of Vatican City, expired at 9:37 on the evening of April 2, 2005"

It is a well-known fact that journalists prepare in advance obituaries of public figures that appear to be nearing their life's end. See for example the article "Quirk in British Computer Privacy Laws" ([RISKS-11.63](#)).

Nevertheless, for the Vatican's content creators to advertise the fact that they were creating the "Vacancy of the Apostolic See" Web page while the Pope was still alive and struggling is at the very least a sign of poor taste; worse, the fact will now provide food to conspiracy theorists who thrive on these details.

The risk: accurate metadata is not always appropriate.

Diomidis Spinellis - <http://www.spinellis.gr>

✈ Bullet trains with faulty speed controls

<Dennis Mullin <dmullin@sentex.net>>

Sat, 26 Mar 2005 13:38:42

Bullet trains run for years with faulty speed controls

[Source: Mainichi Shimbun, Japan, 23 Mar 2005]

<http://mdn.mainichi.co.jp/news/20050323p2a00m0dm013000c.html>

Series 300 bullet trains have been running for years with faulty speed control equipment, Central Japan Railway Co. (JR Tokai) officials said.

Automatic Train Control (ATC) devices that prevent Shinkansen trains from exceeding certain speeds have been faulty on the Series 300 trains, with 52 malfunctions reported this year alone.

In one case, a train traveled at 280 kilometers per hour between Shin-Yokohama and Odawara stations in Kanagawa Prefecture on March 3, even though the speed limit on the line is 270 kilometers per hour.

JR Tokai says the error came from faulty software supplied by the makers of the devices and that the glitch was not even detected during test runs.

Land, Infrastructure and Transport Ministry officials have asked JR Tokai to provide a complete explanation of the case.

JR Tokai said one of the cases involved a Series 300 bullet train driver being forced to reduce speed manually after the ATC on the train he was driving on March 19 failed to work.

A check of the ATC later revealed that software supposed to detect train speeds was not working properly. This caused the ATC to estimate the train was traveling slower than it actually was.

JR Tokai has stopped using the faulty equipment.

[Incidentally, Amtrak's Acela trains have been shut down for the past few days because of detected failures in brake discs. PGN]

✦ Michigan message board says speed limit 100 mph

<Monty Solomon <monty@roscom.com>>

Sun, 10 Apr 2005 02:38:42 -0400

http://www.boston.com/news/odd/articles/2005/04/08/mich_message_board_says_speed_limit_100/

Drivers on southbound Interstate 75 in Michigan saw a construction message board that previously had been alerting drivers in Genesee County near Clio that construction was soon to start. One morning it said

"speed limit 100 mph go go go."

(The speed limit in that area is 70 mph. The sign is controlled remotely by a subcontractor's computer.)

[Source: AP item from *The Boston Globe*, 8 Apr 2005; PGN-ed]

✦ Israeli system for secure e-mail with the government

<Shoshannah Forbes <xslf@xslf.com>>

Mon, 18 Apr 2005 12:32:35 +0400

Israelis to receive secure e-mail address to be used for contacts with authorities

<http://www.ynetnews.com/articles/0,7340,L-3073923,00.html>

"The Social-Economic Cabinet approved Sunday a plan put forth by Finance Minister Benjamin Netanyahu to expand Israel's *approachable Government* program. The government also approved the *safe deposit box* program, a system of secure e-mail boxes that would allow government offices to send official permits, signed forms, receipts and messages to businesses and individuals. [...] At first, the system will support forms in text format (TXT, PDF, RTF, HTML, XML), the last two without Active Script. The `safe' will require the recipient to send a `proof of receipt' to the sender. Each sent message will be coded to identify the sender, to allow the recipient to forward the message to a third party, and an expiry date. [...] In order to use the system, individuals and businesses will be required to obtain a smart card, a card reader (estimated cost: NIS 55 or about USD 12), and to register an electronic signature (approximately NIS 20 or about USD 4.5)."

In addition to all the usual RISKS such a scheme brings up, I should note that to this date, the bill paying website (<http://www.mybill.co.il>) works only with Win/IE, so I won't be surprised if the above setup will also be Win/IE only.

Shoshannah Forbes <http://www.xslf.com>

[... and that it might therefore be subject to exploitation of Winflaws.

PGN]

⚡ The risks of phone number rollover procedures

<Karl Klashinsky <klash@cisco.com>>

Fri, 15 Apr 2005 16:26:43 -0700

A story on the Canadian Broadcasting Corp's web site, from Saint John, New Brunswick:

A federal government toll-free phone line to encourage safe boating is directing callers in New Brunswick to a phone-sex offer instead.

<http://www.cbc.ca/story/canada/national/2005/04/14/boating-sex-mixup050414.html>

The article implies that an internal Canadian government re-organization resulted in a toll-free number being returned to a pool of available toll-free numbers, and the number was then probably picked up four months later by a phone-sex line (again, this is implied by the article above, but not stated as fact).

The risk here is that the "recycle" process does not appear to check that the prior use of a toll-free number doesn't conflict in some social/moral way with the new user's intended use of the number.

Oh, well, it could have been worse... at least the number wasn't previously used for Mattel's "Barbie" hotline.

Semi-related anecdote... our local telephone supplier provides a service whereby we get a toll-free number for my residential phone, with a single (cheap) rate for callers from anywhere in North America. Useful when me or other members of my family are traveling, and even for friends to use to call.

The snag... our toll-free number is one-digit off from the toll-free support number for one of the largest Cable/Internet/Phone service providers in the USA. As a result, I typically get one or two calls a week from customers of the service provider... since they are typically looking for support, they are often a big grumpy. When told "this isn't Company X's support line", some callers berate me, accusing me of trying to dodge their call (it's obviously not their first call to the support line).

⚡ "War" driving a minefield?

<Rob Slade <roslade@sprint.ca>>

Wed, 13 Apr 2005 11:15:18 -0800

The Register reports that the US is deploying newly developed wireless LAN- enabled mines, supposedly code-named Matrix:

http://www.theregister.co.uk/2005/04/12/laptop_triggered_landmine/

(Any comments about "minefield" testing a new technology?)

With the US being one of the few holdouts against the ban on landmines, there are predictable concerns about the danger the new mines hold for civilian populations. However, there would also seem to be any number of potential dangers to the troops using them.

There are very few details provided in regard to the new mines. There appear to be different types. They have some kind of wireless capability. They have remote detonation capability.

Based upon what is said, we can determine some additional aspects of the technology, as well as surmise more. They likely communicate via radio frequencies. They will have some kind of (likely minimal) software for reception of signal, authentication, and activation. (Deactivation is likely accomplished by activating the mine when [hopefully] nobody is around.) The mines are probably individually addressable: blowing an entire minefield for a single intrusion would not seem to be an effective use of resources. Radio communication would imply that either the mines are battery powered, or that they contain an antenna and transponder. Given the purpose and use of mines, it is likely that there is an alternate and more standard triggering mechanism such as pressure plates or tripwires that does not require wireless activation.

There are, of course, other more advanced possibilities for such a technology. Mines could be remotely enabled and disabled, could communicate with each other, or could communicate sensor results with a central location. However, these functions are unlikely in a first generation device.

The potential risks are numerous. With radio communications mines that are buried, or placed under or behind metal or water, may fail to detonate when needed, or deactivate. Any kind of software is, of course subject to failures (which, in this case, could be literally catastrophic). Authentication would be a fairly major issue: sniffing of radio traffic could easily determine commands, replay attacks, static passwords, or number sequences. (Note that the mines require "minimal training" for use.) Failure of authentication could, again, result in failure of either detonation or deactivation. Battery failure would be an issue and therefore transponders are more likely, but transponders would be more difficult to troubleshoot. (Should the transponders retransmit? That would assist with finding and disarming mines, but broadcasting a signal with known improper authentication would result in a means of determining the location of mines.)

Overall, mines still seem to be a pretty bad idea.

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>

🔥 Online security with usability problems

<Ed Taft <taft@adobe.com>>
Tue, 12 Apr 2005 16:43:37 -0700

I recently received "The E*TRADE Complete Security System" for controlling access to my online E*TRADE account. It introduces two-factor authentication to the login process, requiring both something I know (my password) and something I have (a keyfob device). While this seems like a very good idea on the surface, the implementation leaves something to be desired from a usability standpoint.

The keyfob device, which carries E*TRADE and RSA logos, has a 6-digit display that changes once per minute. In order to login, I need to present my username and a password consisting of my regular fixed password appended with the currently displayed 6-digit number.

While this appears to have good security, some potential deficiencies come to mind --

- * It requires more typing than the old scheme, including an unfamiliar sequence of characters that changes every time. A better arrangement would be for the keyfob to have a USB connector that I plug into my computer to prove that I have the keyfob.

- * If multiple service providers adopt this scheme, I'll need a pocket full of keyfobs. A better arrangement would be one keyfob that can hold credentials for logging into multiple sites.

- * The scheme seems to depend on the keyfob and the server to have synchronized clocks. What happens if the keyfob's battery dies or the server's clock becomes misadjusted, as appears to occur with some regularity?

- * What if I need to login when I don't have the keyfob? There is a phone number I can call to obtain temporary-access instructions, assuming that I can convince the agent that I am the legitimate owner of the account. This seems like a potential weak link in the scheme.

Fortunately, use of this security system is optional. The RISK is that nobody will use this scheme because it is too inconvenient.

⚡ So is this a phishing attack or not?

<"Horning, Jim" <Jim_Horning@McAfee.com>>
Fri, 1 Apr 2005 14:35:37 -0800

I really have no way to be sure.

Given that ACM is still sending me invitations to log in to my email spam-filtering service almost daily, it seems plausible that this message inviting risky behavior was actually sent on behalf of ACM. But how can I verify that, short of communicating directly with you?

Either way, sending it on April Fools Day is a nice ironic touch.

Jim H.

<http://horning.blogspot.com/2005/03/phishing-report-through-february.html>

-----Original Message-----

From: Election Services Corporation
[mailto:acmsighelp@electionservicescorp.com]
Sent: Friday, April 01, 2005 1:59 PM
To: Horning, Jim
Subject: ACM SIG 2005 Election
Importance: High

Dear James Horning:

ACM is pleased to offer its Special Interest Group (SIG) members the opportunity to vote by the Internet in the 2005 Election.

You are encouraged to participate in this election. Please note that 12:00 noon Eastern Time, June 15, 2005 is the deadline for submitting your vote. It is important that the voice of ALL members be heard.

To vote electronically, please go to: <https://www.escvote.com/acmsig>

You will need your 7-digit ACM/SIG Member Number to log in to the secure voting site. If you do not know your membership number, please go to <https://campus.acm.org/public/accounts/Forgot.cfm>

For additional help, please visit the help screen on the log-in page by clicking on the "Help" button.

Enter your 7-digit ACM/SIG Member Number to reach the menu of active SIG elections that you are eligible to vote in.

In the on-line menu, select the Special Interest Group seen below.

Enter the 10-digit unique PIN seen below.

Follow the on-line voting instructions.

Special Interest Group: [obscured]

Your Unique PIN is: [obscured]

If you have any questions or would like to request a paper ballot, please e-mail acmsighelp@electionservicescorp.com or call toll-free 1-866-720-4357.

Thank you for taking the time to submit your vote electronically.

Association for Computing Machinery

[Jim CC:ed John White <white@hq.acm.org>, who responded:

Yes, this message was/is legit. The spam-filtering message is changing shortly. Obviously, we have more work to do.]

⚡ Re: Short links and phishing (Pryor, [RISKS-23.83](#))

<"Zimmerman, Alan D." <alan.zimmerman@gd-ais.com>>

Thu, 7 Apr 2005 10:01:01 -0500

In [RISKS-23.83](#), Louise Pryor included a link to the Barclays ATM story that was "shortened" through makeashorterlink.com. Ironically, the article immediately before was about phishers becoming more sophisticated. Acceptance of techniques and services like this are only giving phishers more ammunition.

⚡ Re: Times change ... problems don't ([RISKS-23.82,83](#))

<"Michael (Streaky) Bacon" <himself@streaky-bacon.co.uk>>

Thu, 7 Apr 2005 08:29:40 +0100

Louise Pryor's remarks (Times change ... problems don't ([RISKS-23.82](#)) [RISKS-23.83](#)) about human intervention in the bi-annual time change process, reminded me of my early days when the change was effected by an engineer burrowing inside a cabinet searching for the right switch on the right circuit board. The Leap Year change involved calculating new values for a resistor bank and resoldering!

⚡ Medical errors/usability

<Jim Jewett <jimjjewett@gmail.com>>

Fri, 15 Apr 2005 11:20:51 -0400

There was a recent discussion of medical errors, and whether to blame the computer. Most errors are the sort that happened even before computers. Did the computer really cause a problem, or did it only make them easier to track?

Jakob Nielsen's latest column explains how the interface may actually make the errors more common. For example:

Doctors could always prescribe the wrong dosage, but it happens more often if an incorrect default is offered.

There could always be confusion about when "tomorrow" starts if an order is written at 2:00 am, but humans were likely to understand the intent if they were on the same shift, or coming in to "the morning's orders". After computer entry, it starts to look more like an arbitrary date.

<http://www.useit.com/alertbox/20050411.html>

⚡ Comcast cable daylight savings change over problem

<"Mark A. Biggar" <mark@floorboard.com>>

Wed, 13 Apr 2005 22:24:16 -0700

Comcast cable in Sunnyvale CA, seems to have had some problems with the recent daylight savings change over. The time on my cable box was not adjusted forward 1 hour until around 11:30 Sunday morning, and until then the on-box channel guide was showing the wrong times for all programs, For example it was showing programs usually showing at 8AM as being on at 7AM. This appears to have happened due to lack of testing beforehand. The only adverse effect on me was that it caused me to be late for church as my cable box is the only clock I have in my living room. This is what I deserve for depending on a clock I can't set myself.



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



THE 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 23: Issue 85

Tuesday 26 April 2005

Contents

- [Amtrak's high-speed Acela trains sidelined until summer](#)
[Monty Solomon](#)
- [Amtrak woes echo standard software engineering complaints](#)
[Michael J Harrison](#)
- [Remote computer locks the doors, or does it?](#)
[Mark Lutton](#)
- [Hacker broke into CMU computers](#)
[Bill Schackner](#) via [Monty Solomon](#) [Bob Heuman](#)
- [Another out-of-bounds condition that needs NO checking](#)
[David Leshner](#)
- [A large scale disruption caused by incorrect virus-definition file](#)
[Chiaki](#)
- [The risks of opening a PayPal account](#)
[Ross Anderson](#)
- [Risks of having a distinctive surname](#)
[Stefek Zaba](#)
- [SFPD officer accused of using airport cameras to ogle women](#)
[Bob Van Cleef](#)

- [Trial ID card scheme is withdrawn in Cornwall](#)
[Chris Leeson](#)
 - [Audit shuts down Minnesota Car License Web](#)
[Steven Hauser](#)
 - [Oops! US Air round trip for \\$1.86](#)
[Howard M Israel](#)
 - [Banks still force users to be vulnerable to ID theft](#)
[Brad Hill](#)
 - ["The national phone system failed"?](#)
[Mark Brader](#)
 - [Re: Michigan message board says speed limit 100 mph](#)
[Jeffrey Waters](#)
 - [Re: SecurID and E*TRADE](#)
[Jonathan Lewthwaite](#) [Kurt Raschke](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Amtrak's high-speed Acela trains sidelined until summer

<Monty Solomon <monty@roscom.com>>

Thu, 21 Apr 2005 01:12:32 -0400

Amtrak will not be able to run any of its high-speed trains until the summer because of delays in getting replacement parts to correct brake problems on Acela Express cars. The brakes were to last 1 million miles; the current Acela fleet had about half of that mileage.

Amtrak pulled all of its 20 Acela trains out of service on Friday after finding millimeter-size cracks in 300 of the fleet's 1,440 disc brake rotors. Each Acela train has 72 brakes. This part is unique to the Acela and there is no active production line casting them. Fewer than 70 disc

brakes are currently available.

[Source: The Associated Press, article by Donna De La Cruz, 20 Apr 2005; PGN-ed]

http://www.boston.com/news/local/massachusetts/articles/2005/04/20/amtraks_high_speed_acela_trains_sidelined_until_summer/

[Amtrak had cannibalized parts from other trains to get one or two trains able to run, but quickly abandoned that effort. Risks of custom design and no spare parts... Risks of building a system that really required new tracks, rather than trying to run on old tracks... PGN]

Amtrak woes echo standard software engineering complaints

<Michael J Harrison <mharrison@us.ibm.com>>
Tue, 19 Apr 2005 16:32:23 -0700

A paragraph from an op-ed in **The New York Times**, 19 Apr 2005 (<http://www.nytimes.com/2005/04/19/opinion/19tierney.html>):

"He chronicled the Acela mistakes, starting with Amtrak's decision to build a new train instead of modifying an existing European one, and to build it as a working train without first testing a prototype. The result was a long series of problems, design changes and lawsuits between Amtrak and its Canadian contractor, each accusing the other of botching the job."

It seems that old-fashioned mechanical engineering is not immune

from the
ills commonly ascribed to its software counterpart.

🔥 Remote computer locks the doors, or does it?

<<Mark.Lutton@thomson.com>>

Thu, 21 Apr 2005 11:32:00 -0400

I found this at <http://www.stupidsecurity.com>, which references <http://www.wral.com/news/4354102/detail.html>

Wake County, N.C. uses a central computer to lock 50 of its buildings in

and around Raleigh. The Wake Country Animal Shelter was closed on Easter

Weekend, but the computer didn't know that. The doors were left unlocked

and several animals were stolen from the shelter.

It would be cynical of me to note that animal shelters are one service where

pilferage of the goods reduces net costs, so I won't.

🔥 Hacker Broke Into CMU Computers (Bill Schackner)

<Monty Solomon <monty@roscom.com>>

Sun, 24 Apr 2005 01:09:26 -0400

A hacker who tapped into business school computers at Carnegie Mellon

University may have compromised sensitive personal data belonging to 5,000

to 6,000 graduate students, staff, alumni and others. The breach confirmed

by officials in the Tepper School of Business is the latest in a recent string of campus computer break-ins nationally and the second since early March affecting Tepper. There is no evidence that any data, including Social Security and credit card numbers, have been misused, officials said. But they have begun sending e-mails and letters alerting those affected. They include graduate students and graduate degree alumni from 1997 to 2004, master's of business administration applicants from September 2002 through May 2004, doctoral applicants from 2003 to this year, and participants in a conference that was being arranged by the school's staff. ... [Source: Bill Schackner, *Pittsburgh Post-Gazette*, 21 Apr 2005]

<http://www.post-gazette.com/pg/05111/491836.stm>

Hacker Broke Into CMU Computers

<Bob Heuman <rsh@idirect.com>>

Thu, 21 Apr 2005 16:50:58 -0400

Another case of not knowing how long the exposure existed and therefore how much exposure the personal information really had. Once again we have Social Security Numbers, credit card data, etc. exposed for an indeterminate amount of time. I have gone to the university's own web site and the Tepper School web site and neither has any mention of this report as of the time I checked, which is Apr 21 at 4:45PM EDT.

http://kdka.com/local/local_story_111102454.html

⚡ Another out-of-bounds condition that needs NO checking

<David Lesher <wb8foz@nrk.com>>
Thu, 21 Apr 2005 12:16:07 -0400 (EDT)

X-URL: <http://www.nytimes.com/2005/04/21/nyregion/21check.html?pagewanted=print&position>

The New York Times, 21 Apr 2005

New York City's school system recently agreed to pay \$86,000 to the lawyer of a child with autism to cover special educational services for his client. But when the lawyer opened his mail on Tuesday, he found a check for slightly more: \$8.6 million.

{off-by-one decimal point; usual excuses cited...}

⚡ A large scale disruption caused by incorrect virus-definition file

<Chiaki <ishikawa@yk.rim.or.jp>>
Tue, 26 Apr 2005 02:14:34 +0900

It is widely reported in Japan that an errant virus definition distributed by a anti-virus PC software company caused a large scale disruption of businesses and individual users.

The company, TrendMicro with its headquarters in Tokyo, has been

selling its anti-virus PC software products for quite some time. Its first product was developed in 1991.

Now, on Saturday morning 07:30 (JST), the software's automatic update site in the Philippines released a new virus definition file which, according to the company's comment, was not adequately tested. This file was picked up by many users in Japan and abroad who either automatically or manually invoked the virus definition update function of the software.

Unfortunately, Windows XP sp2 and Windows 2003 server users with this software installed (there are a few variants of the products in the software suite and a few of them were affected.) and updated the definition file AND rebooted the PC after the update (as suggested by the software it seems) saw the CPU usage go up to 100% immediately after booting and could not do much on their PCs.

The problem was that the incorrect update caused the infinite looping of scanning of a certain system file and no CPU time was left for any task to do.

(If the user didn't boot and waited for another several hours, the re-worked update file was again automagically picked up if automatic update feature was enabled and there would be no harm.)

According to the various reports, corporate licensees include media big names such as Asahi Shimbun newspaper, Kyodo wire news service, and

reservation division of railway company JR East. (The company put the user number around 10 million individual users.)

I noticed that the early reports of disrupted computer network at Asahi Shimbun and Kyodo wire service on Saturday morning and wondered what could cause LAN disruption at such well-protected places. (It seems that DHCP client could not get the address after boot due to the heavy CPU load inside the anti-virus service).

After many inquiries began pouring, the company checked and released the re-worked virus definition file. However, 170000 download took place during the incorrect definition was at the download server. Many individual or small business users who didn't realize the problem was caused by the virus definition update brought their PCs to tech service companies or re-installed the OS, etc.. Some had their disks got re-formatted.

The scale of the disruption was rather large and on Saturday evening many TV stations carried the news of the disruption with the correct cause identified. Some affected users who tried to 'fix' their computer noticed these news broadcasts and could now bring their PC into normal status.

The word cyberterrorism came to my mind, but it is ironical that the cause was due to the inadequate testing at an anti-virus software corporation.

Of course, we will see whether the release of the definition file without adequate testing was a deliberate act or simple neglect.

Lucky me: I am using Symantec Anti-Virus software on an Windows PC, and linux on another PC. Diversity is wonderful when we can afford it.

PS: The remedy was to reboot the computer into safe-mode (after forced power-off in many cases) and replaced the errant file and reboot. The anti-virus software now would pick up the new corrected file.

PPS: I think I should add, in order to feel the scale of the problem, we now know Monday morning that on Saturday,

- JR railway reservation division could not check the reservation status (fed via network to PCs?) and so diverted (telephone) inquiring customers to manned counters at railway stations,

- Kyodo wire service could not send out automatic wire service news for a few hours, and so resorted to send out important news via FAX (I believe that the initial news articles from Kyodo was sent in this manner.),

- Osaka subway system saw its computer to distribute accident information to its stations failed to reboot, and

- Toyama city's election committee could not handle advance voting for its mayoral and city alderman elections on their computer and had to resort to manual processing.

These are just a part of problems reported in Japanese press Monday morning.

However, life goes on as usual as of Monday morning as far as I can tell.

(But those unfortunate companies who had suffered from the problem over the weekend may have a hectic time right now.)

✶ The risks of opening a PayPal account

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

Tue, 26 Apr 2005 16:16:33 +0100

Regular RISKS readers know that many things can go wrong with naming and authentication. Here is an interesting example.

I opened a PayPal account on the 18th April and tried to link it to a checking account I have at a UK bank (the NatWest). The PayPal website balked at the name of the bank branch ("Cambridge King's Parade") on the grounds that it contained a non-ascii character. It was also too long for the web form. All I could do was enter "Cambridge" and hope for the best.

Now it's prudent for programmers to check input, but this is rather extreme. After all, most of the names of people and places in this world are non-ascii. Compulsory asciification turns that inoffensive Italian, Signor de'Ath, into the sinister Transylvanian Mr Death. Also, when I worked in banking many years ago, a common source of fraud was that when money arrived at the wrong branch, staff put the money into a "suspense account" while they queried the sender. Fraud and abuse involving suspense accounts was a serious problem.

So I tried to bring to PayPal's attention that their web page was not merely culturally inappropriate, but also a security vulnerability. I was unable to get their help-desk to link up successive e-mails about the issue, let alone refer me to someone who could talk policy.

So far, so broken. I reported the incident on a local mailing list (ukcrypto) where one of the regulars informed me that the King's Parade branch had in fact closed, with all the customers being transferred to another branch. This was the first I'd heard of it! I walked by my bank branch and found it indeed closed. The two small payments that PayPal said it would send to my bank account, to check I have access to the bank statements, have vanished.

You just could not make this up. PayPal relies for authentication on bank branch names, which a large UK bank will change without notifying its customers (at least, not in any way I noticed). I won't even begin to speculate about all the possible risks.

Ross Anderson <http://www.cl.cam.ac.uk/users/rja14/>

✶ Risks of having a distinctive surname

<Stefek Zaba <stefek.zaba@hp.com>>
Thu, 21 Apr 2005 19:40:59 +0100

Generally, having a distinctive forename-surname combination serves me well enough: not much chance of double-booking in hotels, and people find it easy enough to remember. There's a privacy downside, in that once you know the surname and city (country, even) I'm not hard to find. And I acquired the obvious surname-related domain, zaba.com, getting on for a decade ago.

Then, about the middle of March 2005, my inbox started to attract angry emails: "remove me from your Website immediately"! Since the www.zaba.com page has been unchanged since my mid-1997 entry on "what I did in the UK crypto-policy wars", I at first thought this was a new form of e-mail address harvesting -- send an angry accusation, attract an indignant response, email address confirmed. But few of the correspondents' addresses seemed suspect, and when I got one from a .mil address I started filing them away.

It took another week or so for one of the e-mails to identify, by way of a screenshot, which website people were concerned about.

US readers will have cottoned on by now; but for The Rest Of Us: there's a new people-searching website appeared in the US, under the name of zabasearch.com. Frantically trying to deal with their unhelpful "optout" procedures (which change frequently, and require you to submit personal data!), some people hit on the idea that zaba.com would be a better place to send emails, or Googled for the unusual word in question and found my email

address. It's since been circulated in warning messages which get passed on in Craig Shergold fashion.

zabasearch.com themselves say they're 'only republishing publicly available information'. RISKS readers, well-versed in notions of fair information handling, will just about be able to grasp the distance between "on file at the county records office", and "made available at no cost, pre-indexed by name". What's made available for free is basic personal info - name, address, phone numbers, years-at-address; for a fee they'll do further background checks. All with the same rigorous attention to data quality which has led colleagues to find themselves listed under addresses they left several years ago, and having 30 years added to their age.

What's been interesting is receiving over a hundred angry "REMOVE ME"s, only three or four of which identified the website in question. "Clearly", with that website covered in Zaba-this and Zaba-that, the great majority of correspondents observed the name coincidence and inferred identity.

Carl Ellison's "10 RISKS of PKI", and the SPKI work about the unreliability of global naming, just got validated again, at my expense.

More gory details over at < <http://www.zaba.com> >

Stefek Zaba, HPLabs, Bristol, England

[Many thanks. Having a unique name sounds like a recipe for Zaba-loney.

Or maybe someone is being fed Za-baloney? PGN]

⚡ SFPD officer accused of using airport cameras to ogle women

<Bob Van Cleef <bob@vancleef.org>>

Thu, 21 Apr 2005 12:42:08 -0700

Another case of "who is watching the watchers".

According to a report on a local TV station, KTVU 2 in San Francisco, CA, a police officer is facing possible disciplinary action for allegedly using surveillance cameras at San Francisco International Airport to ogle women as they walked through the terminal.

<http://www.ktvu.com/news/4398749/detail.html>

⚡ Trial ID card scheme is withdrawn in Cornwall

<"LEESON, Chris" <chris.leeson@atosorigin.com>>

Tue, 19 Apr 2005 13:33:04 +0100

The BBC News site has an article reporting that an ID card system being used in Cornwall has been withdrawn:

"Plans for national ID cards may need to be reconsidered following the

breakdown of a pilot project in Cornwall. The 'smart card' was tested

through the Cornish Key scheme, but now the trial is to be withdrawn,

despite an investment of £1.5m of government cash."

The withdrawal is being blamed on problems with the readers, and the system

is being replaced by a newer system with "dumber" smart cards.

<http://news.bbc.co.uk/1/hi/england/cornwall/4459493.stm>

✶ Audit shuts down Minnesota Car License Web

<Steven Hauser <hause011@tc.umn.edu>>

Tue, 19 Apr 2005 15:42:28 -0500 (CDT)

The Minnesota Legislative Auditor report shut down a web service: Department of Public Safety Web-based Motor Vehicle Registration Renewal System

Security Audit Security Controls as of March 2005

<http://www.auditor.leg.state.mn.us/fad/2005/fad05-23.htm>

The report based its audit on <http://www.owasp.org/documentation/topten.html>

the Open Web Application Security Project's top ten list and a previous audit in 2001 in which the findings and recommendations were ignored.

This story was front page news in the *Saint Paul Pioneer Press* and

Minneapolis Tribune on 19 Apr 2005.

Other MN Department of Public Safety website shutdowns occurred from the

Minnesota Legislative Auditor include the Bureau of Criminal Apprehension's

CriMNet. The legislative auditor seems to find a lot of RISKS in the

Department of Public Safety.

Steven Hauser <http://www.tc.umn.edu/~hause011/>

✈️ Oops! US Air round trip for \$1.86

<"Israel, Howard M \ (Howard\)" <hisrael@avaya.com>>

Tue, 19 Apr 2005 11:40:11 -0400

http://money.cnn.com/2005/04/19/news/fortune500/usair_cheap_flights/index.htm?cnn=3Dyes

Oops! US Air round trip for \$1.86

Report: Carrier will honor more than 1,000 tickets sold at discounted price due to computer glitch.

The airline also was hit by what its chief executive termed a "meltdown" of its baggage system </2004/12/27/news/fortune500/plane_woes/> during the Christmas holiday. That problem resulted in it sending some flights out of its Philadelphia hub without any bags.

✈️ Banks still force users to be vulnerable to ID theft

<Brad Hill <hillbrad@gmail.com>>

Wed, 20 Apr 2005 12:52:05 -0600

This may have been discussed before, but with the recent spate of DNS cache poisoning attacks and fake WiFi hotspot proliferation I believe it has new relevance.

I was actually rather shocked to find that U.S. Bank (<http://www.usbank.com/>), Chase (<http://www.chase.com>) and Bank of America (<http://www.bankofamerica.com>) all still *force* users to enter

their login and password on an insecure page. This exposes account holders to a great risk of their credentials being stolen. The login forms on their genuine home pages are submitted to a secure site, as they claim. The problem is that you need security **before** you enter your data. If DNS, a router or a proxy server anywhere along the path to their server were compromised, the login page could be substituted for one that submits to another site or injected with JavaScript that sends info elsewhere, asynchronously, before it goes to the real destination. Without an SSL certificate chain there is no way to verify that the insecure page with the form came from a trusted source and no way short of exhaustive code inspection to tell where the form data is actually going.

BankOne, Wells Fargo, Citi, Washington Mutual, Bank of the West, Key Bank and Sun Trust all offer SSL versions of their login page, but for some reason, U.S. Bank, BofA and Chase redirect to an insecure site or return an error when trying to connect with SSL. You **can't** log in securely, even if you try. The existence of this kind of obvious and fundamental security mistake after all the publicity about this category of attack (note that all these banks **do** have a user education page on phishing/fraud prevention!) is definitely something to keep in mind when choosing a bank.

✶ "The national phone system failed"? (Goodman-Jones, [Risks-](#)

23.84)

<msb@vex.net (Mark Brader)>

Mon, 18 Apr 2005 20:45:00 -0400 (EDT)

> Ch7 is one of the three national commercial TV stations in Australia.

"The national phone system failed", and what RISKS hears about is a *television* outage? Please tell me that this was just a careless wording!

Mark Brader, Toronto, msb@vex.net

[Probably not. TV is much more visible than electricity to many people...

PGN]

⚡ **Re: Michigan message board says speed limit 100 mph ([R 23 84](#))**

<"Jeffrey Waters" <jwaters@htimes.com>>

Tue, 19 Apr 2005 13:44:02 -0500

While living in Florida, I always wondered what would happen if one of the message boards on northbound I-95 would have said something along the lines of "Notice - DEA Checkpoint 2 Miles"

⚡ **Re: SecurID and E*TRADE (Taft, [RISKS-23.84](#))**

<"Jonathan Lewthwaite" <JLewthwaite@passgo.com>>

Mon, 25 Apr 2005 16:11:56 +0100

Online security with usability problems?

