



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Index to Volume 25

Forum on Risks to the Public in Computers and Related Systems

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

• [Volume 25 Issue 00 \(\)](#)

- [Subject: SUMMARY OF RISKS VOLUME 25 \(ongoing\)](#)
- [\(archived in ftp file risks-25.00\)](#)

• [Volume 25 Issue 01 \(Monday 7 January 2008\)](#)

- [Fire! Works! oops, too slow \(Mark Brader\)](#)
- [Boeing 787 networking issues \(Martyn Thomas\)](#)
- [Feds Release Pass Card details \(Brock N. Meeks via David Farber\)](#)
- [Has chip-and-pin failed to foil fraudsters? \(Pere Camps\)](#)
- [Sears exposes customers' information via its web site \(Rich Kulawiec via IP\)](#)
- [User Data Stolen From Pornographic Web Sites \(David Leshner\)](#)
- [Election Computers Stolen in Tennessee \(David Leshner\)](#)
- [Er, Airline Captains Do What, Again? \(Rick Moen\)](#)
- [Risks of embedded javascript \(Paul Wallich\)](#)
- [Mercedes console display with conflicting information \(Henry Baker\)](#)
- [Mac Quickbooks update deletes user desktop \(Bonnie Packert\)](#)
- [No more loose lithium batteries in checked luggage \(Peter Gregory\)](#)
- [Risks of believing what you see on the WayBack Machine \(Fred Cohen\)](#)
- [Re: Computer Failure Causes Closure of Seattle Downtown Transit Tunnel \(Stanislav Meduna\)](#)
- [Re: Satnav: Nope, you can't get there from here. \(Craig DeForest\)](#)
- [Re: Satnav \(Martyn Thomas\)](#)
- [Re: Drunk a better guide than sat nav \(Ross Younger\)](#)
- [Passing of Computing and Information Security Pioneer: Jim Anderson \(Gene Spafford\)](#)

• [Volume 25 Issue 02 \(Monday 14 January 2008\)](#)

- [Coffee Grounds Qantas \(Charles Wood\)](#)
- [Computer problem suspected in erratic Airbus flight \(Antonomasia\)](#)
- [Metal structure beneath runway affects aircraft instruments \(David Dixon\)](#)
- [Polish teenager uses city trams as train set \(Peter Houppermans\)](#)
- [Novel approach to reducing electoral fraud \(Peter Mellor\)](#)
- [Risks of believing a GPS system \(Paul Karger\)](#)
- [GPS in a tea shop anecdote \(Mark Brader\)](#)
- [More GPS mishaps \(Paul Saffo\)](#)
- [Nightmare on VoIP Street \(Ed Ravin\)](#)

- [A risk of static analysis tools -- and refereeing \(Peter Gutmann\)](#)
- [Bank gives money to fraudster posing as its chairman \(David Dixon\)](#)
- [REVIEW: "Managing Knowledge Security", Kevin C. Desouza \(Rob Slade\)](#)

• [Volume 25 Issue 03 \(Tuesday 29 January 2008\)](#)

- [Data entry error leads to incompatible transplant \(Mark Brader\)](#)
- [London Heathrow plane crash \(Colin Stamp\)](#)
- ["Butterfly Award": French Bank Says Trader Hacked Computers \(Henry Baker\)](#)
- [Henhouses, guarding of, by foxes: Kerviel Kerfuffle \(Steve Summit\)](#)
- [Problems with the German tax software "Magpie" \(Debora Weber-Wulff\)](#)
- [Florida computer problems halt early voting \(PGN\)](#)
- [The risks of upgrading software \(Clive D. W. Feather\)](#)
- [Charter Cable deletes 14,000 e-mail accounts. No backups. \(Danny Burstein\)](#)
- [IRS: Kansas City lost our tapes. Lots of personal info.... \(Danny Burstein\)](#)
- [Automated parking garage reopens \(Rich Mintz\)](#)
- [Blue Screened Asphalt Jungle... \(David Leshner\)](#)
- [Windows virus protection on NASA Linux machines \(David Leshner\)](#)
- [Authors, pseudonyms, and software \(Steven M. Bellovin\)](#)
- [Re: Metal structure beneath runway affects aircraft instruments \(Roderick A Rees\)](#)
- [Re: Boeing 787 networking issues \(Mark Siegel\)](#)
- [Re: Coffee Grounds Qantas \(Brian Hayes\)](#)
- [Re: More GPS mishaps \(Joel Maslak, Dag-Erling Smørgrav, Paul Saffo\)](#)
- [REVIEW: "Fuzzing", Michael Sutton/Adam Greene/Pedram Amini \(Rob Slade\)](#)

• [Volume 25 Issue 04 \(Saturday 2 February 2008\)](#)

- [Transplant patient has NEW kidney removed after NHS computer blunder \(Richard I. Cook\)](#)
- [Tachometer error caused 2005 runway overrun \(Mark Brader\)](#)
- [Mideast submarine cable disruptions \(David Leshner\)](#)
- [Empire State Building car e-interference mystery \(David Chessler\)](#)
- [Technology Review: Stopping cars with microwaves \(David Chessler\)](#)
- [Manufacturer Blames Bankruptcy on Failed ERP Implementation \(Ken Dunham\)](#)
- [2008 meltdown margin player blames s/w for failure to complete trades \(George Michaelson\)](#)
- [Fifth Amendment: Passphrase cannot be forced \(David Leshner\)](#)
- [British software pirate sells GBP 12K package at 1/1000 \(Peter Mellor\)](#)
- [DTV vs USPS \(Peter Zilahy Ingerman\)](#)
- [Voting Machine Usability Testing \(Ken Dunham\)](#)
- [Impersonating armored car personnel \(Craig Partridge\)](#)
- [Another public data loss in the UK \(Robert Klemme\)](#)
- [Automated calling system glitch locks down school \(Steve Eddins\)](#)
- [Re: Air Canada A319 upset \(Peter Ladkin\)](#)
- [Re: Coffee Grounds Qantas \(Preston de Guise\)](#)
- [Re: Metal structure beneath runway ... \(Neil Youngman\)](#)
- [Hoist by one's own petard: data security: UK Child Benefits \(Adrian Cherry\)](#)
- [REVIEW: "Software Testing Practice: Test Management", Spillner et al. \(Rob Slade\)](#)

• [Volume 25 Issue 05 \(Monday 18 February 2008\)](#)

- [L.A. School payroll system's spectacular failure \(Richard I. Cook\)](#)
- [FBI mistakenly receives supposedly protected e-mail \(Steven M. Bellovin\)](#)
- [Canadian Government Mails Out Confidential Data \(Ken Dunham\)](#)
- [JAL cabin crews sue over personal info \(PGN\)](#)
- [JAL near miss on attempted takeoff \(PGN\)](#)
- [Future of e-voting in doubt in Japan \(PGN\)](#)

- [Computer Error Strands Tanker off Massachusetts \(Lee Rudolph\)](#)
- [Bell Canada Data on 3.4 Million Customers Stolen \(Ken Dunham\)](#)
- [Royal Canadian Mounted Police Censured for Privacy Violations \(Ken Dunham\)](#)
- [Re: Lost Kansas City IRS tapes with personal info. \(Danny Burstein\)](#)
- [Critics chuck MS 'friendly worm' plan on the compost heap \(Chris Leeson\)](#)
- [Another BlackBerry Outage Caused by System Upgrade? \(Ken Dunham\)](#)
- [Vulnerability info suppressed by criminals paying to hide it \(Ken Dunham\)](#)
- [New GAO Report on IRS Information Security Pervasive Vulnerabilities \(Diego Latella\)](#)
- [The GPS miracle \(Rich Mintz\)](#)
- ['Woman Says Being Declared Dead Ruins Life' \(PGN\)](#)
- [A reminder: Eric Sevareid's Law \(Ken Knowlton\)](#)
- [Ah yes, just what you need!!! \(David Leshner\)](#)

• [Volume 25 Issue 06 \(Monday 25 February 2008\)](#)

- [Securing The Wrong Spaces: A Lesson \(Paul Ferguson via Gregory Hicks\)](#)
- [Software problem at London Heathrow Terminal 4 affects baggage \(Peter Mellor\)](#)
- [YouTube outage blamed on Pakistan \(Amos Shapir\)](#)
- [One way not to conduct Internet voting \(Peter Kaiser\)](#)
- [Being declared dead ruins life \(Andrew Koenig\)](#)
- [New RFID ticketless bus system in Brisbane goes live... with glitches \(George Michaelson\)](#)
- [US Treasury "TreasuryDirect" Web site security enhancements \(Jonathan Kamens\)](#)
- [EU money for 4 small businesses IT risk mgmt pilot \(Patrick O'Beirne\)](#)
- [Cold Boot Attacks on Disk Encryption \(Jacob Appelbaum, Declan McCullagh\)](#)
- [Illegal drag race kills eight \(John Curran\)](#)
- [Free-to-download password cracker \(Peter Mellor\)](#)
- [Re: the GPS miracle \(Steven M. Bellovin\)](#)

• [Volume 25 Issue 07 \(Saturday 1 March 2008\)](#)

- [Risks of Leap Years and Dumb Digital Watches \(Mark Brader\)](#)
- [Risks of Leap Years and Dumb Airline Software \(PGN\)](#)
- [\\$1.2 billion up in smoke \(Paul Saffo\)](#)
- [Southeast Florida Massive Power Outage \(Steven J. Greenwald\)](#)
- [FL power failure triggered by human error \(Lauren Weinstein\)](#)
- [Competent? We can't even archive our own e-mail reliably! \(Jim Horning\)](#)
- [DreamHost Accidently Bills Customers \\$7,500,000 \(Dan Jacobson\)](#)
- [IT Project Failure Blog \(Ken Dunham\)](#)
- [Is the "law of unintended consequences" biting W3C DTD reference? \(George Michaelson\)](#)
- [Pakistan, YouTube, Google, and No Simple Answers \(Lauren Weinstein\)](#)
- [Re: YouTube outage blamed on Pakistan \(R A Lichtensteiger, Richard Grady, Jay R. Ashworth\)](#)
- [Cold Boot Attacks: Vulnerable While Sleeping \(Ed Felten via Monty Solomon\)](#)
- [Citibank needs a clue \(Rich B. Astaird\)](#)
- [Re: Hoist by one's own petard: data security: UK Child Benefits \(Merlyn Kline\)](#)
- [REVIEW: "Better Ethics Now", Christopher Bauer \(Rob Slade\)](#)

• [Volume 25 Issue 08 \(Friday 14 March 2008\)](#)

- [Wind Power Risks \(Charles Wood\)](#)
- [FBI Found to Misuse Security Letters \(Lynn via Dave Farber's IP\)](#)
- [RFID hack could crack open 2 billion smart cards \(Sharon Gaudin\)](#)
- [Nasty scanner attack: AccuBasic malware \(PGN\)](#)
- [Hacking a pacemaker \(Gadi Evron\)](#)
- [More on pacemaker risks \(PGN\)](#)
- [Stopping cars with microwaves \(Matthew D. Healy\)](#)

- [It's too easy to access the "off" switch \(Robert P Schaefer\)](#)
- [UK ISPs to sell users' private browsing information \(Mike Scott\)](#)
- [TSA can't believe MacBook Air is a real laptop; owner misses flight \(Paul Saffo\)](#)
- [Deja Vu all over again \(Andrew Koenig\)](#)
- [CAPTCHA attacks \(Monty Solomon\)](#)
- [Safari "beachball" black on black \(Richard A. O'Keefe\)](#)
- [Risks of Leap Years and Dumb Digital Watches \(Clive D. W. Feather, Amos Shapir\)](#)
- [USENIX Announces Open Access to Conference Proceedings \(Lionel Garth Jones\)](#)

• [Volume 25 Issue 09 \(Thursday 27 March 2008\)](#)

- [Billion-dollar IT failure at Census Bureau \(eekid via David Farber\)](#)
- [A Heart Device Is Found Vulnerable to Hacker Attacks \(Barnaby Feder via Monty Solomon\)](#)
- [FL power outage NERC updates \(Catherine M Horiuchi\)](#)
- [Vandals halt some hybrid buses using external 'off' switch \(Rick Damiani\)](#)
- [Flight Service Software Crashes; Pilot Briefings Delayed \(Gabe Goldberg\)](#)
- [Substantial supermarket breach affects millions \(Robert Heuman\)](#)
- [Man arrested by mistake over phone system bug \(Rick Damiani\)](#)
- [Hoax on Craigslist causes duped victims to steal property \(Mark Brader\)](#)
- [Payment by fingerprint disappears \(Jon Van and Becky Yerak via Paul Saffo\)](#)
- [Cute e-mail leak \(Steve Summit\)](#)
- [Search engine bait? \(Steve Schafer\)](#)

• [Volume 25 Issue 10 \(Tuesday 1 April 2008\)](#)

- [A modest proposal for the improvement of Daylight Saving \(Tony Finch\)](#)
- [A Current Affair: Lauren Weinstein, Inside Risks, CACM April 2008 \(PGN\)](#)
- [Chaos Computer Club publishes Minister's fingerprint - and more \(Peter Houppermans\)](#)
- [DST transition time mismatches \(Tony Finch\)](#)
- [Mini-Y2K fears over Aussie daylight saving change \(Max Power\)](#)
- [NYPD erases crime statistics for February 29 \(Ed Ravin\)](#)
- [More flights canceled as Heathrow remains in chaos \(Alan Cowell via David Farber's IP\)](#)
- [Heathrow: The risks of hubris \(Diomidis Spinellis\)](#)
- [GPS Errors are riskier than you may imagine: consider Liability-Critical Applications \(Bern Grush\)](#)
- [Re: Securing The Wrong Spaces: A Lesson \(Rick Damiani\)](#)
- [Re: Arrest over phone system bug: Trailing zeroes \(Graham Reed\)](#)
- [Re: Thieves become victims? \(stanley\)](#)

• [Volume 25 Issue 11 \(Wednesday 9 April 2008\)](#)

- [Crossed wires cited in recent UAL skidding incidents \(Monty Solomon\)](#)
- [Unanticipated GPS risk: foreign translations \(Paul Schreiber\)](#)
- [Census to scrap handheld computers for 2010 count \(Bob Schaefer\)](#)
- [Boston city complaint line lags \(Donovan Slack via Monty Solomon\)](#)
- [Indiana school district wipes out high school grades \(Danny Burstein\)](#)
- [Re: Search engine bait? \(Martin Ward\)](#)
- [Another genuine mail that looks like a phish \(Andy Piper\)](#)
- [Nissan GT-R sports car recognizes racetrack coordinates and aftermarket parts \(Clark Family\)](#)
- [REVIEW: "Security Data Visualization", Greg Conti \(Rob Slade\)](#)

• [Volume 25 Issue 12 \(Tuesday 22 April 2008\)](#)

- [Industrial Control Systems Killed Once, Will Kill Again \(Ryan Singel\)](#)
- [GPS leads a bus astray \(David Caley\)](#)
- [Neighbor's data shows up in my browser \(borborugmus\)](#)
- [Oklahoma Dept of Corrections Website URLs contain raw SQL \(Jim Garrison\)](#)

- [Real-time spying on credit card holders \(Nick Brown\)](#)
- [Larger Prey Are Targets of Phishing \(John Markoff via Monty Solomon\)](#)
- [Aer Lingus economy 5-euro flights to the US after test data leaked to web \(Patrick O'Beirne\)](#)
- [Gone in 60 seconds: Spambot cracks Live Hotmail CAPTCHA \(Emil Protalinski via Monty Solomon\)](#)
- [Bouncing Merrily Along \(Peter B. Ladkin\)](#)
- [The 10,000 web sites infection mystery solved \(Bojan Zdrnja via Monty Solomon\)](#)
- [Re: Census to scrap handheld computers for 2010 count \(Derek P. Schatz\)](#)
- [Re: Search engine bait? \(Randall Roberts\)](#)
- [Re: Another genuine mail that looks like a phish \(Gregory Hicks\)](#)
- [Re: Nissan GT-R sports car and GPS \(Peter Houppermans, JTaylor\)](#)
- [2008 IEEE Symposium on Security and Privacy \(Yong Guan\)](#)
- [REVIEW: "Computer Security: Principles and Practice" \(Rob Slade\)](#)

• [Volume 25 Issue 13 \(Sunday 27 Apr 2008\)](#)

- [Hack into Obama campaign site exploited a coding flaw \(Jordan Robertson via Joseph Lorenzo Hall\)](#)
- [Hacking a rival smart card? \(Robert P. Schaefer\)](#)
- [Face scans for air passengers to begin in UK this summer \(Brian Randell\)](#)
- [30th Spamiversary \(Brad Templeton via Mike Hogsett\)](#)
- [Re: Bouncing Merrily Along \(Paul Karger\)](#)
- [Re: Real-time spying on credit card holders \(Ron Garret\)](#)
- [Re: Neighbor's data shows up in my browser \(Paul D. Smith, Erik Mooney\)](#)
- [Re: GPS leads a bus astray \(Roger Scrafford\)](#)
- [Re: Nissan GT-R sports car and GPS \(Chris Kantarjiev, Dag-Erling Smørgrav, Dag-Erling Smørgrav, Peter Houppermans, Dag-Erling Smørgrav\)](#)

• [Volume 25 Issue 14 \(Friday 2 May 2008\)](#)

- [U.S. Customs computer system fails nationwide \(PGN\)](#)
- [Protecting Yourself From Suspicionless Searches While Traveling \(Jennifer Granick via Monty Solomon\)](#)
- [Air marshals' names tagged on 'no-fly' list \(Audrey Hudson via Monty Solomon\)](#)
- [Italy posts salary details on web \(Amos Shapir\)](#)
- [Tot dies after Internet 911 call fails to reach dispatchers \(Tony Toews\)](#)
- [Canadian Human Rights Commission investigator hijacks woman's Internet connection \(Kelly Bert Manning\)](#)
- [Microsoft anti-encryption toolkit \(David Leshner\)](#)
- ["Default Password" exploits still work \(William Nico\)](#)
- [Protecting credit card holders \(Kearton Rees\)](#)
- [Police officer uses real witness statement as template document \(Identity withheld by request\)](#)
- [False alarm guaranteed after 7 years \(Daniel P.B. Smith\)](#)
- [Facial recognition in airports... please say it's April 1st. \(Fred Cohen\)](#)
- [Re: Face scans for UK air passengers \(Peter Houppermans\)](#)
- [Re: 30th Spamiversary \(Amos Shapir\)](#)
- [Re: Real-time spying on credit card holders \(Nick Brown\)](#)
- [Blown to Bits, Abelson/Ledeer/Lewis \(PGN\)](#)

• [Volume 25 Issue 15 \(Friday 16 May 2008\)](#)

- [No-flies on you? \(PGN\)](#)
- [Gone in 60 seconds: Spambot cracks Live Hotmail CAPTCHA \(Emil Protalinski via Monty Solomon\)](#)
- [Hacker leaks 6 million Chileans' records \(Amos Shapir\)](#)
- [Dilbert site wants to install a widget \(William Ehrlich\)](#)
- [Used hardware containing sensitive data \(Tony Harminc\)](#)
- [88,000 hospital patient records stolen in NYC \(Danny Burstein\)](#)
- [UK CCTV used to create a music video \(Forest Mars\)](#)
- [QWERTYUIOOPS \(Charles C. Mann\)](#)

- [Post Office changes 100 SF addresses \(Rob McCool\)](#)
- [PO-boy \(Peter Zilahy Ingerman\)](#)
- [Debian OpenSSL Predictable PRNG Toys \(H D Moore via Monty Solomon\)](#)
- [Debian OpenSSL Vulnerability \(Monty Solomon\)](#)
- [How not to use SSL \(Nickee Sanders\)](#)
- [A risk for those that own Digital photo frames \(Identity withheld\)](#)
- ['Peel and Stick' Tasers Electrify Riot Control \(Paul Saffo\)](#)
- [Risks of Be-clowning Yourself at Computerized Speeds, Internationally \(R.G. Newbury\)](#)
- [REVIEW: "Geekonomics: The Real Cost of Insecure Software", David Rice \(Rob Slade\)](#)

• [Volume 25 Issue 16 \(Thursday 22 May 2008\)](#)

- [Betting glitch spurs calls for reform \(Will Oremus via PGN\)](#)
- [Animal tricks, take n+1 \(Jeremy Epstein\)](#)
- [Ants and Computers \(Gene Wirchenko\)](#)
- [F.B.I. Says the Military Had Bogus Computer Gear \(John Markoff via Monty Solomon\)](#)
- [Another undeleted/deleted Document - "Krolls Associates" \(Danny Burstein\)](#)
- [Don't phlash that dwarf - hand me the pliers! \(John Leyden via Randall\)](#)
- [Geolocation software risks \(Mickey Coggins\)](#)
- [Shopping centers tracking cell phones \(PGN\)](#)
- [China's All-Seeing Eye \(EEkid via Dave Farber\)](#)
- [Re: Real-time spying on credit card holders \(Curt Sampson\)](#)
- [Microsoft security advice for sale \(Peter Houppermans\)](#)
- [Old-Style Pumps Balk At \\$4-a-Gallon Gas, Too \(Nick Miroff via Monty Solomon\)](#)
- [Clueless in France \(Pete Kaiser\)](#)
- [PayPal XSS Vulnerability Undermines EV SSL Security \(Paul Mutton via Monty Solomon\)](#)
- [More GPS Mishaps \(Gene Wirchenko\)](#)
- [Re: UK CCTV used to create a music video \(Chris Drewe\)](#)
- [Re: Dilbert wants a widget \(Bill Bumgarner\)](#)
- [Re: Debian OpenSSL Predictable PRNG Toys \(Jim Horning\)](#)
- [Re: Securing The Wrong Spaces: A Lesson \(David E. Price\)](#)

• [Volume 25 Issue 17 \(Friday 30 May 2008\)](#)

- [Wrong patient gets appendix removed, software to blame \(Rex Sanders\)](#)
- [E-Voting Banned by Dutch Government \(Udo de Haes\)](#)
- [Don't phlash that dwarf -- hand me the pliers! \(John Leyden\)](#)
- [Firmware-based phone vulnerabilities \(David Magda\)](#)
- [A Low-cost Attack on a Microsoft CAPTCHA \(Jeff Yan and Ahmad Salah El Ahmad via Monty Solomon\)](#)
- [SYN attack from RIAA contractor \(David Leshner\)](#)
- [Random and haphazard are not synonyms \(Andrew Koenig\)](#)
- [An iTunes file database problem Apple will never fix \(Max Power\)](#)
- [Microsoft's Masters: Whose Rules Does Your Media Center Play By? \(Greg Sandoval\)](#)
- [Fundraising that is too Excel-lent to report \(Mark Brader\)](#)
- [On-line registration for College Reunion 2008 \(F John Reinke\)](#)
- [Why not set the pump to half price and post a sign? \(Daniel P. B. Smith\)](#)
- [Re: Securing The Wrong Spaces: A Lesson \(John Sullivan, Bill Hopkins\)](#)
- [An account of the Estonian Internet War \(Gadi Evron\)](#)

• [Volume 25 Issue 18 \(Tuesday 3 June 2008\)](#)

- [Fire at The Planet takes down thousands of websites \(Gene Wirchenko\)](#)
- [UK power rationing causes fires and false fire alarms \(Alistair McDonald\)](#)
- [Beware of Error Messages At Bank Sites \(Brian Krebs via George Sherwood\)](#)
- [Still even more lost data \(Gene Wirchenko\)](#)

- [Mass exploitation with Adobe Flash \(Monty Solomon\)](#)
- [Risks in Instant Runoff Voting \(PGN\)](#)
- [Arkansas Election Officials Baffled by Machines that Flipped Race \(PGN\)](#)
- [Spelling checker runs amok in Pennsylvania high-school yearbook \(Al Stangenberger\)](#)
- [Full Disclosure and why Vendors Hate it \(Jonathan A. Zdziarski via Monty Solomon\)](#)
- [Re: An iTunes file database problem Apple will never fix \(Alistair McDonald\)](#)
- [Re: Wrong patient gets appendix removed, software to blame \(PGN\)](#)
- [REVIEW: "Secure Programming with Static Analysis", Chess/West \(Rob Slade\)](#)

• [Volume 25 Issue 19 \(Sunday 8 June 2008\)](#)

- [Control-Alt-SCRAM; update reboots nuke plant \(Brian Krebs via David Leshner\)](#)
- [Sensor error caused \\$1.4 bill B2 crash! \(David A. Fulghum via Paul Saffo\)](#)
- [UK bank takes 9 months to combine computer systems \(Peter Mellor\)](#)
- [Online registration for US visa waiver scheme from August 2008 \(Donald Mackie\)](#)
- [The ID Divide: Peter Swire and Cassandra O Butts \(Monty Solomon\)](#)
- [ISP Secretly Added Spy Code To Web Sessions: Ryan Singel \(Monty Solomon\)](#)
- [Advice from HM Revenue & Customs on NI number fraud \(Peter Mellor\)](#)
- [Stanford employees' data on stolen laptop \(PGN\)](#)
- [Sometimes the computer is right... \(David Hollman\)](#)
- ["She'll never fail to stop at a railroad crossing ever again" \(Jeff Rosen via Mark Brader\)](#)
- [Experts Revive Debate Over Cellphones and Cancer \(Tara Parker-Pope via Monty Solomon\)](#)
- [Re: Risks in Instant Runoff Voting \(Richard Gadsden\)](#)
- [Re: Fire at The Planet takes down thousands of websites \(Paul Czyzewski\)](#)
- [Re: Whose Rules Does Your Media Center Play By? \(Steve Wildstrom\)](#)
- [Re: Beware of Error Messages At Bank Sites \(Paul Czyzewski\)](#)
- [Re: An iTunes ... problem Apple will never fix \(Henry Baker, Max Power\)](#)

• [Volume 25 Issue 20 \(Sunday 15 June 2008\)](#)

- [Security hole exposes utilities to Internet attack \(PGN\)](#)
- [Representative Frank Wolf's computer owned by China \(PGN\)](#)
- [Hidden Code Costs Poker Players Thousands \(Chuck Weinstock\)](#)
- [Wikipedia for medical students? \(Steven M. Bellovin\)](#)
- [Wartime global temperature anomaly kicks the bucket \(Mark Brader\)](#)
- [Colleges With Federal Contracts Will Have to Use New E-Verify \(PGN\)](#)
- [Google "safebrowsing" diagnostic page \(Rob Slade\)](#)
- [ID cards by the back door \(Peter Mellor\)](#)
- [Spuds and system security \(Rob Slade\)](#)
- [Clothing firm "Cotton Traders" customer database breached \(Peter Mellor\)](#)
- [Update on ISP Actions Regarding C-Porn and Usenet \(Lauren Weinstein\)](#)
- [Re: Risks in Instant Runoff Voting \(Stewart Fist, Andrew Koenig\)](#)
- [Re: Stanford employees' data on stolen laptop \(Hal Murray\)](#)
- [Re: Advice from HM Revenue and Customs \(Edward Rice\)](#)
- [Re: She'll never fail to stop at a railroad crossing \(Leonard Finegold\)](#)
- [Re: An iTunes ... problem Apple will never fix \(Andrew M. Langmead\)](#)
- [Tracking the Trackers: Piatek et al. \(Monty Solomon\)](#)

• [Volume 25 Issue 21 \(Sunday 29 June 2008\)](#)

- [Federal Agency Grounds Light Jet Used as Air Taxi \(Matthew Wald\)](#)
- [Spyware bill cloaks a mini-UCITA \(Ed Foster via Monty Solomon\)](#)
- [Wireless systems called disruptive \(Robert P Schaefer\)](#)
- [More on election system integrity \(Gene Wirchenko\)](#)
- [Re: Risks in Instant Runoff Voting \(Scot Drysdale\)](#)

- [Chrysler announces the rolling WiFi hotspot automobile \(Drew Lentz\)](#)
- [X-rated SMS case gives employees some privacy guarantees \(John Timmer via Monty Solomon\)](#)
- [Attorney-client calls from jail recorded \(Joel Garry\)](#)
- [HTML comments reveal corporate weakness \(jidanni\)](#)
- [Photos and laptop crypto \(Rob Slade\)](#)
- [Michael Fiola fired \(Gene Wirchenko\)](#)
- [REVIEW: "Challenges to Digital Forensic Evidence", Fred Cohen \(Rob Slade\)](#)

• [Volume 25 Issue 22 \(Tuesday 8 July 2008\)](#)

- [InciWeb map coordinate errors for California fire \(Henry Baker\)](#)
- [Oyster and Mifare cracked: NXP sues to silence Oyster researchers \(PGN\)](#)
- [Free Berlin subway rides \(Debora Weber-Wulff\)](#)
- [Citibank ATM breach reveals PIN security problems \(Jordan Robertson\)](#)
- [Web-based SSH key generation with escrow \(Tina Bird\)](#)
- [ComCast in Concrete? \(Robert P Schaefer\)](#)
- [State Dept: Celebrity passport files viewed repeatedly - CNN.com \(PGN\)](#)
- [California's Super-Stupid Anti-Science Cell Phone Law Takes Effect \(Lauren Weinstein\)](#)
- [Re: HTML comments reveal corporate weakness \(Ivor Hewitt\)](#)
- [Re: Approval voting and sincerity \(Andrew Koenig, Dag-Erling Smørgrav\)](#)
- [REVIEW: "The dotCrime Manifesto", Phillip Hallam-Baker \(Rob Slade\)](#)

• [Volume 25 Issue 23 \(Friday 18 July 2008\)](#)

- [E-mail response to wrong address, intended recipient arrested \(Danny Burstein\)](#)
- [San Francisco admin hijacks city net \(David Leshner\)](#)
- [Risks of wrong preprogrammed emergency message system being sent \(C.Y./J.E. Cripps\)](#)
- [P2P Data Breach affects SCOTUS \(Jay R. Ashworth\)](#)
- ["Plug and Play" Hospitals \(Terrence Enger\)](#)
- [Gmail Reveals the Names of All Users \(Gene Wirchenko\)](#)
- [Google Desktop, Word may expose encrypted data \(Gene Wirchenko\)](#)
- [UPS "Virus Warning" virtually indistinguishable from phishing attack \(Jonathan Kamens\)](#)
- [DR/BCM lessons from the Vancouver fire \(Daniel Wesemann in SANS via Brent J. Nordquist\)](#)
- [Re: Map coordinate errors for California fire \(Henry Baker, Al Stangenberger\)](#)
- [California's Super-Stupid Anti-Science Cell Phone Law Takes Effect \(Kurt Thams\)](#)
- [Handheld mobile safety \(Paul D.Smith\)](#)
- [The toll for terrorism is too high \(David Leshner\)](#)
- [Firefox 3's Step Backwards For Self-Signed Certificates \(Lauren Weinstein\)](#)
- [A not-so-obvious hyperinflation risk \(B. Elijah Griffin\)](#)
- [Re: Approval voting and sincerity \(Anthony W. Youngman\)](#)
- [Re: ComCast in Concrete? \(\(Greg Fife, Paul Wallich\)](#)
- [US FTC seeks comments on privacy in contactless payments \(Kevin Fu\)](#)

• [Volume 25 Issue 24 \(Wednesday 23 July 2008\)](#)

- [Washington Metro farecard fraud \(David Leshner\)](#)
- [The \\$100,000 Keying Error \(Patrick O'Beirne\)](#)
- [What happened to handcuffing the briefcase to James Bond's wrist? \(Randall Webmail\)](#)
- [Taking a grab at what's the real system error \(Jared\)](#)
- [What's in a name? \(Peter Houppermans\)](#)
- [Yet more GPS risks: Angry Mob Stones Lost Tourist \(Steven J Klein\)](#)
- [Shocking idea for air passenger security \(Robin Stevens\)](#)
- [Re: Oyster card hack to be published \(Amos Shapir\)](#)
- [Re: San Francisco admin hijacks city net: Paul Venezia \(David Leshner\)](#)
- [Re: ComCast in Concrete? MAC addresses \(R A Lichtensteiger\)](#)

- [Re: P2P Data Breach affects SCOTUS \(Pete Klammer, Jay R. Ashworth\)](#)
- [Re: Approval voting and sincerity \(Geoffrey Brent, Richard Gadsden\)](#)
- [NC State Voter site exposes voter addresses \(John O Long\)](#)

• [Volume 25 Issue 25 \(Sunday 3 August 2008\)](#)

- ["Software bug" downs AA baggage handling at JFK \(PGN\)](#)
- [Intermittent network card causes air traffic control problems \(Steven M. Bellovin\)](#)
- [Crypto box failure causes MTA credit card processing failure \(Steven M. Bellovin\)](#)
- [200,000 medical records sent to wrong patients, some with SSNs \(George Mannes\)](#)
- [DNA Database Searches \(jared\)](#)
- [Another GPS error story \(Gene Spafford\)](#)
- [Electronic voting: Indications of Sanity? \(Geoff Newbury\)](#)
- [Risks of Inflation: new Zimbabwe bank notes \(Jim Reisert\)](#)
- [Bruce Schneier: Inside the Twisted Mind of the Security Professional \(jidanni\)](#)
- [Details of DNS Flaw Leaked \(Kim Zetter via Monty Solomon\)](#)
- [Apple Fails to Patch Critical Exploited DNS Flaw \(Rich Mogull via Monty Solomon\)](#)
- [Fascinating phishing attack: valid links, dangerous toll-free number \(Jonathan Kamens\)](#)
- [Re: San Francisco FiberWAN and Terry Childs \(Jeff Williams\)](#)
- [Re: ComCast in Concrete? MAC addresses \(Tanner Andrews\)](#)
- [REVIEW: "Internet Denial of Service", Jelena Mirkovic et al. \(Rob Slade\)](#)
- [REVIEW: "AVIEN Malware Defense Guide for the Enterprise", David Harley et al. \(Rob Slade\)](#)

• [Volume 25 Issue 26 \(Wednesday 6 August 2008\)](#)

- ['Fakeproof' microchipped British e-passport is cloned in minutes \(Martyn Thomas\)](#)
- [On Metro Fraud and NXP \(David Leshner\)](#)
- [11 charged in largest ID theft in U.S. history \(Paul Saffo\)](#)
- [Theft perils 150,000 on Busch laptop \(PGN\)](#)
- [Verified Identity Pass: CLEAR Suspended Following Laptop Theft \(PGN\)](#)
- [Unsuspected travelers' laptops may be detained at border \(Ellen Nakashima via Monty Solomon\)](#)
- [Neglecting to logout from Skype means sharing your Instant Messages \(Michael Weiner\)](#)
- [Another small interface risk \(Peter Zilahy Ingerman\)](#)
- [E-Z Pass Maryland training customers to visit random sites? \(Mike Porter\)](#)
- [Prescription Data Used To Assess Consumers \(Ellen Nakashima via Monty Solomon\)](#)
- [Re: What's in a name? \(Dag-Erling Smørgrav\)](#)
- [Re: UPS ... indistinguishable from phishing \(G.M.Sigut\)](#)
- [Re: Fascinating phishing attack: valid links, dangerous ... number \(Al Macintyre\)](#)
- [Re: Apple Fails to Patch Critical Exploited DNS Flaw \(Robin Stevens\)](#)
- [Re: Another GPS error story \(J R Stockton\)](#)
- [Survey: Perception of security in online environments \(Gene Spafford\)](#)
- [REVIEW: "The Innocent Man", John Grisham \(Rob Slade\)](#)

• [Volume 25 Issue 27 \(Friday 8 August 2008\)](#)

- [Strange Yahoo! vote count \(PGN\)](#)
- [Trust TSA? Maybe... Trust Akamai...? \(David Leshner\)](#)
- ["How reliable is DNA in identifying suspects?" \(Robert P Schaefer\)](#)
- [GPS causes nightmare vacation \(PGN\)](#)
- [Re: Another small interface risk \(Thomas Wicklund\)](#)
- [Re: Unsuspected travelers' laptops may be detained at border \(Thomas Hamann\)](#)
- [Re: Neglecting to logout from Skype \(Dimitri Maziuk\)](#)
- [Pizza delivery and postal addresses \(Mark Brader\)](#)

• [Volume 25 Issue 28 \(Tuesday 12 August 2008\)](#)

- [Internet attacks against Georgian web sites \(Gadi Evron, Gadi Evron\)](#)
- [Russia/Georgia: Tanks, Bombers, Keyboards \(Edward Rice\)](#)
- [Patch for Web Security Hole Has Some Leaks of Its Own \(John Markoff via PGN\)](#)
- [MIT Students Gagged by Federal Court Judge \(EFF via David Farber\)](#)
- [CloudAV \(Rob Slade\)](#)
- [Two on-line travel booking risks \(Chris Drewe\)](#)
- ['Fakeproof' microchipped British e-passport ... \(Lars Poulsen\)](#)
- [Re: Unsuspected travelers' laptops may be detained ... \(Steven M. Bellovin, R. G. Newbury\)](#)
- [Re: GPS causes nightmare vacation \(Fernando Pereira\)](#)
- [Re: How reliable is DNA ...? \(Michael Black, Steve Schafer\)](#)
- [Re: Neglecting to logout from Skype ... \(Al Macintyre\)](#)

• [Volume 25 Issue 29 \(Tuesday 19 August 2008\)](#)

- [Olympics Windows crash \(PGN\)](#)
- [Translate of device mech auto-reproduce \(Rob Slade\)](#)
- [Electronic voting and antivirus software \(jared\)](#)
- [Officials Say Flaws at Polls Will Remain in November \(Ian Urbina via PGN\)](#)
- [Glitch let hundreds get free transit rail tickets \(William Neuman via PGN\)](#)
- [Big trouble with Germany's New Unified Tax Identification Codes \(Ralf Fritzsich\)](#)
- [Online Consumers at Risk and the Role of State Attorneys General \(CAP/CDT item via Monty Solomon\)](#)
- [11 charged with massive ID theft \(Monty Solomon\)](#)
- [Re: Firefox 3's Step Backwards For Self-Signed Certificates \(Michael Barrett\)](#)
- [Re: 'Fakeproof' microchipped British e-passport \(Hamish Marson\)](#)
- [Billion dollar IT failure at Census Bureau \(Michael Lewchuk\)](#)
- [Attempt to muzzle MIT subway research backfires \(B.K. DeLong\)](#)
- [My date and place of birth are public \(jidanni\)](#)
- [Re: How reliable is DNA ...? \(Geoff Kuenning, Rob Searle, Brian Hayes, Bob Buxton\)](#)

• [Volume 25 Issue 30 \(Thursday 28 August 2008\)](#)

- [Bruce Schneier on Airport Photo ID Checks \(PGN\)](#)
- [Flight-plan FAAilure \(PGN\)](#)
- [Aug 26 FAA flight plan fiasco \(Ken Knowlton\)](#)
- [Commuter Flights Grounded Thanks To Bumbling TSA Inspector \(PGN\)](#)
- [Computer viruses make it to orbit \(Gabe Goldberg\)](#)
- [Ohio Voting Machines Contained Programming Error That Dropped Votes \(PGN\)](#)
- [States throw out costly electronic voting machines \(vim\)](#)
- [Risks of going on Internet record \(Spamcop\)](#)
- [And here we go off the rails: "spam hunter" \(Identity withheld by request\)](#)
- [Educational "testing firm" flunks Internet Security 101 \(Danny Burstein\)](#)
- [A cellphone bill roams to the stratosphere \(Gabe Goldberg\)](#)
- [Weird Clock Issue \(Steven J. Greenwald\)](#)
- [Risks of omitting off-site backups? \(C.Y./J.E. Cripps\)](#)
- [Telephone banking password /in/security \(Tim Bradshaw\)](#)
- [Boston judge tosses MIT students' gag order \(Richard Forno\)](#)
- [Re: DNA Database Searches \(Hal Murray, Ken Knowlton\)](#)
- [Re: Couple of On-Line Travel Booking Risks \(Chris Drewe\)](#)
- [Re: Germany's New Unified Tax Identification Codes \(Ralf Fritzsich\)](#)
- [Re: P2P Data Breach affects SCOTUS \(Hal Murray\)](#)

• [Volume 25 Issue 31 \(Wednesday 10 September 2008\)](#)

- [FAA redundancy -- or the lack thereof \(Tessler and Robertson via PGN\)](#)
- [Corrupt File Brought Down Flight Planning System \(Gabe Goldberg\)](#)