In [RISKS-23.84](#) Ed Taft wrote an article about the potential drawbacks of using a keyfob device to facilitate two-factor authentication. Ed made several observations of his experience and notes that:

"... while this appears to have good security, some potential deficiencies come to mind: It requires more typing than the old scheme, including an unfamiliar sequence of characters that changes every time. A better arrangement would be for the keyfob to have a USB connector that I plug into my computer to prove that I have the keyfob."

This 'deficiency' has already been addressed:

The solution is to allow the 'token' software to be installed on some other device such as a USB memory stick. This can then be used to prove that the authenticating user has the device (by plugging it in). For an example and explanation have a look at:

<http://www.passgo.com/products/softwareTokens.shtml>

To maintain the two-factor authentication plugging in the device by itself is not enough -- the user must supply something they know. As Ed noted this is an unfamiliar sequence of characters that changes every time. With the software token installed on your USB memory stick, supported applications can be configured to require a PIN allowing the challenge/response sequence to be handled automatically.

The solution ports to other common electronics that folks have such as PDA's and Mobile devices giving even greater freedom to the end user.

For further information on the need for strong two factor authentication =

and solutions RISK readers can follow this up at:

<http://www.passgo.com/products/defender/index.shtml>

Jonathan Lewthwaite Technical Account Manager www.passgo.com

✉ **Re: SecurID and E*TRADE (Taft, [RISKS-23.84](#))**

<Kurt Raschke <kurt@raschke.net>>

Mon, 18 Apr 2005 20:59:42 -0400

Ed Taft's commentary in [RISKS-23.84](#) on E*TRADE's apparent use of RSA's SecurID system to authenticate users to their website raised a few points that I think merit additional consideration.

On Ed's first point, about the added typing necessitated by the system and his desire that it have a USB plug: Having a keyfob with a display allows the device to be used with any sort of computer--not every computer out there has a USB port, or one that is user-accessible. What if you log in using a phone or a PDA?

On multiple service providers using SecurID: Theoretically this could become a problem, but there's no reason why a trusted third party couldn't run a copy of RSA's ACE/Server (the app used to authenticate SecurID tokens) that

others could connect to over a VPN to use for authentication.
One token,
many sites. (This, though, has plenty of inherent RISKS too.)

Finally, on his point about the keyfob's battery dying: RSA has
a good plan
for that--replace the unit. It's as simple as that.

Ed raises these issues as though E*TRADE is the first company to
ever
implement SecurID (and they may be the first to implement it for
a
public-facing service, but not the first ever), but in reality
they are not
very grave issues, and many government labs and other
organizations find
SecurID to be a good security method despite them

The real RISK? Weaknesses in the SecurID system:
<http://www.homeport.org/~adam/dimacs.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 23: Issue 86

Friday 6 May 2005

Contents

- [PDF not a good format for redacting classified documents](#)
[Bob Blakley iii](#)
- [Time Warner backup tapes lost with 600,000 records](#)
[PGN](#)
- [Hundreds of Texas driver's licenses mailed to wrong people](#)
[Peter Gregory](#)
- [False negatives on fingerprints](#)
[Jeremy Epstein](#)
- [Re: SecurID and E*TRADE](#)
[Vin McLellan](#)
- [Info on RISKS \(comp.risks\)](#)

PDF not a good format for redacting classified documents

<Bob Blakley iii <bob.blakley@gmail.com>>
Sun, 1 May 2005 17:24:16 -0500

Net-net, just in case you've been in a coma or something: PDF format used to black out portions of the classified report on the Nicola Calipari/Giuliana Sgrena incident; Italian newspaper (Corriere Della Sera) recovered and posted the classified text by performing a "copy and paste" operation on the blacked-out sections. Story here:

<http://it.slashdot.org/it/05/05/01/1314216.shtml?tid=172&tid=103>

COTS strikes again. The main risk is in using something you don't understand.

Another risk is in having allies whose press is eager to publish information which will endanger your troops.

Time Warner backup tapes lost with 600,000 records

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

Mon, 2 May 2005 15:41:49 PDT

Time Warner Inc. data on 600,000 current and former employees stored on computer backup tapes was lost by an outside storage company. The Secret Service is now investigating. The tapes included names and Social Security information on current and former Time Warner employees, dependents, and beneficiaries, back to 1986.

http://money.cnn.com/2005/05/02/news/fortune500/security_timewarner/index.htm?cnn=yes

[See also

<http://www.nytimes.com/2005/05/03/business/media/03warner.html?>

[th&emc=th](#)

<http://finance.lycos.com/home/news/story.asp?story=48820133>

In addition, the *Wall Street Journal*, 3 May 2005, noted that the tapes were lost by Iron Mountain Inc., a data-storage company based in Boston. An Iron Mountain spokeswoman said this is the fourth time this year that Iron Mountain has lost tapes during delivery to a storage facility. PGN]

⚡ Hundreds of Texas driver's licenses mailed to wrong people

<"Gregory, Peter" <Peter.Gregory@wwireless.com>>

Thu, 28 Apr 2005 13:01:52 -0700

An agency that warns Texans not to share personal information with strangers because of the risks of identity theft mistakenly mailed hundreds of driver's licenses to the wrong people. The Texas Department of Public Safety (DPS) blamed the mixup on a malfunctioning machine that was recently installed to sort licenses for mailing. Statewide, at least 500 to 600 people who applied for a license renewal or replacement in late March or early April instead received somebody else's card, said DPS spokesperson Tela Mange. A driver's license contains enough personal information for thieves to open up a line of credit or a bank account in that name, make long-distance phone calls or apply for a Social Security card, according to the Texas attorney general's office. Information on the license includes a

full name, signature, birth date, height, eye color, address and a photograph. The driver's license number, assigned by DPS, is also used by many agencies to verify a person's identity. In the case of the mismailed licenses, no identity theft or other crime has been reported, Mange said.

[Source: *Knight Ridder Tribune*, 26 Apr 2005]

<http://www.kansascity.com/mld/kansascity/news/nation/11497175.htm>

(registration required)

Peter Gregory, CELLULARONE, Western Wireless Corporation
Bellevue, WA
425-586-8386 CISSP, CISA, Information Security Analyst

✶ False negatives on fingerprints

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

Thu, 5 May 2005 16:35:39 -0400

National Public Radio's Morning Edition included a report this morning that an accused murderer using an alias had been stopped and fingerprinted three times, but IAFIS (the FBI's Integrated Automated Fingerprint Identification System) didn't match his fingerprints to those on file under his real name. After the first false positive, it added his fingerprints to the database using his alias, and subsequent matches turned up the alias rather than his real name.

Based on the news report, there seems to be an assumption among the public

that IAFIS is 100% accurate, with 0% false negatives (the failure this time) and 0% false positives (where someone is inaccurately accused of a crime).

IMHO, this isn't a case so much of technology failure, as it is of unrealistic expectations of technology.

<http://www.npr.org/templates/story/story.php?storyId=4631503&sourceCode=RSS>

Also in the *Atlanta Journal Constitution*

<http://www.ajc.com/metro/content/metro/0505/04jones.html>

(free signup required).

[He was already wanted on charges of rape, sodomy, and jumping bond, and

now has been charged with three subsequent murders and suspected of

another. See an article by Ellen Barry and Jenny Jarvie, *Los Angeles

Times*, 5 May 2005]

<http://www.latimes.com/news/nationworld/nation/la-na-killer5may05,0,7657766.story?coll=la-home-nation>

✉ Re: SecurID and E*TRADE (Taft, [Risks-23.84](#))

<Vin McLellan <vin@theworld.com>>

Tue, 03 May 2005 17:38:30 -0400

In [RISKS-23.84](#), Ed Taft <taft@adobe.com>, Principal Engineer at Adobe, and a

respected Adobe spokesman on standards and security issues, expressed

skepticism about the security, reliability, and user-friendliness of the RSA

SecurID, the one-time password (OTP) token that E*TRADE

Financial is distributing to customers to enhance the security of their online market trades, and the privacy and integrity of E*TRADE's brokerage records.

Subsequently, in [RISKS-23.85](#), Jon Lewthwaite <JLewthwaite@passgo.com>, offered the Adobe exec the vigorous if convoluted endorsement of an RSA competitor, while Kurt Raschke <kurt@raschke.net>, a Baltimore high school student, tech editor of the Towson High "Colophon," reacted to Mr. Taft's complaints with wry insight.

"Ed raises these issues as though E*TRADE is the first company to ever implement SecurID," wrote a bemused Raschke, "but in reality they are not very grave issues, and many government labs and other organizations find SecurID to be a very good security method despite them." Mr. Raschke, a teenager who develops open-source projects on SourceForge, turns out to be a veteran sysop, quite familiar with SecurID and practical security issues. By contrast, Mr. Taft, one of the architects of Postscript and PDF, reacted to his new SecurID as if it was the first time he had encountered a blinking LCD:

>I recently received "The E*TRADE Complete Security System" for controlling
>access to my online E*TRADE account. It introduces two-factor
>authentication to the login process, requiring both something I
know (my
>password) and something I have (a keyfob device). While this
seems like a
>very good idea on the surface, the implementation leaves
something to be

>desired from a usability standpoint.

RSA's SecurID is a small, hand-held, personal authentication device that uses the US standard AES cipher, Current Time, and a 128-bit "shared secret" to generate, and continuously display, one-time passwords: 6-8 character "token-codes" that change every 60 seconds. E*TRADE has re-branded the RSA OTP token as its own "Digital Security ID" and is offering it without charge to its "Power" and "Priority" customers: independent market traders who make 15 trades per quarter, or have more than \$50,000 at play in E-TRADE accounts.

A FDIC study published in December 2004 concluded that -- with 24/7 remote global access to financial networks now the norm; and "fraud through impersonation" rampant -- "single-factor" password-based credentials, susceptible to capture and replay, no longer provide financial service customers with the credible security required for remote access to critical infrastructure. "Two-factor authentication," said the FDIC, "should be considered as the new security baseline for remote access to computer systems."

Unlike banks, brokerages are not covered by the FDIC and "Regulation E" rules that limit consumer liability and ensure that defrauded bank customers are made whole. US brokerages usually return money that was transferred from an account due to criminal activity, but they are not obligated to do so. Losses due to online fraud are growing, but financial

institutions
across the board worry far more about the public reaction to the
drumbeat of
headlines about "identity theft" and multiple thefts of personal
information
data files. Perceived risk has already had a noticeable impact
on public
trust. Financial institutions increasingly rely on online
channels for
margins in their delivery of retail financial services, but
Gartner reports
that almost 60 percent of online consumers are "concerned" or
"very
concerned" about the security of financial services' web portals.

Spurred by regulators, carping customers, foreign competitors,
and consumer
surveys, all US financial institutions are looking at two-factor
authentication (2FA) -- but US brokerage firms, led by E*TRADE,
the first
online broker, seem to be adapting to the 2FA requirement more
quickly than
US banks. E*TRADE Financial, with assets exceeding \$17 billion,
is today
the 3rd largest online brokerage (by transaction volume); as
well as the 3rd
largest mortgage originator; and the 8th largest financial
institution
regulated by the US Treasury's Office of Thrift Supervision.

Mr. Taft described E*TRADE's new access protocol:

>The keyfob device, which carries E*TRADE and RSA logos, has a 6-
digit
>display that changes once per minute. In order to login, I need
to present
>my username and a password consisting of my regular fixed
password
>appended with the currently displayed 6-digit number.

E*TRADE is using one of RSA's newer SecurIDs -- a smaller key-
shaped token,
sometimes called a key ring "fob" -- but the SecurIDs deployed

by E*TRADE

are functionally identical to those used daily by over 15 million men and women, largely enterprise corporate employees, at over 15,000 institutions.

E*TRADE chose to substitute its own established password system -- so customers like Mr. Taft need not memorize a new password -- for the small password (aka "PIN") typically required as the second factor in SecurID 2FA installations. These passwords were previously used as E*TRADE's stand-alone authenticators, so they are surely at least marginally more secure than the 4-digit PINs traditionally used with SecurIDs by the White House staff, US Senators, and (as Mr. Raschke noted) employees in numerous government agencies, American and allied, around the globe.

Mr. Taft began a querulous litany:

>While this appears to have good security, some potential deficiencies come

>to mind --

>

>* It requires more typing than the old scheme, including an unfamiliar

>sequence of characters that changes every time.

I've been a consultant to RSA for nearly as long as Mr. Taft has been at Adobe, but Taft's fussy fretful complaints about "potential deficiencies" in the E*TRADE initiative bewilder me. The carefully-nuanced E*TRADE implementation is, to my mind, a case study of how to do 2FA right: application-specific, proportional, and customer-savvy -- with the option of cranking up the security barrier even higher, as needed, with additional changes at the server end of the SSL link.

E*TRADE launched this program in March after an extensive pilot project in which E*TRADE adapted the SecurID to their specific client requirements, and carefully explored the receptivity of E*TRADE customers to 2FA. Online investors expect their brokerage to offer security that will adapt to evolving threats, transparently where possible, overtly when necessary. They also demand immediate and relatively unobstructed access to their accounts, any time, from anywhere. And when they feel secure, they buy more financial services.

Most SecurID token-holders are corporate employees required to use 2FA to safeguard corporate resources. E*TRADE knows consumers march to a different drum. E*TRADE's P&P clients are given a choice: 2FA is voluntary -- and, for these select clients, the token is free. The old password system doesn't change; the OTP is simply an added service option. E*TRADE expects a high opt-in from brokerage customers who realize that it's their own assets and privacy that is at risk.

Instead of an OTP token, Mr. Taft opined, E*TRADE should have provided its customers with digital certificates in USB plugs:

>A better arrangement would be for the keyfob to have a USB connector that
>I plug into my computer to prove that I have the keyfob.

Yet, as young Mr. Raschke noted:

>>Having a keyfob with a display allows the device to be used with any sort

>>of computer -- not every computer out there has a USB port, or one that
>>is user-accessible. What if you log in using a phone or a PDA?

USB authentication tokens are hot, the fastest-growing niche market in personal authentication. USB ports are multi-use connectors, and their widespread use in PC hardware has delighted PKI advocates who waited 25 years for smart-card readers on PCs. But USB is not ubiquitous. Twenty percent of the PCs sold two years ago didn't have USB ports, and the percentage rises rapidly with older PCs. Phones and PDAs, as Kurt noted, lack the port. Publicly accessible PCs -- at airport kiosks, hotel business centers, Internet cafes, conference sites -- often block USB ports to minimize their vulnerability to vandals and other local threats.

A USB plug, for those unfamiliar with the tech, is a small injection-molded dongle, typically with a microprocessor and sufficient memory to securely store digital certificates and crypto keys. Plugged into a computer's USB port and initialized with a password, it can, like a smartcard, provide cryptographic services locally, and -- in conjunction with a public-key infrastructure (PKI) -- over a network: two-way authentication, encryption, digital signatures, assurances of message integrity, even "non-repudiation." Cost-effective PKI is still an institutional challenge, and consumer PKI an irksome Grail, but it's a rich technology.

Against all that, the SecurID offers a stark if elegant simplicity. The OTP is available anytime, anywhere. It provides the functionality

expected, and
no more -- an assurance difficult to obtain from a USB memory
stick or a
smartcard with a direct circuit connection to the CPU and the
Net.

Adobe's market lies largely in institutional sales, where users
are
disciplined to hierarchy and PCs are standardized and routinely
upgraded. A
financial services firm like E*TRADE serves opinionated
individual
investors, like Mr. Taft, who have no common computing platform
-- and
little patience with any service provider which tries to dictate
the
configuration of their computers, let alone what communications
device they
can use, when they get down to business.

(RSA, of course, invented RSA public key crypto and the PKCS
protocols used
to implement certificate-based PKI. So when E*TRADE chose
classic SecurIDs
over USB plugs, it wasn't because RSA didn't offer the USB
option. RSA has
sold USB tokens, smartcards, Keon PKI, and BSAFE crypto modules
for a long
time. RSA's newest SecurID -- one of the five models it now
sells --
actually features both a LCD for OTP display and a USB plug:
<<http://tinyurl.com/9rqog>>.)

Mr. Taft had another worry about the E*TRADE setup:

>* What if I need to login when I don't have the keyfob? There
is a phone
>number I can call to obtain temporary-access instructions,
assuming that I
>can convince the agent that I am the legitimate owner of the
account. This
>seems like a potential weak link in the scheme.

Anything less than 2FA is inherently less secure, but jeeze! -- the problem of temporary credentials exists where E*TRADE still relies on static passwords, and would exist even if the brokerage had issued USB plugs. If Mr. Taft forgets his fob, he can still offer his password, which might gain him some account privileges, but not others. These are local policy issues, and E*TRADE is a financial institution which has had a lot of experience managing this particular risk.

People are always the "weak link" in any security scheme. E*TRADE customers are people with power, with a choice among service providers. Like C-level executives who call their corporate help desk, privileged consumers probably expect E*TRADE to have a human over-ride for rigid technology (and granular levels of authorization at hand).

Mr. Taft had one prescient concern:

>* If multiple service providers adopt this scheme, I'll need a pocket full
>of keyfobs. A better arrangement would be one keyfob that can hold
>credentials for logging into multiple sites.

In the token trade, this is called the "necklace" scenario, which for me always conjures up an image of cargo-cult Polynesian natives dancing with a string of SecurIDs around their necks. Corporate partners deal with this today with "federated identity" mechanisms: bilateral or group agreements to honor one another's authentication credentials, with the privileges of the "visitors" constrained as appropriate. (See, e.g.,

<<http://tinyurl.com/43jfl>>)

In consumer financial services, however, attempts to establish a collaborative "trusted third-party" entity for federated identity management have run afoul of competitive realities. In response, two months ago, RSA announced the RSA Authentication Service, a managed service provider which later this year will offer a network of bilateral authentication services for organizations serving consumer markets.

E*TRADE immediately announced that it would be the first RAS pilot site.

RSA VP Chris Young -- who was the head of safety and security for AOL premium services, when AOL first offered SecurIDs to its subscribers -- leads the product development team.

The RSA Authentication Service (RAS) will require only that each participating institution has to trust RSA, as many already do for mission critical IT services. And the design goal for RAS is for RSA to hold almost zero information about the token-holder or his accounts.

A customer of, say, "BoldBank" may have a SecurID issued by his bank. If he needs a broker, and he sees (on the E*TRADE website) that E*TRADE is willing to use the BoldBank SecurID he already carries as his E*TRADE 2nd authenticator for 2FA -- he simply gives E*TRADE the serial number embossed on that SecurID and creates a password.

E*TRADE then asks RAS to associate that SecurID, by serial number, with an E*TRADE-specific value -- say a pseudo-random number -- that will in the future be used to link authentication requests from that SecurID with a

specific but unidentified E*TRADE account. RAS can now validate SecurID authentication calls from both account providers.

The next time the customer signs on at the E*TRADE SSL portal, he provides his account name, password, and SecurID OTP. E*TRADE will validate the password locally. It will then link the SecurID "token-code" with the PRN identifier it gave RAS, and pass both over to RSA for a blind validation of the OTP.

When E*TRADE receives the RAS's validation of the OTP, it has 2FA. The brokerage then makes the final link to the customer's account and opens that account with whatever privileges it has conferred on the customer. The account providers maintain total control over their customer information; RAS doesn't want to know who or what is involved.

Needless to say, Metcalfe's Law applies. RAS is an ambitious undertaking, perhaps comparable to the introduction of the early ATM networks, or RSA's spin-off of VeriSign ten years ago to exploit the potential of digital certs. The politics of trust, and the potential risks of "one token, many sites," will probably be the subject of RISKS commentaries at least through Mr. Raschke's college years. Expect a few from him.

In his E*TRADE litany, Mr. Taft eventually stepped beyond grounded concerns.

>* The scheme seems to depend on the keyfob and the server to have >synchronized clocks. What happens if the keyfob's battery dies or the

>server's clock becomes misadjusted, as appears to occur with some regularity?

Without sources or citations, without claiming first-hand experience himself, Mr. Taft -- a gentleman of some prominence in this industry -- offers an accusation on the level of a "wife-beating" rumor. If Mr. Taft had a competitive bias in this discussion (as I do), this would rank as FUD: fear, uncertainty, and disinformation

If a battery fails, as Mr. Raschke put it, "replace the token. It's as simple as that." RSA provides a full warranty on its sealed, tamper-resistant, SecurIDs. In 17 years, I can only recall a single batch of SecurIDs that had to be recalled (two years ago) because of electrical or battery problems. SecurIDs are programmed for a pre-designated product life of up to five years -- three years for the E*TRADE token, I think -- but the risk of a flawed SecurID battery is, historically, minuscule

If and when a host server's clock becomes "misadjusted," it may (but not necessarily) require the RSA Authentication Manager to reset -- but the RAM (aka ACE/Server) is itself rarely the cause of any disruption in the host. (Veteran ACE Admins on the list are invited to comment.)

No hardware/software product is perfect, but the stability and reliability of the SecurID and its authentication server is such that it has -- for 15 years -- constantly held about a 70 percent share in a very competitive growth market for OTP tokens. After nearly two decades in the field, RSA's regular enhancements to the SecurID, and functional extensions

for its authentication server, can still pull in a dozen respected "Best New Product" and "Readers' Trust" awards. See the 04/05 prize list at: <http://tinyurl.com/8xbdg>.

Mission-critical applications are necessarily held to a high standard. Does Mr. Taft really believe that RSA's SecurID could be this popular, for this long, if the employees of RSA's customers -- "with some regularity" -- were unable to access network resources? Does anyone believe that Microsoft would open up the Windows logon process, as it did last year -- so that SecurIDs and 2FA could be used to replace Windows XP passwords -- if SecurID 2FA was so undependable?

A series of time-synch patents give RSA exclusive control over the mechanism that keeps the RAM server's clock "virtually" synchronized with the clock chips in each of the SecurIDs pre-registered on that server. Those patents allow for the elegant roll of 60-second OTPs on a SecurID, and that simplicity, historically, conferred on the SecurID an ease-of-use advantage over Challenge/Response tokens.

Some analysts expect the half-billion dollar market for "strong authentication" tech to double over the next three years -- largely because of new regulatory demands, in the US and elsewhere -- but the 2KA market is also increasingly splintered among software and hardware options. OTP tokens; smartcards; USB plugs; GSM SIMs; biometric sensors; and flash drives are all in the hardware mix. Time-synch was the foundation of

RSA's market dominance in OTPs, but it confers no particular advantage over C/R when smartcards or USB plugs can make a direct circuit connection with the network. In an increasingly-level competitive field, RSA has only reliability and innovation to hold customers and win new ones, like E*TRADE.

(OT: RSA has leveraged the SecurID's popularity, and its BSAFE crypto savvy, into an array of oft-lauded products <<http://tinyurl.com/3k334>> for Identity & Access Management, Single Sign-On, Federated Identity Management, and a 2FA-enabled Microsoft security infrastructure: SecurID for Windows.)

Mr. Taft offered a final pessimistic coda:

>Fortunately, use of this security system is optional. The RISK is that
>nobody will use this scheme because it is too inconvenient.

The real RISK here is that someone might be influenced by Mr. Taft.

Mr. Taft, maybe, is going to refuse to use the free E*TRADE token? As an E*TRADE customer, that's his privilege. Risk, like convenience, is relative. Threats that move me or others to mitigate a risk may not motivate Mr. Taft enough to get him to type an additional six digits.

Mr. Taft, however, seems to be recommending that other E*TRADE customers should reject the E*TRADE 2FA tokens. "Fortunately," he concludes, all distant and academic, they don't have to use the SecurIDs. Is Mr. Taft

urging E*TRADE investors to ignore the free E*TRADE tokens?
Urging them,
instead, to continue to use static passwords, on vulnerable PCs,
to execute
market trades and access their financial records?

That, from a prominent IT professional, strikes me as
mischievous, if not
irresponsible.

PS. My bias is overt. I have been a consultant to RSA since
before the
first SecurID was brought to market, and an evangelist for OTPs
even before
that. I beg the indulgence of the List and PGN for length, but
its been a
quiet weekend on the Net, and a rainy Sunday here.

Vin McLellan + The Privacy Guild + <vin@theworld.com>
22 Beacon St., Chelsea, MA 02150



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



THE 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 23: Issue 87

Tuesday 17 May 2005

Contents

- [Prius cars shutdown at speed](#)
[Edwin Slonim](#)
- [The Downside of Wired Hospitals](#)
[Ken Knowlton](#)
- [Medical Usability: How to Kill Patients Through Bad Design](#)
[Dan Jacobson](#)
- [REAL ID](#)
[Bruce Schneier](#)
- [US Government to alter RFID passport regulations](#)
[Avishai Wool](#)
- [Good old-fashioned physical security](#)
[Joseph Shead](#)
- [Social security number seeding](#)
[Pekka Pihlajasaari](#)
- [IT forecast from Dave Patterson](#)
[Marcus H. Sachs](#)
- [Car breakins using bluetooth](#)
[Andrew Nicholson](#)

- [Don't blame the messenger](#)
[Paul Tomblin](#)
 - [Re: PDF not a good format for redacting classified documents](#)
[Bob Blakley](#)
 - [Re: Amtrak's Acelas](#)
[Philip Nasadowski](#) [Martin Ward](#) [Derek P Schatz](#)
 - [Train anomaly](#)
[PGN](#)
 - [Comair: Bound to Fail](#)
[Craig S. Bell](#)
 - [What Search Sites Know About You](#)
[Joanna Glasner via Monty Solomon](#)
 - [Re: BofA agent gives out personal information](#)
[Brent J. Nordquist](#)
 - [SecurID: bad compared to what?](#)
[Rick Smith](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Prius cars shutdown at speed

<"Edwin Slonim" <eslonim@minols.com>>

Tue, 17 May 2005 13:19:35 +0300

The U.S. National Highway Transportation Safety Administration has 13

reports of Toyota's Prius gas-electric hybrid cars (2004 and early 2005)

stalling or shutting down at highway-driving speeds, which Toyota

attributes to software problems. [Source: Toyota Attributes Prius

Shutdowns To Software Glitch Sholnn Freeman, *The Wall Street Journal*, 16

May 2005; PGN-ed]

I have always feared losing power, brakes and steering at high

speed - with
a helpful dashboard indication of "internal error 687, please
reset". Looks
like it is starting to happen. Of course we need to put this
into
proportion - how many cars stall at high speed with a fuel
blockage, or
swerve with a blowout.

Edwin Shalom Slonim, eslonim@minols.com Minols Ltd, 83 Moriah
Blvd,
PO Box 7360, Haifa 31072 Israel +972-4-826-6583

✶ The Downside of Wired Hospitals

<Ken Knowlton <KCKnowlton@aol.com>>

Fri, 29 Apr 2005 19:29:59 EDT

"Computers are making hospitals more dangerous, new research
suggests.
Computer keyboards fester with colonies of bacteria, which can
easily spread
from the medical personnel who use them to the patients they
treat. Some
hospitals now have computers in every patient room, creating
even more
opportunities for contamination. Researchers at Northwestern
Memorial
Hospital in Chicago found that the types of bacteria commonly
found in
hospitals -- some resistant to antibiotics -- could survive on a
keyboard
for 24 hours. Simply cleaning the computers with soap and water
didn't make
a difference. Using a strong disinfectant did kill the germs --
but it also
damaged the computers. 'The difficulty with keyboards is you
can't pour
bleach on them,' Dr. Allison McGreer of Toronto's Mount Sinai

Hospital tells

The Canadian Press. 'They don't work so well when you do that.' Because

it's nearly impossible to keep keyboards sterile, researchers say, the onus

is on doctors and nurses to wash their hands vigorously and often."

[Excerpted from *The Week*, 29 May 2005]

⚡ Medical Usability: How to Kill Patients Through Bad Design

<Dan Jacobson <jidanni@jidanni.org>>

Mon, 02 May 2005 08:48:36 +0800

<http://www.useit.com/alertbox/20050411.html>

⚡ REAL ID

<Bruce Schneier <schneier@COUNTERPANE.COM>>

Sun, 15 May 2005 03:39:20 -0500

[PGN-Excerpted from CRYPTO-GRAM, May 15, 2005

Counterpane Internet Security, Inc.]

<<http://www.schneier.com>><<http://www.counterpane.com>>

The United States will get a national ID card. The REAL ID Act establishes

uniform standards for state driver's licenses, to go into effect in three

years, effectively creating a national ID card. It's a bad idea, and is

going to make us all less safe. It's also very expensive. And it all

happened without any serious debate in Congress.

I've already written about national IDs. I've written about the fallacies of identification as a security tool. I'm not going to repeat myself here, and I urge everyone who is interested to read those essays (links at the end). Remember, the question to ask is not whether a national ID will do any good; the question to ask is whether the good it does is worth the cost. By that measure, a national ID is a lousy security trade-off. And everyone needs to understand why.

Aside from the generalities in my previous essays, there are specifics about REAL ID that make for bad security.

The REAL ID Act requires driver's licenses to include a "common machine-readable technology." This will, of course, make identity theft easier. Already some hotels take photocopies of your ID when you check in, and some bars scan your ID when you try to buy a drink. Since the U.S. has no data protection law, those businesses are free to resell that data to data brokers like ChoicePoint and Acxiom. And they will; it would be bad business not to. It actually doesn't matter how well the states and federal government protect the data on driver's licenses, as there will be parallel commercial databases with the same information.

(Those who point to European countries with national IDs need to pay attention to this point. European countries have a strong legal framework for data privacy and protection. This is why the American experience will be very different than the European experience, and a much more

serious
danger to society.)

Even worse, there's likely to be an RFID chip in these licenses. The same specification for RFID chips embedded in passports includes details about embedding RFID chips in driver's licenses. I expect the federal government will require states to do this, with all of the associated security problems (e.g., surreptitious access).

REAL ID requires that driver's licenses contain actual addresses, and no post office boxes. There are no exceptions made for judges or police -- even undercover police officers. This seems like a major unnecessary security risk.

REAL ID also prohibits states from issuing driver's licenses to illegal aliens. This makes no sense, and will only result in these illegal aliens driving without licenses -- which isn't going to help anyone's security. (This is an interesting insecurity, and is a direct result of trying to take a document that is a specific permission to drive an automobile, and turning it into a general identification device.)

REAL ID is expensive. It's an unfunded mandate: the federal government is forcing the states to spend their own money to comply with the act. I've seen estimates that the cost to the states of complying with REAL ID will be tens of billions. That's money that can't be spent on actual security.

And the wackiest thing is that none of this is required. In

October 2004,
the Intelligence Reform and Terrorism Prevention Act of 2004 was
signed into
law. That law included stronger security measures for driver's
licenses,
the security measures recommended by the 9/11 Commission
Report. That's
already done. It's already law.

REAL ID goes way beyond that. It's a huge power-grab by the
federal
government over the states' systems for issuing driver's
licenses.

REAL ID doesn't go into effect until three years after it
becomes law, but I
expect things to be much worse by then. One of my fears is that
this new
uniform driver's license will bring a new level of "show me your
papers"
checks by the government. Already you can't fly without an ID,
even though
no one has ever explained how that ID check makes airplane
terrorism any
harder. I have previously written about Secure Flight, another
lousy
security system that tries to match airline passengers against
terrorist
watch lists. I've already heard rumblings about requiring
states to check
identities against "government databases" before issuing
driver's licenses.
I'm sure Secure Flight will be used for cruise ships, trains,
and possibly
even subways. Combine REAL ID with Secure Flight and you have an
unprecedented system for broad surveillance of the population.

Is there anyone who would feel safer under this kind of police
state?

Americans overwhelmingly reject national IDs in general, and
there's an
enormous amount of opposition to the REAL ID Act.

If you haven't heard much about REAL ID in the newspapers, that's not an accident. The politics of REAL ID was almost surreal. It was voted down last fall, but was reintroduced and attached to legislation that funds military actions in Iraq. This was a "must-pass" piece of legislation, which means that there was no debate on REAL ID. No hearings, no debates in committees, no debates on the floor. Nothing. And it's now law.