- [UK software upgrade issues \(John Sawyer\)](#)
- [JPMorgan Chase: The Bank Account That Sprang a Leak \(Monty Solomon\)](#)
- [Software problems affect the bottom line at J. Crew \(Steven M. Bellovin\)](#)
- [Google ads and language \(Erling Kristiansen\)](#)
- [Worditudinality \(Rob Slade\)](#)
- [Control-C vs. Bourne-Again SHell \(jidanni\)](#)
- [Control-C Control-C vs. gnus \(jidanni\)](#)
- [Risks of better security and "smarter" users \(Ron Garret\)](#)
- [BNY Mellon Data Breach Potentially Massive \(George Hulme via Monty Solomon\)](#)
- [Student hacker exposes Carleton U cash, ID card security holes \(Sergei Patchkovski\)](#)
- [Whit Diffie and Susan Landau: Internet Eavesdropping \(Randall Webmail\)](#)
- [US .gov website asks for personal info without https protection \(Jonathan Thornburg\)](#)
- [Re: Germany's New Unified Tax Identification Codes \(Kevin Pfeiffer\)](#)
- [Re: Firefox 3's Step Backwards ... \(Dimitri Maziuk\)](#)

• [Volume 25 Issue 32 \(Thursday 11 September 2008\)](#)

- [Google revives 6-year-old news story, sends United shared down 75% \(Steven J Klein, Drew Dean, Scott Nicol\)](#)
- [How Steve Jobs' obit got published \(Philip Elmer-DeWitt via Monty Solomon\)](#)
- [Internet Traffic Begins to Bypass the U.S. \(John Markoff via Monty Solomon\)](#)
- [Global Trail of an Online Crime Ring \(Brad Stone via Monty Solomon\)](#)
- [Automated Bill Payments Are a Cinch: Not So Fast \(Ron Lieber via Monty Solomon\)](#)
- [Hackers prepare supermarket sweep \(Gabe Goldberg\)](#)
- [Antivirus software in critical systems? \(Erling Kristiansen\)](#)
- [Re: States throw out costly electronic voting machines \(Peter Houppermans, Jim Haynes\)](#)
- [Risks of GPS Devices that we had Not Previously Heard Of \(Mark Brader\)](#)
- [Over-reliance on automated real estate valuation \(Jeremy Epstein\)](#)
- [Re: Control-Z vs. Bourne-Again SHell \(David Chau\)](#)
- [Re: Weird Clock Issue - a single bit error \(Chris Smith, Mark Lutton, Amos Shapir\)](#)
- [Re: Bruce Schneier on Airport Photo ID Checks \(Andy Piper, Amos Shapir\)](#)
- [Re: Risks of better security and "smarter" users \(Dag-Erling Smørgrav, Ron Garret\)](#)

• [Volume 25 Issue 33 \(Monday 15 September 2008\)](#)

- [Antivirus software in critical systems? \(Rob Diamond, Robert P Schaefer, PGN\)](#)
- [Re: States throw out costly electronic voting machines \(Patrick J Kobly\)](#)
- [Re: FAA redundancy -- or lack thereof \(Mike Martin\)](#)
- [Misleading headline: 'Big bang' experiment is hacked \(Gabe Goldberg\)](#)
- [Change name, get off no-fly list \(David Magda\)](#)
- [Re: Amos Shapir on Airport Photo ID Checks \(Danny Lawrence\)](#)
- [iPhone Takes Screenshots of Everything You Do \(Brian X. Chen via Monty Solomon\)](#)
- [Re: UAL, Automated trading gets spoofed! \(Howard Israel\)](#)
- [San Francisco officials looking for hidden network device \(Gabe Goldberg\)](#)
- [PayPal phishes their own customers \(Andrew Pam\)](#)
- [Re: Risks of better security ... \(Chris Adams, Ron Garret on David Bliss\)](#)
- [Re: Control-Z vs. Bourne-Again SHell \(Philippe Pouliquen\)](#)
- [Re: Weird Clock Issue -- a single bit error \(David Magda\)](#)
- [Re: Risks of GPS Devices ... \(Sergei Patchkovski\)](#)
- [Re: Automated Bill Payments Are a Cinch: Not So Fast \(CBFalconer, Sten Carlsen, Erling Kristiansen\)](#)

• [Volume 25 Issue 34 \(Sunday 21 September 2008\)](#)

- [SciAm article on Smart Grid \(William P.N. Smith\)](#)
- [Wall Street; where nothing can go wrong wrogn wrngno.... \(David Leshner\)](#)

- [Mortgage loan crisis due to wishful thinking, Garbage In Garbage Out \(Geo Swan\)](#)
- [BNY Mellon data breach now at 200K in Mass, 12M in U.S. \(Monty Solomon\)](#)
- [Risks of financial systems too complex to understand \(Daniel P. B. Smith\)](#)
- [Risks of not using check digits in bank account numbers \(Toby Douglass\)](#)
- [Risks of banking in Holland \(Toby Douglass\)](#)
- [Re: PayPal phishes their own customers \(Sidney Markowitz\)](#)
- [Re: Automated Bill Payments Are a Cinch: Not So Fast \(Huge\)](#)
- [Capability creep strikes again \(Jay R. Ashworth\)](#)
- [Expiration of cryptographic certificate killed airline ticket \(Kenji Rikitake\)](#)
- [Antivirus software in critical systems? \(Martyn Thomas\)](#)
- [Re: Antivirus software in critical systems? Aurora! \(Al Mac Wheel\)](#)
- [Re: Control-Z vs. Bourne-Again SHell \(jidanni\)](#)
- [Re: Risks of GPS Devices ... \(Richard Grady\)](#)
- [USENIX Annual Tech '09 Call For Papers \(Lionel Garth Jones\)](#)

• [Volume 25 Issue 35 \(Monday 22 September 2008\)](#)

- [Sydney road tunnel closed by computer 'glitch' \(John Colville\)](#)
- [DC Primary votes don't add up... even with a fudge factor \(David Leshner\)](#)
- [Hurricane Ike \(Les Denham\)](#)
- [Hacker claims Palin e-mail hacked via password reset \(Rob McCool\)](#)
- [Re: Wall Street; where nothing can go wrong wrogn wrngno.... \(Martin Ward\)](#)
- [Re: Risks of financial systems too complex ,,, \(Jim Horning\)](#)
- [Re: Risks of not using check digits \(Erling Kristiansen, Paul van Keep\)](#)
- [Re: capability creep on red-light cameras \(Paul Wallich\)](#)

• [Volume 25 Issue 36 \(Tuesday 30 September 2008\)](#)

- [Mersenne-aries receive benevolence \(PGN\)](#)
- [Wall Street's Collapse May Be Computer Science's Gain" \(ACM technews\)](#)
- [BBV: Two-Minute warning on voting machines \(Steve Kelem\)](#)
- [Online flight bargains not as good as they seemed \(Donald Mackie\)](#)
- [Risks of all-encompassing backups \(Peter Gutmann\)](#)
- [ATM reprogramming scam; Two arrested \(Kevin Poulsen via PGN\)](#)
- [Default passwords and gasoline thefts \(Jim Haynes\)](#)
- [ATM bug \(Phil Smith III\)](#)
- [Re: Sydney tunnel: When is a backup not a backup? \(Martin Ward\)](#)
- [Sydney Australia or Sydney Nova Scotia? \(Rick Gee\)](#)
- [Too big to fail = single point of failure? \(Bill Hopkins\)](#)
- [Flooded computers disposed of? \(Marty Brenneis\)](#)
- [Burning wheelchair almost destroys airplane \(Andrew Koenig\)](#)
- [Re: Risks of financial systems too complex ,,, \(Robert P Schaefer\)](#)
- [Re: Hacker claims Palin e-mail hacked via password reset \(Scott Miller\)](#)
- [Re: Risks of not using check digits \(Toby Douglass\)](#)
- [Risks in Networked Computer Systems, Andre' N. Klingsheim \(PGN\)](#)
- [Study on InSecurity of Social Networks \(LinkedIn et al. via Klaus Brunnstein\)](#)
- [Estonian Cyber Security Strategy document \(Gadi Evron\)](#)

• [Volume 25 Issue 37 \(Thursday 2 October 2008\)](#)

- [NASDAQ's Google surprise \(PGN\)](#)
- [Computer Failure Hobbles Hubble, Derails Shuttle Mission \(Sharon Gaudin\)](#)
- [Amazon multiple account weirdness \(Graham Bennett\)](#)
- [Alarm sounded on second-hand kit \(Gabe Goldberg\)](#)
- [Seeking tales of IT gone wrong \(Andrew Brandt\)](#)

- [Re: Risks of financial systems too complex ... \(Robert P Schaefer\)](#)
- [Re: When is a backup not a backup? \(Mark F\)](#)
- [The folly of retaining default settings \(Ken Knowlton\)](#)
- [Weak password reset procedures \(identity withheld\)](#)
- [New castle rules in chess? \(Andy Walker\)](#)
- [Re: Hacker claims Palin e-mail hacked ... \(Rob McCool, Scott Miller, Allen Hainer\)](#)

• [Volume 25 Issue 38 \(Tuesday 14 October 2008\)](#)

- [Investigator: Computer likely caused Qantas plunge \(Paul Saffo\)](#)
- [Qantas A330 accident \(Martyn Thomas\)](#)
- [B-2 crash on takeoff \(Ken Knowlton\)](#)
- [Illinois high-speed trains \(Jon Hilkevitch via David Lawver\)](#)
- [D10T: National Debt Clock is out of digits \(Mark Brader\)](#)
- [Passport RFID attack: missing validation \(Aaron Emigh via PGN\)](#)
- [Missing hard drive "not encrypted" because it was "secure" \(John Carlyle-Clarke\)](#)
- [Russian researchers achieve 100-fold increase in WPA2 cracking speed \(Monty Solomon\)](#)
- [Defective news submission website \(Steven M. Bellovin\)](#)
- [Risks of a new laptop \(Nick Brown\)](#)
- [Researcher Liuba Belkin: Workers more prone to lie in e-mail \(Monty Solomon\)](#)
- [Thomas Crown escape, revisited \(Peter Houppermans\)](#)
- [Re: Sydney NS vs. Sydney NSW \(Steve Schafer\)](#)
- [Oyster card hack details revealed \(Gabe Goldberg\)](#)
- [Re: Remarkable -- United Airlines Stock \(Russ Nelson\)](#)

• [Volume 25 Issue 39 \(Friday 17 October 2008\)](#)

- [NSA posts secrets to writing secure code \(Joab Jackson via Jim Innes\)](#)
- [Excel error leaves Barclays with extra Lehman assets \(Gabe Goldberg\)](#)
- [LAPD blames fingerprint errors for false arrests \(PGN\)](#)
- [Maryland Police Put Activists' Names On Terror Lists \(David Hollman\)](#)
- [Airport baggage screener charged with stealing passengers' stuff \(Peter Houppermans\)](#)
- [Credit card readers compromised \(Peter Houppermans\)](#)
- [More Smart Card Cracking \(Gene Wirchenko\)](#)
- [Stolen Votes and Stolen Elections \(Mark E. Smith, PGN\)](#)
- [Online health records \(David Magda\)](#)
- [New Data Privacy Laws Set For Firms \(Ben Worthen via Monty Solomon\)](#)
- [New Massachusetts Regulation Requires Encryption of Portable Devices ... \(Monty Solomon\)](#)
- [Amazon e-mail accounts \(Steve Loughran\)](#)
- [Security questions with unacceptable answers \(Earl Truss\)](#)
- [Worrisome money transfer \(Martin Cohen\)](#)
- [Stallman vs. Cloud Computing \(jidanni\)](#)
- [A comment on "outliers" \(Ken Knowlton\)](#)
- [The Risks of "Something you know" \(Steve Taylor\)](#)
- [Re: D10T: National Debt Clock is out of digits \(Andrew Raybould\)](#)
- ["Sydney NS vs. Sydney NSW" and popup adds! \(Paul D.Smith\)](#)

• [Volume 25 Issue 40 \(Tuesday 21 October 2008\)](#)

- [Treasury Office Faults IRS Computer Security \(AP via PGN\)](#)
- [Springer: Open for all to see \(Debora Weber-Wulff\)](#)
- [TBS leaves baseball championship game viewers in the dark \(Jim Reisert\)](#)
- [Drunk, and Dangerous, at the Keyboard \(Alex Williams via Monty Solomon\)](#)
- [Thousands Face Mix-Ups in Voter Registrations \(Mary Pat Flaherty\)](#)
- [Ohio Secretary of State's Web Site Hacked; voter suppression tactics \(Steve Kelem\)](#)

- [From BBV: Two-Minute warning on voting machines \(Steve Kelem\)](#)
 - [Unbelievable security violation \(Identity withheld\)](#)
 - [Re: More Password Reset Procedures \(Identity withheld\)](#)
 - [Risks: Unlock your house via the Internet \(Gabe Goldberg\)](#)
 - [Re: Remarkable -- United Airlines Stock \(Martin Gregorie\)](#)
 - [Re: Outliers \(Jurek Kirakowski\)](#)
 - [Re: Investigator: Computer likely caused Qantas plunge \(Peter Rieden, Ron Garret\)](#)
 - [Re: Sydney NS vs. Sydney NSW \(Chuck Charlton\)](#)
 - [Re: Illinois high-speed trains \(Joseph Brennan\)](#)
 - [Re: Risks of a new laptop \(Scott Miller\)](#)
 - [Correction/disclaimer re unistable polyhedron \(Ken Knowlton\)](#)
 - [Re: The folly of retaining default settings \(Mark Thorson\)](#)
 - [Re: D10T: National Debt Clock is out of digits \(Mark Hull-Richter\)](#)
- [Volume 25 Issue 41 \(Thursday 23 October 2008\)](#)
- [Re: Computer likely caused Qantas plunge \(Peter Bernard Ladkin, Dag-Erling Smørgrav, Guy Dawson, Chris Kuan\)](#)
 - [U.S. Government to Take Over Airline Passenger Vetting \(PGN\)](#)
 - [IEEE Spectrum review process upgrade curiosity \(PGN\)](#)
 - [Dan Wallach's report on a vote-flipping examination \(PGN\)](#)
 - [Deceptive practices in elections \(PGN\)](#)
 - [Straight Party Voting Issues \(Leonard Finegold\)](#)
 - [GAO report on Social Security Numbers \(PGN\)](#)
 - [Re: More Password Reset Procedures \(Ralph Jacobs\)](#)
 - [Re: Amazon e-mail accounts \(Dimitri Maziuk, Klaus Johannes Rusch\)](#)
 - [2 of 3 navigational devices functioning \(Daniel P. B. Smith\)](#)
- [Volume 25 Issue 42 \(Friday 24 October 2008\)](#)
- [Greenspan says computer input did it \(CWmike via timothy via Wendell Cochran\)](#)
 - [Vint Cerf: Big Changes Ahead for the Internet \(TechNews\)](#)
 - [UW researchers uncover gap in border security \(Peter Gregory\)](#)
 - [Re: Computer likely caused Qantas plunge \(Dag-Erling Smørgrav, Cameron Simpson, Adrian Edmonds\)](#)
 - [Re: Straight Party Voting Issues \(David Phillips, Arthur Flatau\)](#)
 - [Re: Remarkable -- United Airlines Stock \(John Levine\)](#)
- [Volume 25 Issue 43 \(Wednesday 29 October 2008\)](#)
- [Driver hits NIPSCO pole; surge fries sewage treatment plant \(Shawn Merdinger\)](#)
 - [Risks of escalating complexity: AA757 electrical power loss \(David Leshner\)](#)
 - [Schlage BrightBlue wireless lock controllers \(Shawn Merdinger\)](#)
 - [Computer screens out distress call from kidnap victim \(David Tombs\)](#)
 - [Finnish E-Voting System Loses 2% of Votes \(Pertti Huuskonen\)](#)
 - [Article on voting through American history \(*The New Yorker* via Harlan Rosenthal\)](#)
 - [Poison-pill auto-disclosure for security vulnerabilities \(Paul Robinson\)](#)
 - [They got us coming and going: tire monitoring \(Paul Wexelblat\)](#)
 - [Holistic Systems \(Pierre-Jacques Courtois\)](#)
 - [Twitter Jitters \(Zachary Tumin\)](#)
- [Volume 25 Issue 44 \(Saturday 8 November 2008\)](#)
- [U.K. NHS computer system "grinds to a halt" \(Richard Cook\)](#)
 - [Risk of repairing Hubble too soon \(Ted Blank\)](#)
 - [New GPS satellite may crash some receivers \(William P.N. Smith\)](#)
 - [Risks of unilingual vacation-reply messages \(Mark Brader\)](#)

- [US court throws out most software patents \(John Oram via Monty Solomon\)](#)
- [Beware: T-Mobile's Voicemail Paging Trap \(Lauren Weinstein\)](#)
- [Re: BBC Domesday Project \(Mike Tibbetts\)](#)
- [Re: Treasury Office Faults IRS Computer Security \(Paul Robinson\)](#)
- [Computers Freedom & Privacy Conference 2009 - Request For Proposals \(Bruce R Koball\)](#)
- [REVIEW: "Handbook of Research on Technoethics", Luppicini/Adell \(Rob Slade\)](#)

• [Volume 25 Issue 45 \(Monday 17 November 2008\)](#)

- [Chinese hackers breach white house computer systems \(PGN\)](#)
- [Hacker Tool Targeting MS08-067 Vulnerability \(Websense via Monty Solomon\)](#)
- [Lose the BlackBerry? Yes He Can, Maybe: President-Elect Obama \(Jeff Zeleny via Monty Solomon\)](#)
- [Texas Suspends Massive Outsourcing Contract \(Keith Price\)](#)
- [Driver Blames GPS System For Car-Train Collision \(Paul Saffo\)](#)
- [Stop! Buses only! --What do you mean, you ARE a bus? \(Mark Brader\)](#)
- [Martian deep freeze: NASA's Mars Lander dies in the dark \(Sharon Gaudin via PGN\)](#)
- [The "Two Focaccia Buttons Defense" \(Robert Hall\)](#)
- [Risks of assuming constant hours in a day \(Toby Gottfried\)](#)
- [Excel auto-formatting \(David Magda\)](#)
- [Texting bug hits the Google phone \(Amos Shapir\)](#)
- [Vintage IBM tape drive in Apollo moon dust rescue \(Chris Leeson\)](#)
- [gnus-mime-print-part vs. Mom's room \(jidanni\)](#)
- [False security from privacy screens \(David Alan Gilbert\)](#)
- [Re: BBC Domesday Project \(Martin Ward, Theo Bucher\)](#)
- [Re: Poison pill auto-disclosure \(Terje Mathisen, Al Macintyre, Richard O'Keefe\)](#)

• [Volume 25 Issue 46 \(Wednesday 26 November 2008\)](#)

- [E-prescription for IT disaster \(Tom Yager via Gene Wirchenko\)](#)
- [Computer virus shuts down three London hospitals \(Patrick O'Beirne\)](#)
- [The Blackberry, the President, and Reality \(Fred Cohen, Steve Wildstrom\)](#)
- [Choose too large a sample interval and look like an idiot \(Max Power\)](#)
- [The Great RoHS/Tin Whisker Fiasco of 20?? \(Jay R. Ashworth\)](#)
- [ACMS helps recover lost Moon data \(David Shaw\)](#)
- [Re: Vintage IBM tape drive in Apollo moon dust rescue \(David Brunberg\)](#)
- [Re: BBC Domesday Project \(Kees Huyser, Amos Shapir\)](#)
- [Re: NASA's Mars Lander dies in the dark \(John Levine\)](#)
- [Excel user awareness \(Patrick O'Beirne\)](#)

• [Volume 25 Issue 47 \(Monday 8 December 2008\)](#)

- [Chatsworth Wreck May be a Safety Failure \(Chuck Weinstock\)](#)
- [Caltrain computer outage causes extensive schedule disruption \(PGN\)](#)
- [Water pumps failed in Yorba Linda fire \(Jim Geissman\)](#)
- [Dangerous Precedence Set - Federal Criminal Charges for Violation of Commercial Online ToS? \(Stephen via Dave Farber\)](#)
- [A cyber-attack alarms the Pentagon \(Jerry and Virgil Gligor via David Farber\)](#)
- [A secure version of reality \(Andy Piper\)](#)
- [The recovery features of botnets \(Peter Houppermans\)](#)
- [Fingerprints in South Africa \(Heinz M. Kabutz\)](#)
- [Facebook and tracking people \(David Magda\)](#)
- [How *not* to improve data quality \(Richard O'Keefe\)](#)
- [Israeli Labor primaries postponed: electronic systems fail \(Amos Shapir\)](#)
- [Re: Risks of assuming constant hours in a day \(Curt Sampson\)](#)
- [Workshop on GENI and Security: Call for Participation \(Matt Bishop\)](#)

- [MiniMetricon call for participation \(Fred Cohen\)](#)
- [REVIEW: "The History of Information Security", de Leeuw/Bergstra \(Rob Slade\)](#)

• [Volume 25 Issue 48 \(Thursday 18 December 2008\)](#)

- [Computer problem shuts down Toronto Stock Exchange for a day \(Mark Brader\)](#)
- ["Smart" vehicles - do they introduce new risks? \(Mike Martin\)](#)
- [An old clock arithmetic problem \(Kees Huyser\)](#)
- [Another translation adventure \(Hal Murray\)](#)
- [Cute piece of malware engineering \(Drew Dean\)](#)
- [Thieves Winning Online War, Maybe Even in Your Computer \(John Markoff via Monty Solomon\)](#)
- [CheckFree DNS hijacked \(Hal Murray\)](#)
- [Software Security Top-10 Surprises \(Gary McGraw via PGN\)](#)
- [iPhone thief thwarted by MobileMe sync \(Nick Rothwell\)](#)
- [Risks of data retention \(Mark Armbrust\)](#)
- [Password complexity? Not wiith LinkedIn \(Leon Kuunders\)](#)
- [Teacher Throws Fit Over Student's Linux CD \(Mike Rechtman\)](#)
- [FYI - !b404 \(Rob Slade\)](#)
- ["Helpful" authentication \(Erling Kristiansen\)](#)
- [The Perfect Law: Re: Dangerous Precedence Set \(Martin Ward\)](#)
- [REVIEW: "The Business Privacy Law Handbook", Charles H. Kennedy \(Rob Slade\)](#)

• [Volume 25 Issue 49 \(Tuesday 30 December 2008\)](#)

- [Three undersea cables cut \(Dave Burstein via Dave Farber\)](#)
- [Risks of flawed default behavior for your UAV \(John O Long\)](#)
- [Risks of excessive State data collection \(Toby Douglass\)](#)
- [Fun with speed-trap cameras for revenge \(Arthur T., David Hollman, No-Name\)](#)
- [Trust me, I have a cert! \(David Leshner\)](#)
- [Massive Embezzlement Case Involving Fry's Electronics \(Lauren Weinstein\)](#)
- [Fired Fry's executive: 'Caught up in the game' \(Lisa Fernandez and Julia Prodis Sulek via Monty Solomon\)](#)
- [In Move to Digital TV, Confusion Is in the Air \(Eric A. Taub via Monty Solomon\)](#)
- [VHS Rides Off Into The Sunset \(Geoff Duncan via Monty Solomon\)](#)
- [Inauguration Cellular Overloads \(David Leshner\)](#)
- [Automatic URL recognition \(Bill Hopkins\)](#)
- [Shooting Yourself in the Foot - on purpose? \(Marc\)](#)
- [Another method to lose your credit card \(Erich Neuhauser\)](#)
- [Re: Cute piece of malware engineering \(Paul Robinson\)](#)
- [Re: Teacher Throws Fit Over Student's Linux CD \(Kelly Bert Manning\)](#)
- [How to become a digital forensic evidence expert \(Fred Cohen\)](#)

• [Volume 25 Issue 50 \(Sunday 4 January 2009\)](#)

- [Sunrise on the post-leap-second era \(Tony Finch\)](#)
- [Zounds! Zinger: Zune Zapped Zealously with Zero-tolerance \(PGN, David Magda\)](#)
- [Backward Hebrew writing on iPhone calendar \(Steven M. Bellovin\)](#)
- [We can't stop the train because our GPS is broken \(Hawkins Dale\)](#)
- [Medical devices lag in iPod age; Patients' safety is at risk \(Carolyn Y. Johnson via Monty Solomon\)](#)
- [JournalSpace wiped out; no backups \(Lindsay Marshall\)](#)
- [Some *digital* reception will go black in February! \(Daniel P. B. Smith\)](#)
- [Digital photo frames: risks of infecting PCs \(Deborah Gage via PGN\)](#)
- [Risks of Australians shouting at your hard drive? \(Alec Muffett\)](#)
- [Firewall product uses man-in-the-middle attack to defeat SSL crypto \(Mike Coleman\)](#)
- [Woman fools Japan's airport security fingerprint system \(PGN\)](#)
- [The danger of DNA: It isn't foolproof forensics \(Maura Dolan and Jason Felch via Monty Solomon\)](#)

- [Phishing Scam Spreading on Twitter \(Chris Pirillo via David Farber\)](#)
- [Domain registrar hacked; numerous repointings... \(Danny Burstein\)](#)
- [Qwest cuts off Internet subs in NM, including government VoIP \(Lauren Weinstein\)](#)
- [Computer vs. food and warmth \(jidanni\)](#)
- [Yahoo tracking where you go - invasion of privacy \(jidanni\)](#)
- [Intelligent Speed Adaptation \(Martin Ward\)](#)
- [Re: License plate camera readers \(Danny Burstein\)](#)

• [Volume 25 Issue 51 \(Friday 16 January 2009\)](#)

- [Software glitch causes incorrect medication dosages \(Jeremy Epstein\)](#)
- [Police avoid arrests due to time-consuming QPRIME computer system \(Steven J Klein\)](#)
- [Maryland Police surveillance \(Lisa Rein and Josh White\)](#)
- [Army subcontractor sends 7,000 misaddressed letters: 'computer glitch' \(Rob McCool\)](#)
- [Risks in Hating Web Video \(Lauren Weinstein\)](#)
- ["Spy pens" and the future of private speech \(Jerry Leichter\)](#)
- [Risk of Car Sharing: Getting Pinned with Someone Else's Ticket \(Kent Borg\)](#)
- [Taiwan Immigration Computer down for the Count \(jidanni\)](#)
- [Tony Hoare: "Null References: The Billion Dollar Mistake" \(Olivier Dagenais\)](#)
- [Facebook hacked and no avenue for redress \(Mark Neely\)](#)
- [How to NOT perform customer service and updates \(Gene Spafford\)](#)
- [Risks of digital signatures \(Ron Garret\)](#)
- [Update: N.J. officials order paper trail upgrades to voting machines \(Danny Burstein\)](#)
- [Teenagers' Internet Socializing Not a Bad Thing \(Monty Solomon\)](#)
- [SecAppDev 2009 \(Johan Peeters\)](#)
- [REVIEW: "Intellectual Property and Open Source", Van Lindberg \(Rob Slade\)](#)

• [Volume 25 Issue 52 \(Thursday 22 January 2009\)](#)

- [German Train System Computers Down for Hours \(Debora Weber-Wulff\)](#)
- [Yet Another Reason Not to use Windows for Medical Devices \(Jeremy Epstein\)](#)
- [Tricky Windows Worm Wallops Millions \(Brian Krebs via Monty Solomon\)](#)
- [Electronic Medical Records, Google, and Microsoft \(Lauren Weinstein\)](#)
- [Cursive, foiled again: What will become of handwriting? \(David Mehegan via Monty Solomon\)](#)
- [The perils of trusting the UK government to get software right \(Bernard Peek\)](#)
- [New Web Analytics Service Spies on Web Browsing Activity Without Permission \(Lauren Weinstein\)](#)
- [Re: "Spy pens" and the future of private speech \(Henry Baker, Jerry Leichter\)](#)
- [Re: Tony Hoare: "Null References: The Billion Dollar Mistake" \(Henry Baker\)](#)
- [Risks of Avis insufficient customer data checking \(Chris Warwick\)](#)

• [Volume 25 Issue 53 \(Saturday 31 January 2009\)](#)

- [England's NHS loses patient data: bad news, good news, bad news \(Steven J Klein\)](#)
- [Michigan man freezes to death after electric company cuts power \(Mark E. Smith\)](#)
- [Worm Infects Millions of Computers Worldwide \(John Markoff via PGN\)](#)
- [Trojan virus spreads to as many as 20,000 Macs \(Boy Genius via Dave Farber\)](#)
- [Fannie Mae insider attack \(Kevin Poulsen via Jeremy Epstein\)](#)
- [NSW, Australia Govt Jobs website hacked; authorities in denial \(Andrew Jones\)](#)
- [MP3 player contained US military secrets \(Danny Burstein\)](#)
- [Digital road sign in Austin, TX was altered to read, "Zombies Ahead." \(David Hollman\)](#)
- [Friends, Until I Delete You \(Douglas Quenqua via Monty Solomon\)](#)
- [Political risks of poorly configured email advocacy \(Rich Mintz\)](#)
- [Canadian do-not-call list becomes valuable telemarketing database \(Olivier Dagenais\)](#)
- [Staff Finds White House in the Technological Dark Ages \(Anne E. Kornblut via Monty Solomon\)](#)
- [Amex goes phishing \(James J. O'Donnell\)](#)

- [American Express Kept a *Very* Watchful Eye on Charges \(Ron Lieber via Monty Solomon\)](#)
- [Statue of Frauds \[sic\] \(Martyn Thomas\)](#)
- [Re: Yet Another Reason Not to use Windows for Medical Devices \(Bernard Peek\)](#)
- [Re: Tony Hoare: "Null References" \(Michael Albaugh, Jurek Kirakowski, Ray Blaak, Martin Torzewski, Richard O'Keefe\)](#)

• [Volume 25 Issue 54 \(Wednesday 4 February 2009\)](#)

- [Automated BART trains crash during manual operation of one of them \(Rob McCool\)](#)
- [Earthquake Alert System Failed To Work Properly \(Max Power\)](#)
- ['Foul play' suspected in Tucson Super Bowl porn feed \(Brian J. Pedersen via Monty Solomon\)](#)
- [Perils of html e-mail \(Charles Wood\)](#)
- [Votes lost in Finnish e-voting \(Antti Vaha-Sipila\)](#)
- [Fannie Mae Logic Bomb \(Jim Schindler\)](#)
- ["This site may harm your computer" on every search result \(Maxim Weinstein via Monty Solomon\)](#)
- [Google Account Takeover, Mark Ghosh \(jidanni\)](#)
- [Local Police Want Right to Jam Wireless Signals \(Spencer S. Hsu via Monty Solomon\)](#)
- [911 service not prepared for new generation of pranksters \(David Chartier via Monty Solomon\)](#)
- [Re: Digital road sign in Austin, TX was altered ... \(Mark Feit\)](#)
- [Re: MP3 player contained US military secrets \(Geoff Kuenning\)](#)
- [Re: American Express Kept a *Very* Watchful Eye on Charges \(David Alexander\)](#)
- [Re: Statue of Frauds \(Mark Jackson\)](#)
- [Re: Tony Hoare: "Null References" \(Dimitri Maziuk, Tony Finch, Jay Carlson\)](#)

• [Volume 25 Issue 55 \(Tuesday 10 February 2009\)](#)

- [RFID Passports cloned wholesale \(Dan Goodin\)](#)
- [Windshields and Windows combine to provide malware vector \(Mark Brader\)](#)
- [FAA Notifies Employees of Personal Identity Breach \(Danny Burstein\)](#)
- [390,000 to access child database \(Amos Shapir\)](#)
- [Confidential LAPD misconduct files mistakenly posted on Internet \(Danny Burstein\)](#)
- [Risks of computer-gibberish names on forms \(Joseph A. Dellinger\)](#)
- [Mathematics and screening \(Jerry Leichter\)](#)
- [The privacy vs. health tradeoff \(Jeremy Epstein\)](#)
- [Variant of Mac Trojan Horse iServices Found in Pirated Adobe C54 \(Monty Solomon\)](#)
- [Re: Fannie Mae logic bomb \(Wendell Cochran\)](#)
- [Re: Tony Hoare: "Null References" \(Rob Diamond, Robert P Schaefer\)](#)
- [Re: Flat text is *never* what we want \(Tony Finch\)](#)
- [No wikipedia page \(Olivier MJ Crepin-Leblond\)](#)
- [What if you can't pull the plug? \(Rex Sanders\)](#)
- [Security Psychology \(Gadi Evron\)](#)
- [Call for contributions: New Security Paradigms Workshop: NSPW \(Konstantin /Kosta/ Beznosov\)](#)

• [Volume 25 Issue 56 \(Thursday 19 February 2009\)](#)

- [Train brake failure; broken valve \(David Leshner\)](#)
- [Collision - UK and French Nuclear subs \(Charles Wood\)](#)
- [Control-Alt-Eject? French Navy grounded... \(David Leshner\)](#)
- [GCTIP: New Forums for Internet Transparency, Performance, ISP Issues \(Lauren Weinstein\)](#)
- [The mystery of 'Ireland's worst driver': an HR/training problem \(Max Power\)](#)
- [Hiding in plain sight \(Jeremy Epstein\)](#)
- [Stolen military laptop risks \(Atom Smasher\)](#)
- [Risks of reading RISKS \(Bruce Horrocks\)](#)
- [When a bit of knowledge is a dangerous thing \(Jeremy Epstein\)](#)
- ["It leaked into the kiosks and fried our computers" \(Monty Solomon\)](#)

- [Facebook Forever \(John Kolesar\)](#)
- [Opening event goes with a bang \(David Alexander\)](#)
- [Re: Hoare on Null References \(Peter Bernard Ladkin, CBFalconer, William Bader, Dan Franklin\)](#)

• [Volume 25 Issue 57 \(Friday 20 February 2009\)](#)

- [Taiwan immigration computer down again \(jidanni\)](#)
- [Wikipedia prankster dupes German media \(Allen Hainer\)](#)
- [The Trouble with Trusting Trend Micro \(Kevin Way\)](#)
- [ESTA visa waiver online doesn't provide existing waiver ref number \(George Michaelson\)](#)
- [Stove's Bad Crash Handling \(Gene Wirchenko\)](#)
- [Dates of birth are not unique identifiers \(Steven J Klein\)](#)
- [Re: Train brake failure; broken valve \(Matt Roberds\)](#)
- [Re: Collision - UK and French Nuclear subs \(Richard I. Cook, Geoffrey Brent\)](#)
- [Re: What if you can't pull the plug? \(Michael Loftis, David Leshner\)](#)
- [Re: Windshields and Windows combine to provide malware vector \(Tom Perrine\)](#)
- [Re: Godel and correctness \(Martyn Thomas\)](#)
- [Re: Tony Hoare: "Null References" \(Dimitri Maziuk, King Ables\)](#)
- [Re: The mystery of 'Ireland's worst driver' \(David Cantrell\)](#)
- [Re: Opening event goes with a bang \(Mark Brader\)](#)
- [Re: Risks of reading RISKS \(jidanni, Martyn Thomas, Scott Miller\)](#)

• [Volume 25 Issue 58 \(Sunday 22 February 2009\)](#)

- [Buffer overflows in SHA-3 submissions \(Joy Marie Forsythe\)](#)
- [Re: Train brake failure - broken valve \(Al Stangenberger\)](#)
- [Due Diligence or is that "Don't..."? Citibank fraud \(David Leshner\)](#)
- [Digital Archivists, Now in Demand \(Conrad De Aenlle via Monty Solomon\)](#)
- [Re: Wikipedia prankster dupes German media \(Debora Weber-Wulff\)](#)
- [Re: Control-Alt-Eject? French Navy grounded \(CBFalconer\)](#)
- [Capital One Phishing Warning is dangerous \(Marc Auslander\)](#)
- [Re: The mystery of 'Ireland's worst driver' \(Bernard Lyons\)](#)
- [Re: Hiding in plain sight \(Phil Smith III\)](#)
- [Bounds checking in C \(Andrew Koenig\)](#)
- [The risks of Silver Bullets \(Michael Smith\)](#)
- [Re: Tony Hoare: "Null References" \(Steven M. Bellovin, Dimitri Maziuk, Randy Saunders\)](#)
- [Related to blacklists for antispam \(De Vries Duane\)](#)
- [Re: Dates of birth are not unique identifiers \(David E. Ross\)](#)
- [Re: USAA Web site follies \(Jonathan Kamens\)](#)
- [Alert TA09-051A -- Adobe Acrobat and Reader Vulnerability \(US-CERT via Monty Solomon\)](#)

• [Volume 25 Issue 59 \(Sunday 1 March 2009\)](#)

- [Iridium and Cosmos satellites collide \(Ken Knowlton\)](#)
- [When your files are online and you aren't \(Hiawatha Bray via Monty Solomon\)](#)
- [Man charged \\$81 billion for a fuel fill-up \(Peter Gregory\)](#)
- [Computer "Glitch" Results in \\$31 billion Error \(Malcolm Pack\)](#)
- [Best Buy swindled for \\$31 million by chip supplier \(Jim Haynes\)](#)
- [Google Gaffe: Gmail Outage Shows Pitfalls of Online Services \(Jonathan B Spira\)](#)
- [Power outage disables power failure alarm \(Jim Haynes\)](#)
- [UK building society online account open to DOS attack \(Andy Repton\)](#)
- [Wikileaks cracks key NATO document on Afghan war \(Jeff Nye\)](#)
- [Re: Hiding in plain sight \(Al Macintyre, Mark Feit, Phil Smith III, Steve Lamont, Marcos H. Woehrmann\)](#)
- [Urban legends in RISKS \(David Guaspari\)](#)



Volume 25 Issue 60 (Friday 6 March 2009)

- [Health-care: The Computer Will See You Now \(Anne Armstrong-Cohen via PGN\)](#)
- [Turkish Airline disaster and the Altimeter \(Turgut Kalfaoglu\)](#)
- [Britain's Chinook helicopters unusable for years due to software \(Mark Brader\)](#)
- [Conviction in attempted 229 million GBP theft \(Mark Brader\)](#)
- [Altimeter and autopilot possible cause of plane crash near Schiphol \(Ben Blout\)](#)
- [Normal Accidents and Black Swans \(Jerry Leichter\)](#)
- [Building-Security-In Maturity Model: BSIMM \(Gary McGraw\)](#)
- [An insider attack... in the police \(Jeremy Epstein\)](#)
- [Diebold delete button for erasing audit logs \(Kim Zetter via PGN\)](#)
- [Re-examining assumptions \(Jerry Leichter\)](#)
- [Credit card #s plucked out of air at FL Best Buy \(David Ian Hopper via Dave Farber\)](#)
- [Worldpay ATM system breached \(Neil Youngman\)](#)
- [Re: Iridium and Cosmos satellites collide \(Ivan Jager\)](#)
- [Risk Contained In RISKS Posting? \(David E. Price\)](#)
- [Re: Wikileaks cracks key NATO document on Afghan war \(Charles Wood\)](#)
- [Re: Google Gaffe: Gmail Outage ... \(Alain Picard\)](#)
- [Verizon curiosity \(Peter Zilahy Ingerman\)](#)

• [Volume 25 Issue 61 \(Sunday 29 March 2009\)](#)

- [DNA contamination led to serial-killer illusion \(Mark Brader\)](#)
- [Announcing your crime in a chat room may interfere with it \(Mark Brader\)](#)
- [You have won \\$\[2^32-1\]/100, no wait, we mean nothing \(Mark Brader\)](#)
- [Student dead 2 months, told to improve attendance \(Mark Brader\)](#)
- [Phantom Serial Killer \(Dave Mulkey\)](#)
- [E-voting In Ireland \(PGN\)](#)
- [Fairfax County Virginia voting glitches \(Jeremy Epstein\)](#)
- [Arose by any other name: was Diebold \(PGN\)](#)
- ["Security by obscurity Considered Harmful" -- especially for voting \(John Sebes\)](#)
- [Malware installed at manufacturer on Diebold ATMs \(Toby Douglass\)](#)
- [Driver Says GPS Unit Led Him to Edge of Cliff \(Richard Grady\)](#)
- [The Information Security Debt Clock \(Gunnar Peterson\)](#)
- [Google translations used for phishing attacks against ISPs \(Gadi Evron\)](#)
- [Economics of Finding and Fixing Vulnerabilities in Distributed Systems \(Gunnar Peterson\)](#)
- [ZOL downtime and emergency maintenance \(Andrew Yeomans\) \](#)
- [We seem to be going over the top on "risks", forgetting about some realities \(Fred Cohen\)](#)

• [Volume 25 Issue 62 \(Wednesday 1 April 2009\)](#)