We're not defeated, though. REAL ID can be fought in other ways: via funding, in the courts, etc. Those seriously interested in this issue are invited to attend an EPIC-sponsored event in Washington, DC, on the topic on June 6th. I'll be there.

Text of the REAL ID Act:

<<http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00418:>>

Congressional Research Services analysis:

<<http://www.eff.org/Activism/realid/analysis.pdf>>

My previous writings on identification and national IDs:

<<http://www.schneier.com/crypto-gram-0404.html#1>>

<<http://www.schneier.com/crypto-gram-0402.html#6>>

<<http://www.schneier.com/crypto-gram-0112.html#1>>

Security problems with RFIDs:

<<http://www.schneier.com/crypto-gram-0410.html#3>>

My previous writings on Secure Flight:

<<http://www.schneier.com/crypto-gram-0502.html#1>>

Resources:

<http://www.epic.org/privacy/id_cards/>

<<http://www.unrealid.com/>>

EPIC's Washington DC event:

<<http://www.epic.org/events/id/savethedate.html>>

✈ US Government to alter RFID passport regulations

<Avishai Wool>

Fri, 6 May 2005 17:18:40 +0300

Responding to fears raised by privacy advocates that new electronic passports might be vulnerable to high-tech snooping, the State Department intends to modify the design so that an embedded radio chip holding a digitized photograph and biographical information is more secure. [Source: Bowing to Critics, U.S. to Alter Design of Electronic Passports

Eric Lipton, *The New York Times*, 27 Apr 2005]

<http://www.nytimes.com/2005/04/27/politics/27passport.html>

[requires registration]

On a personal (self-congratulatory) note, it seems that a recent paper by Ziv Kfir and myself:

"Picking virtual pockets using relay attacks on contactless smartcard systems"

<http://eprint.iacr.org/2005/052>

was used as ammunition in the campaign to pressure the state department to rethink the e-passport design.

RISKS readers may find interest in this letter from the Berkeley Law School

to the Office of Passport Policy, on behalf of an impressive list of

computer scientists and security experts, explaining what was wrong with the previous design:

[http://www.law.berkeley.edu/cenpro/samuels/papers/other/
ElectronicPassport_Comments_DOS.pdf](http://www.law.berkeley.edu/cenpro/samuels/papers/other/ElectronicPassport_Comments_DOS.pdf)

Curiously, I saw somewhere recently (I don't have the URL handy) that the only country in the world that was ready with the (now defunct) e-passport was Belgium(?). The US was not ready to meet its own deadline... I bet some people in Brussels are less than happy with the news...

Avishai Wool, Ph.D., School of Electrical Engineering, Tel Aviv University,
Ramat Aviv 69978, ISRAEL <http://www.eng.tau.ac.il/~yash>

Good old-fashioned physical security

<"Joseph Shead" <Joe@SheadProgramming.com>>
Sat, 7 May 2005 14:05:02 -0500

Lost items puzzle nuclear research lab: The U.S. federal Idaho National Laboratory nuclear-reactor research lab cannot account for more than 200 missing computers and disk drives that may have contained sensitive information. The computers were among 998 items costing \$2.2 million dollars that came up missing over the past three years. Lab officials told investigators that none of the 269 missing computers and disk drives had been authorized to process classified information. But they acknowledged there was a possibility the devices contained "export controlled" information -- data about nuclear technologies applicable to both civilian

and military use. [Source: AP item from *The Boston Globe*, 7 May 2005, PGN-ed]

✶ Social security number seeding (Re: [RISKS-23.85](#) et al.)

<Pekka Pihlajasaari <pekka@data.co.za>>

Wed, 27 Apr 2005 11:28:56 +0200

Many articles documenting the risks of exposure of personally identifiable information bemoan the possibility of compromise. There seems to be very little quantitative information on the number of cases where the information is used inappropriately.

If a selection of unused social security numbers were identified as probes, these could be used by credit bureaux and other large databases as proxies for compromise. Any use of these numbers would be positive confirmation of breach of the related database, and an indication of the rate at which harvested numbers are utilised. While this does pollute the datasets with incorrect data, this provides an in-band mechanism to detect misuse. The practise has been in use by mailing list rental companies to count the number of times a list is used.

The low occurrence of the probes makes wholesale harvesting easy to detect and difficult for the harvester to protect themselves against. This risk, of course, is that the list of probe numbers is compromised!

Pekka Pihlajasaari pekka@data.co.za +27 (11) 728-0899 Data
Abstraction Ltd

IT forecast from Dave Patterson

<"Marcus H. Sachs">

Wed, 11 May 2005 21:53:10 -0400

"The history of IT is littered with companies that lost substantial leads in this fast-changing field. I see no reason why it couldn't happen to countries. Indeed, at the recent International Collegiate Programming Contest of the Association for Computing Machinery, four Asian teams finished in the top dozen, including the champion, while the best U.S. finish was 17th, the country's worst showing ever. If current U.S. government policies continue, IT leadership could easily be surrendered to Asia."

[ACM President David Patterson gave testimony before a Congressional hearing last week. PGN]

http://news.com.com/Surrendering+U.S.+leadership+in+IT/2010-7337_3-5701653.html

Car breakins using bluetooth

<Andrew Nicholson <andrewn@lesto.com>>

Fri, 6 May 2005 11:35:08 -0700

I recently lost our rental car in one of the huge parking lots of Disney World. The color and license plate entry on the rental car tag were incorrect and we couldn't remember the color and we had the row wrong.

Eventually security drove us around while I pushed the "panic" button on the remote key fob at any likely looking vehicle. Security knew roughly where the cars were parked based on the time that you caught the shuttles. Once we found the car that was it - no further checks.

During the search I asked about car theft from the parking lots given that they are huge and there is little sign of security patrols etc. The claim was that they don't have many car thefts, but they do have 4 to 5 break-ins every day where the contents of the cars are stolen.

Here's the interesting part: every break-in in the past month had involved a laptop with internal bluetooth. Apparently if you just suspend the laptop the bluetooth device will still acknowledge certain requests allowing the thief to target only cars containing these laptops.

⚡ **Don't blame the messenger (Re: Blakley, [RISKS-23.86](#))**

<Paul Tomblin <ptomblin@xcski.com>>

Fri, 6 May 2005 21:38:27 -0400

In [RISKS-23.86](#), Bob Blakley attacks the Italian newspaper who discovered that they could use cut and paste to see "blacked out" text as "having allies whose press is eager to publish information which will endanger your troops".

He's not the only one, as evidenced by the discussion in the Slashdot article he referenced.

It's an incredible mistake to think that America's enemies are so unsophisticated or stupid that they couldn't figure this same method out themselves if the Italian newspaper hadn't published it. Underestimating your enemy is a sure way to lose.

Paul Tomblin <ptomblin@xcski.com> <http://xcski.com/blogs/pt/>

⚡ Re: PDF not a good format for redacting classified documents

<Bob Blakley <bob.blakley@gmail.com>>

Fri, 6 May 2005 12:25:03 -0500

What's most interesting to me about this is that it will undoubtedly generate all sorts of proposals for wildly expensive and demonstrably ineffective fixes.

My prediction is that the preferred proposals will be:

1. A proprietary mil-spec word processor which is guaranteed to delete what it redacts, to be developed bespoke.

2. A complicated PDF file filter which searches for classified information at specified levels and strips it out.

These would be multimillion dollar projects with a customer base of - say - five, and would be predictably behind schedule and ineffective.

The problem, of course, arises because the appearance of the document on the screen does not correspond to its deep structure. However it's easy and cheap to fix this problem.

The \$100 solution would be to designate a redacted-document-release server and configure it so that it only accepts uploads via FAX.

To get documents onto such a server, you'd need to go through the analog hole, which would automatically guarantee that the document's appearance IS its deep structure. Voila.

✶ Re: Amtrak's Acelas ([RISKS-23.85](#))

<Philip Nasadowski <nasadowsk@usermail.com>>

Tue, 26 Apr 2005 22:49:45 -0400

Actually, Acela's problems are a bit deeper:

* The trainset was built 4 inches wider than it was supposed to. Nobody really knows or will fess up as to why. as a result, it can't tilt on trackage owned by Metro-North, which is the curviest part of the system. Elsewhere, it can't tilt as much as it was supposed to.

* The trainsets are built to the US DOT's 'Tier II' standards, which require strength standards roughly 5 times that of UIC (European) railcars. The result is an enormous increase in weight - the unpowered Acela coaches are nearly as heavy as the TGV's locomotives (!).

* The above weight issues result in the train being unstable at running speeds, a problem never totally solved. In addition, the curve speeds must be lower (because of the weight).

* TGVs use their locomotives for a large amount of the total braking on the train (easily 33%). Acelas can't do this because they're so heavy. Thus, higher use of friction braking.

* Lower curve speeds mean slowing down more after a straight run...

* And that means more, heavier use of the brakes.

* Unwillingness on the part of Amtrak and the US DOT to adopt a distributed setup where every car is powered meant additional weight (locomotives at the ends) and only 4 axles with regenerative braking, i.e. braking with the motors.

The real issue is that Amtrak and the DOT insisted on a custom, untested design based on a design concept that was out of step (180 degrees!) with every other high speed train built in modern times. Had Amtrak simply purchased a modified form of the X-2000 tested here in the early 90's, we wouldn't have this fiasco today. Ironically, the X-2000 was

cleared for
higher curve speeds than the Acela can achieve safely...

Sometimes reinventing the wheel isn't a good idea...

⚡ Re: Amtrak's Acelas (Harrison, [RISKS-23.85](#))

<Martin.Ward@durham.ac.uk>

Fri, 29 Apr 2005 14:10:04 +0100

> It seems that old-fashioned mechanical engineering is not
immune from the
> ills commonly ascribed to its software counterpart.

Of course not. Its just that when it happens in mechanical
engineering, the
result is news stories, lawsuits and (usually) action taken to
prevent
recurrence of the problems.

In software engineering, these problems are accepted as normal
business
practices.

Martin.Ward@durham.ac.uk <http://www.cse.dmu.ac.uk/~mward/> Erdos
number: 4

G.K.Chesterton web site: <http://www.cse.dmu.ac.uk/~mward/gkc/>

⚡ Re: Amtrak's Acelas (Harrison, [RISKS-23.85](#))

<"Schatz, Derek P" <Derek.P.Schatz@boeing.com>>

Wed, 4 May 2005 10:18:07 -0700

Lack of replacement brake parts is interesting, but what's the computer-related risk here?

["Risks to the Public in the Use of Computers and Related Systems." We

keep stressing the importance of systems in the large. Also, the

maintenance problem of letting essentially all of the trains fall apart

with no spare parts is symptomatic. PGN]

Train anomaly

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

Sat, 30 Apr 2005 20:46:43 PDT

I was on a "baby bullet" train last week that goes at the same speed as the regular trains but only stops a few times over the stretch from SF to SJose, and "the door is closing" recording kept playing between Palo Alto and Mountain View while the train whizzed past two stations with the door in front of me wide open. A conductor finally heard the repeated recording after about 5 minutes and tried to close the door manually with no success. I asked him if that happened often, and the answer was, with a shrug, ``Well, it does happen now and then.''

Comair: Bound to Fail

<"Craig S. Bell" <craig_s_bell@yahoo.com>>

Tue, 3 May 2005 17:27:44 -0700 (PDT)

Followup to the Comair incident:

CIO Magazine offers timeline. Stephanie Overby

<http://www.cio.com/archive/050105/comair.html>

The crash of a critical legacy system at Comair is a classic risk management mistake that cost the airline \$20 million and badly damaged its reputation.

What Search Sites Know About You (Joanna Glasner)

<Monty Solomon <monty@roscom.com>>

Thu, 28 Apr 2005 23:34:32 -0400

[Source: Article by Joanna Glasner, Wired.Com, 5 Apr 2005]

For most people who spend a lot of time online, impulsively typing queries into a search engine has become second nature.

Got a nasty infection in an embarrassing spot? Look up a treatment on your favorite search site. Obsessing about an ex? Try Googling his or her name. Chances are the queries will unearth some enlightening information.

But while search engines are quite upfront about sharing their knowledge on topics you enter in the query box, it's not so clear what they know about you. As operators of the most popular search engines roll out more services that require user registration, industry observers and privacy

advocates say

it's become more feasible to associate a particular query with an individual.

"You should think about what you put in that search box, because it may not

be as anonymous as you think," said Danny Sullivan, editor of SearchEngineWatch.com.

It has long been standard practice, Sullivan noted, for search sites to

employ cookies, which track activity on a computer's internet browser. But

cookies don't identify a person by name. If two people access a site on the

same browser, the cookie wouldn't distinguish between them.

However, when people provide personal information to register for services

offered by search engine companies, such as free e-mail accounts, news

alerts or personalized homepages, they're no longer anonymous. ...

<http://www.wired.com/news/privacy/0,1848,67062,00.html>

Re: BofA agent gives out personal information (Dickson, [RISKS-23.84](#))

<"Brent J. Nordquist" <brent@nordist.net>>

Tue, 19 Apr 2005 07:48:53 -0500

Given that the agent is using a BofA computer application in the course of

providing service, doesn't this seem like a problem you could solve with an

expert system? Design the BofA app. to require the agent to quiz the caller

on the standard birthdate, mother's maiden name or security password, last 4 of SSN, etc. authenticators, and enter that data before *any* identifying data is displayed back to the agent. If the agent can't see it, they can't violate (what I hope are) BofA's policies not to disclose it to someone who isn't authenticated.

Brent J. Nordquist <brent@nordist.net> N0BJN

Other contact information: <http://www.nordist.net/contact.html>

✦ **SecurID: bad compared to what? (McLellan, [RISKS-23.86](#))**

<Rick Smith <smith@smat.us>>

Sat, 07 May 2005 15:27:22 -0500

Lest people discount Vin McLellan's comments about SecurID by accusing him of being a shill for RSA, let me offer an independent observation. I made a detailed study of token technology a few years back while working for a competing vendor (Secure Computing, owner of the SafeWord token line) and while writing a book on authentication technology (aptly named "Authentication").

First, the typical alternative to SecurID's clock-based key fobs are "event based" key fobs, like SafeWord, in which the user must push a button to retrieve the next one time password. The effective differences between the two systems are minor, assuming they use comparable crypto. SafeWord tokens are based on DES technology and 56-bit keys, while traditional

SecurID

products used an internally-developed crypto algorithm with 64-bit keys.

The real difference today, however, is that the newer, high-end SecurID

products are based on AES with 128-bit keys. I don't know what key size is

used in the E*Trade token - none of the reports on this, including

Gartner's, have identified the token's key size.

Second, I agree with Vin's opinion regarding USB tokens. While I hope that

they're the wave of the future, they don't work with most of today's

authentication transactions, which tend to involve passwords embedded in web

pages. It's much easier to retrofit a web site to support a key fob's one

time password than it is to update both ends of the system to support

USB-based authentication.

Third, I agree with Vin that you can't fault E*Trade for providing a back

door so that users can still access their accounts after misplacing their

key fob. It may be lousy security, but it's what the user community needs.

Rick Smith, University of St. Thomas/Cryptosmith, Minnesota



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



THE 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 23: Issue 88

Tuesday 31 May 2005

Contents

- [Landing gear problem due to apparent computer glitch](#)
[Steven M. Bellovin](#)
- [The ChoicePointSyndrome](#)
[Robert Ellis Smith](#)
- [A bank you might not want to have Wachovia](#)
[PGN](#)
- [Hyperthreading vulnerability](#)
[Olin Sibert](#)
- [MarketScore exploit](#)
[Aaron Emigh](#)
- ["Rumplestiltskin worm" on the loose?](#)
[Brett Glass via Dave Farber](#)
- [The latest in clever spammer technique](#)
[Dan Wallach](#)
- [Trojan attack in Israel](#)
[Amos Shapir](#)
- [Re: PDF not a good format for redacting classified documents](#)
[Steven M. Bellovin](#)

- [Interesting typo](#)
[Jon Callas](#)
 - [Conference on Electronic Entertainment Policies, Problems, Solutions](#)
[Lauren Weinstein](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Landing gear problem due to apparent computer glitch

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Fri, 20 May 2005 15:33:15 -0400

The AP reports that an Airbus flown by a Turkish charter company had landing gear problems when arriving at Ben Gurion airport. Apparently, the pilot received indications that the nose wheel had not descended properly. In fact, it was down; the plane landed normally after the tower observed it visually.

The problem? According to the Anatolia news agency, it was a "glitch in a computer system".

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

⚡ The ChoicePoint Syndrome

<"Robert Ellis Smith" <ellis84@rcn.com>>

Thu, 19 May 2005 12:41:03 -0400

To appreciate THE CUMULATIVE EFFECT, Privacy Journal newsletter in its May

issue compiled the following list of breaches of sensitive personal information, disclosed just since January. It's not an atypical list for a three-month period, but breaches are obviously getting more press attention.

* Tepper School of Business at Carnegie Mellon University reported that a hacker had access to Social Security numbers and other sensitive personal information relating to 5000 or more graduate students, staff, and alumni.

Another department at the university is responsible for receiving complaints of Internet breaches and solving them.

* Tufts University notified 106,000 alumni, warning of "abnormal activity" on its fund-raising computer system listing names, addresses, phone numbers, and, in some cases, Social Security numbers and credit-card account numbers.

* ChoicePoint, the insurance and employment investigative company and "information broker" based in Georgia, sold personal data on from 100,000 to 500,000 or more persons to fraud artists posing as legitimate businesses.

(Still, the State of California plans to award a \$340,000 contract to the Equifax-created company to gather information on suspected criminals and terrorists, according to The Sacramento Bee.)

* DSW Shoe Warehouse experienced a hacking incident involving access to an estimated 1.4 million credit-card numbers and names, 10 times more than investigators estimated at first, as well as driver's license numbers and

checking-account numbers from 96,000 transactions involving other customers.

* A computer system breach at an unnamed retailer involved at least 180,000 customers, perhaps more. HSBC North America, which issues GM's MasterCard, urged all customers to replace their cards as quickly as possible because the personal data was compromised. The Wall Street Journal identified the retailer as Polo Ralph Lauren Corp., but the company insisted that in fact no information was leaked, although a computer flaw was discovered and fixed.

* Ameritrade Holding Corp., the online discount broker, informed about 200,000 current and former customers that a back-up computer tape containing their account information was lost when a package containing the data was damaged during shipping.

* Canadian Imperial Bank of Commerce, CIBC, one of Canada's leading banks, "failed to recognize" that misdirected confidential faxes sent to outside parties over a three-year period were a breach of customers' privacy that could have been prevented, according to a finding by the federal Privacy Commissioner in Canada. Bank of Montreal, Royal Bank of Canada, Scotiabank, TD Bank, and National Bank have also misdirected faxes with customer information.

* Motor vehicle departments in four states have lost personal data. The Texas Department of Public Safety mailed to 500 to 600 licensed drivers

renewal documents that pertained to other persons. In March, burglars rammed a vehicle through a back wall at a Nevada Department of Motor Vehicles facility near Las Vegas and drove off with files on about 9000 people, including Social Security numbers. In April police arrested 52 people, including three examiners at the Florida Department of Motor Vehicles, in a scheme involving the sale of more than 2000 fake driver's licenses. Also, Maryland police arrested three people, including a DMV worker there, in a plot to sell about 150 fake licenses.

* A Boston-based storage company named Iron Mountain Inc., lost Time Warner Inc.'s computer back-up tapes with Social Security numbers and names of 600,000 current and former employees and dependents. This is the fourth time this year that Iron Mountain has lost tapes during delivery to a storage facility, according to The Wall Street Journal.

* Someone gained access to the personal information of 59,000 current, former, and prospective students at California State University, Chico, the university revealed in March.

* A laptop that contains about 100,000 Social Security numbers of students and personnel at the University of California, Berkeley was stolen from the school's campus.

* Someone hacked into a database at the Kellogg School of Management at Northwestern University, possibly exposing data pertaining to 21,000 individuals at Northwestern.

* More than 1600 parents discovered in January that records in the Colorado State Health Department relating to an autism study were lost. A laptop computer left in a health department employee's automobile was apparently stolen last October.

*** A free copy of the current issue of Privacy Journal is available through orders@privacyjournal.net. Specify e-mail copy or hard copy (and include a mailing address).

Robert Ellis Smith, Publisher, Privacy Journal, PO Box 28577, Providence RI 02908 401/274-7861 fax 401/274-4747 <http://www.privacyjournal.net>

⚡ A bank you might not want to have Wachovia (bad pun)

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

Mon, 23 May 2005 16:56:33 PDT

More than 48,000 customers of Wachovia Corp. and 600,000 of Bank of America Corp. have been notified that their financial records may have been stolen by bank employees and sold to collection agencies. Nearly 700,000 customers of four banks may be affected, according to police in Hackensack, N.J. Nine people have been charged, including seven bank workers. Also affected were Commerce Bank and PNC Bank of Pittsburgh. Collection agent Orazio Lembo Jr., 35, of Hackensack made millions of dollars through the

scheme. Lembo received lists of people sought for debt collection and turned that information over to the seven bank workers, who would compare those names to their client lists. The bank workers were paid \$10 for each account they turned over to Lembo, Zisa said.

In a separate case with the potential for identity theft, a laptop containing the names and Social Security numbers of 16,500 current and former MCI Inc. employees was stolen last month from the car of an MCI financial analyst in Colorado.

[Source: An AP item by Paul Nowell, Banks Notify Customers of Data Theft, PGN-ed]

http://story.news.yahoo.com/news?tmpl=story&cid=528&e=3&u=/ap/20050523/ap_on_bi_ge/data_theft

Hyperthreading vulnerability

<Olin Sibert <u2190@siliconkeep.com>>
Tue 17 May 2005 08:56:03 -0400

Security researcher Colin Percival recently (13 May) announced a security vulnerability caused by the combination of the Hyperthreading and shared cache features of Intel Pentium 4 processors. By carefully measuring the time required for instructions to execute in one thread while the other thread is performing a cryptographic calculation, the secret key can be

determined. A paper describing the flaw is here:

<http://www.daemonology.net/papers/htt.pdf>

Colin notified OS vendors about the problem some months earlier, and fixes are available for several BSD and Unix distributions. It's been designated CAN-2005-0109 in the Common Vulnerabilities and Exposures list; more details here:

<http://www.daemonology.net/hyperthreading-considered-harmful/>

This vulnerability was also announced by Adi Shamir during the Cryptographer's Panel at RSA in February 2005. I thought it was the most interesting item in all the keynotes (although the hash function announcements were a close second), but it got essentially no press coverage (unlike this time, where it is being widely reported). Adi subsequently told me that he had a working implementation and planned to present it at the Eurocrypt rump session next week. The two attack implementations (Colin's and Adi's) are apparently quite different, but yield the same result, underscoring the severity of the problem. It's also similar to Paul Kocher's classic timing attacks.

The problem is particularly bad for processors with simultaneous multithreading ("Hyperthreading"), since that allows context switches to take place at a granularity of individual instructions, and thus allows very fine-grained time measurements. However, the same basic problem is present in any computer with a cache that is physically shared by processes in different security domains.

Although cache timing has been known as a covert channel for a long time, I

think this particular exploitation is really slick. I "discovered" a similar cache timing vulnerability during the covert channel analysis in the Multics B2 evaluation back in 1983/84, but I didn't have the wit to understand how interesting the consequences might be. I put "discovered" in quotes because of the way I was gently discouraged from further pursuit (or, horrors, publication) by some of the NSA personnel who were also involved. I was disappointed at the time, but in hindsight it seems likely they knew precisely where such pursuit might lead. Indeed, I understand that a similar vulnerability was uncovered by Marv Schaffer et al. in 1979 during the KVM/370 secure operating system project.

The RISK here is a classic example of relying on underlying abstractions (the hardware memory model) to behave in an ideal manner, rather than understanding their implementations. Many security flaws result from the adversary breaking the veil of abstraction to look at the soft, juicy parts inside. Even when the higher-level model is perfect (or formally verified), the mapping to implementation can hide a multitude of sins.

🔥 MarketScore exploit

<"Aaron Emigh" <aaron-risks@radixlabs.com>>

Fri, 27 May 2005 01:10:19 -0700

A company called MarketScore has a spyware product that includes a

full-fledged man-in-the-middle attack on all web traffic, including encrypted traffic. While any malware running in administrative mode is potentially catastrophic for subsequent trust and privacy, the MarketScore attack is especially ingenious and simple.

MarketScore/NS configures the user's machine to proxy all web traffic through their external server. One would ordinarily expect that SSL traffic would pass through the proxy opaquely. However, MarketScore also installs itself as a trusted root certification authority (under the name "Netsetter" or "MarketScore," depending on the version). Whenever the user connects to a secure site, MarketScore self-signs a certificate for the site and presents it to the user's machine. Since MarketScore is a trusted CA for the user's machine, the user sees no warning and gets the lock icon and yellow URL bar. However, MarketScore decrypts the traffic at the proxy server and re-encrypts it for its SSL session with the actual host. MarketScore is therefore able to play a man-in-the-middle on all traffic, including SSL traffic.

Apart from this exploit, MarketScore seems to be garden-variety spyware, which offers an e-mail virus scanning service in exchange for monitoring surfing activities as a sort of Nielsen service. The risks of this technique being applied toward identity theft and other malicious ends are, however, clear.

Aaron Emigh, Radix Labs 415-297-1305 aaron-risks@radixlabs.com

✦ "Rumplestiltskin worm" on the loose? (From Dave Farber's IP)

<Brett Glass <brett@lariat.org>>

May 7, 2005 12:15:03 AM EDT

This week, I have begun to see evidence -- in the form of "bounced" e-mails and error messages in our servers' log files -- that "zombie" machines which are infected by malware (either worms or spyware) are launching aggressive "Rumplestiltskin attacks" against mail servers throughout the Internet.

What is a "Rumplestiltskin attack?" As described in a paper I wrote several years ago (where I coined the term for lack of a better existing one), it is an e-mail address harvesting attack in which a machine attempts to send e-mail messages to randomly guessed addresses at a domain. It might try common first names -- for example, "john@domain.com", "joe@domain.com," and "mike@domain.com" -- and then proceed to common last names and combinations of names and initials. (In some cases, we've seen some very unusual guesses that appear to have been extracted from lists of AOL screen names.)

If mail for a guessed address is accepted, the "zombie" machine records the address and sends it back to its "master" -- a controlling machine which adds it to a database of addresses which will become targets for spam.

Because the address guessing process is expensive (both in terms of computing time and in terms of bandwidth), the best way to achieve results is via a rogue form of distributed computing, in which large numbers of "zombies" (machines co-opted via malware) are pressed to the task.

On our servers, these attacks and other traffic from spammers are now consuming approximately ten times more resources than all of our legitimate mail combined.

Because the "zombies" are generally not mail servers, the most effective way to mitigate these attacks -- though it might offend the sensibilities of the "Orthodox End-to-Endians" -- is for ISPs and enterprised to block outgoing port 25 traffic from client computers that are not designated as, or intended to be, mail servers. These computers should send outgoing mail only through a designated mail server, which in turn monitors them for excessive outgoing traffic.

ISPs' firewalls should monitor and log attempts to send such traffic, so that infected machines can be spotted and cleansed of their infections.

As I've mentioned above, there will be some people who are philosophically opposed to the notion of restricting Internet traffic so as to limit abuse. Alas, such idealism is inappropriate for the real world, where spam is now consuming so many resources that it threatens not only to choke off not only legitimate e-mail but to consume the lion's share of ISPs'

bandwidth.

[IP Archives: <http://www.interesting-people.org/archives/interesting-people/>]

🔥 The latest in clever spammer technique

<Dan Wallach <dwallach@cs.rice.edu>>

Mon, 09 May 2005 12:34:12 -0500

Earlier this year, we switched over to DSPAM, a fancy Bayesian spam classification system. We're also running SpamAssassin, which gives DSPAM a chance to see SpamAssassin's automatic classifications and determine, for itself, what weights are appropriate for each of those filters. After a couple months of this hybrid usage, I'm now getting about 99.4% classification accuracy (maybe two or three errors per day). What's interesting is what's still getting through.

Recently, I've gotten a number of spams that have perfect spelling and vanilla plain text (as opposed to the insane HTML ov3rki!! variety). If you look at the mail headers, there's some evidence of zombie machines being used to transmit the spam (i.e., received lines not matching up to the From or Sender line) but otherwise the headers are quite clean. For the message in front of me right now, the user agent is even listed as Mozilla on Linux. DSPAM has a clever feature where it will tell you what factors in the message it used to make its decision. In this case, DSPAM

latched onto the User-Agent string and other Mozilla-esque headers as having a very low probability of being spam. This outweighed a few strings that otherwise should have tipped it off (e.g., "credit history" or "secure, private").

In some sense, this is exactly what Paul Graham predicted would eventually happen in "A Plan For Spam". My hope is that I can eventually untrain DSPAM of its love for Mozilla headers; we'll see how well it does. My fear is that there will always be an avenue of attack for a "contrarian spammer" who engineers spam to be unlike all the other spams out there.

P.S. At this point, virtually all of my false positives (normal messages misclassified as spam) are coming from infrequent events that DSPAM would never enough data from which to be properly trained, such as the e-mail generated by a dot-com store when I bought a new camera lens.

⚡ Trojan attack in Israel

<"Amos Shapir" <amos083@hotmail.com>>

Mon, 30 May 2005 19:29:02 +0300

A large scale industrial espionage case is now unfolding in Israel (see <http://www.haaretz.com/hasen/spages/581790.html>). A hacker had developed a Trojan horse application and sold it to several private eye companies -- it seems the Trojan was used for keyboard sniffing as well as file

transfer.

The private eyes' clients chose the the targeted victims, and the Trojan was sent there by e-mail or posted CD, masquerading as legitimate business presentation.

The collected info was transferred from the victims' computers into an FTP server site (it's not clear if this site was maintained by the private eyes or the hacker) to which access was sold to the clients in the form of one-time passwords at 2000 Euro per entry.

It seems none of the targeted systems was hardened in any way to detect such an intrusion, and the scheme was discovered only because the hacker had posted some of the illegally obtained items over the net.

⚡ Re: PDF not a good format for redacting classified documents

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Fri, 20 May 2005 15:26:35 -0400

Bob Blakley writes:

> To get documents onto such a server, you'd need to go through the analog
> hole, which would automatically guarantee that the document's appearance IS
> its deep structure. Voila.

When NSA declassified the Skipjack cipher, many people laughed because the document was a scanned image. "Doesn't the NSA know how to use PDF properly?" Seems to me that NSA has understood this principle

for many
years.

⚡ Interesting typo (Wool, [RISKS-23.87](#))

<Jon Callas <jon@callas.org>>
Tue, 17 May 2005 17:34:22 -0700

In [RISKS-23.87](#), "US Government to alter RFID passport regulations"

"... embedded radio chip holding a digitized photograph and biographical information is more secure...."

Bio*graphical* information? This is new. Hold on a cotton-pickin' minute here. What sort of biographical information is it going to hold, and what about those of us whose biographies don't fit on a smart card.

Yeah, yeah, metric, graphic, what's the difference? It's just a measure of inaccuracy in the writing.

⚡ Conference on Electronic Entertainment Policies, Problems, Solutions

<Lauren Weinstein <lauren@vortex.com>>
Mon, 30 May 2005 07:59:54 -0700 (PDT)

EEPI 2005

Conference and Workshop on Electronic Entertainment
Policies, Problems, and Solutions

Los Angeles, California USA
Late Summer/Early Fall 2005
(2 to 3 days)

*** Call For Interest ***

*** Conference Web Page: <http://www.eepi.org/eepi2005> ***

EEPI - Electronic Entertainment Policy Initiative

<http://www.eepi.org>

EEPI main address: eepi@eepi.org

EEPI conference/workshop: eepi-conf@eepi.org

Greetings. EEPI is organizing a combined conference and workshop in Los Angeles for late Summer or early Fall 2005. The purpose of this gathering is to fulfill a number of related objectives, all aimed at fostering cooperative, interdisciplinary work toward finding solutions to an array of issues related to entertainment technology policies and their impacts on other aspects of technology and society at large.