- [GPS Outages Feared \(Mike Tashker\)](#)
- [Conficker \(Ned Potter via PGN\)](#)
- [A Peering risk \(Chris Leeson\)](#)
- [Google Calendar as a single point of failure? \(Jeremy Epstein\)](#)
- [Safety and man/machine interactions: Traffic crossings \(Jerry Leichter\)](#)
- [The Chinese iTunes Gift Voucher Trick \(Monty Solomon\)](#)
- [The Police don't send chain letters \(Richard O'Keefe\)](#)
- [UK considering generalised use of deep packet inspection \(Toby Douglass\)](#)
- [Software Related Accident: Pipe-Laying Equipment \(David Smith\)](#)
- [Spam as an indicator of network health \(jidanni\)](#)
- [When Clouds go Bad: Losing Data in MobileMe \(Nick Rothwell\)](#)
- [Only allow 1, 2, and 100 year domain name registration \(jidanni\)](#)
- [Re: ESTA visa waiver online \(Chris J Brady\)](#)

• [Volume 25 Issue 63 \(Sunday 5 April 2009\)](#)

- [ElcomSoft to Recover Passwords with a Tambourine \(Olga Koksharova via Michel Kabay\)](#)
- [More on Google calendar \(Pat Lincoln and Jeremy Epstein via PGN\)](#)
- [Woman follows GPS, gets stuck in snowmobile trail \(Monty Solomon\)](#)
- [A firmware glitch of router software: 32-bit integer handling \(Chiaki Ishikawa\)](#)
- [No remittance, no ignition: Auto 'electronic repo' in action \(Henry Baker\)](#)
- [Risks of on-line backups -- is it still safe once there? \(David Leshner\)](#)
- [Domino's dishes out 11,000 free pizzas by mistake \(Monty Solomon\)](#)
- [Australian DST in the news \(Tony Finch\)](#)
- [Medical histories on the Internet \(A Subscriber\)](#)
- [Playboy TV fined over explicit content \(Max Power\)](#)
- [Re: E-voting in Ireland \(Robert 'Jamie' Munro\)](#)
- [Oldest Data Loss Incident Contest \(Monty Solomon\)](#)
- [2009 IEEE Symposium on Security and Privacy \(David Du\)](#)

• [Volume 25 Issue 64 \(Monday 20 April 2009\)](#)

- [Lisa Wangness: Inaccuracies in Google Health records \(Martin Ward\)](#)
- [Woman killed by laptop in crash \(Walter Roberson\)](#)
- [San Francisco South Bay phone vandalism \(PGN\)](#)
- [Vesta tire-pressure warnings \(Click and Clack\)](#)
- [Finnish e-voting results annulled; municipalities to hold new elections \(PGN\)](#)
- [CIA agent testifies on risks of electronic voting \(PGN\)](#)
- [Conficker C Analysis from SRI \(Monty Solomon\)](#)
- [Japanese vending machine face recognition accepts 10-yr-old as adult \(Paul Saffo\)](#)
- [Pro-regulation viewpoint on cyber vulnerability \(via David Farber\)](#)
- ["Nowt for owt" with Amazon \(Chris J Brady\)](#)
- [Credit-Card Activation \(Kees Huyser\)](#)
- [Bad authentication question \(Erik Mooney\)](#)
- [Re: The Security By Obscurity Myth \(Dick Mills\)](#)
- [Re: Driver Says GPS Unit Led Him to Edge of Cliff \(jidanni\)](#)
- [Re: flat text is *never* what we want \(Tony Finch\)](#)
- [Workshop on Service oriented Enterprise Architecture for Enterprise Engineering: EDOC'09 \(Selmin Nurcan\)](#)

• [Volume 25 Issue 65 \(Wednesday 29 April 2009\)](#)

- [New cybersecurity report, National Research Council \(PGN\)](#)
- [CNN gets it right on swine flu scare \(Jeremy Epstein\)](#)
- [President Obama says 3% of GDP on R&D \(PGN\)](#)
- [Computer Spies Breach Fighter-Jet Project \(Danny Burstein\)](#)
- [Pencils, not pixels: Ireland scuttles electronic voting machines \(Matthew Kruk\)](#)
- [Russian Voting in Berlin? \(Debora Weber-Wulff\)](#)
- [Second chance for French Net bill \(Amos Shapir\)](#)
- [US Senate bills 773 and 776 \(Mabry Tyson\)](#)
- [The Risk of Namespace Collision \(Gene Wirchenko\)](#)
- [Re: Tire-pressure warnings and RFI \(Philippe Pouliquen, Bill Hopkins, John Curran\)](#)
- [Re: The Security By Obscurity Myth \(Phil Colbourn, Steven M. Bellovin, Ted Lemon, Fred Cohen\)](#)
- [Firewalls are ineffective? \(Fred Cohen\)](#)
- [Re: "Nowt for owt" with Amazon \(Julian Bradfield\)](#)

• [Volume 25 Issue 66 \(Sunday 10 May 2009\)](#)

- [FAA ATC shutdown \(Linda Gorman\)](#)
- [Documented risks to FAA computers \(John Sawyer\)](#)

[Pipe Leak at NY Indian Point Nuclear Plant Raises Concerns \(Gabe Goldberg\)](#)

- [Minnesota court says defendants have right to see source code \(Mark Thorson\)](#)
- [Obama, McCain legal teams promote state-level clean election practices \(David Leshner\)](#)
- [Richard A. Clarke: Obama's Challenge in Cyberspace \(David Farber\)](#)
- ['Computer glitch' disrupts Boston city payroll \(Monty Solomon\)](#)
- [Teenage hiker's calls ignored; no street address \(Rohan Sullivan\)](#)
- [Hackers Break Into Virginia Health Professions Database, Demand Ransom \(Brian Krebs via Monty Solomon\)](#)
- [UCBerkeley health service hacked, with 160,000 at risk of ID theft \(Henry Lee via Ari Ollikainen\)](#)
- [How to guarantee bad passwords \(Jeremy Epstein\)](#)
- [Lexis Nexis does an Ooops. Data breach... \(Danny Burstein\)](#)
- ["Server issues" delay Nielsen ratings \(George Mannes\)](#)
- [Researchers Take Over Dangerous Botnet \(ACM TechNews\)](#)
- [Materials Database Problem \(Gene Wirchenko\)](#)
- [Strange cash register arithmetic favors the house \(Bart Thielges\)](#)
- [Re: Credit card numbers *not* plucked out of the air at FL Best Buy \(Jonathan Kamens\)](#)
- [Real-Time Networks RTN'09 \(ECRTS\)](#)

• [Volume 25 Issue 67 \(Saturday 16 May 2009\)](#)

- [Emirates Tail Strike at Melbourne 20 Mar 2009 \(David Landgren\)](#)
- [Joke foils chess software \(Fred Gilham\)](#)
- [Canada's tax agency computers pile up \(Ken Knowlton\)](#)
- [New key-derivation function \(David Magda\)](#)
- [iCal/iPhone/iPod dislike senior citizens? \(Steven M. Bellovin\)](#)
- [JHU insider may have breached more than 10,000 patient records \(PGN\)](#)
- [DC financial-aid agency discloses personal data of 2,400 students \(George Mannes\)](#)
- [DHS Sensitive But Unclassified sharing platform hacked \(PGN\)](#)
- [French net piracy bill signed off \(Amos Shapir\)](#)
- [Kiwibank discovers perils of Google Adwords with 100% Interest campaign \(Max Power\)](#)
- [Australian emergency services can't break through their own firewall \(Danny Burstein\)](#)
- [Re: FAA ATC shutdown \(Gene Wirchenko, Al Macintyre, Pete Kaiser, Mike Coleman, Linda Gorman\)](#)
- [REVIEW: "Googling Security", Greg Conti \(Rob Slade\)](#)

• [Volume 25 Issue 68 \(Saturday 23 May 2009\)](#)

- [NY voter voted absentee, then died; ballot ruled invalid \(PGN\)](#)
- [In a Lab, an Ever-Growing Database of DNA Profiles \(David Hollman\)](#)
- [Computers and Medical Practice: Some actual data \(Jerry Leichter\)](#)
- [Risks: Hackers 'destroy' flight sim site \(Gabe Goldberg\)](#)
- [A Lesson in Internet Anatomy: The World's Densest Meet-Me Room \(jidanni\)](#)
- [Re: "Server issues" delay Nielsen ratings \(Jesse W. Asher\)](#)
- [Re: Materials Database Problem \(Stuart Levy\)](#)
- [Re: Australian emergency services \(Bob Frankston\)](#)
- [How small does the disk chunk have to be? \(Fred Cohen\)](#)
- [Authentication and Identity theft \(Jay R. Ashworth\)](#)
- [Re: Tail strikes from improper settings \(Ken Knowlton\)](#)
- [Re: FAA ATC shutdown \(Stewart Fist\)](#)
- [Is "security through obscurity" being called for in RISKS? \(Fred Cohen\)](#)
- [Re: On Government IT competence \(Scott Miller\)](#)
- [Book Review: The Science of Fear, Daniel Gardner \(Bruce Schneier\)](#)

• [Volume 25 Issue 69 \(Sunday 24 May 2009\)](#)

- [Another Boston subway crash with cell-phone implications](#)
- [HIV patients sue after records left on MBTA \(Elizabeth Cooney\)](#)

- [NZ bank lends \\$10M instead of \\$10K; couple takes the money and runs \(Ian Wells\)](#)
- [Re: NY voter voted absentee, then died; ballot ruled invalid \(Paul Wallich, Harvey Fishman\)](#)
- [Fragility of telephone system \(Jim Haynes\)](#)
- [SANS NewsBites gets it very wrong, fails to post a correction \(Jonathan Kamens\)](#)
- [Re: Nielsen Ratings \(Rupert Moss-Eccardt\)](#)
- [How to make memorable but secure passwords \(Phil Colbourn\)](#)
- [Re: A Lesson in Internet Anatomy: The World's Densest Meet-Me Room \(Jidanni\)](#)
- [Re: FAA ATC shutdown \(Walter Roberson, Chris Drew, Gene S. Berkowitz, Al MacIntyre, Fred Cohen\)](#)
- [Re: On Government IT competence \(Pete Kaiser\)](#)
- [eCrime Researchers Summit CFP \(Monty Solomon\)](#)

• [Volume 25 Issue 70 \(Monday 1 June 2009\)](#)

- [Municipal politician unseated over fake e-mail \(Kelly Bert Manning\)](#)
- [A new biometrics risk? \(Lee Rudolph\)](#)
- [No-risk intelligence gathering? \(PGN\)](#)
- [iDEAL is not so ideal \(Erling Kristiansen\)](#)
- [Failures of eCommerce are Human not Computers \(Chris J Brady\)](#)
- [No 911 Service \(Gene Wirchenko\)](#)
- [Risks On Rails \(Rob Slade\)](#)
- [Train and iPod do not mix \(Gene Wirchenko\)](#)
- [Cycle-omatic complexity needed? \(Jeremy Epstein\)](#)
- [NZ bank lends \\$10M instead of \\$10K; plus Facebook \(Rob Slade\)](#)
- [Re: Tail strikes from improper settings \(Dick Mills\)](#)
- [Radio-isotope shortage, again... \(Danny Burstein\)](#)
- [Hutber's Law, Clarke's Third Law and Weasley's Law \(Michael Bacon\)](#)
- [Re: How small does the disk chunk have to be? \(Jeremy Epstein, Fred Cohen, Jeremy Epstein\)](#)
- [Re: secure but memorable passwords \(David Alexander, Dave Martin, Paul Karagianis\)](#)

• [Volume 25 Issue 71 \(Tuesday 23 June 2009\)](#)

- [Metro train fatal accident -- too much automation? \(Joe Thompson\)](#)
- [Air France crash and computers? \(Steven M. Bellovin\)](#)
- [Electronic health record systems fails; ambulances turned away from hospital \(Dale Hawkins\)](#)
- [Demolition: GPS vs Address; Well, we were close... \(David Leshner\)](#)
- [Shoreline music-food event fiasco: electronic pay system fails \(PGN\)](#)
- [Green Dam Youth Escort \(PGN\)](#)
- [China dominates NSA-backed coding contest \(Eugene H. Spafford\)](#)
- [Electricity Industry to Scan Grid for Spies \(Danny Burstein\)](#)
- [Google Street View functions as CCTV \(Mark Brader\)](#)
- [Smart electric meter risks; disastrous GPS misuse \(Nicky L Sizemore\)](#)
- [Copier short-changes users \(Matt Bishop\)](#)
- [GM & Segway to make 2-wheeled car \(Paul Czyzewski\)](#)
- [Another High-Tech Accident? \(Gene Wirchenko\)](#)
- [Reducing Risks of Implantable Medical Devices \(Kevin Fu\)](#)
- [Woman Gets Others' Medical Records In Mail \(Adolphus St. Clair\)](#)
- [Bozeman asking job applicants for their userid/password \(Arthur T.\)](#)
- [Risks of copyright lobbyists hiring someone to plagiarize PR spin \(Kelly Bert Manning\)](#)
- [A new way to lose money via ATM... \(David Leshner\)](#)
- [Re: Security through obscurity \(Steven M. Bellovin\)](#)
- [REVIEW: "Zero Day Threat", Byron Acohido/Jon Swartz \(Rob Slade\)](#)

• [Volume 25 Issue 72 \(Monday 6 July 2009\)](#)

- [More on the DC Metro collision 22 June 2009 \(David Leshner, Al Stangenberger\)](#)

- [Re: Train collisions \(Dave Parnas via PGN\)](#)
- [Earlier autopilot problem on New York City subway trains \(George Mannes\)](#)
- [More focus on computers in the Air France crash \(Steven M. Bellovin\)](#)
- [Clear clears its ownership, but not stored data \(PGN\)](#)
- [Use of GPS leads to wrong house being destroyed \(PGN\)](#)
- [Sequoia Voting Systems vs DC \(David Leshner\)](#)
- [A Less than Simple Flight from Rome to Heathrow \(Chris J Brady\)](#)
- [Train and iPod do not mix \(Barry Munns\)](#)
- [Billions stolen in online robbery \(PGN\)](#)
- [HOW many? 12.000 laptops lost PER WEEK in US airports \(Peter Houppermans\)](#)
- [That old "object reuse" problem ... \(Rob Slade\)](#)
- [Politicians, personal e-mail, and the ECPA \(Bob Gezelter\)](#)
- [RISKS at catless.ncl.ac.uk \(Lindsay Marshall\)](#)
- [Google Earth a tool for thieves and scoundrels? \(John Hatpin via Mark Brader\)](#)
- [Re: A new way to lose money via ATM... \(Jim Haynes\)](#)
- [Re: Bozeman \(Andrew Koenig\)](#)
- [I think we're all Bozemans on this bus \(Steve Lamont\)](#)

• [Volume 25 Issue 73 \(Thursday 16 July 2009\)](#)

- [Massive Visa overcharge \(Steven M. Bellovin\)](#)
- [German electronic health card system failure \(Martyn Thomas\)](#)
- [Boston Ballet School data breach \(Concerned Parent\)](#)
- [Risks of the Cloud: Liquid Motors \(Gene Wirchenko\)](#)
- [Facebook fraud about to get more interesting? \(Paul Wallich\)](#)
- [Taiwan man rescued after getting lost via GPS \(jidanni\)](#)
- [July 4 Fireworks cyber-attack \(PGN\)](#)
- [Twitter Attack Raises Flags on Security \(PGN\)](#)
- [Teenager Falls Into Manhole While Texting \(Michael Barkoviak via Monty Solomon\)](#)
- [When Texting Is Wrong \(Randy Cohen via Monty Solomon\)](#)
- [TV station forced to go old school after fire \(Denise Caruso\)](#)
- [Re: More on the DC Metro collision 22 June 2009 \(Steven M. Bellovin, Rick Dickinson, David Leshner\)](#)
- [Saltzer-Kaashoek Computer System Engineering book finally published \(PGN\)](#)
- [paypal accounts \(Toby Douglass\)](#)
- [SPAM: Phishing - the state of the art? \(Dirk Fieldhouse\)](#)
- [Re: Bozeman \(D.F. Manno, Mark Brader\)](#)
- [Oakland 2010, IEEE Symposium on Security and Privacy, CFP \(Ulf Lindqvist\)](#)

• [Volume 25 Issue 74 \(Wednesday 22 July 2009\)](#)

- [Elements of Programming, Alexander Stepanov/Paul McJones \(PGN\)](#)
- [The NSA wiretapping story nobody wanted: Whistleblower Klein \(jidanni\)](#)
- [Amazon Erases Orwell Books From Kindle Devices \(Brad Stone via Monty Solomon\)](#)
- [Re: Amazon takes-back Kindle e-books \(Hal Murray\)](#)
- [Net-filtering tables turned \(Geoff Kuenning\)](#)
- [Jonathan Zittrain, "Lost in the Cloud" \(PGN\)](#)
- [Re: cloud computing & server loss \(Harlan Rosenthal\)](#)
- [Ruhr University team breaks code of KeeLoq system \(David Leshner\)](#)
- [U.S. Passport RFID security \(Erica Naone via Monty Solomon\)](#)
- [U.S. Passports: Special alloy sleeves urged to block hackers? \(Todd Lewan via Monty Solomon\)](#)
- [Arming ATMs with Pepper Spray? \(Thomas Dzubin\)](#)
- [Eye tracking to prevent screen snooping \(Peter Houppermans\)](#)
- [U.S. Withheld Data on Risks of Distracted Driving \(Matt Richtel via Monty Solomon\)](#)
- [Adobe Terms Gone Wild \(Gene Wirchenko\)](#)
- [Taiwan president in ruckus over prerecorded web messages \(jidanni\)](#)

- [Canadian Mint says missing gold may have been stolen \(Darryl Dueck\)](#)
- [Re: July 4 cyber attack \(Joseph Brennan\)](#)
- [Risks of hierarchical map displays \(Paul Wallich\)](#)
- [An interesting reversal of the usual credit card problem \(Roger Leroux\)](#)
- ["Don't freak out," says ING Direct. At least I THINK it's ING Direct! \(Daniel P. B. Smith\)](#)

• [Volume 25 Issue 75 \(Thursday 6 August 2009\)](#)

- [Software never fails, people decide that it does \(Paul Robinson\)](#)
- [Seven water mains break due to computer glitch \(Joseph Lorenzo Hall\)](#)
- [Stock Traders Find Speed Pays, in Milliseconds \(Charles Duhigg via Monty Solomon\)](#)
- [GPS typo saves couple? \(Joel Baskin\)](#)
- [How To Hijack 'Every iPhone In The World' \(Andy Greenberg via Monty Solomon\)](#)
- [10 ways your voice and data can be spied on \(Gene Wirchenko\)](#)
- [The NSA Is still Listening to You \(jidanni\)](#)
- [Beware of Outdated E-mail Addresses \(Gene Wirchenko\)](#)
- [Funniest security faux pas this week \(Ron LaPedis\)](#)
- [You think Adobe bug reports are tough to submit... \(Michael Albaugh\)](#)
- [Re: Risks of hierarchical map displays \(Leonard Finegold, Gavin Treadgold, Gene Wirchenko\)](#)
- [Industrial object-oriented language made void-safe \(Bertrand Meyer\)](#)
- [Ari Juels, Tetraktys, a `cryptographic thriller' \(Ben Rothke via PGN\)](#)

• [Volume 25 Issue 76 \(Saturday 15 August 2009\)](#)

- [Amusement rides without Fail-safe States \(Debora Weber-Wulff\)](#)
- [Taipei rapid transit line closed until further notice \(jidanni\)](#)
- [Twitter disruption \(Jenna Wortham via PGN\)](#)
- [UK national ID card cloned in 12 minutes \(PGN\)](#)
- [Social security to pay \\$500 million to victims of database error \(Rob McCool\)](#)
- [Computer Error Caused Rent Troubles for Public Housing Tenants \(Manny Fernandez via Monty Solomon\)](#)
- [Kentucky election fraud indictments \(PGN\)](#)
- [Sequoia e-voting machine manipulated without insider info \(Peter Houppermans\)](#)
- [Boy Dies After Mom Says GPS Left Them Stranded in Death Valley \(Richard Grady\)](#)
- [China backs off on censorship software ... \(Lauren Weinstein\)](#)
- [Revealingerrors.com \(Robert P Schaefer\)](#)
- [Apple keyboard firmware hack demonstrated \(Monty Solomon\)](#)
- [Re: Software never fails ... \(Martyn Thomas, George Jansen, Andrew Brydon, Paul Edwards, Rob Seaman, Devin Moore, Nick Keighley, Martin Cohen\)](#)
- [Re: Ari Juels, Tetraktys, a `cryptographic thriller' \(Dag-Erling Smørgrav\)](#)

• [Volume 25 Issue 77 \(Tuesday 1 September 2009\)](#)

- [UK Chinook helicopters grounded for *years* due to software problems \(Danny Burstein\)](#)
- [DNA Evidence Can Be Fabricated, Scientists Show \(Monty Solomon\)](#)
- [Computer-driven class schedules \(David Leshner\)](#)
- [Computer to blame for man's fiery death \(Gene Wirchenko\)](#)
- [RFI isn't all harmless: turns on oven \(David Leshner\)](#)
- [Pepper-spray ATMs \(Jeremy Epstein\)](#)
- [The VA erroneously informs over a thousand vets of fatal diagnosis \(Rob McCool\)](#)
- [ROTC Computer Files Found in the Public Domain \(Monty Solomon\)](#)
- [Hackers break into police computer as sting backfires \(Andrew Pam\)](#)
- [3 Indicted in Theft of 130 Million Card Numbers \(Monty Solomon\)](#)
- [AT&T unable to protect Kevin Mitnick's account \(David Magda\)](#)
- [Swiss Data Protection orders Google Streetview offline \(Peter Houppermans\)](#)
- [Canadian model gets Google to unmask nasty blogger \(Simon Avery via PGN\)](#)

- [Cannot print on Tuesdays! \(Phil Colbourn\)](#)
- [GSM's A5/1 cipher being brute forced \(David Magda\)](#)
- [The Pirate Bay Returns With Guns Blazing \(jidanni\)](#)
- [Bad questions for account retrieval \(Jeremy Epstein\)](#)
- [Take only pictures *we* like \(David Leshner\)](#)
- [Re: Kentucky election fraud indictments \(Drew Dean\)](#)
- [Stephen Albin. The Art of Software Architecture \(David Schneider\)](#)

• [Volume 25 Issue 78 \(Monday 14 September 2009\)](#)

- [South Africa's Telkom: For the Birds or Not For the Birds \(Gene Wirchenko\)](#)
- [OLPC: Sic Transit Gloria Laptopi \(jidanni\)](#)
- [Smart Cars? \(Gene Wirchenko\)](#)
- [Boston city employees routinely deleted e-mail \(D.Slack/M.Levenson via Monty Solomon\)](#)
- [Networks and Nationalization With Respect to Cyberwar \(jidanni on Suresh Ramasubramanian\)](#)
- [Heavy Data Use Puts a Strain on AT&T Service \(Jenna Wortham via Monty Solomon\)](#)
- [Snow Leopard: A gigabyte by any other name \(Monty Solomon\)](#)
- [Humbert Humbert \](#)
- [Quantum Chip Helps Crack Code \(Anne-Marie Corley via Monty Solomon\)](#)
- [Nonprofit for collecting info on SCADA & PCS security incidents \(Stephanie Neil via PGN\)](#)
- [Utah Gets Tough With Texting Drivers \(Matt Richtel via Monty Solomon\)](#)
- [Re: UK Chinook helicopters grounded for *years* \(Peter Duncanson\)](#)
- [Bertrand Meyer, *Touch of Class*, Springer, 2009 \(PGN\)](#)
- [Re: VA erroneously informs over a thousand vets \(Alexandre Peshansky\)](#)
- [Interesting disclaimer added by my ISP to the latest RISKS \(Glenn Chambers\)](#)

• [Volume 25 Issue 79 \(Friday 25 September 2009\)](#)

- [Complex Machinery: a parody \(Ken Knowlton\)](#)
- [Los Angeles Drought Restrictions: Unintended Consequences? \(Thomas Russ\)](#)
- [More on the DC Metro collision 22 June 2009 \(David Leshner\)](#)
- [New York Nuclear Plant Mistakenly Bares Emergency Alarm \(PGN\)](#)
- [Air Force loses control of autonomous aircraft, shoots it down \(Rob McCool\)](#)
- [Policemen's sanitary habits result in high breathalyzer reading \(Matt Fichtenbaum\)](#)
- [Children's hospital in Ohio infected with spyware \(Rob McCool\)](#)
- ['Robot' computer to mark English essays \(Polly Curtis via Tom Heathcote\)](#)
- [Swiss watchdog sets court ultimatum for Google Street View \(Peter Houppermans\)](#)
- [*NYTimes* Web Ads Show Security Breach \(Matthew Kruk\)](#)
- [Google Buys reCAPTCHA, Creating a Potential Privacy Issue \(Lauren Weinstein\)](#)
- [DMAchoice.org - a case study in how to run an insecure website \(Jonathan Kamens\)](#)
- [Retailer Must Compensate Sony Anti-Piracy Rootkit Victim \(jidanni\)](#)
- [Re: Quantum chip helps crack code \(Steve Wildstrom\)](#)

• [Volume 25 Issue 80 \(Friday 9 October 2009\)](#)

- [The computers did it -- differently \(Wendell Cochran\)](#)
- [Lobstermen Get Wrong Number for a Hot Line \(Ian Austen via PGN\)](#)
- [Swine flu brings down Kaiser Permanente servers \(Tony Lima\)](#)
- [Restricted manual on avoiding leaking sensitive data is leaked \(Mark Thorson\)](#)
- [Subject: Mass. Blue Cross physicians' personal info on stolen laptop](#)
- [\(Kay Lazar via Monty Solomon\)](#)
- [Airline status display follies \(Steven Bellovin\)](#)
- [For Washington Metro, it's the appearance of risk \(Jeremy Epstein\)](#)
- [Man forged 12,500 pounds worth of train tickets \(Mark Brader\)](#)
- [System diversity helps in power control system \(Jeremy Epstein\)](#)

- [How Hackers Snatch Real-Time Security ID Numbers \(Saul Hansell via Monty Solomon\)](#)
- [Perils of password reuse plus password security hall of shame \(Jonathan Kamens\)](#)
- [WordPress inadvertent disclosure bug \(Jonathan Kamens\)](#)
- [The risks of being cute, Re: Complex Machinery: a parody \(Donald Norman, PGN, Bluejay\)](#)
- [Re: Snow Leopard: A gigabyte by any other name \(Phil Hobbs\)](#)
- [Re: South Africa's Telkom: For the Birds or Not For the Birds \(Richard Botting\)](#)
- [Re: Software never fails, people decide that it does \(Paul Robinson\)](#)

• [Volume 25 Issue 81 \(Monday 12 October 2009\)](#)

- [Microsoft's Danger Data Service disrupts users \(John F. McMullen\)](#)
- [Microsoft's Danger SideKick and cloud computing \(Daniel Eran Dilger via Monty Solomon\)](#)
- [Microsoft's Sidekick due to dogfooding/sabotage \(Daniel Eran Dilger via Monty Solomon\)](#)
- [Cloud Danger, literally... M\\$ loses T-mobile data \(David Leshner\)](#)
- [Excess CAT scan radiation -- the return of Therac 25? \(David Leshner\)](#)
- [A Time Machine time bomb \(Ron Garret\)](#)
- [Why E-mail No Longer Rules \(Jessica E. Vascellaro via Monty Solomon\)](#)
- [Re: Airline status display follies \(Peter R Cook, Arthur Flatau\)](#)
- [Re: The risks of being cute \(Rob Seaman, Ken Knowlton\)](#)
- [Re: The computers did it -- differently \(Wendell Cochran\)](#)
- [Re: Software never fails, people decide that it does \(Martyn Thomas, Michael Smith, Geoffrey Brent, Dimitri Maziuk\)](#)

• [Volume 25 Issue 82 \(Tuesday 20 October 2009\)](#)

- [Toyota uncontrolled acceleration \(David Leshner\)](#)
- [Another Therac-25 rerun \(Jeremy Epstein\)](#)
- [Custom license plate lands man a database full of fines \(Rob McCool\)](#)
- [Risks of namespace conflicts among city names \(Cody Boisclair\)](#)
- [More on hospital error leads to radiation overdoses \(Gene Spafford\)](#)
- [Internet Pioneers Speak Out on Net Neutrality \(Lauren Weinstein\)](#)
- [Accessing your legacy \(Peter Bernard Ladkin\)](#)
- [Re: A Time Machine time bomb \(Alan J Rosenthal\)](#)
- [Re: Microsoft's Danger Data Service \(David Leshner, John Murrell via John F. McMullen\)](#)
- [Inexcusable Complexity, Re: The risks of being cute \(Ed Lowry\)](#)
- [Re: The risks of being cute \(Curt Sampson\)](#)
- [Re: System diversity helps in power control system \(Ian Botham\)](#)
- [Rethinking What Leads the Way: Science, or New Technology? \(John Markoff on W. Brian Arthur, via PGN\)](#)
- [Computers, Freedom and Privacy 2010 Conference: Call for Proposals \(CFP\)](#)

• [Volume 25 Issue 83 \(Friday 6 November 2009\)](#)

- ["Jimmy Carter era" computer causes traffic jams \(Jeremy Epstein\)](#)
- [Central Traffic unControl === gridlock \(David Leshner\)](#)
- [Washington Metro system communications depend on single data center \(Jon Eisenberg\)](#)
- [T-Mobile suffers major outage: nationwide or nearly so \(Lauren Weinstein\)](#)
- [File share leaks data on US Congress members under investigation \(Jeremy Epstein, PGN\)](#)
- [Fugitive caught via Facebook updates \(Mark Brader\)](#)
- [Facebook 'Suggests Contacting Dead Friends' \(Matthew Kruk\)](#)
- [Massive Gene Database Planned in California \(David Talbot via Jim Schindler\)](#)
- [Drivers ticketed for not speaking English - misapplication of UI \(Frank Jimenez\)](#)
- [Privacy of health care info & health insurers \(Henry Baker\)](#)
- [Spam forged from .gov and .mil \(PGN\)](#)
- [AMEX sends USB trojan keyboards in ads \(David Leshner\)](#)
- [Risks of Using Encryption \(Roger Grimes via Gene Wirchenko\)](#)

- ['Robot' computer to mark English essays \(Polly Curtis via Randall\)](#)
- [Is Net Neutrality a Communist Plot? "Declassified DoD Film" \(Lauren Weinstein\)](#)
- [Speaking of cable modem insecurity \(Danny Burstein\)](#)
- [Re: Toyota uncontrolled acceleration \(Anton Ertl, Matt Roberds\)](#)
- [Re: Danger and Paris Hilton \(Peter Houppermans\)](#)

• [Volume 25 Issue 84 \(Wednesday 25 November 2009\)](#)

- [Apostrophe in Your Name? You Can't Fly! \(Chris J Brady\)](#)
- [NY area bank claws back over 50,000 pension payments \(Danny Burstein\)](#)
- [Hacking ring steals \\$9 million from ATMs globally \(Gadi Evron\)](#)
- [Teleportation via Skyhook \(Jerry Leichter\)](#)
- [Warren Buffett cell phone skills: did they doom Lehman? \(jidanni\)](#)
- [Two Are Charged With Helping Madoff Falsify Records \(Robert Schaefer\)](#)
- [Brevity of text message leads to rumor of death \(Mark Brader\)](#)
- [Nasty iPhone Worm Hints at the Future \(Robert Lemos via Jim Schindler\)](#)
- [Australian Emergency operator hangs up; no street address \(Darryl Smith\)](#)
- ["Your smart meter is watching" \(Cavoukian-Polonetsky via David Magda\)](#)
- [Failure begets failure? \(Aahz\)](#)
- [At Checkout, More Ways to Avoid Cash or Plastic \(Matthew Kruk\)](#)
- [Mafia Wars CEO Brags About Scamming Users From Day One \(Matthew Kruk\)](#)
- [NY State Proposing Laws to Restrict Trucker Use of GPS \(jidanni\)](#)
- [Re: Jimmy Carter era" computer causes traffic jams \(JosephKK\)](#)
- [Re: Drivers ticketed for not speaking English \(Jerry Leichter\)](#)
- [REVIEW: "Security and Usability", Lorrie Faith Cranor/Simson Garfinkel \(Rob Slade\)](#)

• [Volume 25 Issue 85 \(Saturday 28 November 2009\)](#)

- [London's stock exchange crashes again \(John Oates via Kevin Pacheco\)](#)
- [Your wallet in the cloud \(Martin Ward\)](#)
- [Used ATM Machines for Sale on Craigslist \(Ben Moore\)](#)
- [The Joy of satellite navigation failures \(Steve Loughran\)](#)
- [Re: Toyota Toyota uncontrolled acceleration \(David Leshner, JC Cantrell\)](#)
- [Patients' data used as Packing \(Robert \(Bob\) Waixel\)](#)
- [Re: Apostrophe in Your Name? You Can't Fly! \(Andy Behrens, JosephKK, Dag-Erling Smørgrav, Bob Frankston\)](#)
- [Re: Warren Buffett cell phone skills: did they doom Lehman? \(Curt Sampson, Henry Baker\)](#)
- [Re: Teleportation via Skyhook \(Charles Wood\)](#)
- [Android Mythbusters \(Matt Porter via jidanni\)](#)
- [Solving the Android "Grayed Out Application" Deadlock \(Lauren Weinstein\)](#)

• [Volume 25 Issue 86 \(Monday 14 December 2009\)](#)

- [Stryker Operating Room System II Surgical Navigation System recall \(Richard Cook\)](#)
- [Northwest Flight 188 \(Curt Sampson\)](#)
- [Chase Quicken and MS Money bill pay broken for 2 weeks, no fix ETA \(John Rivard\)](#)
- [UK Digital Economy Bill -- Blocking Illegal Downloaders \(Chris D.\)](#)
- [Massive New UK Internet Wiretapping Plan Announced \(Lauren Weinstein\)](#)
- [Public servant fired over leak of private info of 14,000 \(Gene Wirchenko\)](#)
- [Farmer claims GPS led him to breed clams in the wrong place \(Rob McCool\)](#)
- [My mother regarding LED traffic lights and Wisconsin winters \(Richard Cook\)](#)
- [Were you talkin' to me? \(Jerry Leichter\)](#)
- [All the best efforts gone to naught... \(Jeremy Epstein\)](#)
- [Various Internet Issues, Succinctly Put \(Peter Ladkin\)](#)
- [Re: The Joy of satellite navigation failures \(Jerry Leichter\)](#)

• [Volume 25 Issue 87 \(Tuesday 15 December 2009\)](#)

- [A Deluge of Data Shapes a New Era in Computing \(John Markoff via PGN\)](#)
- [Forensics, COFEE, and Decaf \(PGN\)](#)
- [Encryption Considered Harmful \(Curt Sampson\)](#)
- [Toronto subway line closed for 6 hours after tunnel pierced by gas line crew \(Tony Harminc\)](#)
- [Happy Holidays? \(Zach Tudor, Jeremy Epstein\)](#)
- [Re: The Joy of satellite navigation failures \(Michael D. Sullivan\)](#)
- [Re: Teleportation via Skyhook \(Jonathan de Boyne Pollard\)](#)
- [Re: Android Mythbusters \(Phil Colbourn\)](#)
- [Re: Toyota uncontrolled acceleration \(Jeremy Epstein, Graham Reed\)](#)

• [Volume 25 Issue 88 \(Saturday 26 December 2009\)](#)

- [Insurgents Hack U.S. Drones \(PGN\)](#)
- [Another user interface fatal accident in Afghanistan \(Mark Thorson\)](#)
- [Security in the Ether: Cloud Computing? Or "Swamp" Computing? \(Lauren Weinstein\)](#)
- [HP's facial-recognition can't recognize black people's faces \(Randall Webmail\)](#)
- [Alert: Twitter apparently hacked \(Lauren Weinstein\)](#)
- [Silent Hybrid Nearly Causes Carbon Monoxide Poisoning \(Bob Gezelter\)](#)
- [UAL: Another risk of weather for computer based systems \(Jared Gottlieb\)](#)
- [When the human model doesn't match the system model \(Sean W. Smith\)](#)
- [Disconnects between the Real World and Cyberspace \(Bob Gezelter\)](#)
- [Obscure GPS problems not just in remote areas \(Jeremy Epstein\)](#)
- [On the Road with a GPS System \(Gene Wirchenko\)](#)
- [GPS ads for captive bus riders \(jidanni\)](#)
- [Cruise control failed to disengage \(Steve Cody\)](#)
- [Re: LED Traffic Lights are efficient but cannot melt away snow \(John Johnson\)](#)

• [Volume 25 Issue 89 \(Thursday 7 January 2010\)](#)

- [Y2K+10 problem 1: German contactless bank cards \(Debora Weber-Wulff\)](#)
- [Y2K+10 problem 2: Symantec \(PGN\)](#)
- [Y2K+10 problem 3: Bank of Queensland Eftpos system \(Jared Gottlieb\)](#)
- [Y2K+10 problem 4: SpamAssassin tags "2010" e-mail as spammish \(Danny Burstein\)](#)
- [Y2K+10 Bug, for those who thought that Y2K was a made up crisis \(Bob Gezelter\)](#)
- [Verizon: I just don't know what to say \(Geoff Kuenning\)](#)
- [Eurostar Risks \(Anthony Thorn\)](#)
- [Display: none; visibility: hidden; overflow: hidden \(jidanni\)](#)
- [Crumbling Crypto: RSA 768 modulus factored + security implications \(PGN\)](#)
- [Couple Stuck in Oregon Snow for 3 Days After GPS Leads Them Astray \(Richard Grady\)](#)
- [Risks of Relying on Downstream Syndication \(Bob Gezelter\)](#)
- [Re: Teleportation via Skyhook \(Gary Bliesener\)](#)
- [Toyota acceleration: is it just the gas pedal or not? \(David Leshner\)](#)
- [Re: Another user interface fatal accident in Afghanistan \(Curt Sampson\)](#)
- [Re: LED Traffic Lights are efficient ... \(Dick Mills, Jerry Leichter,](#)
- [Amos Shapir, Rob Seaman\)](#)

• [Volume 25 Issue 90 \(Friday 8 January 2010\)](#)

- [NIST-certified USB Flash drives with hardware encryption cracked \(PGN\)](#)
- [Skype: the case of disappearing telephone numbers \(Chrisf J Brady\)](#)
- [Libel by Twitter? \(Al Stangenberger\)](#)
- [Risks of USB chargers for cell phones \(Paul Pomes\)](#)
- [Y2K+10: look at the Hex \(Dave Hansen\)](#)

[Y2K+10: what's underlying? \(Chris Smith\)](#)

- [Y2K+10: The problems with sticky tape \(Peter Houppermans\)](#)
- [Weight of a Land Rover incorrectly input into UK VCA database \(Matthew Wilson\)](#)
- [Re: Eurostar RISKS \(Richard Pennington\)](#)
- [Leaves on Tracks \(Curt Sampson\)](#)
- [Re: LED Traffic Lights are efficient \(Dick Mills, Terrence Enger\)](#)
- [Re: Silent Hybrid Nearly Causes Carbon Monoxide Poisoning \(Walt Strickler\)](#)
- [NDSS Program \(Internet Society\)](#)

• [Volume 25 Issue 91 \(Tuesday 19 January 2010\)](#)

- [New Massachusetts unemployment insurance employer website crashes and burns upon launch \(Jonathan Kamens\)](#)
- [Moscow grinds to a halt: spoofed traffic signs? \(PGN\)](#)
- [Despite Risks, Internet Creeps Onto Car Dashboards \(Matthew Kruk\)](#)
- [Software Firms Fear Hackers Who Leave No Trace \(Markoff/Vance via PGN\)](#)
- ["--b" parsed as a double-negation \(jidanni\)](#)
- [Network flaw connects Facebook users to wrong accounts \(Steven J Klein\)](#)
- [Fraudulent Facebook group leads to malware scam \(Matthew Kruk\)](#)
- [A5/3 attack \(Alexander Klimov\)](#)
- [S&P loses 8.5% \(Daniel P.B. Smith\)](#)
- [Dangerously wrong trailer weight in Web tool \(Rex Sanders\)](#)
- [Australian man dies after being crushed by computers \(Darryl Smith\)](#)
- [Update Your XZZZY Web Site Password \(Dale E. Coy\)](#)
- [Offensive shutting down of botnets \(Kelly Jackson Higgins via PGN\)](#)
- [Y2K+10 problem 1910 in BPCS 8.1 ERP \(Al MacIntyre\)](#)
- [Y2K+10: Windows Mobile has 2010 problems too \(Jeremy Epstein\)](#)
- [Y2K? Taiwan, N. Korea calendars facing Y1C in 2011! \(jidanni\)](#)
- [Re: Couple Stuck in Oregon Snow for 3 Days After GPS Leads](#)
- [Them Astray \(Al Stangenberger\)](#)
- [Other Traffic Risks \(Gene Wirchenko\)](#)
- [REVIEW: "Into the Breach", Michael J. Santarcangelo \(Rob Slade\)](#)