Primary goals of this meeting include both providing attendees with insight into the many often conflicting points of view and complex characteristics related to these issues, and to work towards establishing a long-term framework for finding and implementing practical, cooperative solutions wherever possible. This will not be a place for finger-pointing or name-calling. Attendees should be interested in learning more about these issues and helping to solve the many complex problems in this

arena that we must deal with today and that we will be facing with increasingly rapidity in the future.

We urge you to view <http://www.eepi.org> for more details regarding EEPI and the entertainment technology issues of concern, and some thoughts on the categories of groups and individuals who may be particularly interested in attending this meeting.

Formal papers are welcome but are not required for presentations at the conference or workshop sessions. Student registration discounts will be available.

Our aim is to bring together involved and interested parties from across the electronic entertainment spectrum and beyond: record labels; film studios; broadcasters; artists; technical development and manufacturing firms; computer firms and organizations; Internet, government, legal, and public interest individuals and groups; educators; students; media; concerned members of the public, and more.

Since the focus for this gathering is interdisciplinary in nature, highly-detailed technical presentations (as opposed to technical "overviews") will be discouraged in main sessions, however, more detailed technical discussions may be appropriate in particular workshop sessions during the meeting. Sessions may be organized on multiple tracks as deemed appropriate, to be determined as meeting details are finalized.

Below is an alphabetical, non-inclusive list of some categories

of issues that are appropriate for this gathering, as they relate to electronic entertainment. Many of these are interrelated, of course:

- Academic Institution Concerns
- Alternative Licensing Models
- Artists' Economic Concerns
- Artists' Rights
- Broadcasting Issues (Broadcast Flag, Copy Controls, Digital TV, etc.)
- Cable TV Issues
- Children's Online Protection Act (COPA)
- Consumer Economic Concerns
- Consumer Rights
- Content Distribution Issues (Music, Films, etc.)
- Content Filtering and Blocking (Internet, Other Media, etc.)
- Copyright Issues
- Corporate Economic Concerns
- Corporate Rights
- Criminal Prosecutions
- Digital Rights Management (DRM) / Copy Protection Systems
- Digital Video Recording (DVR), etc. and Related Impacts
- Downloading of Audio and Video (Legal and Illegal)
- DVD and "Next-Generation" DVD Issues (eg. Blu-Ray, HD-DVD, etc.)
- Electronic Games (Content, Piracy, etc.)
- Fair Use Issues
- Intellectual Property Issues
- International Issues
- Internet Issues (the broad range of related Internet applications)
- Judicial Issues (court rulings and their effects)
- Lawsuits and other Civil Actions
- Legislative Issues (local, state, and federal legislative actions)
- Micropayment Issues
- Payment Models
- Peer-to-Peer (P2P) File Sharing Issues
- Piracy Issues (Music, Films, Videos, other Content, etc.)
- Regulatory Issues (Regulatory Agency Actions, e.g. FCC, DOJ, ITU, etc.)
- Streaming Audio and Video Issues

- Video on Demand Issues
- Video to Consumers over Fiber, DSL, Internet Issues

... and a host of others!

- - -

Obviously we will not be able to solve all of the many complex problems related to these topics at this single gathering! However, we hope to demonstrate that it is possible for people to work together on these problems, help attendees understand other persons' points of view regarding these contentious issues, and lay the groundwork for long-term, continuing efforts by interested individuals and groups to simultaneously find solutions, and to reduce the level of animosity and its counterproductive effects in the areas of concern.

- - -

If you might consider attending, please send a note (all e-mail to this address will be read by a human!) to:
eepi-conf@eepi.org

or FAX to:
+1 (818) 884-7502

Please let us know your level of interest, any relevant organizational affiliations if you wish, and any related comments or questions. Unless you specify otherwise, we'll add your e-mail address to a private mailing list, which will only be used to provide more information as additional details of the meeting (exact location, dates, registration fees, etc.) are determined

and finalized.

Please also feel free to contact EEPI co-founder Lauren Weinstein by phone via +1 (818) 225-2800.

We hope to see you at EEPI 2005!

Thank you very much for your consideration.

- - -

EEPI - Electronic Entertainment Policy Initiative
"Working Together Toward Sensible Policies and Solutions"

<http://www.eepi.org>

EEPI main address: eepi@eepi.org

EEPI conference/workshop: eepi-conf@eepi.org

This document is subject to change and elaboration at any time.
5/30/05



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



THE 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 23: Issue 89

Friday 10 June 2005

Contents

- [United abandons Denver Airport baggage system](#)
[PGN](#)
- [More on the FBI Virtual Case File demise](#)
[Dan Eggen via PGN](#)
- [Plane diverts after erroneous hijack alert](#)
[Geoff Kuenning](#)
- [Self-service photo kiosk retains images, leads to prosecution](#)
[Matt Fichtenbaum](#)
- [Search Engine Dependence Syndrome](#)
[PGN](#)
- [Intelligence vs. Common Sense](#)
[Kevin N Haw](#)
- [The Risks of HTML](#)
[William Colburn](#)
- [Method discovered of cracking Bluetooth security](#)
[Pete Mellor](#)
- [Messaging and Security Feature Pack for Windows Mobile 5.0](#)
[Alpha Lau](#)

- [Challenge/response e-mail filtering](#)
[Atom Smasher](#)
 - [Wide-scale industrial espionage using Trojan horses in Israel](#)
[Gadi Evron](#)
 - [Bold thieves build complete ATM](#)
[James Bauman](#)
 - [Spammer using Yahoo service and Google's name to hide actual server](#)
[Joe Smith](#)
 - [Future ChoicePoint-related flaws](#)
[David B. Lewis](#)
 - [Re: Michigan message board says speed limit 100 mph](#)
[Bob Heuman](#)
 - [Zabasearch, and coverage thereof](#)
[Jay R. Ashworth](#)
 - [Re: MarketScore exploit](#)
[Chris Smith](#) [Doug Burbidge](#)
 - [Re: "Rumplestiltskin worm" on the loose?](#)
[James W. Adams](#)
 - [Info on RISKS \(comp.risks\)](#)
-

United abandons Denver Airport baggage system

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

Thu, 9 Jun 2005 14:27:05 PDT

United Airlines has decided to stop using its controversial automated baggage-handling system at Denver International Airport, reverting to a conventional manual system by the end of 2005. The automated system (which began operation in 1995) never lived up to original expectations. It had enormous difficulties in its early days, including construction delays, cost overruns, lost bags, damaged luggage, derailed cars, traffic

jams, upgrade problems, political battles, and so on. (For example, see [RISKS-17.61](#) and 18.66). United is apparently obligated to pay \$60 million a year for another 25 years under its lease contract with the city of Denver (which owns the airport). However, United expects to save \$1 million a month in operating costs by NOT using the automated system. The airport cost \$250 million to build (BAE Automated Systems of Dallas, no longer in existence), and the city reportedly put up another \$100 million for construction and \$341 million to get it to work. [Source: AP item, 7 Jun 2005; PGN-ed]
<http://msnbc.msn.com/id/8135924/>

[The system will soon be carrion! Carry on with carry-on.
PGN]

🔥 More on the FBI Virtual Case File demise

<"Peter G. Neumann" <neumann@csl.sri.com>>
Sun, 5 Jun 2005 18:57:18 PDT

A recent report for the House Appropriations Committee has once again put the FBI's Virtual Case File (VCF, see [RISKS-23.66](#)) development effort under scrutiny. (The \$170 million project was scuttled earlier this year.) An FBI report in 2004 had identified 400 problems with early versions, but the contractor was never informed. \$17 million was spent on a testing program in December 2004 even after it seemed evident that the project

would have to
be scrapped. The new report documents many "errors and
misjudgments that
were made during the software project's troubled
history." [Source: an
article by Dan Eggen, FBI Pushed Ahead With Troubled Software,
*The
Washington Post*, 6 June 2005; PGN-ed]

[http://www.washingtonpost.com/wp-dyn/content/article/2005/06/05/
AR2005060501213.html](http://www.washingtonpost.com/wp-dyn/content/article/2005/06/05/AR2005060501213.html)

✶ Plane diverts after erroneous hijack alert

<Geoff Kuenning <geoff@cs.hmc.edu>>
04 Jun 2005 23:34:45 +0200

The following story:

<http://news.bbc.co.uk/go/rss/-/1/hi/uk/4607657.stm>

tells of a U.S.-bound aircraft diverted to Canada (with fighter
escort)
after accidentally transmitting a hijack warning.

The thing that strikes me most about the article is the
following sentence:

...the false alarm was caused by a malfunction which meant
that when the
transponder began transmitting the 4-digit hijack code, the
crew were
unable to shut it off.

Huh? It seems to me that "unable to shut off the alarm" is the
proper
behavior for such a system. You don't want a hijacker to hold a
gun to the
pilot's head, saying "Either shut off the hijack code or I'll
kill you and

crash the whole plane." Much better to make the switch one-way and spend the extra money and inconvenience to escort the plane to a safe landing spot while you investigate whether there really was a hijacking or it was a false alarm.

Sometimes the proper fail-safe response is to insist on a human decision.

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

✈ Self-service photo kiosk retains images, leads to prosecution

<Matt Fichtenbaum <mattfic@rcn.com>>

Thu, 09 Jun 2005 21:17:39 -0400

The Boston Globe 9 Jun 2005 carries an Associated Press story about a man in New Hampshire who had taken some 'risque' digital photos of his granddaughter. He printed them out at a Kodak self-service print kiosk at a CVS pharmacy. Maybe he'd attracted the attention of the clerk -- or maybe it's normal practice - the store manager looked at the photos *that had been retained by the innards of the printer* and notified police. There must have been some more modest pictures as well, and these were shown on national TV, leading to the girl's parents calling in and identifying the perpetrator, who was then arrested.

Want privacy and anonymity? Buy a printer.

⚡ Search Engine Dependence Syndrome

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

Mon, 9 May 2005 15:54:20 +0100

"We have allowed concepts from information technology to enter the cognitive consciousness of physicians without critical analysis of their impact."

Steven Merahn, MD, identifies Search Engine Dependence Syndrome as a neuropsychological disorder:

1. The assumption/perception that computers are "smart"
2. The task interference associated with competing problem-solving paradigms
3. The loss or lack of development of critical thinking skills that comes with prolonged reliance on IT infrastructure

<http://www.cliniscience.com/objects/Cliniscience%20TEPR.pdf>

[Thanks to Lindsay Marshall for finding the 25-slide presentation from which this item is PGN-ed.]

⚡ Intelligence vs. Common Sense

<Kevin N Haw>

Wed, 8 Jun 2005 10:09:28 -0700

The *London Evening Standard* is reporting that the "world's biggest computer hacker" has been arrested in London, giving us more evidence once

again that intelligence and common sense do not necessarily go hand in hand:

The unemployed former computer engineer is accused of causing the US

government \$1 billion of damage by breaking into its most secure computers

at the Pentagon and NASA. He is likely to be extradited to America to

face eight counts of computer crime in 14 states and could be jailed for

70 years... Friends said that he broke into the networks from his home

computer to try to prove his theory that the US was covering up the

existence of UFOs.

The mind simply boggles.

Full story:

<http://www.thisislondon.co.uk/news/articles/19164714?source=Evening%20Standard&ct=5>

Commentary:

<http://it.slashdot.org/article.pl?sid=05/06/08/137249&tid=172>

[Biggest hacker? He would perhaps have to exceed 450 pounds in weight

to justify that claim.

Pentagon's and NASA's most secure computers? Wow! Are we impressed? PGN]

The Risks of HTML

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

Mon, 6 Jun 2005 08:49:45 -0600

I received e-mail from B&H Photo video about my order. I don't use an

HTML-capable e-mail reader, and they don't send a text version.

```
<td> <p><br>
```

```
Dear WILLIAM D. COLBURN ,<br>
```

```
<br>
```

```
We are pleased to inform you that the following order  
has been
```

```
shipped.</p>
```

```
<!-- Comment out by YYW per bug #29992-->
```

```
<!-- <p>PLEASE NOTE:</p>-->
```

```
<!-- <p>You should be receiving your order shortly. </p>-->
```

```
<!-- <p>Please review the information and verify that  
everything is  
correct.</p>-->
```

Since I hate waiting, I had ordered prompt delivery of my new possession.

Unfortunately, due to bug 29992 I will not be receiving my order shortly,

and I should not review my order to make sure that it is correct. I hate

bug 29992. B&H could be slowly shipping me the wrong thing, and I won't know it until it arrives.

I'm also pretty baffled by what bug could possibly be fixed by commenting

out a textual note that my order will arrive soon and I should check what I

ordered to make sure it is correct.

⚡ Method discovered of cracking Bluetooth security

<Pete Mellor <pm@csr.city.ac.uk>>

Sat, 4 Jun 2005 11:19:41 +0100 (BST)

Avishai Wool and Yaniv Shaked of Tel Aviv University in Israel have

demonstrated a method of cracking Bluetooth security. Every Bluetooth device broadcasts its ID code to everything in the vicinity. The method is to pick up an ID code, then send a message to another device, spoofing the ID code, and telling it that the 'link key' used for encrypting communication has been 'forgotten'. This forces the two devices to go through a 'pairing' exercise to establish another link key. (Normally this is done only on the first occasion on which two devices communicate with each other.) The attacker can then eavesdrop on the messages exchanged in the pairing session, and analyse these using software which implements the Bluetooth algorithm. The four-digit PIN (set on each device by the legitimate user) can be cracked by 'brute force'. The link key can then be derived, and the attacker can then communicate with either device by pretending to be the other.

Shaked and Wool will present their findings at the MobiSys conference next Monday in Seattle.

For a more detailed description, see the on-line news item from New Scientist magazine:

<http://www.newscientist.com/article.ns?id=dn7461>

Peter Mellor, Centre for Software Reliability, City University,
Northampton Square, London EC1V 0HB +44 (0)20 7040 8422

✦ Messaging and Security Feature Pack for Windows Mobile 5.0

<Alpha Lau <avlxyz@yahoo.com>>

Mon, 6 Jun 2005 18:46:38 -0700 (PDT)

Local and remote device wipe. The ability to remove all information, over the air, and reset a device to its original state enables IT administrators to better manage sensitive information on a misplaced Windows Mobile-based device. In addition, the administrator can choose to have the local memory on a device erased if the correct password is not entered after a designated number of attempts.

<http://www.microsoft.com/presspass/press/2005/jun05/06-06SFPWindowsMobilePR.msp>

Oh sure, just wipe the device. Encryption is not an option, is it? :)

Challenge/response e-mail filtering

<Atom Smasher <atom@smasher.org>>

Tue, 10 May 2005 20:40:23 -0400 (EDT)

I recently received an e-mail challenge to a message claiming to be "From" me. if i choose to click the link provided, my e-mail address would be added to the recipients white-list. if i don't click the link then the message would be deleted... or filed in a folder where no one looks... i'm not sure...?

this allows two distinct failure modes:

1) I ignore the challenge and a legitimate message is not delivered

2) I acknowledge the challenge and spam is delivered, "From" me

regarding the first failure mode: when i post to a mailing list and receive a challenge, i will always ignore it. if the recipient wants to receive mail from the list, the list should be white-listed (not necessarily with an obvious header, such as "To: mailing-list@example.com").

regarding the second failure mode: this particular challenge (from earthlink) that i recently received only identified the message by the recipient and subject line, making it difficult to determine if i sent the message or not. i did not recognize the recipient or subject, so i had no reason to respond to the challenge. but, if one were to acknowledge the challenge without first determining the legitimacy of the message, 1) the recipient will receive the spam and 2) the person who acknowledged the challenge may ultimately be blacklisted for "sending" spam.

it is assumed that a challenge/response system such as this works because spammers usually use invalid "From" addresses, and people would take the time to scrutinize any challenge they receive before responding to it. i know plenty of e-mail users who will be more than happy to click on any link in their e-mail to ensure that someone gets "their" mail.

should the challenge include the original message? this introduces the risk of using "From" addresses of the intended recipient and "bouncing" the spam off of an account that generates challenges. the "sender" (as identified in a forged From address) would then receive the spam.

this is in addition to the other flaw of challenge/response filter systems, which is that viruses may attack an address book and/or saved messages. this will facilitate spam that uses addresses that are likely white-listed. more than once i have received spam "From" my wife... we live and work in a m\$ft-free home in NC, the messages originated from a cable modem in NYC. the simplest explanation is that our names and e-mail addresses were both participants in a message or address-book that was harvested by a virus. had i been white-listing her name and/or e-mail address those spams would have landed in my inbox; instead they were properly filtered and sent to my spam folder.

another flaw that may be exploited in these automated challenge/response systems is if mail is sent "From" evil-spammer@spammer.com and that mailbox is read by a program that clicks every link that comes in. variations on this (better mousetraps, better mice, etc) would further destroy the utility of such filtering systems (while consuming about three times the bandwidth of normal spam).

my conclusion is that challenge/response systems, although at first seem like a Good Idea (tm), are no match for a good spam filter (CRM114, DSPAM, SpamAssassin, etc). i've been enjoying >99.95% accuracy with CRM-114, and now that i've trained it to recognize e-mail challenges as spam i'm not bothered by them so often.

🔥 Wide-scale industrial espionage using Trojan horses in Israel

<Gadi Evron <ge@linuxbox.org>>

Sun, 29 May 2005 19:45:37 +0400

Apparently, a Trojan horse was developed for three major private investigators' companies in Israel, and later used for industrial espionage with some of the biggest corporations in Israel.

Apart from the technical side of this attack and the extreme wide-scale of it, another interesting aspect is the use of social engineering.

In one description, I heard that a woman called a certain individual at one of the companies with a business offer, and later sent him a presentation via e-mail. When that presentation did not work, she proceeded to send him a CD, which did not work either.

You can find an article in English detailing some of the events here:

<http://www.haaretz.com/hasen/spages/581718.html>

This is not the first time this happened, and not the first time we've seen industrial espionage in IL, or private investigator companies developing their technological and operational capabilities. I've personally been approached about such a job twice in the past 2 years.

Interesting tidbit of data:

The perps paid 17K UK pounds per COMPUTER per MONTH.

Gadi Evron, Infosec Manager, Israeli Government Internet Security.

⚡ Bold thieves build complete ATM

<"Bauman, James" <James.Bauman@safety-kleen.com>>

Wed, 11 May 2005 09:47:12 -0400

<http://www.reuters.com/newsArticle.jhtml=3Ftype=3DoddlyEnoughNews&storyID=3D8412873&src=3Drss/oddlyEnoughNews>

Audacious thieves in Romania have constructed a complete automated teller machine (ATM), minus the cash box, to steal the details of account holders.

Fake ATMs have appeared at apartment buildings or in areas of the capital where there are no banks. Usually criminals only place a fake panel over an existing ATM, and do not construct a complete machine.

Romania's biggest bank, Banca Comerciala Romana (BCR), said customers should only use ATMs situated around bank branches. "Banks do not install ATMs in blocks of flats," BCR spokesman Cornel Cojocaru said.

Jim Bauman S-K Lotus Notes Group 847-468-3014 jbauman@safety-kleen.com

⚡ Spammer using Yahoo service and Google's name to hide actual server

<Joe Smith <Joe.Smith@instantis.com>>

Mon, 06 Jun 2005 04:06:35 -0700

I expect that many of you have received spam messages containing "Your existing loan situation makes you eligible..." and "If your decision is not to make use of this final offer going here...".

The URL for Request Form and opt-out look respectable, but they are not.

They are in the form of

http://rds.yahoo.com/a=b/*-http://www.google.com_cr3am.net/del.asp

where "a=b" is about 100 characters and the "_" is another period.

Yahoo must be running some sort of redirection service on their RDS server.

It ignores everything between rds.yahoo.com/ and "*-", then issues a

redirect to what's left. The end result is a URL pointing to a server that

was registered in China on 2005-06-02. It's using a subdomain of www.google.com to trap the unwary.

⚡ Future ChoicePoint-related flaws

<"David B. Lewis" <dblen@earthlink.net>>

Fri, 3 Jun 2005 14:25:35 -0400

I had occasion to contact my ISP to reset the password on an account (which I had misremembered). But instead of resetting the password to a whatever

value and giving it to me, so that I could change the password to what I

wanted, the ISP told me what the password had been! We went through a

little back-and-forth about how they shouldn't be storing clear-text

passwords ("but the login screen is secure!") without any impact.

✶ Re: Michigan message board says speed limit 100 mph (Waters, [R 23 85](#))

<"R.S. Heuman" <rsh@idirect.com>>
Tue, 26 Apr 2005 21:49:25 -0400

I have to wonder if the individual controlling the message board is one of the people living in Windsor who commute to Detroit to work, and who is more familiar with kph, as used to the east and north of Michigan :-)

Or, as an alternative, it really said 100 kph and someone expecting the mph misread the board. After all, when we cross the border at Sarnia/Port Huron or Windsor/Detroit or Sault Ste. Marie/Sault Ste. Marie perhaps they are telling us the Michigan speed limit in terms that match our speedometers [KPH] :-)

If either or those were the case, 100 kph is 62.5 mph and the 'error' makes more sense or was not an error but a misread of one letter. I wonder if we will ever know...

✶ Zabasearch, and coverage thereof (Re: Zaba, [RISKS-23.87](#))

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

Fri, 20 May 2005 11:33:33 -0400

At <http://writ.news.findlaw.com/ramasastry/20050512.html> it is written, amongst other things:

> True, much information was available publicly before. But now it can be
> collected together, online, at the press of a button. One scholar,
> Professor Daniel Solove, calls such collections of data "digital
> dossiers".
>
> And there's no reason these dossiers must be limited to addresses,
> phone numbers, birth years, and property information. Digital
> footprints can be tracked - so that digital dossiers could include
> Internet activity. In theory, they could also be connected to security
> camera footage from private stores, identification photos, and much
> more.
>
> Such dossiers can be permanent, and may be instantaneously disseminated
> around the world.
>
> They can also be stolen: Collecting information on an individual, and
> making the dossier publicly accessible, risks making identity theft
> virtually undetectable. The thief who steals your wallet may not know
> your mother's maiden name, or the name of your pet - common security
> questions. But what if that information ends up in your digital
> dossier?

And, of course, the answer is "then maybe companies will stop using such

puerile choices of authenticators and get serious about security"... but that's politically incorrect to say aloud.

So I'll say it here, instead.

While Zabasearch may have problems, that's not one of them.

The world is changing, and while there may be some risks involved in that, we would be well served to think long and hard about what those risks are, and where they *really* come from... instead of killing the messenger.

Peter Brin's *TheTransparent Society* and Simson Garfinkel's *Database Nation* have interesting, if opposing, takes on this issue.

Jay R. Ashworth, Ashworth & Associates, St Petersburg FL USA
<http://baylink.pitas.com> +1 727 647 1274 jra@baylink.com

✉ Re: MarketScore exploit (Emigh, [RISKS-23.88](#))

<Chris Smith <smith@interlog.com>>

Thu, 2 Jun 2005 03:26:27 -0400 (Eastern Daylight Time)

In [RISKS-23.88](#), Aaron Emigh includes a valuable summary of the operation of MarketScore. However, recent changes have made this description badly out of date. A different concern, however, is whether this is an "exploit" and an "attack".

Although MarketScore does not tell their users precisely how the technology works, they are quite clear about what they are doing. Their

End User

Licence Agreement (EULA) specifically states that the examined data includes secure sessions. It's not at all clear that it is still a man-in-the-middle *attack* if one end of the connection has agreed to the process. Like many technologies, this one can be used for bad things. But just because this technology is used is not sufficient to make what is done with it a bad thing.

MarketScore appears to now use a different technology, effectively summarized in this analysis from Cornell:

<http://www.cit.cornell.edu/computer/security/marketscore/technical.html>

Simply put: the proxy has been moved from MarketScore servers to the users' own machines, and MarketScore now simply records a datastream from the proxy. Where destination sites could formerly detect that proxied traffic arrived from marketscore servers, now the proxied traffic arrives from the users' regular IP address.

Furthermore, the use of a LSP (Layered Service Provider) appears to allow the proxy to examine the contents of secured sessions without having to re-encrypt traffic under the special trusted certificate. If you check a site's credentials, it will show as secured by the site's own certificate, not by Marketscore's.

✦ **Re: MarketScore exploit (Emigh, [RISKS-23.88](#))**

<Doug Burbidge <dougburbidge@dougburbidge.com>>

Thu, 02 Jun 2005 22:15:27 +0800

They're not the only ones. Microsoft ISA (Internet Security and Acceleration) Server 2004 does the same thing: it allows clients to establish a secure connection with it, and then it establishes a secure connection with the remote site.

It does not log the content of the session (though future versions of ISA Server may allow this). But it does log the full URL, and HTTP headers (such as user agent) that you would normally expect to be invisible over an https connection.

It can perform these tricks invisibly from the client's perspective because it is integrated with the rest of the LAN's infrastructure. It similarly needs a root certificate, but since this is automatically installed on the client when it is joined to a Windows domain with a certificate server, the added certificate is inconspicuous.

The risk here, I guess, is trusting that the people who wrote the software have your best interests at heart. This is not the case for MarketScore, and is evidently not the case for end users of IE, Windows client, and ISA proxy.

Doug Burbidge <http://www.dougburbidge.com/>
dougburbidge@dougburbidge.com

Re: "Rumplestiltskin worm" on the loose? (Glass, [RISKS-23.88](#))

<"James W. Adams" <jadams84@columbus.rr.com>>

Wed, 01 Jun 2005 02:34:43 -0400

> As I've mentioned above, there will be some people who are philosophically
> opposed to the notion of restricting Internet traffic so as to limit abuse...

Yes, I am very opposed to such a notion. I'm sorry, but the Internet is not your private playground. If you have a spam problem, deal with it or buy your own intranet. Such "idealism" is what lets people use the Internet to communicate. The US FCC rules about devices which use radio frequency transmissions having to accept any "interference" come to mind. If some specific agent is disrupting your operations illegally, track down their activities, record them, and turn it over to law enforcement. Otherwise, just deal with the fact that the Internet is no longer a closed society, and you may have to deal with the same sorts of mischief you would in any other public arena, as well as a large number of people who just need to tell grandma about junior's first bowel movement with photos attached.

I don't like the fact that the USPS promotes the delivery of junk mail to my home, but I don't demand that we require senders of postage to pass some sort of security interrogation. I just recycle or dispose of the junk. The fact is that the fees paid to mail this junk subsidize my

ability to receive
mail at my home, so I accept it as a cost of doing business or a
cost of
living.

Much spam is identifiable and can be blocked by well established
means.

What can't is the cost of doing business in any public venue.
Your
convenience and avoidance of risk does not constitute an
entitlement to
restrict the expression or actions of others any more than you
have the
right to restrict the use of public highways to yourself and
your assigned
agents, or, within reason, to dictate what sorts of vehicles
they may
operate, who may occupy them or where and when they may travel.

Furthermore, the argument you raise about bandwidth is largely
absurd. One
of the reasons for the collapse of WorldCom was overcapacity.

If I have a dialup feed, I likely won't appreciate someone e-
mailing me a
five megabyte graphic file, but I have little right to demand
that nobody do
so unless there is obvious malicious intent. There are also
workarounds
such as IMAP.



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



THE 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 23: Issue 90

Wednesday 15 June 2005

Contents

- [Details of F/A-22 crash December 2004](#)
[Peter B. Ladkin](#)
- [Database error makes half of Norway's cellphones go offline](#)
[Olav Langeland](#)
- [When Crypto/Signature Plans Go Wrong: Sony PSP Exploit](#)
[Lauren Weinstein](#)
- [Encryption Illegal in Minnesota](#)
[Al Macintyre](#)
- [Seven voting machines under scrutiny in Wayne County](#)
[Lillie Coney via PGN](#)
- [LSAC gives SSNs to recommenders](#)
[Jerry Saltzer](#)
- [Risks of letting marketing spec your messages](#)
[Mike Albaugh](#)
- [Microsoft censoring blogs in China](#)
[PGN](#)
- [The Scramble to Protect Personal Information](#)
[Tom Zeller via PGN](#)

- [ID Theft vs. Colorado Attorney General](#)
[Al Macintyre](#)
 - [Private, Personal Medical Info Faxed To Wrong Location](#)
[Bob Heuman](#)
 - [What Europe can teach us about identity theft](#)
[Amos Shapir](#)
 - [Paris Hilton Hack Started With Old-Fashioned Con](#)
[Brian Krebs via Monty Solomon](#)
 - [Ted Koppel: Take My Privacy, Please!, 13 Jun 2005](#)
[Monty Solomon](#)
 - [Mom charged with stealing identity of soldier son](#)
[Julia Silverman via PGN](#)
 - [Re: Plane diverts after erroneous hijack alert](#)
[Michael Bacon](#) [Andrew Koenig](#) [Rob Bailey](#)
 - [Re: Challenge/response e-mail filtering](#)
[David Cantrell](#)
 - [REVIEW: "CISSP Exam Notes", K. Wan](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Details of F/A-22 crash December 2004

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Wed, 15 Jun 2005 11:10:34 +0200

On 20 Dec 2004, an F/A-22 Raptor, the USAF's new air-superiority fighter, crashed 11 seconds after takeoff from Nellis AFB, Nevada. It is the first production aircraft to be lost. They are said to cost \$133 million each. The results of the investigation from the USAF Accident Investigation Board (AIB) are reported in this week's Flight International (14-10 June, 2005, p9).

The pilot ejected with the aircraft near-inverted. The aircraft struck the end of the runway going backwards.

There are three rate-sensor assemblies (RSA), manufactured by BAE Systems in the flight control system (FCS). There is a known "quirk" in the RSA, which is "programmed so that it could interpret a momentary power loss [to the FCS] as an instruction to enter test mode, which freezes or "latches" the unit, according to the AIB report."

The pilot shut down the engines during a maintenance check pre-take-off, thinking the FCS was continuously powered by the auxiliary power unit (APU). The FCS in fact loses power briefly during a shutdown, and that appeared to suffice to latch all three RSAs. "The AIB attributed the pilot's mistake to "ambiguous" language in the aircraft's technical orders."

The manufacturer, Lockheed Martin, has returned about 20 RSAs to BAE Systems for suspected latching events. Before this crash, such events only affected one or two of the RSAs, not all three together. There is a pilot warning for partial RSA latching, but no warning if all three latch.

The RSA has been redesigned and is being installed on the fleet.

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

Database error makes half of Norway's cellphones go offline

<"Olav Langeland" <olav.langeland@active24.com>>

Wed, 15 Jun 2005 14:08:46 +0200

Customers of Netcom, the second largest cellular provider in Norway, experienced sporadic or close to no service for days earlier this week.

Companies that earlier abandoned "normal" phones and went all cellular are now installing land phones and/or IP phones.

"Hundreds of thousands of customers and a government minister alike

remained up in arms Tuesday, after losing use of their mobile telephones

in recent days. ... NetCom has actively promoted the concept of the

"wireless office," and companies from building giant NCC to Aftenposten

have made the switch, also as a means of saving money.

Instead, it's left

them vulnerable to communications breakdown and even dangerous situations."

Problem? Database indexing issues, after a upgrade the previous week.

More details here: <http://www.aftenposten.no/english/local/article1059215.ece>

⚡ When Crypto/Signature Plans Go Wrong: Sony PSP Exploit

<Lauren Weinstein <lauren@vortex.com>>

Wed, 15 Jun 2005 12:33:14 -0700

As we know, often even the most elaborate attempts at controlling

access to hardware and software, even using the very latest technologies, may be less than entirely successful.

An example is the just-announced "exploit" of Sony's powerful and popular new "PSP" portable gaming system (which includes WiFi and other advanced capabilities). The unit employs digital signing and hardware AES encryption to try prevent the running of "unofficial" applications.

However, as I detail in two messages on the EEPI (Electronic Entertainment Policy Initiative - <http://www.eepi.org>) discussion list, the PSP exploitation door has apparently been opened quite wide both for piracy and a vast array of homebrew applications.

In ("The Waiting Tide? Major PSP Exploit May Appear in a Few Hours ...")

I discuss the imminent release of the exploit:

<http://www.eepi.org/archives/eepi-discuss/msg00099.html>

and in ("PSP Exploit Apparently Confirmed")

I've provided additional information and thoughts:

<http://www.eepi.org/archives/eepi-discuss/msg00100.html>

Lauren Weinstein Tel: +1 (818) 225-2800 <http://www.pfir.org/lauren>

Co-Founder, PFIR (<http://www.pfir.org>) Co-Founder, EEPI (<http://www.eepi.org>)

Lauren's Blog: <http://lauren.vortex.com> DayThink: <http://daythink.vortex.com>

Encryption Illegal in Minnesota

<Al Mac <macwheel99@sigeom.net>>

Sat, 28 May 2005 06:55:10 -0500

We are all being encouraged to use encryption to protect sensitive files from data theft, but a Minnesota Court of Appeals has declared that merely having the ability to do encryption is de facto proof of criminal intent. It may be that courts not need to prove what criminal act you did, just having encryption software is like having burglary tools, or high explosives. It is assumed that only burglars have burglary tools, so mere possession means conviction, and the legislature can decide what constitutes a burglary tool.

I got this summary from <https://thei3p.org/pipermail/security-news-html>

Title: PGP use ruled relevant in child abuse case

Source: The Register

Date Written: 2005-05-25

Date Collected: 2005-05-27

The Minnesota State Court of Appeals has rejected an appeal from David Levie on charges of soliciting a nine-year-old girl to pose for naked pictures, ruling that the prosecution's introduction of an encryption program on his computer as evidence was admissible. During a search of his computer, police found the PGP (Pretty Good Privacy) encryption program. Levie's lawyers argued that forensic examination yielded no evidence of any encrypted files on his computer and so the presence of encryption software should not be used as evidence against Levie. One police officer testified that PGP may be included with every Apple computer on the market. The appeals court ruled

that the presence of encryption software was relevant to the prosecution's case and refused to order a retrial, though the case will be sent back for re-sentencing. The case could establish a precedent in Minnesota of accepting the presence of encryption software as evidence of criminal intent.

http://www.theregister.co.uk/2005/05/25/pgp_admissable_child_abuse_case/

Al Macintyre <http://www.ryze.com/go/Al9Mac>
<http://radio.weblogs.com/0107846/stories/2002/11/08/bpcsDocSources.html>

Seven voting machines under scrutiny in Wayne County

<"Peter G. Neumann" <neumann@csl.sri.com>>
Wed, 25 May 2005 19:06:45 PDT

[Courtesy of Lillie Coney <coney@epic.org>, Associate Director, Electronic Privacy Information Center (EPIC) 1718 Connecticut Avenue, NW, Washington, DC 20009 1-202-483-1140 x111, National Committee for Voting Integrity, www.votingintegrity.org]

The accuracy of some Republican votes cast 17 May 2005 in seven voting booths in three Wayne County voting districts is being investigated, potentially affecting the outcome of two township supervisor races. For example, in Lehigh Township, 163 Republicans voted, but 211 votes were

counted. [Source: Andrew M. Seder, Seven voting machines under scrutiny in Wayne County, Scranton Times-Tribune, 25 May 2005; PGN-ed] http://www.zwire.com/site/news.cfm?newsid=14583638&BRD=2185&PAG=461&dept_id=416046&rfi=6

✶ LSAC gives SSNs to recommenders

<Jerry Saltzer <Saltzer@mit.edu>>
Sat, 11 Jun 2005 16:55:50 -0600

This note came from a faculty member at a California University:

I'm doing a letter of recommendation for a student who wants to go to law school. He is required to submit all recommendation letters to a clearinghouse called the Law School Admission Council.

He gave me their form, which has pre-printed his name, home address, birth date, and Social Security Number. Pretty lame, and he is required to use it. What is really amazing is they also list his LSAC Account number which is not the SSN.

If you visit the LSAC web site and propose to create an account, it will present a form that requests your SSN. The HELP button next to the SSN field responds with this explanation:

This information is needed to match your online account to your LSAC records. It also allows LSAC to match such items as transcripts, letters of recommendation, score reports, and law school requests to

your

file. Your Social Security number or Social Insurance number is necessary

to obtain your username and password or to reset your password if you forget it.

In other words, everyone who has anything to do with your application will learn your SSN. And by the way, it is also a secret key to your password.

Given all of the recent publicity about identity theft and of organizations that have managed to lose track of customer data, "lame" is an understatement.

⚡ Risks of letting marketing spec your messages

<Mike Albaugh <albaugh@perilin.com>>

Mon, 13 Jun 2005 16:08:31 -0700

The spam-filter of my web-based e-mail provider is not perfect, so I (like most of you, probably) periodically check my "probable spam" folder for false positives. Today it contained a "change of address" e-mail from a casual correspondent. Of course, it was not just a plain-text message from the old, well-known address indicating the new one. Rather, it was HTML-Mail, with a couple largeish images, sent "on behalf of" my correspondent, from the new address, with the essential part buried in an endorsement of the ease of switching e-mail addresses via this nifty new service. Even human eyeballs would count it as spam at first glance, and

since we do not often correspond, there is a high probability I would not have any idea "where he went" when I did send him e-mail (at the old address), if I didn't regularly rummage through my trash. And he, of course, will never know how many of his friends tossed his notice, unless he notifies them some other way, which makes the whole "easy switching" deal pointless.

I'm assuming that this service is offered primarily as a way to get people to upload their address books for future spamming, so it wouldn't kill them to make it more effective at its purported task, and less like spam.

Microsoft censoring blogs in China

<"Peter G. Neumann" <neumann@csl.sri.com>>
Wed, 15 Jun 2005 11:23:03 PDT

Microsoft is cooperating with China's government to censor MSN's Spaces Chinese-language Web portal. Bloggers are prevented from posting words such words as *democracy*, *human rights*, and *Taiwan independence*. 5 million blogs have been created since the service started on 26 May 2005. China reportedly has 87 million online users. [Source: AP item by Curt Woodward, 14 Jun 2005, seen in the *San Francisco Chronicle*.]

[I wonder whether this issue of RISKS will be blocked because of those

OFFENSIVE words? (And I thought *democracy* and *human rights* were DEFENSIVE words?) PGN]

✶The Scramble to Protect Personal Information (Tom Zeller)

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

Fri, 10 Jun 2005 12:05:45 PDT

In Feb 2004, a Japanese division of Citibank had a mag tape disappear during shipment by truck from its data management center in Singapore, with information on about 120,000 customers. The tape has never been found.

This week it happened again to a box of tapes sent by United Parcel Service, with info on nearly 4,000,000 American customers. Citigroup is apparently in the process of responding to the Singapore case with the company-wide introduction of "secure electronic channels" -- although that process is not yet complete. [Tom Zeller Jr., *The New York Times*, 9 Jun 2005; PGN-ed]]

<http://www.nytimes.com/2005/06/09/business/09data.html?th&emc=th>

Zeller's article has more on ChoicePoint, 10 million consumers falling

victim to identity theft each year, discussion of the 2003 California law

that mandates reporting, and this delightful quote from Mike Gibbons

(former FBI chief of cybercrime investigations, now a consultant for Unisys):

"I think there are some people who dismiss this as a sky-is-

falling

problem. But the sky has already fallen and it's just a matter of when a piece hits you in the head."

Also a quote from Bruce Schneier:

"There are social expectations about security that can't be met,
but the practices are still so shoddy."

⚡ ID Theft vs. Colorado Attorney General

<Al Mac <macwheel99@sige.com.net>>

Mon, 13 Jun 2005 11:59:41 -0500

Colorado Attorney General John Suthers became a victim of identity theft when checks issued by a credit card company for a cash advance promotion were stolen from his home mailbox last week, police said.

The lessons here:

* How easy is it for someone to break into your mail box and steal stuff,
especially stuff you not know you be getting, like some promotion from a credit card company?

* I think for people living in a rural area with mail boxes out on the street for the convenience of the postal service, they need to rethink how they get their mail, perhaps lobby for the postal service to categorize some mail to go to lock boxes at the post office, where you periodically pick up that which could put you at id theft risk if it is stolen.

* If you live in an apartment complex, with "locked" mail boxes, how many people have the key?

- you and your family
- whoever rented the apartment before you
- the mailman [and substitutes]
- apartment management and maintenance
- former employees of the above
- anyone who knows how to "pick" a lock

[and so on. PGN]

⚡ Private, Personal Medical Info Faxed To Wrong Location

<"R S (Bob) Heuman" <rsh@idirect.com>>

Tue, 17 May 2005 22:06:19 -0400

Once more, with no good answer as to why, and no good reaction to the report of the problem... Oh well... Full details 16 May 2005 at: <http://www.wftv.com/news/4494998/detail.html>

40 pages of private medical information for hundreds of people was incorrectly faxed to a Seminole County Florida airplane parts business, containing the usual sensitive stuff. The recipient tried to call a HIPPA hotline, the response from which was that they were not interested.

[PGN-ed]

⚡ What Europe can teach us about identity theft

<"Amos Shapir" <amos083@hotmail.com>>

Mon, 13 Jun 2005 21:40:00 +0300

An article of that title, by Liz Pulliam Weston:

<http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P116528.asp?GT1=6582>

There's some good advice there (which may seem obvious to regular RISKS readers), but IMHO, most of the supposed advantages of the European system stem mostly from the fact that European financial institutes (and fraudsters) haven't caught up yet with their US counterparts.

Paris Hilton Hack Started With Old-Fashioned Con

<Monty Solomon <monty@roscom.com>>

Sun, 29 May 2005 03:14:46 -0400

The privacy violation of heiress Paris Hilton ([RISKS-23.76](#)) in which her wireless phonebook had been compromised was actually the result of one phone call and a little social engineering, with one of the culprits posing as a cell-phone company operative. Exploitation of security flaws then resulted from the information gathered. [Source: Brian Krebs, subtitled *Source Says Hacker Posed as T-Mobile Employee to Get Access to Information*, *The Washington Post**, 19 May 2005; PGN-ed]

Ted Koppel: Take My Privacy, Please!, 13 Jun 2005

<Monty Solomon <monty@roscom.com>>

Tue, 14 Jun 2005 09:25:16 -0400

The Patriot Act - brilliant! Its critics would have preferred a less stirring title, perhaps something along the lines of the Enhanced Snooping, Library and Hospital Database Seizure Act. But then who, even right after 9/11, would have voted for that?

Precisely. He who names it and frames it, claims it. The Patriot Act, however, may turn out to be among the lesser threats to our individual and collective privacy.

There is no end to what we will endure, support, pay for and promote if only it makes our lives easier, promises to save us money, appears to enhance our security and comes to us in a warm, cuddly and altogether nonthreatening package. [...]

<http://www.nytimes.com/2005/06/13/opinion/13koppel.html?ex=1276315200&en=ca684bc680a0d6c0&ei=5090>

⚡ Mom charged with stealing identity of soldier son

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

Fri, 10 Jun 2005 14:56:04 PDT

[Source: Julia Silverman, AP, 9 Jun 2005; KATU 2 News - Portland, Oregon, [www.katu.com](http://katu.com/stories/77696.html), via Jim Schindler, <http://katu.com/stories/77696.html>]

An Oregon National Guardsman recently returned from Iraq and discovered \$10,000 missing from his bank account. A police investigation resulted in charging his mother with aggravated theft, identity theft, and fraudulent use of a credit card, and concluded that she had opened up mail with his new ATM card and pin number. His mother said that she used the money for video poker, electronic entertainment devices, medical expenses, and daily living expenses. "The 'maternal bond' made me do it."

✈️ **Re: Plane diverts after erroneous hijack alert ([RISKS-23.89](#))**

<"Michael \ (Streaky\) Bacon" <himself@streaky-bacon.co.uk>>
Sat, 11 Jun 2005 07:13:37 +0100

In [RISKS-23.89](#) Geoff Kuenning wrote about the airliner's hijack warning that could not be turned off. He makes the point that 'duress' alarms should not be easily cancelable. In this particular instance, the aircraft was escorted by fighters to another country. The outcome might have cost the airline a penny or two and might have annoyed and possibly scared the passengers, but at least it ended without loss of life.

Now consider the case where the accidental alert was generated when the aircraft was already over American soil, perhaps close to a major city. The outcome could very well have been terribly tragic.

The article does not make clear whether the original alert was accidentally triggered manually or by a malfunction ("the plane's transponder ... had inadvertently sent code used for hijack warnings"). However, the article does appear to suggest that the operator is investigating the technical reason for "a malfunction which meant that ... the crew were unable to shut it off", but this could be journalistic licence or lazy sub-editing .

There is no easy answer to these puzzles, but perhaps the design and inherent reliability of the alerting system in question would bear attention.

At least some of the RISKS lie in deciding which is the greater RISK, coupled with designing, installing, maintaining and operating a 'fail-proof' system.

Michael 'Streaky' Bacon

✉ Re: Plane diverts after erroneous hijack alert (Kuenning, [R-23.89](#))

<"Andrew Koenig" <ark@acm.org>>

Fri, 10 Jun 2005 17:40:44 -0400

I haven't flown in a while, and the procedures may have changed, but the situation is actually slightly more complicated (and, I think, more reasonable) than Geoff suggests.

Every airplane used for airline transportation is equipped with a transponder, which, when hit by a radar signal, sends back a coded signal that includes the airplane's altitude and a 12-bit code that the pilot can set.

If you're not talking to a controller, you set 1200 (octal). If you are talking to a controller, the controller gives you a code to set.

There is a specific code that means "I am being hijacked." Once you set that code, the controller's radar will pick it up. Once that happens, the controllers are supposed to assume a hijack is in progress even if the code subsequently changes.

So there is no need for a latching mechanism in the cockpit, which could presumably be defeated by disconnecting the circuit breaker on the transponder. And yes there has to be such a breaker. What else do you do if the thing catches fire?

⚡ **Re: Plane diverts after erroneous hijack alert ([RISKS-23.89](#))**

<Rob Bailey <wm8s@pobox.com>>

Fri, 10 Jun 2005 14:59:45 -0400

When I was an attorney for the United States government, we had panic alarms under our desks. If one got pressed accidentally (by a knee, for example), we could not shut it off, as suggested was a good idea in [RISKS-23.89](#), so a

cadre of US Marshals would come charging into our office to see what was going on. [The alarms used a little button that took a key to reset.]

The difference between that system and the "hijack alarm" to which the news article in [RISKS-23.89](#) might have been referring explains why the hijack alarm can't be un-resettable: It, too, is not impossible to accidentally activate, but it serves another important purpose to which the pilot would be denied access if the alarm couldn't be reset, presumably until the plane landed and was serviced.

The hijack alarm was probably just the pseudo-secret transponder code for "Help! I'm being hijacked." There are a couple of these codes, for "Help, Emergency," "My radios have stopped working; please don't shoot me down," and so on. They are set by flipping four thumbwheel switches, buttons, etc., one at a time to dial up the right code.

Occasionally, it's possible to "scroll by" one of the special codes when switching from one transponder code to another. For example, if you were assigned to squawk 3456, and then reassigned 2222, you would probably briefly transmit codes 4456, 5456, 6456, etc., as you scrolled the first digit around to two. Then you'd probably transmit 2556, 2656, 2756, etc., and 2266, 2276, etc., and finally, 2227, 2228, etc.

If any one of these codes meant something special and you "fell across" it, you'd want to keep going, but couldn't if you couldn't leave the special

code.

⚡ **Re: Challenge/response e-mail filtering ([RISKS-23.89](#))**

<David Cantrell <d.cantrell@outcometechnologies.com>>

Mon, 13 Jun 2005 16:26:23 +0100

> [e-mail challenge-response] allows two distinct failure modes:
> 1) I ignore the challenge and a legitimate message is not delivered
> 2) I acknowledge the challenge and spam is delivered, "From" me [...]

I also know some who would deliberately respond to the challenge and so make the spam go through in a misguided attempt to punish the person using the broken challenge-response system.

Mr. Smasher misses a third failure mode, one which concerns me far more than the other two. That is that it's not generally possible for a recipient of a challenge to tell if it's real or not. It is conceivable that it could have been sent from a spammer attempting to verify that the recipient address is read by a person, and when they respond they are doomed to an eternity of exciting special offers on penis refills and toner cartridge enhancement.

⚡ **REVIEW: "CISSP Exam Notes", K. Wan**

<Rob Slade <rslade@sprint.ca>>
Thu, 19 May 2005 16:14:18 -0800

BKCISPEN.RVW 20050330

"CISSP Exam Notes", K. Wan, 2003, 988-97323-1-9, U\$24.95
%A K. Wan kplab@pacific.net.hk
%C Hong Kong
%D 2003
%G 988-97323-1-9
%I KP Lab Limited
%O U\$24.95 <http://www.kp-lab.com/>
%O <http://www.powells.com/cgi-bin/biblio?inkey=91-9889732319-0>
%O Audience i- Tech 2 Writing 1 (see revfaq.htm for
explanation)
%P 196 p. (PDF ebook)
%T "CISSP Exam Notes - All you need to pass the exam"

This appears to be a self-published ebook, available from the author, in PDF format. Despite the fact that an ebook softcopy could readily be edited, it has not been updated in the two years since it was published: some of the CISSP requirements have changed since then, and the book does not reflect that.

The ten domains of the CISSP CBK (Common Body of Knowledge) are covered in ten chapters, with the material provided in point form. The structure and flow of the material bears a striking resemblance to the slides in the (ISC)² CISSP review seminar. However, given minor discrepancies, I suspect that the book is not directly based on the (ISC)² slides, but rather on another course that, itself, was based on the (ISC)² CBK review seminar. (In response to the initial draft of this review, the author responded that

his ebook was based on the other books that followed the course outline, rather than on the course itself.) (Wan's company, KP Lab, seems to be restricted to producing training guides for various certifications.)

As noted, the points in the book follow the structure of the course slides. There is usually a sentence or phrase expanding or explaining each point from the Common Body of Knowledge listing, so the material is slightly longer than the subject outline that is available from the (ISC)² site. The explanations are, however, briefer even than those in the first edition of "The CISSP Prep Guide" by Krutz and Vines (cf. BKCISPPG.RVW), which is, itself, one of the tersest guides on the market. As with that work, and other similar texts, if you do not already know the content, this tome will not help you very much. Unlike most other CISSP study guides, there are no "sample" questions.

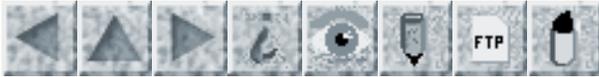
Overall, the points are reasonably well selected. (The section on malware is very disappointing, and the section on legal concepts is rather weak.) The material is more up-to-date than any other besides the "Official (ISC)² Guide to the CISSP Exam" (cf. BKOIGTCE.RVW). In terms of books dealing with an overall familiarization with the topics to be covered on the CISSP exam, this one does have an advantage in price, and in speed of access. (I requested a copy directly from the author by e-mail, and got it within two hours. If, for example, you are in a boot camp course situation, you may

need all the help you can get, quickly.)

copyright Robert M. Slade, 2005 BKCISPEN.RVW 20050330
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 23: Issue 91

Wednesday 22 June 2005

Contents

- [New Zealand Outage Shut Down Stock Exchange](#)
[Marcus H. Sachs](#)
- [First no more air maps, next no more road maps?](#)
[Dan Jacobson](#)
- [TSA kept passenger information it promised not to](#)
[PGN](#)
- [Libraries Say Yes, Officials Do Quiz Them About Users](#)
[Eric Lichtblau from Richard Forno via Dave Farber](#)
- [SOFTWARE 2015](#)
[Jim Horning](#)
- [US e-government risks](#)
[Al Macintyre](#)
- [Asian Hackers Blamed for Attacks On U.K., U.S. Computer Networks](#)
[Cassell Bryan-Low](#)
- [CardSystems' noncompliant practice compromises credit information](#)
[Eric Dash via Monty Solomon](#)
- [CardSystems' Systems](#)
[Al Macintyre](#)
- [Hacker accesses files at Equifax](#)
[Bob Heuman](#)

- [Cell Phones Now Playing Role of Wallet](#)
[Bruce Meyerson via Monty Solomon](#)
 - [SIM Cards with GPRS](#)
[Darryl Smith](#)
 - [New 'Heathrow Connect' Trains - do not want to go to Heathrow!](#)
[S Byers](#)
 - [Re: Plane diverts after erroneous hijack alert](#)
[Dan Jacobson](#)
 - [REVIEW: "Brute Force", Matt Curtin](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ **New Zealand Outage Shut Down Stock Exchange**

<"Marcus H. Sachs" <marcus.sachs@sri.com>>
Mon, 20 Jun 2005 19:57:49 -0400

A major outage in New Zealand Telecom Corp.'s cable network Monday disrupted data services, electronic cash transactions, mobile phone, and Internet services, as well as shutting down the nation's stock exchange for hours (the third time in the past nine months that data link failures have halted trading). Widespread disruption to business and private services was caused by two cable breaks on its North Island network. They were repaired by mid-afternoon Monday--at least five hours after they occurred. [Internet service and mobile phones were also out of commission due to two cable breaks. MHS]

The outage was caused by two separate incidents, including a fiber cable break north of the capital, Wellington, and a second cable being cut in Taranaki province on the west coast of North Island, more than 300 kilometers (188 miles) north of Wellington. [Source: Associated

Press, 20

Jun 2005; PGN-ed]

[http://www.informationweek.com/story/showArticle.jhtml?
articleID=164900973](http://www.informationweek.com/story/showArticle.jhtml?articleID=164900973)

✚ First no more air maps, next no more road maps?

<Dan Jacobson <jidanni@jidanni.org>>

Mon, 20 Jun 2005 19:06:46 +0800

The U.S. National Geospatial-Intelligence Agency (NGA) has proposed to withdraw all aeronautical data and products from public distribution.

http://www.urisa.org/Board_Initiatives/NGA.htm

✚ TSA kept passenger information it promised not to

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

Tue, 21 Jun 2005 11:15:52 PDT

"The Transportation Security Administration has done exactly what Congress

told it not to do -- and what it said it wouldn't do." [Source: Associated

Press item, 20 Jun 2005]

<http://www.news4jax.com/travelgetaways/4631077/detail.html>

✚ Libraries Say Yes, Officials Do Quiz Them About Users

<Richard Forno <rforno@infowarrior.org>>

June 20, 2005 4:29:12 PM EDT

(from article by Eric Lichtblau, via Dave Farber's IP)

Law enforcement officials have made at least 200 formal and informal inquiries to libraries for information on reading material and other internal matters since October 2001, according to a new study that adds grist to the growing debate in Congress over the government's counterterrorism powers. In some cases, agents used subpoenas or other formal demands to obtain information like lists of users checking out a book on Osama bin Laden. Other requests were informal -- and were sometimes turned down by librarians who chafed at the notion of turning over such material, said the American Library Association, which commissioned the study. [Source: Eric Lichtblau, *The New York Times*, 20 Jun 2005; PGN-ed]

<http://www.nytimes.com/2005/06/20/politics/20patriot.html?>

Dave Farber's IP Archives:

<http://www.interesting-people.org/archives/interesting-people/>

SOFTWARE 2015

<"Horning, Jim" <Jim.Horning@sparta.com>>

Thu, 16 Jun 2005 13:06:52 -0700

There's a recent report by the Center for National Software Studies that does not seem to have been adequately publicized, and hence has not received the attention it deserves: "SOFTWARE 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness"

<http://www.cnsoftware.org/nss2report/NSS2FinalReport04-29-05PDF.pdf>

Risks loom large in the discussion, including

- * Risk of critical infrastructure failures
- * Risk of sudden and severe economic loss
- * Risk of loss of life and limb

- * Risk of loss of public confidence
- * Risk of loss of our technological edge and leadership

I've posted excerpts from the Executive Summary at both
<http://bayosphere.com/node/554>

and

<http://horning.blogspot.com/2005/06/software-2015.html>

US e-government risks

<Al Mac <macwheel99@sigecon.net>>

Thu, 16 Jun 2005 08:35:28 -0500

The GAO surveyed what passes for computer security at scores of US Government agencies, and conducted some tests to see what is needed.

This

investigative arm of the US Congress determined that the fast majority of

US Gov agencies are oblivious to most of the threats, detailing what they

found in a 79 page report

<http://www.gao.gov/cgi-bin/getrpt?GAO-05-231>

with a 1 page summary

<http://www.gao.gov/highlights/d05231high.pdf>

Your pal Al read through the whole story and wrote up a 5 page summary which you can find in the archives of other discussion groups

<http://groups.yahoo.com/group/e-com-sec/message/1729>

<http://groups.yahoo.com/group/TYR/message/23897>

<http://groups.yahoo.com/group/VeeWire/message/2736>

Al Macintyre <http://www.ryze.com/go/Al9Mac> BPCS/400 Computer Janitor

Asian Hackers Blamed for Attacks On U.K., U.S. Computer Networks

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

Mon, 20 Jun 2005 17:12:34 PDT

Bid to Steal Valuable Data Targets Corporate Systems, Government Institutions

Article by Cassell Bryan-Low, *The Wall Street Journal*, 20 Jun 2005; PGN-ed]

A U.K.'s National Infrastructure Security Coordination Center (NISCC) report says unidentified hackers from Asia have been launching a wave of attacks on government and corporate computer systems in the U.S., Canada, and the U.K. in an effort to steal sensitive commercially and economically valuable information.

CardSystems' noncompliant practice compromises credit information

<Monty Solomon <monty@roscom.com>>

Mon, 20 Jun 2005 01:45:54 -0400

(Eric Dash)

CardSystems (a Tucson AZ company that handles credit card transactions for smaller banks and merchants) turns out to have been the source what was reported as the potential compromise of 40,000,000 credit cards (Visa, MasterCard, and American Express). In violation of established procedures, CardSystems was keeping old transactions online -- for research purposes -- with the intent of analyzing incompletely processed transactions. Something on the order of of 200,000 cards may be particularly at risk, and 70,000 bogus charges have already been reported. The CardSystems systems were hit with a virus that resulted in the capture of the information.

[Source: Lost

Credit Data Improperly Kept, Company Admits, Eric Dash, *The New York Times*, 20 Jun 2005; PGN-ed]

<http://www.nytimes.com/2005/06/20/technology/20credit.html?ex=1276920000&en=04e9ba4fe5ae0543&ei=5088>

CardSystems' Systems

<Al Mac <macwheel99@sige.com.net>>

Tue, 21 Jun 2005 04:55:38 -0500

We can figure out what kind of computer system was at CardSystems when they

(a) placed 40 million credit card transactions at risk of breach

(b) had 200,000 actually hacked

<http://www.nytimes.com/2005/06/20/technology/20credit.html?hp&ex=3D111932640=0&en=3Dd0b4ff6a62629204&ei=3D5094&partner=3Dhomepage>

May 22 they discovered the breach by magic, independently of Master Card

tracing fraud to them, and fixed the problem immediately May 27 they flunked

a Visa security audit, to check whether in fact they had fixed the problem

<http://www.redherring.com/Article.aspx?a=3D12451&hed=3DCardSystems+May+Face+=Fine>

According to <http://www.cardsystems.com/car=ADeers.html> (the recruiting page

for the company), CardSystems has the following types of systems installed:

Microsoft .NET (and Windows servers)

Oracle databases

VMS

http://groups-beta.google.com/group/bit.listserv.ibm-main/browse_thread/thread/7924e794e51d444d/719ed6452cf16035?q=3Dwww.cardsystems.com%2F&rnum=3D1&hl=3Den#719ed6452cf16035

A few years ago CardSystems advertised for a Programmer Analyst in Experience in one or more of the following areas:

C++, Java, Visual Basic reqd.

E-commerce, HTML, XML, ASP, MTS, COM, CORBA, UML Windows/NT

http://groups-beta.google.com/group/az.jobs/browse_thread/thread/ae4469478c923be4/ac08e9e84f79560b?q=3Dwww.cardsystems.com%2F&rnum=3D5&hl=3Den#ac08e9e84f79560b

A few days before this breach news story hit the fan, CardSystems was boasting about their great systems.

CardSystems Solutions Inc. is a leading provider of integrated payment solutions to associations, financial institutions, Independent Sales Organizations and retail merchants.

With CardSystems' comprehensive and flexible array of processing services, clients can manage the entire payment processing cycle and customize services to fit their needs while maintaining complete control of risk, dispute resolution and proprietary customer data. CardSystems' intelligent enabling technologies include an expert system, neural network and service offerings optimized for the card processing industry. CardSystems products include traditional terminals, integrated applications and e-payment solutions. The company processes payment transactions for more than 125,000 customer locations.

http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=3Dnews_view&newsId=3D20050614005656&newsLang=3Den

Data at risk: Credit Card Account #s, their expiration dates, what brand (e.g. Visa), what bank (e.g. MBNA) Names of people on the credit cards the 3-4 security #s found on back of cards

Data NOT taken: addresses, phone #s, date of birth, mother's maiden name, nationality, gender, social security #s etc. for the names of people on the credit cards PIN # where the credit card can be used in an ATM machine

Al Macintyre <http://www.ryze.com/go/Al9Mac>

✦ Hacker accesses files at Equifax

<RsH <rsh@idirect.com>>

Fri, 17 Jun 2005 21:55:34 -0600

As per CBC news, 17 June 2005, another hack into a sensitive area at one of

Canada's two major credit bureaus:

A computer hacker has accessed the files of about 600 consumers at Equifax Canada, one of Canada's major credit bureaus. Most of the files are for consumers from British Columbia. Equifax Canada uses data provided by banks to compile credit records on Canadian consumers. Those records include personal information such as social insurance numbers, bank account numbers and up to six years of credit and banking history ... Equifax said all affected customers in this latest breach have been contacted. The RCMP is investigating.

<http://www.cbc.ca/story/business/national/2005/06/17/equifax-050617.html>

R.S. (Bob) Heuman, Toronto, ON, Canada, Indep. Computer Security Consulting
Web Site Auditing for Compliance with Standards rsh@idirect.com

✦ Cell Phones Now Playing Role of Wallet (Bruce Meyerson)

<Monty Solomon <monty@roscom.com>>

Sat, 18 Jun 2005 00:11:34 -0400

With the number of cell phones in the world is reportedly about 1/4 of the world's population, the next step seems to be incorporating all of your credit and debit cards into a single wireless multipurpose mobile device.

In Japan, DoCoMo already has 3 million cell-phone subscribers using its Mobile Wallet. The next step seems to be the incorporation of checkbooks, Quicken, PayPal, CheckFree, etc. [Source: Bruce Meyerson, Associated Press,

17 Jun 2005; PGN-ed]

<http://finance.lycos.com/home/news/story.asp?story=49940191>

Risks??? What risks?

SIM Cards with GPRS

<"Darryl Smith" <Darryl@radio-active.net.au>>

Thu, 16 Jun 2005 18:54:04 +1000

I am a GPS tracking consultant - and I usually use GPRS, which is a packet switched data service built on top of GSM. Unlike AMPS and CDMA, the personality of each mobile device is stored in a Smart Card called a SIM card. This stores the local encryption key as well as a serial number that points to your phone number. It also stores information on the preferred GSM network to connect to and your phonebook.

If you want to swap phones you just swap SIM cards. This makes upgrading phones really easy, and also makes it easy to rent a phone in another country if your phone does not work in that country because it operates on a different frequency.

One of my clients was issued 80 SIM cards for a project I was doing for them. The carrier supplied the SIM cards as well as printed documentation listing the serial number for each card. This serial number is the reference that translates into a phone number and a billing identifier.

This customer also arranged to have their own VPN set up so that their data traffic would not pass over the internet but over a private link between the carrier and customer. The way this is done is by assigning a different APN or Access Point Name. This APN was specific to this customer, and no-one else had access to it.

When I was testing the equipment with the SIM cards and the custom APN, the SIM cards would not work. So I tried it in my GPRS phone - and strangely it worked using the standard APN. This did not surprise me as the carrier was notorious for not correctly configuring the APN.

My customer then sent the list of SIM cards to the carrier for them to fix, attaching the custom APN. This was the same list the carrier had provided to them, but thanks to business processes it was easiest for my client to e-mail the carrier the list back. The changed the APN on all 80 cards to the custom APN, removing GPRS access through the default APN to all cards.

24 hours later I tried the equipment again, and it still did not work. So I rang my client, and for a joke I told him the serial number of the SIM card, and asked him if it was on his list. I was rather surprised when he could find no reference of it. Comparing his list of serial numbers to my list of serial numbers, we worked out that only 3 out of 80 of the SIM cards were on his list.

So my client then contacted the carrier. After some discussions, the carrier then transferred the 77 SIM cards to my client, and presumably restored the correct APN to the other 77 SIM cards being used by other clients returning GPRS functionality.