• [Volume 25 Issue 92 \(Tuesday 26 January 2010\)](#)

- [*NY Times* expose on medical radiation overexposure \(Jeremy Epstein\)](#)
- [Air-traffic control glitch due to the installation of new software \(Chiaki Ishikawa\)](#)
- [Extending TCP/IP into space \(Randall Webmail\)](#)
- [Y2K+10 and SMS \(Richard Gadsden\)](#)
- [Bodyscanners that don't work \(Peter Houppermans\)](#)
- [Corporate espionage in the news: Hilton and the Oil industry \(Gadi Evron\)](#)
- [Have the Chinese Really Hacked into MSN's DB? \(Chris J Brady\)](#)
- [Cyberattacks on Google in China \(PGN\)](#)
- [Unsearchable stores \(Mark Brader\)](#)
- [ICSI claims "effectively perfect" spam blocking method \(Lauren Weinstein\)](#)
- [LORAN being retired \(David Magda\)](#)
- [PROVINCE OF CHI \(jidanni\)](#)
- [Google Maps won't be taking my address for a ride \(jidanni\)](#)
- [Upgrading a World of Warcraft account ends in tears \(Turgut Kalfaoglu\)](#)
- [Unique PINs \(Dag-Erling Smørgrav\)](#)
- [Re: Offensive shutting down of botnets \(Dick Mills\)](#)
- [Cloud Computing Security \(Ivan Arce\)](#)

• [Volume 25 Issue 93 \(Friday 29 January 2010\)](#)

- [Doug Maughan's CACM article & Roadmap for Cybersecurity Research \(PGN\)](#)
- [UI fix freezes NYSE, affects 975 stocks \(T Byfield\)](#)
- [False positives galore in SARs \(Geoff Kuenning\)](#)
- [DC Metro - only kills average of 1 customer each 3 years \(Paul Robinson\)](#)
- [GPS Control Software Glitch: NANU Issued \(PGN\)](#)
- [How Not to Design Authentication \(Alexander Klimov\)](#)
- [Radiation Offers New Cures, and Ways to Do Harm \(David Hollman\)](#)
- [Warning: Your Cell Phone May Be Hazardous to Your Health \(Christopher Ketcham via PGN\)](#)
- [Driver watching laptop movie kills woman \(Walter Roberson\)](#)
- [It depends on which bus you take \(Paul Robinson\)](#)
- [Driving and walking through buildings \(Pete Kaiser\)](#)
- [Re: Teleportation via Skyhook \(Tony Lima\)](#)
- [Re: Extending TCP/IP into space \(Mark Jackson\)](#)

• [Volume 25 Issue 94 \(Sunday 14 February 2010\)](#)

- [Electronic Systems That Make Modern Cars Go \(Jim Motavalli\)](#)
- [Toyota Braking Problem Link \(Gene Wirchenko\)](#)
- [How computers took over our cars \(Amos Shapir\)](#)
- [Ex-Toyota lawyer points to electronic throttle control \(PGN\)](#)
- [Motor racing solution to Toyota runaway \(Dave Crooke\)](#)
- [Mercedes Benz E Class Commercial \(Richard S. Russell\)](#)
- [Medical privacy: They never, ever learn \(Geoff Kuenning\)](#)
- [Who Owns Your PC? \(Lauren Weinstein\)](#)
- [EMV busted \(David Magda\)](#)
- [Website glitch drives up parking penalty \(Nick Rothwell\)](#)
- [The Century Bug will repeat ... \(Jonathan de Boyne Pollard\)](#)
- [Making the grade or changing the grade? \(Jeremy Epstein\)](#)
- [Phishing Scam Cripples European Emissions Trading \(Danny Burstein\)](#)
- [Meta-spearphishing \(Jeremy Epstein\)](#)
- [CAPTCHA with the answer in the ALT text \(jidanni\)](#)
- [Re: GPS Control Software Glitch: NANU Issued \(Andy Piper\)](#)
- [Re: Unsearchable Stores \(Bob Bramwell\)](#)

• [Volume 25 Issue 95 \(Sunday 28 February 2010\)](#)

- [Growing Threat to GPS Systems From Jammers \(Jerry Leichter\)](#)
- [Sat-nav systems under growing threat from 'jammers' \(Amos Shapir\)](#)
- [More on Risks of EMV Legacy Compatibility \(Anthony Thorn\)](#)
- [Self-Signed Certificates Strike Again? \(Bob Gezelter\)](#)
- [Facebook friended, boyfriend offended, tragically ended \(John Linwood Griffin\)](#)
- [Google: Serious threat to the web in Italy \(Monty Solomon\)](#)
- [Fault-Tolerance as a Risk \(Gene Wirchenko\)](#)
- [School District Spying on Students at Home? \(Gene Wirchenko\)](#)
- [A Message from Ric Edelman about data lost \(fjohn reinke\)](#)
- [Nationwide Technetium shortage: coinciding reactor failure/maintenance \(Richard I. Cook\)](#)
- [IEEE Symposium on Security and Privacy: 30th anniversary \(David Evans\)](#)
- [FOSE 2010 \(Kalin Tyler\)](#)

• [Volume 25 Issue 96 \(Saturday 13 March 2010\)](#)

- [Silly season: DST is approaching \(David Magda\)](#)
- [Sony PS3: Yet Another leap year folly \(Steve Summit\)](#)
- [Sony thinks 2010 is a leap year \(Debora Weber-Wulff\)](#)
- [Old models of PS3 failed to connect to network due to leap-year miscalculation \(Chiaki Ishikawa\)](#)

- [Re: The Century Bug Will Repeat \(Jerry Leichter\)](#)
 - [Death in the Atlantic: The Last 4 Minutes of Air France Flight 447 \(F John Reinke\)](#)
 - [Software flaws may be at the root of Toyota's woes \(Gene Wirchenko\)](#)
 - [Risk: Toyota secretive on 'black box' data \(AP via Gabe Goldberg\)](#)
 - [Breakthrough in Electron Spin Control Brings Quantum Computers Closer to Reality \(NSF\)](#)
 - [German Data Retention Law Overturned \(Bob Gezelter\)](#)
 - [USGov rescinds 'leave Internet alone' policy \(Richard Forno\)](#)
 - [Man posts "wanted" poster of himself on own Facebook page \(Mark Brader\)](#)
 - [Car insurance bug \(Clive D.W. Feather\)](#)
 - [Daily cyber attacks on the UK \(Martyn Thomas\)](#)
 - ["Traffic analysis" from data \(David Magda\)](#)
 - [Paranoia 101 \(Paul Wexelblat\)](#)
 - [Risks of having friends with computers \(Rob McCool\)](#)
 - [Computer core risks \(Robert Schaefer\)](#)
 - [4th International Conference on Network and System Security \(NSS 2010\)](#)
 - [IEEE Symposium on Security and Privacy \(Ulf Lindqvist\)](#)
- [Volume 25 Issue 97 \(Friday 26 March 2010\)](#)
- [Unmanned goods train crash in Norway \(Martyn Thomas\)](#)
 - [NRC to VA: you endangered patients, you owe us \\$227k \(Danny Burstein\)](#)
 - [FBI Faces New Setback in Computer Overhaul \(Eric Lichtblau via David Leshner\)](#)
 - [IRS systems can't be trusted \(Randall Webmail\)](#)
 - [Risks to the power grid \(Gary McGraw\)](#)
 - [Pwn2Own 2010: iPhone hacked, SMS database hijacked \(Ryab Naraine via Monty Solomon\)](#)
 - [Warnings about Wifi-enabled air travel \(David Strom via Gabe Gold\)](#)
 - [Cops inadvertently harass couple: real address used as test data \(Mark Brader\)](#)
 - [Police raid wrong address 50+ times \(David Leshner\)](#)
 - [UK SAS base "exposed" through Google Streetview \(Peter Baker\)](#)
 - [Netflix Data De-anonymized \(Bob Gezelter\)](#)
 - [Hacked "miss a payment, brick your car" system \(Jeremy Epstein\)](#)
 - [Colombian vote count delayed \(PGN\)](#)
 - [Surveillance via bogus SSL certificates \(Matt Blaze\)](#)
 - [More on School Webcam Scandal \(Gene Wirchenko\)](#)
 - [Couldn't logout from Facebook Mobile \(jidanni\)](#)
 - [Re: Old models of PS3 failed to connect to network \(DoN Nichols\)](#)
- [Volume 25 Issue 98 \(Thursday 1 April 2010\)](#)
- [The 2010 Census as of April 1 \(Rebecca Mercuri\)](#)
 - [Silver Iodide Can Seed Cloud Computing \(PGN\)](#)
 - [Clouding Men's Minds \(Cecelia Kang via PGN\)](#)
 - [CalJOBS Security is a Mess \(Tony Lima\)](#)
 - [Why Won't USPS Let Me File This Complaint? \(Jim Reisert\)](#)
 - [Incorrect software change to emergency ambulance call-handling system may have resulted in hundreds of deaths \(Bruce Horrocks\)](#)
 - [Ohioans are dunned for long-paid fines \(\(Peter Zilahy Ingerman\)](#)
 - [User-friendly speed cameras in Belgium \(Peter Houppermans\)](#)
 - [Academic Paper in China Sets Off Alarms in U.S. \(Markoff/Barboza\)](#)
 - [Water-treatment computer: No, not the Three Stooges, but close \(Jeremy Epstein\)](#)
 - [3.3 million student-loan records pilfered \(Gene Wirchenko\)](#)
 - [Old-fashioned computer risks, Re: 3.3 million student-loan data \(Jeremy Epstein\)](#)
 - [High-tech copy machines a gold mine for data thieves \(David Hollman\)](#)
 - [Survey: Millions of users open spam e-mails, click on links \(Dancho Danchev via Monty Solomon\)](#)
 - [Plain Dealer sparks ethical debate by unmasking anonymous poster \(Ferdinand Reinke\)](#)

- [In Bid to Sway Sales, Cameras Track Shoppers \(Stephanie Rosenbloom via Monty Solomon\)](#)
- [TJX Hacker Sentenced \(Gene Wirchenko\)](#)
- [USENIX Health Security and Privacy Workshop due 9 Apr 2010 \(Kevin Fu\)](#)
- [GameSec 2010: Conference on Decision and Game Theory for Security \(Albert Levi\)](#)

• [Volume 24 Issue 99 \(and RISKS 24.00 1 April 2010\)](#)

- [Info on RISKS \(comp.risks\), contributions, subscriptions, FTP, etc.](#)
- [SUMMARY OF RISKS VOLUME 25 \(7 January 2008 to April 2010\)](#)



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 1

Monday 7 January 2008

Contents

- [Fire! Works! oops, too slow](#)
[Mark Brader](#)
- [Boeing 787 networking issues](#)
[Martyn Thomas](#)
- [Feds Release Pass Card details](#)
[Brock N. Meeks via David Farber](#)
- [Has chip-and-pin failed to foil fraudsters?](#)
[Pere Camps](#)
- [Sears exposes customers' information via its web site](#)
[Rich Kulawiec via IP](#)
- [User Data Stolen From Pornographic Web Sites](#)
[David Lesher](#)
- [Election Computers Stolen in Tennessee](#)
[David Lesher](#)
- [Er, Airline Captains Do What, Again?](#)
[Rick Moen](#)
- [Risks of embedded javascript](#)
[Paul Wallich](#)
- [Mercedes console display with conflicting information](#)
[Henry Baker](#)
- [Mac Quickbooks update deletes user desktop](#)
[Bonnie Packert](#)
- [No more loose lithium batteries in checked luggage](#)
[Peter Gregory](#)
- [Risks of believing what you see on the WayBack Machine](#)
[Fred Cohen](#)
- [Re: Computer Failure Causes Closure of Seattle Downtown Transit Tunnel](#)
[Stanislav Meduna](#)
- [Re: Satnav: Nope, you can't get there from here.](#)
[Craig DeForest](#)
- [Re: Satnav](#)
[Martyn Thomas](#)
- [Re: Drunk a better guide than sat nav](#)
[Ross Younger](#)
- [Passing of Computing and Information Security Pioneer: Jim Anderson](#)

[Gene Spafford](#)

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

Fire! Works! oops, too slow

<msb@vex.net (Mark Brader)>

Wed, 2 Jan 2008 13:33:53 -0500 (EST)

Due to "a corrupted computer file", a New Year's fireworks show in Seattle had to be set off manually. Not only did that mean that the technicians had to *press all the buttons themselves*, but the display was *not properly synchronized* with the music that accompanied it! What a horrible fiasco! Oh the humanity!

http://seattletimes.nwsourc.com/html/localnews/2004102891_spaceneedle02m.html

[I suppose Manual-ed Fire could have been accompanied by Manuel De Falla. I defy-ya' to play Noches en los jardines de Seattle as accompaniment. On the other hand, if the manual operation had misfired, they might have been sheepless in Seattle. PGN]

Boeing 787 networking issues

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

Sun, 06 Jan 2008 09:56:56 +0000

The FAA has issued "special conditions" for certification of the Boeing 787. (mirrored at <http://cryptome.org/faa010208.htm>).

In part, these state:

"Novel or Unusual Design Features

The digital systems architecture for the 787 consists of several networks connected by electronics and embedded software. This proposed network architecture is used for a diverse set of functions, including the following: 1. Flight-safety-related control and navigation and required systems (Aircraft Control Domain). 2. Airline business and administrative support (Airline Information Domain). 3. Passenger entertainment, information, and Internet services (Passenger Information and Entertainment Domain). The proposed architecture of the 787 is different from that of existing production (and retrofitted) airplanes. It allows new kinds of passenger connectivity to previously isolated data networks connected to systems that perform functions required for the safe operation of the airplane. Because of this new passenger connectivity, the proposed data network design and integration may result in security vulnerabilities from intentional or unintentional corruption of data and systems critical to the safety and maintenance of the airplane. The existing regulations and guidance material did not anticipate this type of system architecture or electronic access to aircraft systems that provide flight critical

functions. Furthermore, 14 CFR regulations and current system safety assessment policy and techniques do not address potential security vulnerabilities that could be caused by unauthorized access to aircraft data buses and servers. Therefore, special conditions are imposed to ensure that security, integrity, and availability of the aircraft systems and data networks are not compromised by certain wired or wireless electronic connections between airplane data buses and networks."

According to the story in Wired

(http://www.wired.com/politics/security/news/2008/01/dreamliner_security)

"Boeing spokeswoman Lori Gunter said the wording of the FAA document is misleading, and that the plane's networks don't completely connect. Gunter wouldn't go into detail about how Boeing is tackling the issue but says it is employing a combination of solutions that involves some physical separation of the networks, known as "air gaps," and software firewalls. Gunter also mentioned other technical solutions, which she said are proprietary and didn't want to discuss in public. "There are places where the networks are not touching, and there are places where they are," she said. Gunter added that although data can pass between the networks, "there are protections in place" to ensure that the passenger Internet service doesn't access the maintenance data or the navigation system "under any circumstance." She said the safeguards protect the critical networks from unauthorized access, but the company still needs to conduct lab and in-flight testing to ensure that they work. This will occur in March when the first Dreamliner is ready for a test flight."

So that's all right, then. After all, no security problem has ever shown up after testing, has it?

[The planned test flight should be interesting. Where can you get a plane-load of suicide hackers at short notice? MT]

[This risk also spotted by Edwin Slonim

<http://www.avweb.com/eletter/archives/avflash/1028-full.html#196896>
and Ric Steinberger. PGN]

✶ Feds Release Pass Card details [from David Farber's IP]

<"Brock N. Meeks" <bmeeks@cox.net>>

December 31, 2007 4:13:01 PM EST

The government has dragged its feet in releasing the final details about its Pass Card technology, and now they dump it into the Federal Register on the last day of the year. The government has decided to go with a technology that is more suited to tracking inventory and can be read from up to 20 feet away. Govt. officials counter by saying privacy protections will be built into the cards.

Passport cards for Americans who travel to Canada, Mexico, Bermuda and the Caribbean will be equipped with technology that allows information on the

card to be read from a distance. The technology was approved on 30 Dec 2007 by the U.S. State Department. Privacy advocates were quick to criticize the Department for not doing more to protect information on the card, which can be used by U.S. citizens instead of a passport when traveling to other countries in the western hemisphere. The technology would allow the cards to be read from up to 20 feet away. The technology is "inherently insecure and poses threats to personal privacy, including identity theft," said Ari Schwartz of the Center for Democracy and Technology. [Source: Eileen Sullivan, Passport card technology criticized, Associated Press; from the Ft. Worth Star-Telegram; PGN-ed]

<http://www.star-telegram.com/464/story/384245.html>

✶ Has chip-and-pin failed to foil fraudsters?

<Pere Camps <pere@pere.net>>
Thu, 03 Jan 2008 10:31:22 +0100

Interesting Chip-and-PIN article by the Guardian here:

<http://www.guardian.co.uk/technology/2008/jan/03/hitechcrime.news>

[Purveyors and law enforcement folks say crime is down.
The article says maybe not. (Starkly PGN-ed)]

✶ Sears exposes customers' information via its web site (via IP)

<Rich Kulawiec [rsk@gsp.org]>
Fri, 4 Jan 04 2008 1:26 PM

[From David Farber's IP group]

Summary: if you know someone's name, address and phone number, you can retrieve their purchase history from Sears' web site.

<http://www.benedelman.org/news/010408-1.html>

This is an interesting follow-on to the recent discovery that Sears is pushing spyware:

<http://community.ca.com/blogs/securityadvisor/archive/2007/12/20/sears-com-join-the-community-get-spyware.aspx>
<http://www.benedelman.org/news/010108-1.html>

✶ User Data Stolen From Pornographic Web Sites

<"David Leshner" <wb8foz@panix.com>>
Sun, 6 Jan 2008 21:39:13 -0500 (EST)

Consumers of Internet pornography who secretly signed up for memberships on adult-oriented Web sites in the past few months may be in for a shock -- some of their personal information, including e-mail addresses, may have been compromised by a security breach. The breach has raised serious alarm in the world of adult-oriented Web sites, with many concerned about the effect on customers if they learn that their most secret transactions are not so secret after all. [Source: *The Washington Post, 3 Jan 2008]
http://www.washingtonpost.com/wp-dyn/content/article/2008/01/03/AR2008010303549_pf.html

[This gives new meaning to "Porn site exposes ... PGN]

✂ Election Computers Stolen in Tennessee

<David Lesher <wb8foz@nrk.com>>
Fri, 28 Dec 2007 21:21:09 -0500

Thieves stole laptop computers containing the names and social security numbers of every registered voter in the city from election commission offices over the Christmas holiday. The computers also contain voters' addresses and phone numbers. [Associated Press, 28 Dec 2007]

[In David Farber's IP, Brad Malin noted an article by Michael Cass in the *Tennessean*, 3 Jan 2008. The building had weekend 12-hour periods without guards, and had no alarms or video surveillance. PGN]
<http://www.tennessean.com/apps/pbcs.dll/article?AID=/20080103/NEWS0202/801030369>

✂ Er, Airline Captains Do What, Again?

<rick@linuxmafia.com (Rick Moen)>
Sun, 30 Dec 2007 18:25:15 -0800

A nicely articulate Blog piece of *The New York Times* about TSA-screening absurdities drew the usual litany of wry anecdotes and complaints, but this one stood out for its peerless irony value:
<http://jetlagged.blogs.nytimes.com/2007/12/28/the-airport-security-follies/index.html>

#61. 29 Dec 2007

About two years after 9/11 I was selected at random by a TSA agent for additional security screening at an airport checkpoint. I was asked to remove my hat, shoes, belt, and jacket, after which I was told to spread my arms and legs for electronic "wanding".

When I asked why I had been chosen for the extra attention, two more agents quickly appeared, and their unsmiling faces emphasized that airport security was, indeed, very serious business. "We need to be sure you don't have anything you can use to take control of an aircraft", the screener told me. I will never forget the absurdity of his words.

You see, I was, in fact, about to take control of an aircraft, an Airbus A320 to be precise, and fly it up the Potomac River to LaGuardia. That's what airline Captains like me get paid to do. That's why I had showed up at the airport in full uniform, properly credentialed and ready to go.

Security was then, and remains now, largely a sham. It's all about politics and the appearance of vigilance. It's about collecting pocket knives from forgetful, but otherwise law-abiding people.