What had happened is that the carrier did not provide the correct SIM Serial Numbers to my client in the first place. My client assumed that this list was correct. I did not care what the serial numbers were, but I recorded them on each piece of equipment anyway, copying the number from the cards themselves, rather than copying from his list.

Then my client, assuming his list was accurate e-mailed the carrier, and the carrier assumed that this list was correct. And then changed the SIM cards to 'Fix Them', breaking many other services at the same time. Management in the carrier took some time to be convinced that they had not issued the correct serial numbers to the client - even wanting to speak to me directly to verify that I physically had these SIM cards in my possession.

Right now my clients GPRS devices seem to be working, but I have no idea about the 77 SIM cards being used by other clients. This is likely to be a huge billing nightmare too. Thankfully we only used a few cents worth of GPRS bandwidth on cards that did not (at the time) belong to my client.

The risk? Don't rely on information that a supplier gives you. Do not rely on information a customer gives you without cross checking it. Do not rely on mobile devices for critical purposes if there is any chance that someone

could re-configure your mobile device.

Darryl Smith, VK2TDS, POBox 169 Ingleburn NSW 2565 Australia +61 4 12 929 634

www.radio-active.net.au/blog/ www.radio-active.net.au/web/tracking/

✶ New 'Heathrow Connect' Trains - do not want to go to Heathrow!

<"SB" <s_byers666@yahoo.co.uk>>

16 Jun 2005 05:47:38 -0700

A new electric train service has just started between Heathrow Airport and Paddington Station in West London, UK. This uses brand new multi-million-pound trains made by Siemens in Germany/France. They were specially designed for the British Airports Authority (BAA) and First Great Western Link (FGWL) who have the main franchise for services out of Paddington (in West London). The emergency evacuation instructions engraved on the windows are all in French - somewhat important since there have been at least three very major fatal crashes on the line.

The trains are highly computerised but not so automated in that they still need revenue protection officers (ticket inspectors) to check tickets in the three carriages. They are short trains. The route is a short one but ordinary tickets and Travel Cards (one day go anywhere 'seasons') are available - EXCEPT for the one mile link between the last station on the mainline and Heathrow Airport itself. This is priced at 6 UK pounds, making it the most expensive train fare in the world for the distance. Fare more expensive per mile or kilometre than even for Concord. The equivalent bus fare is a mere one pound 20 pence.

However these multimillions trains have a fault. This doesn't bother regular travelers on the line well used to the vicissitudes of the alternative ex-Thames Trains and FGWL services. But it might bother travelers from overseas. This is that the on-board announcements are computerised. Unfortunately however the computer controlling them hasn't a clue where the train is and keeps on announcing that the "next stop is Paddington where the train terminates," and "please mind the step between the train and the platform." And "please make sure you take all of your belongings with you when you leave the train." On the way to Heathrow every next station is announced as Ealing Broadway (an intermediate stop) even if Ealing Broadway has long been called at. And other intermediate stations, e.g. Southall, are announced as being Hanwell or somewhere else.

There is also a problem with the computerised braking system in that at Hayes and Harlington Station the trains invariable pull up a LONG way from the entrance. Other trains pull up near the entrance. This means that announcements from station staff passengers have to run after the train in order to board it.

The trains are soon to be extended to four carriages long. For this they have to be shipped back to Siemens in Europe. Apparently it is not possible to do this work in the UK.

And the Risks?

Emergency instructions do need to be in the majority language of the country in which the trains are designed for.

Computerised announcement systems have been around for a long while, passengers do need the correct information especially when there is a charge of 6 pounds if they inadvertently stay on board for the extra very

short
trip into Heathrow itself, and staff are there to make sure they pay
up.

Adding an extra carriage should not have to entail shipping an entire
train
unit back to the manufacturers in a different country.

At least these trains do not have the fault of earlier electric units
that
were so computerised that the doors wouldn't open at stations to let
passengers on/off - because the sun had gone behind a cloud and there
wasn't
enough power to operate the door release mechanism.

✈ **Re: Plane diverts after erroneous hijack alert (Kuenning, [R-23.89](#))**

<Dan Jacobson <jidanni@jidanni.org>>

Sun, 19 Jun 2005 06:12:15 +0800

<http://www.faa.gov/atpubs/ATC/Chp10/atc1002.html>

<http://www.faa.gov/atpubs/AIM/Chap4/aim0401.html>

When making routine code changes, pilots should avoid inadvertent
selection
of Codes 7500, 7600 or 7700 thereby causing momentary false alarms at
automated ground facilities. For example, when switching from Code
2700 to
Code 7200, switch first to 2200 then to 7200, NOT to 7700 and then
7200. This procedure applies to nondiscrete Code 7500 and all
discrete codes
in the 7600 and 7700 series (i.e. 7600-7677, 7700-7777) which will
trigger
special indicators in automated facilities. Only nondiscrete Code
7500 will
be decoded as the hijack code.

✈ **REVIEW: "Brute Force", Matt Curtin**

<Rob Slade <rslade@sprint.ca>>

Thu, 16 Jun 2005 16:06:54 -0800

BKBRTFRC.RVW 20050531

"Brute Force", Matt Curtin, 2005, 0-387-20109-2, U\$25.00/C\$33.50

%A Matt Curtin <http://ergo-sum.us/brute-force/>

%C 233 Spring St., New York, NY 10013

%D 2005

%G 0-387-20109-2

%I Copernicus/Springer-Verlag

%O U\$25.00/C\$33.50 800-842-3636, 212-460-1500, fax: +1-212-254-9499

%O <http://www.amazon.com/exec/obidos/ASIN/0387201092/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0387201092/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0387201092/robsladesin03-20>

%O Audience i+ Tech 2 Writing 3 (see revfaq.htm for explanation)

%P 291 p.

%T "Brute Force: Cracking the Data Encryption Standard"

As the subtitle states, this is the story of the assessment of the strength (and weakness) of the Data Encryption Standard, particularly as computer power increased over time. Specifically, it is the tale of the formation and development of the DESCHALL operation, one of the forerunners of distributed.net. It is not just a story, though: Curtin tells the tale from a specific social and political perspective. An indication of this position is given in the forward, where John Gilmore reiterates the somewhat questionable assertion that DES was "deliberately ... flawed." Although this work does not address more technical aspects of cryptography, using hyperbolic arguments such as this may weaken the overall case of the book in regard to cryptographic censorship.

There are forty-one very short chapters to the book, the first describing the particular machine that found the key for the first DESCHALL distributed

cracking attempt. A brief history and background for cryptography is given in chapter two.

Chapter three outlines the process of transforming Lucifer into DES. However, there are numerous errors in the account. Some are minor. (The Data Encryption Standard and the Data Encryption Algorithm are not equivalent: the algorithm is the engine, while the standard includes additional functions for real world operations.) Other problems include issues such as the fact that the modification of S-boxes (the substitution function, which the book refers to as permutation) is mentioned, while that of the P-boxes (permutation) is not. Most references state that the Lucifer version finally submitted for DES was 70 bit, rather than 112 bit. It is quite misleading to say that a 112 bit key is "fifty-six times" as strong as a 56 bit key. The Diffie-Hellman objections to the 56 bit key length are not given in detail, which makes the arguments hard to assess. Not all the dates are given, which sometimes creates difficulty in following the thread. (In response to a first draft of this review, Curtin has noted that he has collected a fairly extensive errata for the book, and hopes to correct the issues in a second edition.)

Chapter four is a rather mixed bag: despite the "Key Length" title, it touches on various algorithms, cryptanalytic concepts, and other topics. (There is a seeming confusion of the Vernam cipher with a one-time pad, and triple DES is generally considered to have an effective 112 or 113 bit key, rather than 168, due to the meet-in-the-middle attack.) The author's personal involvement with cryptology, and analysis of the feasibility of cracking cryptosystems, is outlined in chapters five through eight, culminating in a review of the possibilities of distributed computing. The

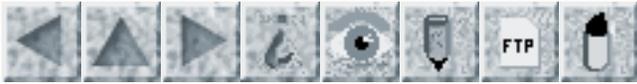
technical, social, and political factors involved in creating and operating the DESCHALL team are discussed in chapters nine to thirty-eight. (It is odd that explanations of IP addresses almost always use the non-routable 192.168.x.x range. Specific IP addresses have a depressing tendency to change and so non-routable addresses are often used in explanations, but it seems particularly inappropriate when the subject deals with identification and location of machines.) The material is fascinating, instructive, and even exciting at times. Interspersed are mentions of legislative debates and hearings into cryptographic policy during that time. Two chapters cover events subsequent to DES Challenge I, while analysis and lessons learned are reviewed in forty- one.

The density of errors in the early chapters is unfortunate, since it is not representative of the work as a whole, and yet it may lead readers to distrust the facts in the book. In reality, there are significant points to be made, not only in terms of cryptography and public policy, but also in regard to distributed computing itself. The book is certainly useful for those interested in the issue of brute force attacks against cryptographic systems, and is an engaging read for anyone into technology.

copyright Robert M. Slade, 2005 BKBRTFRC.RVW 20050531
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 23: Issue 92

Wednesday 29 June 2005

Contents

- [Single Point of Failure paralyzes Swiss Railsystem for 3 hours](#)
[Debora Weber-Wulff](#) [Anthony Thorn](#)
- [The continuing saga of the German unemployment scheme Hartz IV](#)
[Debora Weber-Wulff](#)
- [New Heathrow Connect Trains - Now Can't Even Connect!](#)
[S Byers](#)
- [Flaw Is Found in Software Used to Accredite Hospitals](#)
[Milt Freudenheim](#) via [Monty Solomon](#)
- [Robot runs riot at California hospital](#)
[Thom Kuhn](#)
- [Frozen Windows in Delivery Room](#)
[Charles Palmer](#)
- [Re: New Zealand Outage Shut Down Stock Exchange](#)
[Russell Smiley](#)
- [One Week to Shattered Security: Lessons from the Sony PSP Exploit](#)
[Lauren Weinstein](#)
- [Encryption Illegal in Minnesota](#)
[James R. Cottrell Jr.](#)

- [U.K. firm boasts totally "hacker proof" ID card system](#)
[Ben Tudor via Declan McCullagh](#)
 - [CVS limits ExtraCare info access](#)
[Marion Davis via Monty Solomon](#)
 - [Yahoo Filters Phish](#)
[B Brown](#)
 - [Re: "Rumplestiltskin worm" on the loose?](#)
[Crispin Cowan](#)
 - [Breach tracking](#)
[Adam Shostack](#)
 - [REVIEW: "Spies Among Us", Ira Winkler](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Single Point of Failure paralyzes Swiss Railyystem for 3 hours

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

Thu, 23 Jun 2005 20:56:34 +0200

On 22 Jun 2005 at 5.08pm, a power short occurred between Amsted (Canton Uri) and Rotkreuz (Canton Zug, which in German means "train") on the Swiss train line. The SBB (Schweizerischen Bundesbahnen) operated their own power lines, and this short circuit caused a sharp drop in voltage, which quickly spread throughout the ENTIRE country of Switzerland.

Trains were stalled in the middle of nowhere, with no air conditioning in the heat of the summer. Some train doors could not be opened. More than 200,000 passengers were affected. It took about two hours to get everyone out of the trains. SBB used busses to transport stranded passengers and

diesel locomotives to drag trains to the nearest station.

It took two more hours before enough power was restored in order for the trains to begin moving. But the efficient Swiss worked all night moving trains so that everything moved rather smoothly the next day.

There were allegedly no computers involved, but the single point of failure was a vivid illustration of many RISKS concepts, not the least of which is:
don't throw out those diesel locomotives yet!

Debora Weber-Wulff, FHTW Berlin, FB 4, Intern.Medieninf.
Treskowallee 8,
10313 Berlin +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

✶ Single Point of Failure paralyzes Swiss RAILSsystem for 3 hours

<Anthony Thorn <anthony.thorn@bluewin.ch>>
Thu, 23 Jun 2005 09:54:23 +0200

[...] My concern --and arguably the risk-- is the impact of such an incident on passenger trains in the new Gotthard "base"-tunnel which will open in 2011. This will be 57 Km (35 miles) long and run at depths up to 2000 meters (7000 feet) which means that the tunnel temperature will exceed 45 C. (113 F). If a train is stopped in the tunnel a very rapid response would be required to avoid a catastrophe.

⚡ The continuing saga of the German unemployment scheme Hartz IV

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

Sat, 25 Jun 2005 13:16:22 +0200

In our previous installments ([RISKS-23.53](#) and 23.60), we heard about problems with the new German combined unemployment and social fee scheme.

Because of so much public unrest about the scheme, the parliament decided to pass new rules permitting people to earn a little bit more money each month before the entitlement is cut off. Just a small program change, one would think, and with time until 1 Oct 2005 it should be no problem.

The **Berliner Zeitung** reported on 25 Jun that the program change will not be finished until early 2006. The new rules are too complicated for the software authors, T-Systems, it seems:

* Everyone can earn 100 Euros a month additionally without penalty.

* If you earn up to 800 Euros you can keep 20%.

* If you earn more, you get to keep 10% of what you earn above that, until

your earnings reach the point where you no longer get the social fee.

About 700.000 people are affected, the administrative workers will have to do the calculations by hand until the software is finished - meaning they have no time to advise people on strategies for finding work.

Maybe I am being naive, but how difficult is it to set up a new table

"Earnings" with (Pnr, date, earnings) and fixing the method "calculate_entitlement" to consult this table. There needs to be a screen

for entering in the data and recording who entered it in when.

This takes a large company > 6 months to fix?

<http://www.berlinonline.de/berliner-zeitung/politik/460429.html>

✈️ New Heathrow Connect Trains - Now Can't Even Connect!

<"SB" <s_byers666@yahoo.co.uk>>

23 Jun 2005 03:56:57 -0700

The new trains whilst widely advertised as 'Heathrow Connect' (in the local press, on the HC website, etc.) have now stopped connecting to Heathrow altogether!! Passengers are now being advised to detrain at Hayes & Harlington - the local stop before - and catch a 140 bus to the Airport. This only costs an additional 1.20 (pounds) rather than the 6 (pounds) - but entails negotiating a steep flight of steps - not easy with heavy luggage and no station staff to help.

The reason for this curtailment is a signal fault - apparently when the trains reach Heathrow the signalling system there wont change aspect to let them back out again!!

Also the Heathrow Connect trains use the two local slow tracks in order to stop at local stations. The other two tracks (there are four in total) are for high-speed Intercity services. In order to swing off the

local tracks
into/out of the Airport Branch the Connect Trains have to cross
over the
Intercity tracks. This means stopping all other trains to allow
them to do
so. This is playing havoc with the timekeeping for all of the
other services
using this very busy route.

The Risks:

* Didn't the planners realise the operational (and safety)
problems of
local trains crossing Intercity tracks every 30 minutes and
thereby
holding up high speed (100 mph) trains?

* For a multi-million pound prestige project shouldn't there
have been
something called 'UAT' (user acceptance testing)?

* Actually shouldn't there have been something called 'testing'
prior to
launching such a high profile service?

* The other problem is the young staff checking tickets whilst
ensuring that
bona-fide passengers have paid, are starting to get bullied by
the local
feral youths who on the late evening trains are damned if they
are going to
pay whatever.

* Meanwhile the many computerised on-board inane announcements
are beginning
to grate for regular passengers and are still frequently wrong -
and they
can't even be changed to omit 'Heathrow' from the current list of
destinations.

✶ Flaw Is Found in Software Used to Accredite Hospitals

<Monty Solomon <monty@roscom.com>>

Sat, 25 Jun 2005 02:29:17 -0400

Joint Commission Resources, a unit of the Joint Commission on Accreditation of Healthcare Organizations that enforces quality standards for hospitals found a flaw in software that it had sold to more than 1,000 hospitals that helps qualify for accreditation and payments from Medicare. The problem was a missing identification marker that alerts a hospital to the 250 standards among the 1,300 that the commission and its auditors regard as essential.

[Source: Milt Freudenheim, *The New York Times*, 24 Jun 2005; PGN-ed]

<http://www.nytimes.com/2005/06/24/technology/24glitch.html?ex=1277265600&en=ad248571c0f51b3d&ei=5090>

✶ Robot runs riot at California hospital

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

Sat, 25 Jun 2005 11:47:22 -0400

Staff and patients at San Francisco's UCSF Medical Center were left fearful and shaken last week, when a robotic nurse threw off its shackles and went on the rampage.

http://www.theregister.co.uk/2005/06/15/psycho_robot/

Thomson Kuhn, American College of Physicians

✶ Frozen Windows in Delivery Room

<Charles Palmer <ccpalmer@us.ibm.com>>

Thu, 23 Jun 2005 23:10:10 -0400

As my dear laboring spouse was rolled into the O.R. to deliver twin boys last month, all of the machines in the room were happily humming along, including several displaying a far too familiar screensaver. One of the attending physicians ordered "a quick ultrasound" to ensure things were indeed as they should be. The nurse turned to one of the machines with little windows flitting about on the screen. Just as she moved the mouse to wake up the machine, the flitting stopped and the machine was no more. All fifteen people in the room, including the soon-to-be mommy of plummeting patience, then waited for the nurse to power-cycle the machine and await its resurrection.

While this turned out not to be a life and death situation, it very well could have been, especially with a multiple birth. In addition to checking the background of physicians, do we now have to check what software they're running???

PS: the twins Bennet and Bryan, while premature, are gonna be ok over time.

Charles C. Palmer, IBM Research

⚡ Re: New Zealand Outage Shut Down Stock Exchange

<"Russell Smiley" <smiley@nortel.com>>

Wed, 22 Jun 2005 15:03:11 -0400

The New Zealand Herald 20 Jun 2005 had this explanation for the telecommunications failure noted in [RISKS-23.91](#):

A fibre "ring" exists between Auckland and Wellington running up the east and west sides of the North Island. In theory at least if one cable fails the other can continue at reduced capacity. Apparently in this case they lost both cables - one to a contractor digging and the other possibly to a rodent. http://www.nzherald.co.nz/index.cfm?c_id=1&ObjectID=10331826

⚡ One Week to Shattered Security: Lessons from the Sony PSP Exploit

<Lauren Weinstein <lauren@vortex.com>>

Wed, 22 Jun 2005 08:39:44 -0700

Greetings. It only took around a week for the exploit to evolve from unwieldy but powerful hack, to user-friendly production program, but the "signed-code" security system of the Sony PSP Portable running 1.5 firmware, designed to prevent the execution of pirated or other "unofficial" (e.g. homebrew) code, appears to have been obliterated.

I note in:

"The Camel Fully Enters the Tent?":

(<http://www.eepi.org/archives/eepi-discuss/msg00108.html>)

that only about seven days after the release on the Internet of an exploit permitting running of unsigned code via an "impractical for routine use" memory-stick swapping technique, rumors were already circulating that a program eliminating the stick swap was about to be released.

This appeared on schedule this morning, meaning that for all practical purposes the widely available U.S. version of the Sony PSP with 1.5 firmware is now as fully exploitable as the original limited-quantity Japanese-market 1.0 firmware units.

As mentioned in the referenced link above, Sony will attempt to minimize the damage from these events. But any path they choose is strewn with potential pitfalls. Newer firmware versions in shipped units may prove to be more difficult or impossible to hack through non-hardware-invasive techniques. But forcing firmware upgrades with new game releases may have the effect of actually suppressing purchases of legitimate copies of games, and encourage the use of pirated copies that won't trigger the firmware updates and the likely loss of the ability to run unofficial, homebrew programs.

In an ever more pervasively Internet-connected world, it appears increasingly likely that any error -- any opening -- in the implementation of a security system for a "desirable target" will be quickly exploited and that exploit widely distributed -- and probably much more rapidly than the

designers of the system would imagine in their worst nightmares. This is a security vulnerability "sea change" that we really haven't come to grips with either as technologists or as businesses, and it goes far beyond the running of programs on a portable gaming device.

There's a key question that we need to explore. Given this new environment, to what extent do "closed" systems still make sense? The answers will vary between applications and situations, but it clearly is foolhardy in the extreme to simply assume that security paradigms, even those based on the most advanced encryption and signature models, will long remain invulnerable to successful attacks. These penetrations will range from those initiated by persons who are simply intellectually curious without evil or financial motivations, to individuals who may have very dark intentions indeed.

Something to think about.

Lauren Weinstein, +1 (818) 225-2800 <http://www.pfir.org/lauren>
Co-Founder, PFIR People For Internet Responsibility <http://www.pfir.org>

Co-Founder, EEPI Electronic Entertainment Policy Initiative
<http://www.eepi.org>

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

Lauren's Blog: <http://lauren.vortex.com> DayThink: <http://daythink.vortex.com>

Encryption Illegal in Minnesota

<"James R. Cottrell Jr." <jxc@mitre.org>>

Wed, 22 Jun 2005 13:03:47 -0400

Well the state of Minnesota had better start renting rooms in the prisons of other states, since the Minnesota State Web site supports encryption. About the third URL I tried after accessing the web site showed a secure URL.

<https://www.officesupplyconnection.org/statemn/catalog.srv>

Unless they have set up these computers in a different state or country that allows the use of encryption! If that is the case, maybe the FBI would like to get involved since they would have crossed state lines to avoid prosecution.

🔥 U.K. firm boasts totally "hacker proof" ID card system [Politech]

<Declan McCullagh <declan@well.com>>

Wed, 29 Jun 2005 01:10:26 -0400

[O UK ID? O U KID! Who U KIDDing? PGN]

----- Original Message -----

Date: Tue, 28 Jun 2005 20:05:49 +0100

From: Ben Tudor <Ben_Tudor@vnu.co.uk>

Subject: Oh dear - Don't worry about UK ID card insecurity - here's a

totally 'hacker proof' system

This press release makes an IT journo's job look rather like shooting fin tuna in a barrel. Using cluster bombs. There's so many holes in the argument presented in this press release that I almost don't

know where to
start. Now that I know a company has been working on 'hush-hush
software',
of course, all my concerns about national ID cards have simply
sloughed
away. Cheers, Ben

Ben Tudor, Features Editor, Computer Reseller News
ben_tudor@vnu.co.uk
<http://crn.vnunet.com>

Subject: Biometric ID Card breakthrough
PRESS RELEASE, June 29th 2005

Further information: 02476 236644

Press Office: John Fisher - 01785 840978
M: 07808 171 664
John.g.fisher@btinternet.com
jfisher@senselect.com

<http://www.senselect.com>

Biometric Innovation Breakthrough answers UK ID Card Security
Fears

A biometric identity card system that is hacker and thief-proof
and puts
the missing privacy and security into the UK ID project - has
been unveiled
today (Wednesday).

The British inventors of the BiometricPIN system say the system
can be used
in the new UK ID cards, overcoming all security fears and
objections and
putting control on the use of biometrics in the hands of the
user. Instead
of using a single, easily lifted or stolen fingerprint,
BiometricPIN will
allow any sequence of finger prints determined by the user. No
one has been
able to achieve this so far and the implications will be global

as spin-off
projects emerge.

The sequence creates a digital pattern that can only be recreated by the user. When it is stored on a Government or central database it simply becomes an unidentifiable "blob" that cannot be stolen.

Behind the world-first breakthrough is West Midlands biometric company, Senselect Limited, which has been working on the hush-hush software-based system for five years. John Topping, Managing Director of Senselect, said BiometricPIN would have implications for everyday life across the world, but the company has concentrated so far on the ID card security problem and the "big brother" fears it instills in people.

"This is totally secure, fast and "hacker-proof", said Mr Topping. "The sequence simply cannot be replicated by anyone other than by the user. It also allows the user to determine just how much information others can see about them. A doctor, for example, could be restricted to medical history whilst a bartender will only get confirmation that the customer is over 18."

With BiometricPIN there will be no "big brother", said John Topping and identities stored on Government databases are safe from theft. With single finger biometrics everyone has a right to be scared because, while you can change a pin number if you are compromised, fingerprints are for life.

Biometrics using single fingerprints as an identifier have been

used for
some years, and despite them being capable of being "lifted",
their use has
grown. Their use in government ID cards - even with the backup
of iris and
facial biometrics - is considered a step backwards by many.

"With BiometricPIN there would be total security as the pattern
decided on
uniquely by the user cannot be lifted from a single finger
reader or hacked
from a database", said John Topping. "BiometricPIN produces a
unique
biometric print that just cannot be copied. It also needs live
fingers."

Mr Topping said BiometricPIN would solve a huge worldwide
problem. Anyone
concerned that their ID could be copied can rest assured that
this will
allay all their fears. Protecting peoples ID is already written
into our
law but with BiometricPIN it will be in the hands of the user.
Senselect
says BiometricPIN, because it is software-based, can be used in
conjunction
with all existing technology, along with iris and facial
biometric systems.

The company says it already has several European governments
interested in
implementing BiometricPIN and Senselect has produced a set of
security
standards for cross border biometric identification. This is now
being
considered by the European Union for adoption.

Added John Topping: "We believe we have solved a huge problem
for the world
and are ready to share our knowledge. This is the biggest
breakthrough in
computer technology for many years and will have a huge impact
on everyday

commerce as further applications for BiometricPIN emerge".

Senselect Limited, Coventry University Technology Park, The
Innovation Centre
Puma Way, Coventry, UK, CV1 2TT <http://www.senselect.com>

For further information, please reply to john.g.
fisher@btinternet.com

CVS limits ExtraCare info access (Marion Davis)

<Monty Solomon <monty@roscom.com>>

Wed, 29 Jun 2005 03:49:02 -0400

Marion Davis, pbn, 22 Jun 2005

The CVS Corp. has cut off Web access to ExtraCare card holders' detailed purchase information after a consumer group showed reporters how easily an intruder could log into the system and find out, say, how many condoms or enema kits someone's bought. CVS has issued about 50 million of the loyalty cards, which allow the drugstore chain to track each customer's purchases and, in exchange, provide a 2-percent rebate on those purchases, along with customized coupons. To log into your account on CVS.com, all you need is the card number, your ZIP code, and the first three letters of your surname. Even now, anyone with that information can easily find out the card holder's home address, phone number, and total purchases each quarter. But until last week, the Web site also allowed customers to request a detailed

purchase report to be e-mailed to them - to any address they put in. ...

<http://www.pbn.com/contentmgr/showdetails.php/id/115431>

⚡ Yahoo Filters Phish

<bbrown@spsu.edu>

Wed, 29 Jun 2005 10:43:29 -0400

I take phishing scams a little more seriously than other spam, and often spend a few minutes directing complaints to the right places. A phishing e-mail this week used a link in a domain registered using Yahoo's domain registration. Pinging the domain name revealed an IP number that ARIN says is Yahoo's. So, I sent off a copy of the message with full headers etc. etc. to abuse@yahoo.com. It was rejected by Yahoo's spam filter because, so the bounce said, it was a phishing e-mail. Well, duhhh!

Undeterred, I send another message to abuse@yahoo.com, explaining that I had received a phish that pointed to one of their machines and provided the URL of a page that imitates an on-line payment service. It got an auto-response that told me I needed to send the full message, including headers. Double-duhhh!

No doubt Yahoo will be shocked, *shocked*! when a TV station or law enforcement agency reveals that Yahoo's Web hosting service is being

employed to run scams, just as they were when a television station reported last week that their user-created chat rooms were being used to attempt to lure children into having sex with adults.

Re: "Rumplestiltskin worm" on the loose? (Adams, [RISKS-23.89](#))

<Crispin Cowan <crispin@immunix.com>>

Sat, 25 Jun 2005 10:09:51 -0700

> I'm sorry, but the Internet is not your private playground.
> If you have a
> spam problem, deal with it or buy your own intranet. Such
> "idealism" is
> what lets people use the Internet to communicate. <freedom
> argument
> continues>

This is so deeply wrong that I feel I must rebut.

Bandwidth-based DoS attacks are fundamentally impossible to stop. If an attacker can compromise even a trivial fraction of the Internet, and then command those nodes to all flood your site with traffic, then your site collapses under the load, and no legitimate traffic can reach you because your connection is full. There is nothing to be done except track down the attacking nodes and have them shut down until they are cleaned up. This is an extortion attack that is in widespread use now, particularly against sites that have time sensitivity, such as gambling sites that hope to take bets on some big game: pay up, or we DoS you into the ground

during your
critical period.

Widely enforced Internet hygiene of some form would go a long way towards stopping this kind of attack. At some point in the future, this DoS attack is going to become so pervasive that there **will** be Internet hygiene rules imposed. Get used to it.

Personally, I hope that it comes sooner than later. That would mean that it is at least an industry self-imposed practice, rather than a government requirement.

Crispin Cowan, Ph.D. <http://immunix.com/~crispin/>
CTO, Immunix, a Novell Company <http://immunix.com>

⚡ Breach tracking

<Adam Shostack <adam@homeport.org>>
Fri, 24 Jun 2005 17:05:05 -0400

Since many of the entries in RISKS have been on security breaches, I'd like to draw your attention to my weblog: <http://www.emergentchaos.com> I've been cataloging breaches, and the fairly extensive (albeit not complete) is at http://www.emergentchaos.com/archives/cat_breaches.html

⚡ REVIEW: "Spies Among Us", Ira Winkler

<Rob Slade <rslade@sprint.ca>>
Wed, 22 Jun 2005 08:24:57 -0800

BKSPAMUS.RVW 20050531

"Spies Among Us", Ira Winkler, 2005, 0-7645-8468-5,
U\$27.50/C\$38.99/UK#16.99

%A Ira Winkler www.irawinkler.com

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2005

%G 0-7645-8468-5

%I John Wiley & Sons, Inc.

%O U\$27.50/C\$38.99/UK#16.99 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0764584685/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0764584685/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0764584685/>

[robsladesin03-20](#)

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

%P 326 p.

%T "Spies Among Us"

In the introduction, Winkler admits that the title is slightly
misleading:

most surveillance is not done by international spies, but by
common or
garden thieves, competitors, and so forth. The point that he is
trying to
make is that non-terrorists can hurt you, although he raises the
issue with
illustrations that are not completely clear.

Part one deals with espionage concepts. Chapter one reviews
spying
terminology, but makes points about the process by explaining
the jargon and
distinctions. Risk analysis is introduced in chapter two, but
the
calculations used may not be clear to all readers. An attempt

to assess the value of information is made in chapter three. Chapter four outlines threats (entities that might harm you) and five covers vulnerabilities--the way your own operations can make you subject to attack.

Part two describes some case studies of spying. The content is interesting, although the value is rather concentrated in the short "vulnerabilities exploited" section at the end of each chapter. I must say that I've read all manner of similar stories and case studies in various security books, and Winkler's are more interesting than most.

Part three deals with protection. Chapter twelve lists a number of countermeasures. These are described in a level of detail that is appropriate for non-specialists (in security), although the content related to technical safety might be a bit thin. How to plan and implement an overall security program is outlined in chapter thirteen, which includes a very interesting section on how the Department of Homeland Security has taught us valuable lessons about how **not** to execute safeguards.

While not structured in a formal manner that would make for easier reference, this book nonetheless has some excellent content. Like Schneier's "Beyond Fear" (cf. BKBYNDFR.RVW), it is easy enough, and engaging enough, for those outside of the security profession to read. Busy managers may find the work a bit wordy and disorganized, but it makes useful points, and has constructive suggestions. Home users and amateurs will find the

style most suited to them, although the recommended controls are aimed at businesses. Security professionals will not (or should not) find anything new here, but may appreciate the "war stories" and explanations that can be employed in security awareness training.

copyright Robert M. Slade, 2005 BKSPAMUS.RVW 20050531
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 23: Issue 93

Sunday 10 July 2005

Contents

- [Monitor misprogrammed, air quality suffers](#)
[Bill Hopkins](#)
- [US-VISIT](#)
[Marc Rotenberg](#)
- [Pentagon Creating Student Database](#)
[PGN](#)
- [USC application system cracked](#)
[PGN](#)
- [Indian call centre 'fraud' probe](#)
[S Byers](#)
- [Life gets messy online/offline in China](#)
[Esther Dyson via Dave Farber](#)
- [Future Combat Systems procurement problems: GAO report](#)
[Dawn Onley via Pete Mellor](#)
- [PayPal, a Risk when you do, and a risk when you don't...](#)
[David Leshner](#)
- [More on Minnesota encryption](#)
[Steve Peterson](#)

- [WWW 2006 Call For Papers: Security, Privacy & Ethics Track](#)
[Angelos D. Keromytis](#)
 - [REVIEW: "Silence on the Wire", Michal Zalewski](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Monitor misprogrammed, air quality suffers

<"Bill Hopkins" <whopkins@wmi.com>>

Wed, 6 Jul 2005 14:45:46 -0400

Our local newspaper reports in print (but not on line) that Exelon Power's Cromby generator in Phoenixville, PA exceeded pollution limits for seven months in 2004 after an unidentified "vendor" programmed an emissions monitor for the wrong standards, and that the company will pay 600 grand. Websites for the company and the PA Dept of Environmental Protection confirm the story. Exelon is the parent company of PECO Energy, formerly Philadelphia Electric Co., which supplies power to the area.

Cromby has two generators, one coal-fired and one switchable between oil and natural gas. The vendor ("a big company" says Exelon) set the monitor for the coal-fired unit to standards for the other unit. (I would guess that the SO2 limits for oil might be higher.) Exelon discovered the problem while aggregating data "for a large use," stopped it and turned itself in. DEP assesses a fine for each day of violation.

Risks for a company: trusting the dials and trusting the vendor when you're on the hook.

Risks for the rest of us: breathing in.

Exelon report: http://www.exeloncorp.com/NR/rdonlyres/DDDBE22B-94E3-4EE1-9F3C-ED4266DB0093/977/environ_rpt_2004.pdf (see page 16, numbered 12)

PA DEP: <http://www.depesf.state.pa.us/news/cwp/view.asp?a=3&q=465363>

Daily Local News (West Chester, PA): www.dailylocal.com (The article appeared 2005-07-05; who knows, it might yet show up on the site.)

✶ US-VISIT (from EPIC Alert 12.13)

<Marc Rotenberg <rotenberg@epic.org>>
Tue, 5 Jul 2005 08:48:33 -0400

E P I C A l e r t

Volume 12.13
30, 2005

June

Published by the
Electronic Privacy Information Center (EPIC)
Washington, D.C.

http://www.epic.org/alert/EPIC_Alert_12.13.html

EPIC Keeps Watchful Eye on US-VISIT

Foreign visitors to the United States are experiencing a new kind of jet lag: delays and secondary security screenings prompted by technological glitches in the border security program known as the United States Visitor and Immigrant Status Indicator Technology (US-VISIT). Documents obtained by

EPIC under the Freedom of Information Act from the Department of Homeland Security show that US-VISIT has resulted in many cases of mistaken identity. Commercial aircrew members, vacationers, and businesspersons have all been delayed by the gaffes. The problems caused unnecessary delays in the visitors' travels and resulted in the improper flagging of crewmembers by government watch lists.

US-VISIT was launched at 115 airports and 14 seaports in January 2004. By the end of 2005, the program will be operational at all of the nations more than 400 ports of entry. US-VISIT requires foreign nationals entering or exiting the country to submit biometric and biographical information. This data collection often begins before a visitor buys her plane ticket, as U.S. consular offices abroad may, before issuing a U.S. visa, collect fingerscans from potential visitors and compare them against those in a criminal database. Fingerscans are again collected upon the visitor's arrival in the U.S. for verification and then stored in a government database, as are travelers' arrival and departure records. Failure to be processed through this departure confirmation system could jeopardize a visitor's re-admittance to the U.S., as the government compares the manifest information provided by air and cruise lines to ascertain that visitors have not overstayed their visas.

Last September, US-VISIT expanded to include visitors from the 27 nations who are members of the Visa Waiver Program, thus requiring the

screening of an additional 33,000 persons per day. Except for visiting diplomats and officials and persons under 14 or over 79 years old, US-VISIT now applies to virtually all foreign nationals holding nonimmigrant visas, regardless of country of origin.

The documents obtained by EPIC show that some travelers are aware that the US-VISIT database contains erroneous information well before DHS realizes its own mistake and fear that their next visit to the U.S. will result in misidentification. Visitors reported missing their connecting flights due to errors in the database system, and airline crewmembers reported being delayed up to ninety minutes after a long international flight. Some travelers reported that the operator collecting fingerprints at a port had erroneously reversed their left and right index fingerprints, labeled a husband's fingerprints as his wife's, failed to collect the data required under US-VISIT, or collected data from travelers exempt from the program, such as holders of a G-4 visa.

Passengers' numerous requests to the DHS for correction of erroneous personal information suggest that the rush to implement US-VISIT has come at the expense of data accuracy and passenger privacy. IDENT, the government database containing US-VISIT fingerprints, is based on technology that even the DHS considers outdated, even though the government has already invested about \$1 billion in the program. The current fingerprint technology does not

meet the government's biometric standard, which mandates imaging of all ten fingerprints. Last fall, Stanford University professor Lawrence M. Wein testified before Congress that the chance of identifying a terrorist by matching two index fingerscans poorly imaged by IDENT against the government's biometric watch list is no more than 53%. Privacy concerns are increasing as the government turns to the private sector for full implementation of US-VISIT; global consultant Accenture received a \$10 billion contract last year for full-scale implementation over the next decade.

Freedom of Information Act documents obtained by EPIC on US-VISIT:

http://www.epic.org/foia_notes/note7.html

EPIC's US-VISIT Page:

<http://www.epic.org/privacy/us-visit/>

More information on the US-VISIT technology and cost is available at:

<http://www.epic.org/redirect/wpvisit605.html>

⚡ Pentagon Creating Student Database

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

Thu, 23 Jun 2005 7:03:01 PDT

[Noted by Keith Rhodes. This is another database full of unreliable information that will inadvertently released?]

The Defense Department has begun working with BeNow Inc, a private marketing firm, to create a database of high school students ages 16 to 18

and all college students to help the military identify potential recruits in a time of dwindling enlistment in some branches.

The program is provoking a furor among privacy advocates. The new database will include personal information including birth dates, Social Security numbers, e-mail addresses, grade-point averages, ethnicity and what subjects the students are studying.

Chris Jay Hoofnagle, West Coast director of the Electronic Privacy Information Center, called the system "an audacious plan to target-market kids, as young as 16, for military solicitation." He added that collecting Social Security numbers was not only unnecessary but posed a needless risk of identity fraud. Theft of Social Security numbers and other personal information from data brokers, government agencies, financial institutions and other companies is rampant. "What's ironic is that the private sector has ways of uniquely identifying individuals without using Social Security numbers for marketing."

The Pentagon statements said the military is "acutely aware of the substantial security required to protect personal data," and that Social Security numbers will be used only to "provide a higher degree of accuracy in matching duplicate data records."

[Source: Recruiting Tool For Military Raises Privacy Concerns, Jonathan Krim, *The Washington Post*, 23 Jun 2005; PGN-ed]

⚡ USC application system cracked

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

Wed, 6 Jul 2005 16:53:55 PDT

A programming error in the University of Southern California's online system for accepting applications from prospective students left the personal information of ``hundreds of thousands of records'' publicly accessible.

The flaw was discovered by a student in the process of applying. [Source:

Robert Lemos, SecurityFocus; PGN-ed]

http://www.theregister.co.uk/2005/07/06/usc_site_cracked/

[We hope that the student's application was not rejected because

he had discovered the flaw! PGN]

⚡ Indian call centre 'fraud' probe

<"SB" <s_byers666@yahoo.co.uk>>

23 Jun 2005 05:16:01 -0700

Information passed on could have been used to clone credit cards
Police are investigating reports an Indian call centre worker sold the bank account details of 1,000 UK customers to an undercover reporter.

The Risks?

Obvious really - overseas call centres in poverty stricken third world

countries, the staff of whom have unlimited access to personal and private information of the more wealthy, are the worst security risks ever devised by financial organisations.

See: <http://news.bbc.co.uk/1/hi/uk/4121934.stm>

🔥 Life gets messy online/offline in China

<Esther Dyson <edyson@edventure.com>>

July 1, 2005 7:50:56 AM EDT

http://www.pacificepoch.com/newsstories?id=33425_0_5_0_M

Game Accounts Take Center Stage In Divorce

Legend of Mir 2, Online Game, SNDA, Shanda

Posted by: <http://www.PacificEpoch.com/members/profile_view_ind.php?id=164>

Zhou Zhengqian on Jul 01 | 17:07

A divorce in Chongqing has turned ugly when both parties want their joint online game accounts, Chongqing Business Post reports. Mr. Wang from Chongqing and Ms. Ye from Huibei met last September on Shanda's (Nasdaq: SNDA) online game Legend of Mir 2. Wang saved Ye's character from being killed by another player. The couple married at the end of October but decided to get a divorce in June. During their marriage, the couple jointly played over ten Mir 2 accounts, attaining level 40 to 50 status for all of them. The characters and virtual items are estimated to be worth 40,000 to 50,000 Yuan. Wang said that he wants to keep the accounts and virtual items

Common Operating Environment (SOSCOE) - would likely fail to meet aggressive schedules due to immature technologies.

"As currently structured, the JTRS, WIN-T and SOSCOE programs are at risk of not delivering intended capabilities when needed, particularly for the first spiral of FCS," according to GAO. "They continue to struggle to meet an ambitious set of user requirements, steep technical challenges and stringent time frames."

FCS is designed to link 18 manned and unmanned weapons systems via a common computer network known as WIN-T and the System of Systems Common Operating Environment.

The Army restructured its FCS program last year into spirals, with officials announcing the first spiral would happen in fiscal 2008. But GAO said the first spiral may not demonstrate key networking capabilities.

GAO found the FCS program faces network, developmental and financial challenges that continue to slow progress. FCS' information network is dependent on the success of JTRS, WIN-T and SOSCOE - programs that are not included in FCS costs.

"Because JTRS, WIN-T and SOSCOE all rely on significant advances in current technologies and capabilities and must be fully integrated to realize FCS, there are substantial risks to this effort," wrote Paul L. Francis, GAO's director of acquisition and sourcing management,

in the
report.

For the full article, with a link to the original GAO report,
see:

http://www.gcn.com/vol1_no1/daily-updates/36302-1.html

Peter Mellor, Centre for Software Reliability, City University,
Northampton Square, London EC1V 0HB +44 (0)20 7040 8422

✶ PayPal, a Risk when you do, and a risk when you don't...

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

Wed, 6 Jul 2005 10:39:14 -0400 (EDT)

So I ordered some parts on-line. They arrived.

Then 45 days later, my credit card bill listed a PayPal charge.
Whoa... I
don't engage in such foolishness; certified letter to CC Co,
asking
"huh?"...

Two weeks later, PayPal starts sending ME email about fraudulent
use of MY
account...to the email address that I use for on-line buying.

Doh! The *merchant* uses PayPal to do their processing. OK.

But I try to write to PayPal to explain. No Joy. Only option to
contact them
is to FIRST log into my PayPal account; and use the webform...
and I don't
HAVE an account..

Write CC Co, dropping protest.

Now, 4 months later, PayPal writes again. My account is

locked.... (Need I
continue?)

Paypal assumes only account holders have a reason to reach them.
They can't
grok that that merchants and/or buyers may be involved. Further,
they wrote
ME about the holder's account. [They did NOT, at least give me
his account
ID just a incident number.]

Risks: Identity theft is sometimes TOO easy....

✦ More on Minnesota encryption (Cotrell, [RISKS-23.92](#))

<Steve Peterson <speterson@computer.org>>

Wed, 29 Jun 2005 15:12:17 -0500

Folks, get a grip. The opinion doesn't say anything about
encryption being
illegal.

Quoting from the opinion, the justices were trying to determine:
Did the district court err in admitting evidence concerning
appellant's
internet usage and encryption capability for his computer?

They wrote:

... Appellant first argues that he is entitled to a new trial
because the
district court erred in admitting irrelevant evidence of his
internet usage
and the existence of an encryption program on his computer.
Rulings
involving the relevancy of evidence are generally left to the
sound
discretion of the district court. State v. Swain, 269 N.W.2d

707, 714

(Minn. 1978). And rulings on relevancy will only be reversed when that

discretion has been clearly abused. Johnson v. Washington County, 518

N.W.2d 594, 601 (Minn. 1994). "The party claiming error has the burden of

showing both the error and the prejudice." State v. Horning, 535 N.W.2d

296, 298 (Minn. 1995).

Appellant argues that his "internet use had nothing to do with the issues in

this case;" "there was no evidence that there was anything encrypted on the

computer;" and that he "was prejudiced because the court specifically used

this evidence in its findings of fact and in reaching its verdict." We are

not persuaded by appellant's arguments. The record shows that appellant

took a large number of pictures of S.M. with a digital camera, and that he

would upload those pictures onto his computer soon after taking them. We

find that evidence of appellant's internet use and the existence of an

encryption program on his computer was at least somewhat relevant to the

state's case against him. See Minn. R. Evid. 401. ...

Think of it this way:

(child pornography, (digital pictures, digital camera, computer, crypto

software, photo sharing))

is like

(check fraud, (computer, blank check stock, list of account numbers, MICR

printer, ink removing solvent))

or

(assault, (baseball bat, bloody towel, footprint))

or

(burglary, (lock picks, bolt cutters, black cap, gloves)).

✦ WWW 2006 Call For Papers: Security, Privacy & Ethics Track

<"Angelos D. Keromytis" <angelos@cs.columbia.edu>>

Fri, 08 Jul 2005 12:35:59 -0400

WWW2006 Refereed Track: Security, privacy & Ethics

Viruses, spyware, and identity theft are turning the World Wide Web into a dangerous place. By undermining consumer trust, these problems are hampering e-commerce and the growth of online communities. A basic lesson is coming home to researchers, operators, and ordinary users alike: Security and privacy are not frills or features, but vital and enabling building blocks. As Web-based systems take on a physical dimension through wireless devices and sensors, and as they absorb varied media -- from books to online games to home movies -- digital security is ramifying in its economic and social reach.

This track promotes the view that security, privacy, and sound guiding ethics must be part of the texture of a successful World Wide Web. In addition to devising practical tools and techniques, it is the duty of the research community to promote and guide business adoption of security technology for the Web and to help inform related legislation.

The organizers seek novel research in security, privacy, and ethics as they relate to the Web, including but not limited to the following

areas:

- * Biometrics and secure template management
- * Digital Rights Management from its technical, ethical, and legal perspectives
- * Economic / business analysis of Web security and privacy
- * Electronic commerce, particularly security mechanisms for e-cash, auctions, payment, and fraud detection
- * Intrusion detection, insider threats, auditing, and honeypots
- * Legal and legislative approaches to issues of Web security and privacy
- * Location-based services
- * Knowledge-based authentication, such as security questions for password recovery
- * Privacy-enhancing technologies, including anonymity, pseudonymity and identity management
- * Public-key infrastructure and supporting concepts like digital signatures and certification
- * Secure and robust management of server farms
- * User interfaces as they relate to digital signing, encryption, passwords, and online scams like phishing
- * Wireless devices that interface with the Web, including RFID, sensors, and mobile phones
- * Web-services and supporting standards like XML

Chairs

- * Ari Juels (RSA Laboratories) (Vice Chair)
- * Angelos Keromytis (Columbia University) (Deputy Vice Chair)

PC Members [see website]

For more details, see <http://www2006.org/tracks/security.php>

The World's WWW Conference

WWW2006 will bring together the international communities of researchers, developers and business that drive the Web forward, shaping and developing its potential for new areas of communication, research, business and public administration.

Since the first international WWW Conference in 1994, this prestigious event, organized by the International World Wide Web Conference Committee (IW3C2), has provided the annual public forum for communicating research and development of the Web infrastructure and applications, as well as W3C initiatives.

The fifteenth conference in the series comes to the UK for the first time, and to one of the great historical centres of science and technology. Edinburgh is Scotland's capital city, home to one of the UK's oldest universities, an epicentre of the IT business sector and one of the world's great festival cities.

The WWW2006 programme addresses topics in media, e-government, e-commerce, education and e-science. The technical programme will draw on global research and industrial strengths to provide a strategic forum for the dissemination of new techniques and applications throughout the research community, the business and company sector and government agencies.

REVIEW: "Silence on the Wire", Michal Zalewski

<Rob Slade <rslade@sprint.ca>>
Mon, 27 Jun 2005 08:28:54 -0800

BKSLNWR.RVW 20050603

"Silence on the Wire", Michal Zalewski, 2005, 1-59327-046-1,
U\$39.95/C\$53.95
%A Michal Zalewski lcamtuf@coredump.cx lcamtuf.coredump.cx/
silence/
%C 555 De Haro Street, Suite 250, San Francisco, CA 94107
%D 2005
%G 1-59327-046-1
%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/1593270461/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1593270461/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/1593270461/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1593270461/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/1593270461/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1593270461/robsladesin03-20)
%O Audience s- Tech 2 Writing 1 (see revfaq.htm for
explanation)
%P 281 p.
%T "Silence on the Wire"

I don't know why, exactly, the phrase "self-taught information security researcher" (in "About the Author") should give me such a sense of foreboding. (The phrase could apply to me, and to many colleagues, although we tend not to use it.) And even before I read it, a number of people had warned me I wouldn't like it.

Well, I did like it, once I figured out what it was. I think a lot of people don't understand it. It is not a security text, by any means, but rather a series of explorations that take our "professional paranoid" mentality and examine some issues we seldom consider.

The subtitle states that the book is about passive and "indirect" attacks. Although passive attacks are well defined, indirect does not have a formal distinction, and the introduction does not help in explaining what the author intends.

Part one covers activities that occur at the origin of data and processing. Chapter one is titularly about typing, but spends a lot of time dealing with the problems of pseudo-random number generation, and seed data acquisition, and finally outlines an unlikely and very complex attack, heavily dependent upon specific functions and data availability, and seemingly directed at finding out if someone is typing at the computer. (The attack is also active, not passive.) A discussion of digital electronics, boolean algebra, and processor architecture, in chapter two, eventually leads to a brief discussion of the timing and power attacks that are well known in cryptology circles. (There are also odd and careless errors: readers are asked to contrast figure 2-4 with figure 2-4. There is a difference, it just isn't explained.) Chapter three reviews a few random and unrelated vulnerabilities. It is very difficult to determine what the point of chapter four might be, but it seems to be a screed against the use of Web crawling bots.

Part two appears to address local communications links. Chapter five provides a brief review of data communications 101, and then notes the "flickering modem LED" vulnerability. The ethernet frame padding problem is described in chapter six, while chapter seven lists some other networking difficulties, and eight briefly mentions miscellaneous topics such as identification by keystroke

analysis and war driving. (It should be noted that chapter length varies widely: chapters one, two, and five average twenty-five pages each, while the rest are closer to five.)

Part three moves out to the Internet. Chapter nine reviews most of the TCP/IP protocol, and then discusses how the ways that different systems populate fields of the IP header can be used to identify operating systems without a direct connection. The discussion in chapter ten starts with passive mapping of an inaccessible network, but the attack described seems to be intended for sequence number guessing (and session hijacking). Chapter eleven addresses weaknesses in various types of firewalls. Dissection of an odd packet is in chapter twelve, a method of third party scanning in thirteen, some possible metrics for identifying software in fourteen, and some ways of recognizing attacker machines in chapter fifteen.

Part four supposedly attempts to relate these disparate elements, apparently without much success. Chapter sixteen describes a storage method using packets bouncing around the net, seventeen looks at different methods of mapping the net and some possible uses, and eighteen considers the discovery of worms and other malware via the capturing of unusual packets.

The material in the book is fascinating in places. However, the work is not structured in a way that makes the security implications obvious (the writing is not very direct, and the narrative or topical thread tends to wind around subjects), and, in fact, the security implications aren't very powerful at all. Yes, in the end, the author has written mostly about passive and indirect attacks, but the

methods

covered are unusual, and probably not very useful. Most of the material concentrates on rather weak covert channels. In this regard

it can have some uses in a minor way: covert channel examples are not

abundant in the general security literature. The attacks suggested

are interesting thought experiments, but have limited uses either in

attack or defence. As "Trivial Pursuit" (meaning the game of oddball

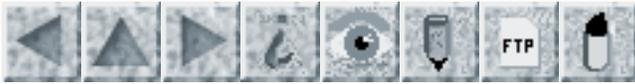
facts) for the tech crowd it's great, but the author never intended

the text to be a vulnerability warning.

copyright Robert M. Slade, 2005 BKSLNOWR.RVW 20050603
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 23: Issue 94

Tuesday 26 July 2005

Contents

- [2,000 patients hit by lab test mix-up in Calgary, Alberta](#)
[R.A. Tremonti](#)
- [Information system for Lisbon hospitals stopped for ten days](#)
[Fernando Pereira](#)
- [Why doesn't meter reading use sanity checking?](#)
[PGN](#)
- [Proposed daylight saving time changes](#)
[David Magda](#)
- [Virginia DMV fraud again](#)
[PGN](#)
- [Fraud on VoIP](#)
[uk.telecom.voip via Pete Mellor](#)
- [Physical-layer network vulnerabilities](#)
[Michael Tandy](#)
- [Multiple vulnerabilities in Diebold Optical Scan](#)
[Bruce O'Dell](#)
- [UK Government statistics show Home Office leads in stolen computers](#)
[Ian Cuddy](#)

- [Mixing data from multiple customers](#)
[art](#)
 - [European Parliament rejects Software Patent Directive](#)
[Pete Mellor](#)
 - ["Perspectives on Free and Open Source Software"](#)
[PGN](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✦ 2,000 patients hit by lab test mix-up in Calgary, Alberta

<"R.A. Tremonti" <robert.tremonti@shaw.ca>>

Mon, 11 Jul 2005 15:09:11 -0600

It seems a web database used by the Calgary Health Region to track and distribute results of lab tests has suffered a "glitch". According to the article that appeared today, "The Calgary Health Region announced Sunday that an Internet database - which physicians use to view lab work such as blood and urine tests - mixed up results between patients and posted records under the wrong names. Officials are now contacting the offices of nearly 400 doctors and other health providers who saw the incorrect records, to ensure patients are receiving proper treatment." Doctors are concerned that the mix-up means some patients are now receiving incorrect treatments which can complicate their conditions, or that patients are receiving treatments they don't need. Additionally, some patients may be fretting needlessly over their lab results because of the mix-up while others may be in for some unpleasant surprises when they receive the correct results!

<http://www.canada.com/calgary/calgaryherald/index.html>

[Also noted by Robert Israel at the University of British Columbia]

<http://www.theglobeandmail.com/servlet/story/RTGAM.20050711.wcalgary0/BNStory/National/>

<http://calgary.cbc.ca/regional/servlet/View?filename=ca-chr-tests20050711>

✦ Information system for Lisbon hospitals stopped for ten days

<Fernando Pereira <pereira@cis.upenn.edu>>

Sun, 17 Jul 2005 10:29:55 -0400

Lisbon newspaper "O Público" reports today that the main information system for the Lisbon Hospital Center, which supports three large Lisbon hospitals, has not worked since July 8. It appears that the master patient index has become inaccessible, and may be lost. If a patient shows up without a hospital-issued card, which includes a patient id number, the patient's records cannot be accessed. Out-patient consultations and admissions are being processed manually, causing "great confusion." Emergency room admissions are much slower than usual. The waiting list for surgery also appears lost, although that has not been confirmed. A doctor at one of the hospitals and board member for a doctors union said that "No one knows for certain what will happen or when the problem will be solved." The assistant to the director of the hospital group explains that "The system

failed totally eight days ago, and technicians tried to restore it immediately, but without success. At the beginning of last week, the US firm who supplied the system was brought in, and it is expected that the situation will be resolved by Monday." He also said that the failure was unexpected, that the hospital group did not have the ability to fix it on their own, and that the breakdown "has had no impact on the normal functioning of the hospitals, except for the slowdown in patient registration."

So, it takes much longer to admit patients, their medical records are inaccessible unless they have registered before and bring with them their registration card (something that anyone dealing with a medical emergency will for sure remember to do), and doctors report confusion, but there's really no impact, according to the hospital group administration. A mission-critical system has no backup or immediate access to repair expertise.

For readers not familiar with Portugal, Lisbon public hospitals are notorious for poor financing, inefficiency, bureaucracy, and long waiting lists. They cater mostly to those who cannot afford private care, especially many pensioners in an aging city. Another common problem with public institutions in Portugal are poor procurement controls, especially for technology and information services. Many purchases are made without much attention to cost of ownership, service guarantees, or access to parts and

service. Some administrators are too easily seduced by fancy presentations by local representatives of foreign suppliers who have no local expertise or staying power.

Fernando Pereira, Dept. of Computer and Information Science, U. of Pennsylvania

⚡ Why doesn't meter reading use sanity checking?

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

Thu, 14 Jul 2005 15:03:33 PDT

The utility department in Mascoutah (Illinois) sent Rose Mary Cook a bill for the use of 10 million gallons of water in a month, totalling \$29,787 for the water and \$43,581 for the ensuing sewer usage. The cause was not surprisingly the result of a broken meter. [Source: AP item, 14 July 2005]

<http://www.cnn.com/2005/US/07/14/hot.summer.ap/index.html>

In past years we have seen similarly large charges attributed to the installation of a new meter that was set slightly behind the old one.

⚡ Proposed daylight saving time changes

<David Magda <dmagda@ee.ryerson.ca>>

Wed, 20 Jul 2005 22:25:52 -0400

The US Congress is considering changing the way daylight saving time is

orchestrated, e.g.:

<http://www.cbc.ca/story/canada/national/2005/07/20/daylight-savings-folo050720.html>

Regardless of whether you actually think daylight saving is a good idea, there are definite risks when you decide to change the rules on how it

works. In this case, the proposal is to have the change take effect this

fall. I'm curious if Congress realizes that just about every single computer

system would have to be updated so that it would keep the correct time.

And this does not effect just people in the US. In the above link it

discusses the effect on us Canadians. At this point in time about 80% of

Canada's exports go to the US (and 25% of America's exports go to Canada):

the two countries are heavily linked economically. If the US changes its

system, it is all but a foregone conclusion that we Canadians would have to

change the way we do things as well.

If Congress really wants to go through with this change it would be prudent

to at least push off the rule change until next year to give people time to

update and test their systems.

Mentions of daylight savings in past RISKS include 13.48, 18.04, 19.43, 9.80,

17.84, 20.28, 6.47, etc.

More information on daylight saving time is available on Wikipedia (among

other places):

http://en.wikipedia.org/wiki/Daylight_saving_time

✶ Virginia DMV fraud again

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

Wed, 13 Jul 2005 18:26:59 PDT

Do you believe in drivers' licenses as proof of someone's identity? The manager of the Virginia Department of Motor Vehicles office at the Springfield Mall was charged with selling at least 40 illicit licenses for up to \$3,500 each. Many years ago we reported that the VA DMV rate for bogus licenses was \$25, when a ring of inside perpetrators was busted. Two years ago, two employees of the Tysons Corner Virginia DMV pleaded guilty to fraudulently selling licenses. Coincidentally the manager's wife was also charged, and she had previously worked in the Tysons Corner DMV! The latest case was uncovered not by the DMV's oversight program, but by the U.S. State Department's Bureau of Diplomatic Security. [Source: *The Washington Post*, 13 July, B05; PGN-ed]

<http://www.washingtonpost.com/wp-dyn/content/article/2005/07/12/AR2005071201421.html>

✶ Fraud on VoIP (fwd from newsgroup uk.telecom.voip)

<Pete Mellor <pm@csr.city.ac.uk>>

Mon, 11 Jul 2005 00:46:41 +0100 (BST)

The following item might be of interest. Note that fraud recently brought down a VoIP supplier in the US.

Newsgroup address: <http://www.usenet.org.uk/uk.telecom.voip.html>

By Carolyn Schuk, for VOXILLA.COM

It's one of the best kept secrets in the Voice over IP industry. The biggest problem facing VoIP providers isn't the specter of costly E911 requirements, overzealous regulators, or even competition from a myriad of sources. The biggest issue is fraud, perpetrated by scammers who take advantage of lax international communications standards and regulations, and make thousands of minutes of calls through carriers - many of them fly-by-night operators - in places such as Afghanistan and Lichtenstein, who charge exorbitant rates for call termination, leaving the originating service provider with sky high bills and no one to charge for them.

VoIP scams have already caused start-ups in the fledgling industry millions of dollars in losses and are blamed, in part, for the recent demise of one service provider. "It is the single largest problem facing providers," says Ravi Sakaria, VoicePulse CEO, "because the development cost associated with addressing the issue is significant enough that it could be prohibitive for the smaller players."

⚡ Physical-layer network vulnerabilities

<Michael Tandy <m.j.tandy@warwick.ac.uk>>

Mon, 11 Jul 2005 13:56:07 +0100

During the construction of an extension to my house, builders had to take down a wall bordering the garden. This wall ran parallel to an extension to the building next door, with a gap a about two inches wide in between.

After the wall was taken down, I found the house next door had a hole drilled in the now-revealed wall, with Cat5 network cable extending from it; the Cat5 originally ran through the gap between their wall and ours.

I did not splice into the cable, but to do so would have been easy.

The risk is fairly obvious: Networks that are physically secure can be made physically insecure by building work, particularly when said networks run close to other properties.

⚡ Multiple vulnerabilities in Diebold Optical Scan

<"Bruce O'Dell" <bodell@digitalagility.com>>

Wed, 13 Jul 2005 13:35:39 -0500

A Technical Report published by BlackBoxVoting.org (4 Jul 2005) details multiple critical security vulnerabilities in the Diebold Optical Scan

voting equipment that was used to tally approximately 25 million votes in the 2004 US election.

Overview: <http://www.bbvdocs.org/general/BBVreport-1sheet.pdf> and Full technical report: <http://www.blackboxvoting.org/BBVreport.pdf>

Harri Hursti, an independent security consultant - with the consent of election officials in Leon County, Florida - was able to take full control of the Diebold optical scan device and manipulate vote totals and audit reports at will.

The Diebold Precinct-Based Optical Scan 1.94w device accommodates a removable memory card. It had been believed that this card contained only the electronic "ballot box", the ballot design and the race definitions; astonishingly enough, the memory card also contains executable code essential to the operation of the optical scan system. The presence of executable code on the memory card is not mentioned in the official product documentation. This architecture permits multiple methods for unauthorized code to be downloaded to the memory cards, and is wide open to exploitation by malicious insiders.

The individual cards are programmed by the Diebold GEMS central tabulator device via a RS-232 serial port connection or via modem over the public phone network. There are no checksum mechanisms to detect or prevent tampering with the executable code, and worse yet, there are credible exploits which could compromise both the checksum and

executable. The report notes that this appears to be in violation of Chapter 5 of the 1990 Federal Election Commission Standards for election equipment, and therefore should never have been certified for use.

The executable code is written in a proprietary language, Accu-Basic.

Accu-Basic programs are first compiled into ASCII pseudocode, which is then executed by an interpreter residing in the optical scan device.

Hursti

located an inexpensive device capable of reading and updating the memory cards advertised on the Internet, and using a publicly-available version of the Accu-Basic compiler (found on the Internet, along with Diebold source code and other documents, by Bev Harris in 2003) was able to exploit these vulnerabilities - and publicly demonstrated the ability to modify vote totals and audit reports at will.

According to the report:

"Exploits available with this design include, but are not limited to:

"1) Paper trail falsification - Ability to modify the election results reports so that they do not match the actual vote data

"1.1) Production of false optical scan reports to facilitate checks and balances (matching the optical scan report to the central tabulator report), in order to conceal attacks like redistribution of the votes or Trojan horse scripts such as those designed by Dr. Herbert Thompson. (19)

"1.2) An ingenious exploit presents itself, for a single memory card to mimic votes from many precincts at once while transmitting votes to the central tabulator. The paper trail falsification methods in this report will hide evidence of out-of-place information from the optical scan report if that attack is used.

"2) Removal of information about pre-loaded votes

"2.1) Ability to hide pre-loaded votes

"2.2) Ability to hide a pre-arranged integer overflow

"3) Ability to program conditional behavior based on time/date, number of votes counted, and many other hidden triggers.

"According to public statements by elections officials(20), the paper trail produced by the precinct optical scan has been placed into the role of a vital safeguard mechanism. The paper report from the optical scan machine is the key record used to confirm the integrity of the central tabulator record. The exploits demonstrated in the false optical scan machine reports ("poll tapes") shown on page 16 do not change the votes, only the report of the votes. When combined with the Trojan horse attack demonstrated by Dr. Thompson, this attack vector maintains an illusion of integrity by producing false reports to match the contaminated central tabulator report.

"The [second] exploit demonstrated in the poll tape with a true report containing false votes, shown on page 18, changes the votes but not the

report. This example pre-stuffs the ballot box in such a way as to produce an integer overflow. In this exploit, a small number of votes is loaded for one candidate, offset by a large number of votes for the opposing candidate such that the sum of the numbers, because of the overflow, will be zero. The large number is designed to trigger an integer overflow such that after a certain number of votes is received it will flip the vote counter over to begin counting from zero for that candidate... combining the false report method (demonstrated on page 16) with the pre-arranged integer overflow (demonstrated on 18) seems to be an especially efficient exploit because it is a one-step process that takes out both the actual process and its safeguard at the same time, while surviving scrutiny of almost anything short of a full manual recount."

Reportedly, at least 500 jurisdictions used the vulnerable optical scan system in 2004; for example, the Diebold Precinct-Based Optical Scan 1.94w system counted approximately 2.5 million votes in 30 counties, or about one-third of all the votes in Florida, and nationwide, approximately 25 million votes (<http://www.freddevan.com/blog/archives/00006724.html>).

Although the exploits described in the report could be uncovered if a full hand recount was performed, in practice, detection is unlikely. Most jurisdictions limit the time frame for contesting an election. For numerous reasons, both candidates and election administrators are reluctant

to question the official tally, while hand recounts are expensive - with costs borne by the contesting party. Few elections tallied by optical scan equipment are ever fully recounted, and automatic recounts legally triggered by a narrow margin of victory will, of course, fail to detect large-scale manipulation that shifts results outside the recount threshold. Finally, there are classic problems with paper ballot chain of custody; the more time passes, and the further a paper artifact travels from its point of origin, the more vulnerable it is to tampering.

Therefore, the mere presence of a paper trail will not deter or detect electronic vote manipulation by malicious insiders unless the voter-verified paper ballot or optical scan ballot is actually randomly audited - preferably, in-precinct, on election night . Yet the cost and time required by a truly effective and random audit protocol undermines the case for electronically-assisted vote tallying. Therefore some analysts now recommend US implementation of the Canadian system - hand-counting of paper ballots in-precinct on Election Night, with accommodation for the visually-impaired - as the best countermeasure to systematic electronic election fraud.

Based on my experience in the financial services industry, discovery of multiple security vulnerabilities of this severity in equipment in use by any bank or brokerage house would trigger an immediate shutdown of all the affected systems, followed by a full internal and external audit, and, in

all likelihood, formal investigation by regulatory and law enforcement agencies. We should accept no less from the election services industry.

The affected Diebold optical scan equipment should be immediately withdrawn from use in any election until independent recertification is achieved, or a secure alternative is obtained. All other election equipment - manufactured by Diebold or by other vendors - should be examined, and if subject to the same vulnerability, should also be withdrawn. An investigation to determine how equipment with such serious vulnerabilities to insider manipulation could ever have been certified should also be launched, and certification and oversight procedures enhanced.

Good people died to gain and defend our right to vote. Election administration must not be exempt from industry best practices for security, audit and control.

Bruce O'Dell, Partner, Digital Agility Incorporated www.digitalagility.com
Member, ACM SIGSOFT, SIGMETRICS, SIGART bodell@digitalagility.com

UK Government statistics show Home Office leads in stolen computers

<"Ian Cuddy" <ic@egovmonitor.com>>
Tue, 12 Jul 2005 15:52:29 -0000

Whitehall Fails to Plug IT Theft (eGov monitor Newdesk)
An online version with embedded links is available at:
<http://www.egovmonitor.com/node/1843>

Central government departments have reported to have suffered at least 150 cases of computer theft in the last six months, according to official figures. The Home Office alone recorded 95 incidents of computer items being stolen between January and June 2005 - equivalent to a theft taking place in the Department every other day.

By comparison, the Ministry of Defence reported 23 computer thefts to date in 2005, down from a total of 153 in the previous year.

Ministers made the disclosures in response to a series of parliamentary questions tabled by Liberal Democrat MP Paul Burstow into incidents of computer hacking, fraud and theft in each department.

In a written answer, Doug Touhig, a junior minister at the MoD, said the Ministry had also experienced 30 attempted computer hacking incidents so far in 2005, having only reported 36 for the whole of 2004. However the Minister gave an assurance that "none of the reported incidents of hacking had any operational impact". Most of these incidents were due to internal security breaches, rather than external threats. Half of the cases were classed as "internal - misuse of resources".

Instances of reported computer thefts in other departments were in single figures so far this year, and most recorded no cases of IT systems being accessed illegally.

The Department for Transport said it had experienced 71 cases of computer

hacking in 2003-4, 31 in the following year and one incident since April.

The Treasury, the Department for International Development and the

Department for Education and Skills said their IT systems had been breached

on one occasion in 2004-5. Figures from the DfES show that in the two years

since 2003/4, it experienced 37 incidents of computer theft, all but one of

which were "perpetrated by insiders". The Department of Health said it did

not distinguish between losses and theft of IT equipment, but said there

were 44 such incidents in 2004-5, costing it almost 40,000 pounds. Figures

provided by Health Minister Jane Kennedy put the total sum lost by the

Department over the last four years at 233,000 pounds.

Ian Cuddy, Chief Editor, eGov monitor, Hurlingham Studios, Ranelagh Gardens,

London SW6 3PA UK 020 7384 1551 ian.cuddy@egovmonitor.com www.egovmonitor.com

⚡ Mixing data from multiple customers

<art-risks@dontsharemyemail.com>

Sun, 10 Jul 2005 15:35:56 -0400

I signed up for a mailing list from a potential vendor that my company was considering using a few months back (well, I submitted a request for info which got put on their mailing list).

A few weeks later I received a marketing e-mail from them. OK, that was expected. But I got the same e-mail on my home e-mail. That was

not
expected.

I have a domain, dontsharemyemail.com, that I use exclusively for signing up for lists. I use a unique address for each list I sign up for so I can track leaky e-mail lists.

Looking into the e-mail I received at home from the vendor I found that it was sent to a mailing list that I used for a charity I give to. I contacted both the vendor and the charity. The vendor confirmed the address was on their list, but they said they had no record of how they got it. They don't by lists (their marketing dept. complains about this) and they were very puzzled. The charity confirmed that they had no record of sharing the address (they claim they don't do that either).

After a little while it dawned on me what could have happened. Sure enough, I looked at the headers of both e-mails and found that both parties used Microsoft's bcentral.com mailing list service.

As far as I can figure, Microsoft's programmers figured that since the same name, address, phone, etc., info was attached to both e-mail addresses, they should be stored as a single entity. Thus when the vendor sent to "me" it was sent to both e-mail addresses. Even though both were completely separate mailing lists from completely separate customers.

The risks are in keeping your customer's private data private when you manage multiple customers.

✶ European Parliament rejects Software Patent Directive

<Pete Mellor <pm@csr.city.ac.uk>>

Mon, 11 Jul 2005 14:37:44 +0100 (BST)

On 6 July 2005, the European Parliament decisively rejected the directive of the European Commission, which would have brought software into the patent system.

For those like me who have followed the argument about software patents over the last many years, this comes as a relief. I was first alerted to the potential damage of software patents many years ago when I heard Richard Stallman talk. He gave another set of seminars in London around two years ago. I find his arguments against software patents totally convincing. He has summarised these neatly in an article in The Guardian on 23rd June:

<http://www.guardian.co.uk/online/story/0,,1511965,00.html>

A search on the Guardian site turns up several related articles and letters.

My colleague David Dodson has circulated the press release from the FFII ("Foundation for a Free Information Infrastructure"), a campaigning group. The web sites listed at the foot of the release are worth visiting by anyone who still needs to be convinced that software patents are a bad thing. In particular, see: <http://webshop.ffii.org/>

This does not mean that we can relax, of course, since further attempts to sneak in such legislation will probably be made. "The price of freedom is eternal vigilance."

> The Foundation for a Free Information Infrastructure (FFII) is a
> non-profit association registered in several European countries, which
> is dedicated to the spread of data processing literacy. The FFII
> supports the development of public information goods based on copyright,
> free competition, open standards. More than 3,000 companies and 90,000
> individuals have entrusted the FFII to act as their voice in public
> policy questions concerning software copyright and patents. The FFII
> maintains an office in Brussels and national sections in many countries.

It's essentially a cross-European grassroots group of volunteers, organised primarily by e-mail lists and websites/wiki systems, primarily focussed on the campaign against software patents and the software patent directive, and which in the process has slowly learned its way around some of the Brussels political jungle.

Increasingly, it has also acted as a focus for statements and support from concerned SMEs:

<http://www.economic-majority.com/testimony/index.en.php>

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V 0HB p.mellor@csr.city.ac.uk +44 (0)20 7040 8422

✦ "Perspectives on Free and Open Source Software"

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

Mon, 18 Jul 2005 15:42:45 PDT

edited by Joseph Feller, Brian Fitzgerald, Scott Hissam, and
Karim Lakhani,
24 chapters, with a foreword by Michael Cusumano and an epilogue
by Clay
Shirky, The MIT Press, 2005. 538pp+xxxi. ISBN 0-262-06246-1.

Part I: Motivation of F/OSS Development
Part II: Evaluation of F/OSS Development
Part III: F/OS Processes and Tools
Part IV: F/OSS Economic and Business Models
Part V: Law, Community, and Society

[Everything anybody ever wanted to know about F/OSS (which is
the
book's way of abbreviating "Free and Open Source Software")?
Probably not, but may be useful. 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 23: Issue 95

Monday 1 August 2005

Contents

- [Reuters: FDA warns Hitachi Medical about MRI systems](#)
[Craig S. Bell](#)
- [Too many features in medical device](#)
[Colin Percival](#)
- [Embedded Systems vs Us](#)
[Bob Paddock](#)
- [Elbtunnel computer crash](#)
[PGN](#)
- [New Microsoft anti-piracy program circumvented](#)
[Monty Solomon](#)
- [USC Database hacked](#)
[Randall via Dave Farber](#)
- [Spyware soaring](#)
[John Leyden via PGN](#)
- [Privacy Guru Locks Down VOIP](#)
[Kim Zetter via Monty Solomon](#)
- [TV channel inadvertently broadcasts link to porn site](#)
[David Hollman](#)

- [NSW State Transit Authority decommissions servers --- and data, too](#)
[Florian Liekweg](#)
 - [Hacking the Hotel TV -- and more](#)
[Florian Liekweg](#)
 - [Two reports of possible interest](#)
[Gene Spafford](#)
 - [Low Threshold for Fraud Detection](#)
[Mark Rockman](#)
 - ['Insane' Quebec Govt Online PAC ID system](#)
[Michael Hackett](#)
 - [Partisan e-mail censorship as spam filtering: afterdowningstreet.org](#)
[Pete Klammer](#)
 - [Risks of REAL ID](#)
[Robert Tanner via Monty Solomon](#)
 - [Re: Diebold Optical Scan security](#)
[Stanley F. Quayle](#)
 - [Re: Proposed daylight saving time changes](#)
[Stuart Prescott](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Reuters: FDA warns Hitachi Medical about MRI systems

<"Craig S. Bell" <craig_s_bell@yahoo.com>>
Fri, 29 Jul 2005 11:23:13 -0700 (PDT)

Hitachi appears to be experiencing injury problems with their medical imaging equipment. The FDA is on their case, mostly for their lack of reporting on recent incidents.

The RISK: As with the Therac-25, prompt and responsible reporting by the manufacturer is key to minimizing the risk of further injury.
Craig S. Bell, Portland, Oregon USA

The U.S. Food and Drug Administration warned Hitachi Medical Systems America Inc. that it failed to properly report burns, hearing losses, and other injuries to patients using its magnetic resonance imaging (MRI) systems. The FDA suggested that this "may be symptomatic of serious problems in your firm's manufacturing and quality assurance systems. You must promptly initiate permanent corrective and preventive action. The FDA described one unreported case in which a woman complained she was "shocked and burned on the top of her head while being scanned" by a Hitachi MRI system, and another in which an MRI device caught fire. [Source: A Reuters item, 26 Jul 2005; PGN-ed]

⚡ Too many features in medical device

<Colin Percival <cperciva@sfu.ca>>
Tue, 26 Jul 2005 02:37:15 +0000 (UTC)

This morning I received notice of an important product recall: Apparently the blood glucose meter I've been using for the past two years has too many features.

Some background: There are two different units used for measuring blood glucose levels -- mM and mg/dL. The metric world uses mM; the USA uses mg/dL. In order to provide a product which is useful to everybody, most blood glucose meters support both units, and allow the user to select which

units they want to use.

Unfortunately, it seems that some people have managed to put their meters into the wrong mode, and have subsequently failed to realize this. How this is possible, I am not sure -- if you are expecting an answer of "5" it should be immediately clear that the value "90" is in the wrong units -- but it seems that this is sufficiently concerning to require a complete recall of the "defective" products, in order that they can be replaced with a newer model which can only display results in mM.

This brings to mind two risks -- one which the manufacturer has responded to, and the other which they seem to be blithely ignoring:

RISK #1: If you add too many features to your software, you'll probably end up confusing some of your users.

RISK #2: If you add a feature and then subsequently remove it, there will inevitably be some unhappy customers who were using that feature.

In this case, while mM are the units which Canadians "should" be using, many of them use mg/dL because those are the units which are most common on informational sites online.

I think I'll keep my "defective" product.

Embedded Systems vs Us

<Bob Paddock <bob.paddock@gmail.com>>

Wed, 20 Jul 2005 18:46:29 -0400

I parked my Chrysler Voyager in my garage on Friday afternoon, no problems.

Later that day there was a lightning strike near by.

Got the van out Friday night. I pulled out of the garage and as soon as I hit the road the Check Engine Light came on and the speedometer dropped to zero, as I continued to gain speed, going up the hill. The automatic transmission was now stuck in 1st-gear. I turned around a few driveways up the street and went back to the house. Made appointment to take it in for servicing the next morning.

Dealer is about four miles down the street. Limped along in 1st-gear to the dealer the next morning until we reached the only major four way intersection in this four mile gauntlet.

Right in the middle of the intersection the engine died like I turned the key off. A good Samaritan pushed the van off the road. The dealer came and towed the van for the last mile of the trip.

The dealer said that a tachometer feedback sensor had gone bad "and the van didn't know what speed it was going so it shut down to be safe".

Now for the Us vs Embedded part of the story: Isn't it sufficient that **I** knew stopping in the middle of a busy four way intersections was a Really Bad Thing to do? **It** thought it knew better than I did.

I'm really glad I did not have to cross any railroad tracks when **it** decided to stop on the crossing because it thought it was safe,

rather than
listen to my commands.

<http://www.softwaresafety.net/> <http://www.unusualresearch.com/>
<http://www.bpaddock.com/>

⚡ Elbtunnel computer crash

<"Peter G. Neumann" <neumann@csl.sri.com>>
Sat, 30 Jul 2005 15:42:15 PDT

Germany: The crash of a PC controlling both tubes of Hamburg's Elbtunnel traffic system caused traffic to back up for 14 kilometers on the A7 during the morning of 28 July 2005. [Source: *Der Spiegel*, auf deutsch, thanks to Bruce Schneier; PGN-ed]
<http://www.spiegel.de/reise/aktuell/0,1518,367185,00.html>

⚡ New Microsoft anti-piracy program circumvented

<Monty Solomon <monty@roscom.com>>
Fri, 29 Jul 2005 21:06:43 -0400

Days after Microsoft Corp. launched a new anti-piracy program (Windows Genuine Advantage), hackers have found a way to get around it. It requires computer users to go through a process validating that they're running a legitimate copy of the Windows operating system before downloading any software updates except for security patches. But the check can

be bypassed
by entering a simple JavaScript command in the Web browser's
address bar and
hitting the "Enter" key. When that's done, the validation does
not run and
the user is taken directly to the download. ... [Source:
Associated Press
item, 29 Jul 2005; PGN-ed]

<http://finance.lycos.com/home/news/story.asp?story=50799944>

✶ USC Database hacked (via Dave Farber's IP list)

<Randall <rvh40@insightbb.com>>

Tue, 19 Jul, 2005 5:17:54 PM EDT

A University of Southern California database containing about
270,000
records of past applicants including their names and Social
Security numbers
was hacked in June 2005, and reported to USC by a journalist on
20 Jun. The
breach of the university's online application database exposed
"dozens" of
records to unauthorized individuals, according to Katharine
Harrington, USC
dean of admissions and financial aid. "There was not a
sufficiently precise
tracking capability" but records were able to be viewed only
randomly. "We
are quite confident that there was no massive downloading of
data."

USC has since shut down the Web site and has notified people
whose names and
Social Security numbers were in the database of the security
breach (as
required by the new California law.) [Source: Univ. of Southern

Calif. says

database hacked, Yahoo! News, 19 Jul 2005, 3:46pm; PGN-ed]

<http://tinyurl.com/bc8gd>

[IP Archives:]

<http://www.interesting-people.org/archives/interesting-people/>

Spyware soaring

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

Tue, 26 Jul 2005 16:54:18 PDT

Outbound spyware transmissions from infested machines accounted for up to eight per cent of total outbound web traffic in pilot tests of a new managed spyware screening service. UK web security firm ScanSafe said the volume of traffic observed during a 10-week pilot test of its Spyware Screening service showed that spyware applications are becoming stealthier in their ability to hide their outbound 'covert' channels among normal web traffic. That's bad news because data sent when spyware "calls-home" can include confidential and even privileged information.

Spyware now accounts for around 20 per cent of web-based threats, which includes other malware such as worms and Trojans, and is still on the increase, according to ScanSafe. The firm said malware such as CoolWebSearch, which hides on an infected client using newly developed root-kit architecture, often evades detection.

[Source: Spyware 'calling home' volumes soar, By John Leyden, *The

Register*, 25 July 2005]

http://www.theregister.co.uk/2005/07/25/spyware_screening/

✶ Privacy Guru Locks Down VOIP (Kim Zetter)

<Monty Solomon <monty@roscom.com>>

Sat, 30 Jul 2005 23:50:42 -0400

[Source: Kim Zetter, 26 Jul 2005]

First there was PGP e-mail. Then there was PGPfone for modems. Now Phil Zimmermann, creator of the wildly popular Pretty Good Privacy e-mail encryption program, is debuting his new project, which he hopes will do for internet phone calls what PGP did for e-mail. Zimmermann has developed a prototype program for encrypting voice over internet protocol, or VOIP, which he will announce at the BlackHat security conference in Las Vegas this week.

Like PGP and PGPfone, which he created as human rights tools for people around the world to communicate without fear of government eavesdropping, Zimmermann hopes his new program will restore some of the civil liberties that have been lost in recent years and help businesses shield themselves against corporate espionage.

VOIP, or internet telephony, allows people to speak to each other through their computers using a microphone or phone. But because VOIP uses broadband

networks to transmit calls, conversations are vulnerable to eavesdropping in the same way that e-mail and other internet traffic is open to snoops. Attackers can also hijack calls and reroute them to a different number.

Few people consider these risks, however, when they switch to VOIP. ...

<http://www.wired.com/news/technology/0,1282,68306,00.html>

TV channel inadvertently broadcasts link to porn site

<David Hollman <david.hollman@gmail.com>>

Sat, 23 Jul 2005 18:56:49 +0100

ITN apologises for porn link blunder [METRO (London), 19 Jul 2005]

Newscaster ITN apologised yesterday after a TV bulletin inadvertently featured a link to a hardcore porn website. ... A viewer who accessed the site was horrified to see X-rated images and complained. ... ITN said it kept the address in the story as it thought the site was no longer active. It later realised access to the site had been blocked by its firewall software.

The risk is that the web may not look the same from every vantage point.

NSW State Transit Authority decommissions servers --- and data, too

<Florian Liekweg <liekweg@ipd.info.uni-karlsruhe.de>>

Sun, 31 Jul 2005 17:15:56 +0200

In his blog at <http://www.geoffreyhuntley.com>, Geoffrey Huntley reports his findings about eighteen IBM RS/6000 E30 servers that his company purchased after they had been decommissioned by the State Transit Authority of New South Wales (STA NSW).

While the fact that the 'root' password was set to "root" could be seen as a courtesy of the SAT-NSW administrators to the new user, the systems contained not only the complete software used by the SAT-NSW but also employee data including PIN information used to "secure" the system against unauthorized access, and ticketing data including incident reports filed by customers. For good measure, the backup tapes were also included.

Full story at <http://www.geoffreyhuntley.com/news/data-security-101/>

Amazingly, it's the government agencies that are often criticized for creating a needless bureaucratic overhead by having a procedure for all and every situation. One should assume that installing the "wipe the disks before selling a computer" routine would be possible.

Florian Liekweg, IPD Universität Karlsruhe

⚡ Hacking the Hotel TV -- and more

<Florian Liekweg <liekweg@ipd.info.uni-karlsruhe.de>>

Sun, 31 Jul 2005 17:29:26 +0200

Adam Laurie, tech director of the London security and networking firm "The Bunker", apparently got bored on a recent trip and found the time to hack the Hotel's TV system which lets customers not just watch 'normal' TV programming, but also, for a fee, provides access to not-safe-for-work flicks and access to the Internet including e-mail.

The article at <http://www.wired.com/news/privacy/0,1848,68370,00.html>

reports that a laptop running linux, its IrDA port and an USB TV tuner can be used to trick the TV into doing more than it was supposed to do, including gaining access to the NSFW content without being charged for it, snooping on other people's TV watching habits, their Internet browsing habits and their e-mails. Also, the "coding" system used for infrared-based access control to the hotel minibars doesn't seem to be insurmountable either.

The bill so far: Lost profit for the hotel, lost privacy for the customers, the possibility for corporate espionage. Return value: Easy network access. Good deal, eh?

Florian Liekweg, IPD Universität Karlsruhe

⚡ Two reports of possible interest

<Gene Spafford <spaf@cerias.purdue.edu>>

Wed, 27 Jul 2005 12:01:10 -0500

The Computer Security Industry Alliance <<http://www.csialliance.org>>

recently issued three reports of possible interest:

CSIA Calls for Increased Adoption of Telework by the Federal Government:

Cites Need to Ensure Continuity of Federal Operations in a Disaster

https://www.csialliance.org/resources/pdfs/CSIA_Telework.pdf

CSIA Urges the Administration and Congress to Elevate Cyber Security

and Research & Development Efforts:

CSIA voices concern over the dissolution of a Presidential committee focused

on information security issues and calls for a national vision for cyber

security R&D.

https://www.csialliance.org/resources/pdfs/CSIA_RD.pdf

CSIA Calls for a National K-12 Cyber Awareness Program:

A Focused, Organized National Effort is Needed to Teach Children Cyber Security, Cyber Ethics and Cyber Safety.

https://www.csialliance.org/resources/pdfs/K12_White_Paper.pdf

⚡ Low Threshold for Fraud Detection

<"Mark Rockman" <mrockman@acm.org>>

Wed, 27 Jul 2005 17:35:59 -0400

The State of Maryland runs a "high risk" insurance pool for otherwise medically uninsurable patients. The pool exists to take care of those patients that regular health insurance companies deem unprofitable and who may ring up large losses. The pool, called MHIP, contracts with Magellan Health Services to evaluate health issues of insured. Magellan is a highly profitable gate keeper service who decide, in advance, using non-peer-reviewed methods, how many visits it will take to cure each patient. In one case, Magellan reported an incorrect, out-of-state address (a PO BOX) for an MHIP client. This was a simple data entry error and it was the only "evidence" that the client was trying to live outside the state and take unfair advantage of a program for Maryland residents. Result: MHIP announces it is terminating coverage effective in less than six weeks. "This letter is to inform you that your MHIP policy will terminate effective August 31, 2005, because of your lack of residency." The letter was sent to a Maryland address -- a house -- owned by the alleged evil-doer -- taxed as a primary residence. Guilty until proven innocent. MHIP provides an out: the client is given the opportunity to try to prove residency by (what call center denizens breezily describe as) filling out the Questionnaire. Oh, any by the way, send in ALL of the following documents:

- * Did you come to Maryland for the purpose of obtaining MHIP coverage?
- * Do you own or rent living quarters in Maryland?
- * Send in a copy of the rental agreement or the deed.
- * Send in copies of the rent checks.

- * Send in evidence from the rental agent.
- * Where did you live during the past 6 months?
- * Is substantially all of your stuff in Maryland?
- * Did you file income tax returns recently?
- * What state did you file to?
- * Send in copies of your income tax returns.
- * Send in copies of your W-2 forms.
- * Do you own vehicles?
- * If yes, send in purchase date, copies of titles, registration cards,
and operator permits.
- * If sold, send in a bill of sale.
- * What state issued your operator's permit?
- * Did you renew your operator's permit in the last 6 months?
- * Are you registered to vote?
- * If yes, where are you registered to vote?
- * Send in a copy of your voter registration card.
- * Have you registered to vote in some other state in the past 6 months?
- * Are you on welfare?
- * If yes, from what state are you receiving welfare?

Can you say "invasion of privacy?"

Perhaps this is a "slight" case of overreaching by the hired administrators of a government program (a company called Schaller-Anderson). Some effort to confirm damning data before taking drastic action might be appropriate. Assuming the client is committing fraud is insulting to the client and highlights the State's apparent attitude toward its citizens.

Risks: computer data "proves" a case of fraud. This goes in the pile of cases where the POE-LEESE arrest an individual based on erroneous or out-dated computer data. When the computer says it is so then it is so. Thus spaketh the machine.

'Insane' Quebec Govt Online PAC ID system

<Michael Hackett <dist23@juno.com>>

Thu, 28 Jul 2005 23:57:51 -0700

Only Franz Kafka could dream up such a crazy government on-line ID system ():

Web text relating to the Quebec Regie PAC ID scheme

http://www.rrq.gouv.qc.ca/an/services/15_09_06.htm

(Provincial services that use the PAC)

http://www.rrq.gouv.qc.ca/an/services/15_09_06_02.htm

[Personal access code (PAC)]

== The Website Text ==

Why do we authenticate your identity before giving you access to some of our services? Some of our services, for example, CompuPension and the on-line Application for a Retirement Pension require information contained in your file at the Régie. We must be sure of your identity so that you will be the only person who has access to your information. [...] While you are on-line, you can obtain a user code and choose a password. They will give use rapid access to the personalized services offered by Revenu Québec and by the Régie des rentes du Québec. [...]

We can also authenticate your identity without using Clic Revenu if you have a personal access code (PAC) issued by the Régie des rentes du Québec. Your code will be valid for 2 years and will be sent to you by regular mail.

[+++++ The authentication itself (editor)] :

http://www.rrq.gouv.qc.ca/an/services/15_09_06_02.htm

Personal access codes are issued by the Régie des rentes du Québec and give access only to the Régie's on-line services.

You can obtain a PAC if:

- * you are 18 years of age or over and
- * you are a contributor to the Québec Pension Plan or
- * you are a beneficiary of the Québec Pension Plan or
- * you are entitled to child assistance payments

Your PAC is confidential; you alone knows the code. It is sent to you by mail and is valid for 2 years following its effective date.

Why the PAC 'ID scheme' is poorly (+ badly) designed, especially for
NON-QUEBEC RESIDENTS:

- * I know I have ZERO income from Quebec entities.
(True for most nonresidents.)
- * I know I know I owe no taxes to Quebec entities.
(True for most nonresidents.)
- * Anyone aged 16-72 that has a Canadian SIN is a 'Contributor' to the
Quebec Pension scheme.
- * I know that I have not contributed to any PQ Govt entities
separate from
taxes, as above.
- * I have no other relations with Quebec entities that could
alter the above
conditions.

Knowing all inputs are ZERO -- should be sufficient enough to be given a
PAC.

Why use the PAC: for some people in some situations

The PAC ID scheme may be a slightly better system for some people -- recent immigrants or Xpats not living in Canada for example. There is no guarantee that one will be able to get the non-PAC ID submission forms to work properly! (I guess the 'Risk' is here!) The PAC rejection form is here:

http://hireme.geek.nz/Insane_PO_gov_doc.jpg

The current arrangement makes it impossible for long term (outside of Canada) Quebec Xpats to easily conduct business with the Quebec Government.

✶ Partisan e-mail censorship as spam filtering: afterdowningstreet.org

<"Pete Klammer" <pklammer@comcast.net>>

Wed, 27 Jul 2005 15:24:20 -0600

In the run-up to the 2004 election, I found activist messages about (against) Arnold Schwarzenegger were being screened by ACM's e-mail screening service controlled by Postini. I was only able to verify this, and retrieve my messages, because I had chosen the "quarantine" option, and checked the quarantine area soon enough, before the messages were permanently expunged.

Now we hear that messages regarding the Downing Street memos have been blocked from Comcast.net customers (one of the largest high-speed cable internet providers in the U.S.), based on content of the message -- a URL --

rather than subject line or sender address or domain.

The potential for (mis)information manipulation by large and powerful corporations is frightening, particularly as U.S. law exempts them from "common carriage" legal requirements. We would never (I hope!) stand for our telephone company to redirect our flight-reservation phone call to a different airline "partner" company; why must we tolerate such distortion on the Internet?

Pete Klammer, P.E. 3200 Routt Street / Wheat Ridge, Colorado
80033-5452
(303)233-9485 / PKlammer@ACM.org

⚡ Risks of REAL ID (Robert Tanner)

<Monty Solomon <monty@roscom.com>>

Wed, 20 Jul 2005 03:36:45 -0400

Fees for a new driver's license could triple. Lines at motor vehicles offices could stretch out the door. U.S. Governors warned yesterday that states and consumers would bear much of the burden for a terrorism-driven push to turn licenses into a national ID card. Ed Rendell, Democrat of Pennsylvania: "'Trying to make this work, there will be hell to pay'" and could cost Pennsylvania "\$100 million plus" to restructure motor vehicle offices to respond to the REAL ID Act. By 2008, states must begin to verify whether license applicants are legal residents of the United States.

[Source: Governors balk at new US license rules; Warn of higher costs, privacy concerns in push for standard IDs Robert Tanner, Associated Press, 19 Jul 2005; PGN-ed]

http://www.boston.com/news/nation/articles/2005/07/19/governors_balk_at_new_us_license_rules/

⚡ Re: Diebold Optical Scan security (O'Dell, [RISKS-23.94](#))

<"Stanley F. Quayle" <squayle@insight.rr.com>>

Wed, 27 Jul 2005 00:13:26 -0400

A \$1 lottery ticket is serially numbered, with UV-encoded information, on tamper-evident paper, and tracked with a heavily-audited central system. Reasonable, since that ticket could be worth hundreds of millions of dollars.

Your ballot has a level of protection equal to its projected value: Zero.

Until votes are worth something, they will continue to be worthless.

Stanley F. Quayle, P.E. N8SQ +1 614-868-1363 stan-at-stanq-dot-com
8572 North Spring Ct., Pickerington, OH 43147 USA <http://www.stanq.com>

⚡ Re: Proposed daylight saving time changes ([RISKS-23.94](#))

<Stuart Prescott <stuart@nanonanonano.net>>

Thu, 28 Jul 2005 14:08:04 +1000

For the Olympics in 2000, the state government (New South Wales) decided to start daylight saving almost 2 months early (in August) so that the Olympics visitors would benefit from the longer evenings. Some of the other states in Australia followed suit.

In the organisation I was then working for, the problem was that it took quite some time for a patch to come from Microsoft to update the Windows NT and 2000 operating systems that were being used.

The RISK was not that we had to revert to the good old days of manually changing the time on the computer with the widely used calendar applications like Microsoft Outlook. It turned out that MS Outlook stores all appointment times in UTC, converting between local time and UTC when the appointment is made and then back again when displaying the appointment. Installing the updated TZ info from MS changed this conversion but not the stored UTC data.

So what ended up happening was that every appointment that was scheduled in the period between between August and October that was entered into the diary before the TZ update was applied was wrong by one hour after the TZ patch was applied. Similarly, if you sent an appointment to someone who didn't have the TZ patch installed (but had manually changed their time for those two months), then the times would also be out for that appointment.

For those who were heavily reliant on their MS Outlook calendar, it made for an interesting couple of months...

[Various other comments were received on this topic. PGN]



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