We have been lead to believe that we now have the best secured aviation system in the world. And if success is measured with flow-charts, color codes, and administrative name changes, maybe we do.

In truth, we have all been let down by the very people in charge. They would have us believe that they are actually addressing security issues, when in fact they are doing little more than staging public relations theater.

Posted by Rick Reahr

Plus ça change.... My father, Pan Am Captain Arthur Moen always marveled at the foolishness of taking pocket knives from airline pilots, and tried fruitlessly for decades to get the airlines and FAA to install intrusion-resistant cabin doors, something they did only three decades after his death (by defective jet).

✂ Risks of embedded javascript

*<Paul Wallich <pw@panix.com>>
Mon, 07 Jan 2008 10:57:08 -0500*

This one is old, but I bet it still bites plenty of people who would know better if they gave it a thought. Last night I was configuring a new wireless access point, and after some gymnastics getting it to show up on my wired network (it comes hard-coded to an inconvenient IP address) I got ready to configure the password, same as the old one. So I clicked on the setup page of the browser-based configuration program, and nothing. WEP, but no WPA. I checked the package; it claimed to do WPA. I read the instructions; there was the part about setting WPA encryption and a screen shot that looked nothing like the one in front of me.

Then I remembered that my browser is set by default to disallow javascript. I told it that I trusted my wireless access point, and suddenly a whole raft of new options and menus appeared on my screen. Obviously it's convenient for widget designers to be able to use javascript for their user interfaces, but nowadays the user without javascript is more likely to be tech-savvy (and slightly paranoid) rather than a luddite with an outdated browser. (This in turn leads to an unlikely but attractive risk scenario where an attacker embeds browser-eating malware in one of the myriad software libraries that the typical widget designer pulls together to make a working machine; if you can't trust your access point, whom can you trust?)

#Mercedes console display with conflicting information

<Henry Baker <hbaker1@pipeline.com>>

Fri, 14 Dec 2007 10:48:39 -0800

[Henry sent me a photo that he might have taken himself. PGN]

The console display says "check engine" & "no malfunction" at the same time!
Dueling messages!

It is supposed to say "check engine" & "1 malfunction", if "check engine" is
the only malfunction being reported.

BTW, my ever-lying Verizon DSL line finally got fixed after replacing about
4 bad splices. (The computer kept calling me to tell me that the
malfunction in my phone line had been fixed, but since it hadn't, the good
news rolled over into voice mail!) I think that the old-style POTS phone
system is now in its state of "graceful decline", and will join the
hand-cranked phone on the dustbin of history within 15 years.

#Mac Quickbooks update deletes user desktop

<Bonnie Packert <bpsubs943@hyperlogic.com>>

Mon, 31 Dec 2007 12:50:41 -0800

On Sunday 16 Dec 2007, I ran Quickbooks 2006 on my Mac. I got an error that
said there was not enough room to download an update, that it needed 100
bytes (!). I thought it was likely a bad error message because I do not
normally use an account that has administrator access, so it probably was
unprepared for some protection violation and gave a bad error message. I
logged in as admin to try to get the updated but got the same error. I
checked the Inuit Quickbooks web site and found that I already had the
latest version available. When I logged back into my regular account, I
discovered my desktop was empty, that the folders and files had
disappeared. Using a shell I saw that the Desktop directory was now a
regular file with 0 bytes. After some disk integrity checks and cleanup
that failed to pinpoint a problem, I later ran Quickbooks again and realized
that my Desktop had ben trashed again. Searching online, I discovered a
number of Quickbooks Mac users had been similarly afflicted.

By 9am PST Monday morning, Intuit had corrected the problem on their server.
Unfortunately, this was after a large number of users had lost files. A
representative from the company called to collect information about my
situation and explained that it had been a scripting problem in the server,
which incorrectly deleted user information after no update had been found.

I was surprised that I never saw anything about it in mainstream press. Here
are some links about the issue from the Quickbooks community web site. More

is available by googling "Quickbooks deletes desktop".

<http://quickbooksgroup.com/webx/forums/mac/1917>

<http://quickbooksgroup.com/webx/forums/mac/1907>

✂ No more loose lithium batteries in checked luggage

<Peter Gregory <petergregory@yahoo.com>>

Mon, 31 Dec 2007 15:03:07 -0800 (PST)

In a move to prevent lithium battery fires on commercial aircraft, U.S. airline passengers will no longer be able to pack loose lithium batteries in checked luggage beginning 1 Jan 2008 once new federal safety rules take effect. The new regulation, designed to reduce the risk of lithium battery fires, will continue to allow lithium batteries in checked baggage if they are installed in electronic devices, or in carry-on baggage if stored in plastic bags.

Common consumer electronics such as travel cameras, cell phones, and most laptop computers are still allowed in carry-on and checked luggage. However, the rule limits individuals to bringing only two extended-life spare rechargeable lithium batteries, such as laptop and professional audio/video/camera equipment lithium batteries in carry-on baggage - but none in checked baggage.

Entire press release here: <http://tinyurl.com/29fnue>

Peter Gregory, CISA, CISSP | petergregory@yahoo.com | www.isecbooks.com
Skypeid peterhgregory | Join InfraGard

✂ Risks of believing what you see on the WayBack Machine (archive.org)

<Fred Cohen <fred.cohen@all.net>>

Mon, 31 Dec 2007 06:56:36 -0800

I have now encountered 2 legal cases in 3 months in which a plaintiff saw images on the WayBack Machine (www.archive.org) and believed that they indicated events in the past that never happened. To provide some insight into the problem, and to provide proof to our legal system, I arranged a small demonstration that risks readers might want to take a look at:

Disable javascript in your Web browser.

Goto the URL <http://www.archive.org/>.

Enter "<http://all.net/>" into the WayBack Machine (and click as appropriate).

Select the entry from 1997.

At this point, you will see what all.net looked like in 1977 - or so you would think. But look at the picture on the right side of the page about half-way down. You might want to open that picture in a new window to get a

clear look at it.

I think you will agree that the WayBack Machine cannot always be counted on for digital forensic evidence. This demonstration has now been used in a US Federal Court case.

Fred Cohen & Associates tel/fax: 925-454-0171
<http://all.net/> 572 Leona Drive Livermore, CA 94550
Join <http://tech.groups.yahoo.com/group/FCA-announce/join> for our mailing list

Re: Computer Failure Causes Closure of Seattle Downtown Transit Tunnel

*<Stanislav Meduna <stano@meduna.org>>
Sun, 06 Jan 2008 11:23:53 +0100*

> Who would have thought a tunnel would be subject to a computer
> failure? ... Too many eggs in one basket...

Sometimes you only have one basket...

I worked on SCADA software that runs in quite a few tunnels in Europe.

A modern tunnel is a complex system where the subsystems are connected in ways that require to be controlled by a (logically) single computer system. E.g. a fire event starts a sequence where everything is involved - sensors spot the gases, signs switch to red on the entry, fans switch to a mode sucking out the smoke, staff is alerted etc. Everything has to be logged (preferably tamper-resistantly) so that there is evidence what happened and how the staff reacted. Surely the lower level systems will go to sane failsafe values in the case of problems, but nobody will risk to operate such system in full traffic with major subsystems disabled.

This application is normally redundant so there is no hardware single point of failure, but this of course does not guard against programming errors, inadequate testing and other things well-known to the RISKS reader.

Tunnel retrofitting is not an easy task, normally much worse than building one from scratch - the main problem is that you have to interface things you are probably not familiar with that are given and the number of interfaces explodes.

And let me tell you, when there was a real fire in a tunnel controlled by our software, we were very relieved that everything worked as expected. One is never sure that the tests caught everything...

Re: Satnav: Nope, you can't get there from here.

*<Craig DeForest <deforest@boulder.swri.edu>>
Mon, 31 Dec 2007 12:48:18 -0700*

Reading the various satnav articles (Shapir, [RISKS-24.91](#), Jacobson, [RISKS-24.92](#)) reminds me of my own favorite satnav folly.

My 2007 Prius has a satnav. Recently, I tried to navigate from Boulder, Colorado to Sunspot, New Mexico (Google directions: "<http://tinyurl.com/ywwbvz> ") for an observing run at the National Solar Observatory. The nav system found Sunspot OK, and the onscreen map showed the dedicated state highway (NM 6563) but asserted that there was no route there from here.

Likewise, once I was at the observatory, the system wouldn't let me navigate to practically anywhere else in the U.S.! I played with it a bit and found the key -- force it to route through the nearby town of Cloudcroft.

I believe Toyota's nav system uses a regress-to-the-nearest-highway algorithm, which fails spectacularly for Sunspot: the nearest U.S. highway (US54) is only about 7 horizontal miles away at closest approach, but nearly a mile down in altitude. To get to the observatory you have to take a much longer, windier route through Cloudcroft -- it's nearly 40 miles (as the car winds) from the closest approach point.

Google Maps finds the route perfectly.

✉ Satnav (Ashworth, [RISKS 24.93](#))

<Martyn Thomas <martyn@thomas-associates.co.uk>>
Mon, 31 Dec 2007 10:03:08 +0000

It's a little troubling to me that none of the articles that seem very popular lately on "how dangerous it can be to depend entirely on your satellite navigator" make clear the point that GPS is very susceptible to in-band jamming (either accidental or deliberate) and that it is steadily becoming a single point of failure for private transport, commercial transport, and the emergency services.

Navigation systems based on the known location of cell-phone transmitters would be more resilient.

✉ Re: Drunk a better guide than sat nav (Ashworth, [RISKS-24.93](#))

<Ross Younger <crazyscot@gmail.com>>
Thu, 3 Jan 2008 11:16:26 +0000

A friend of my father's drives a taxi for a living, and recently fitted a satnav to it.

Now, whenever a customer gets in, he offers them a choice - do they want to go by the satnav's directions, or by his idea of the best route?

Most people opt for the satnav. This makes him happy; he has been driving for years and knows all the tricks for getting around town, whereas the satnav - following its own idea of "best" - tends to get stuck in jams (with the meter running, of course).

"Best" route for him, perhaps, not for his customers? Reportedly the satnav paid for itself within a few weeks!

✈ Passing of Computing and Information Security Pioneer: Jim Anderson

<Gene Spafford <spaf@cerias.purdue.edu>>

Wed, 2 Jan 2008 20:08:22 -0500

On 18 Nov 2007, noted computer pioneer James P. Anderson, Jr., died at his home in Pennsylvania. Jim, 77, had finally retired in August. Jim, born in Easton, Pennsylvania, graduated from Penn State with a degree in Meteorology. From 1953 to 1956 he served in the U.S. Navy as a Gunnery Officer and later as a Radio Officer. This later service sparked his initial interest in cryptography and information security.

Jim was unaware in 1956, when he took his first job at Univac Corporation, that his career in computers had begun. Hired by John Mauchly to program meteorological data, Dr. Mauchly soon became a family friend and mentor. In 1959, Jim went to Burroughs Corporation as manager of the Advanced Systems Technology Department in the Research Division, where he explored issues of compilation, parallel computing, and computer security. While there, he conceived of and was one of the patent holders of one of the first multiprocessor systems, the D-825. After being manager of Systems Development at Auerbach Corporation from 1964 to 1966, Jim formed an independent consulting firm, James P. Anderson Company, which he maintained until his retirement.

Jim's contributions to information security involved both the abstract and the practical. He is generally credited with the invention and explication of the reference monitor (in 1972) and audit trail-based intrusion detection (in 1980). He was involved in many broad studies in information security needs and vulnerabilities. This included participation on the 1968 Defense Science Board Task Force on Computer Security that produced the "Ware Report", defining the technical challenges of computer security. He was then the deputy chair and editor of a follow-on report to the U.S. Air Force in 1972. That report, widely known as "The Anderson Report", defined the research agenda in information security for well over a decade. Jim was also deeply involved in the development of a number of other seminal standards, policies and over 200 reports including BLACKER, the TCSEC (aka "The Orange Book"), TNI, and other documents in "The Rainbow Series".

Jim consulted for major corporations and government agencies, conducting reviews of security policy and practice. He had long-standing consulting arrangements with computer companies, defense and intelligence agencies and telecommunication firms. He was a mentor and advisor to many in the

community who went on to prominence in the field of cyber security. Jim is well remembered for his very practical and straightforward analyses, especially in his insights about how operational security lapses could negate strong computing safeguards, and about the poor quality design and coding of most software products.

Jim eschewed public recognition of his many accomplishments, preferring that his work speak for itself. His accomplishments have long been known within the community, and in 1990 he was honored with the NIST/NCSC (NSA) National Computer Systems Security Award, generally considered the most prestigious award in the field. In his acceptance remarks Jim observed that success in computer security design would be when its results were used with equal ease and confidence by average people as well as security professionals - a state we have yet to achieve.

Jim had broad interests, deep concerns, great insight and a rare willingness to operate out of the spotlight. His sense of humor and patience with those earnestly seeking knowledge were greatly admired, as were his candid responses to the clueless and self-important.

With the passing of Jim Anderson the community has lost a friend, mentor and colleague, and the field of cyber security has lost one of its founding fathers.

Jim is survived by his wife, Patty, his son Jay, daughter Beth and three grandchildren. In lieu of other recognition, people may make donations to their favorite charities in memory of Jim.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 2

Monday 14 January 2008

Contents

- [Coffee Grounds Qantas](#)
[Charles Wood](#)
- [Computer problem suspected in erratic Airbus flight](#)
[Antonomasia](#)
- [Metal structure beneath runway affects aircraft instruments](#)
[David Dixon](#)
- [Polish teenager uses city trams as train set](#)
[Peter Houppermans](#)
- [Novel approach to reducing electoral fraud](#)
[Peter Mellor](#)
- [Risks of believing a GPS system](#)
[Paul Karger](#)
- [GPS in a tea shop anecdote](#)
[Mark Brader](#)
- [More GPS mishaps](#)
[Paul Saffo](#)
- [Nightmare on VoIP Street](#)
[Ed Ravin](#)
- [A risk of static analysis tools -- and refereeing](#)
[Peter Gutmann](#)
- [Bank gives money to fraudster posing as its chairman](#)
[David Dixon](#)
- [REVIEW: "Managing Knowledge Security", Kevin C. Desouza](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

☛ Coffee Grounds Qantas

<"Charles Wood" <j.charles.wood@gmail.com>>
Fri, 11 Jan 2008 18:39:51 +0900

Qantas Flight QF2 from London To Sydney via BKK (Bangkok) (a Boeing 747-400) suffered a total AC electrical loss 15 minutes before landing at BKK on 8

January 2008. The effect of the AC loss was that all AC powered equipment in the aircraft stopped working and the crew was forced to revert to standby battery power for instrumentation. A number of electrically controlled sub-systems were disabled. Some passenger cabin services were re/started including emergency lighting. The crew landed successfully at BKK but with reduced functionality. Power was available only to the Captains PFD, ND and standby Attitude indicator. They also had to contend with alt gear/flap extension, no anti-skid, no autobrakes, and no thrust reverser.

Inspection of the aircraft showed that water from the first class galley had overflowed down onto the sub-floor E racks which contained the GCU's (controllers for engine generators) and BPCU (backup PCU) All controllers were disabled resulting in total loss of AC power. The remaining power source was the inverter that generated power from the backup battery. Luckily his was out of reach of the flood so kept working.

Extrapolation of this event to long-haul flights over sea would have seen loss of all navigation aids and communications, and reliance of the crew on basic aids - if available - such as magnetic compass and sight of stars or sun.

The incident cause was most probably a combination of factors and events that finally resulted in a major problem.

1. The fiberglass drip shield above the E rack had a crack that allowed water to drip through.
2. The last C check at Avalon depot did not discover and remedy the crack. (QF maintenance as opposed to outsourced).
NB. As of 11 January ABC Radio News disclosed that six other QF x -- 747's were found to have cracked drip trays.
3. Flooding of the first class cabin from the galley is a regular occurrence, usually from ice trays but also from blocked drains.
4. When the galley floods the water goes down onto the equipment bay directly below.
5. The galley drains in first class on OJM at BKK were blocked by coffee grounds.
6. Qantas has changed from 'pillow' style coffee bags to ground coffee machines - based on cost saving. This results in the possibility of coffee grounds being dumped in the galley sinks.
7. First class in Qantas has a cappuccino machine (also producing coffee grounds).

When you look at it, there are a number of problems that in their own right are perhaps acceptable but in conjunction are a major problem.

- Fundamentally the overflow system for the galley should have been forced to flow to non critical areas.
- The rack drip tray should have been sound and if not the inspection should have picked that up and remedied it.
- The drainage system in the galley should have been immune to blockage.
- The cabin staff should have been trained to avoid provoking blockages in the drain system.
- Qantas should have avoided operational changes (coffee system) that would enable cabin staff to block the drain system.

As a final note. If Seven QF 744 aircraft have cracked drip trays, how many aircraft with other operators have the same problem?

<http://www.smh.com.au/news/travel/powerhit-qf2-finally-touches-down/2008/01/09/1199554718579.html>

✂ Computer problem suspected in erratic Airbus flight

<ant@notatla.org.uk (Antonomasia)>

Fri, 11 Jan 2008 00:54:26 +0000

An Air Canada flight that rolled suddenly from side to side then plunged in the air may have suffered technical problems, according to passengers interviewed after the plane was diverted to Calgary. ... there had been a computer failure and that they were flying the plane manually ..

<http://www.cbc.ca/canada/calgary/story/2008/01/10/injuries-landing.html?ref=rss>

Antonomasia ant notatla.org.uk See <http://www.notatla.org.uk/>

✂ Metal structure beneath runway affects aircraft instruments

<"David Dixon" <dgxon9@gmail.com>>

Thu, 10 Jan 2008 17:44:40 +0000

London City Airport has warned pilots their instruments may be affected by magnetic interference from metal structures found below the runway.

A report was carried out after an aeroplane was forced to turn back when its autopilot system failed.

Railway lines, and other metal structures left from the days when the airport was a dock, were found to be causing "significant interference".

A spokeswoman said action would be carried out "wherever necessary".

An investigation was launched by the Air Accident Investigation Branch (AIB) after a jet was unable to follow a standard departure route, because of an autopilot problem, after taking off on 31 October 2006.

<http://news.bbc.co.uk/1/hi/england/london/7181021.stm>

✂ Polish teenager uses city trams as train set

<Peter Houppermans <peter@houppermans.com>>

Fri, 11 Jan 2008 16:32:20 +0100

Here is an item that almost defies belief:

A Polish 14-year-old boy allegedly turned the tram system in the city of Lodz into his own personal train set, triggering chaos and derailing four vehicles in the process. Twelve people were injured in one of the incidents. He modified a TV remote control so that it could be used to change track points. Four trams were derailed, and others had to make emergency stops that left passengers hurt. [Source: *The Register* (<http://theregister.co.uk>); PGN-ed]

My observation is that whoever designed those weakly protected remote control capabilities must not have thought about the consequences either -- and that was supposedly a paid adult.

Peter Houppermans, Houppermans GmbH, Zurich, Switzerland

[Also noted by Michael Hogsett, and by Mike Radow, who commented: "Given the idiocy of such an unprotected system, any comment would be superfluous." PGN]

Novel approach to reducing electoral fraud

<MellorPeter@aol.com>

Wed, 9 Jan 2008 15:10:54 EST

The New York Times, 7 Jan 2008

<http://www.nytimes.com/2008/01/07/opinion/07poundstone.html?th&emc=th>

The idea, proposed by Ronald L. Rivest of MIT and Warren D. Smith, is that votes are cast on paper and tallied by scanner or by hand. After casting their vote, each voter is given a photocopy of a randomly selected ballot ****cast by another voter****. (A serial number, but no name, is on each ballot.)

At the end of the day, all votes cast are entered on a web site. The holder of each copy connects to the site and confirms that the ballot whose copy they hold is present and correct, or not. The theory is that, even with a low proportion of web confirmations, any electoral malpractice will be revealed with a high degree of confidence, and that the knowledge that the scheme is in force will, in any case, deter any attempt to rig the ballot.

Comments on the article put forward most of the obvious objections, which are answered by the author or by Smith. There are links to the papers in which Rivest and Smith describe their method in detail.

Peter Mellor +44 (0)20 8459 7669 MellorPeter@aol.com

Risks of believing a GPS system

<Paul Karger <karger@watson.ibm.com>>

Tue, 08 Jan 2008 09:35:59 -0500

A driver of a rental car turned right when the GPS unit said to turn right. Unfortunately, he turned onto the Metro North Harlem line railroad tracks in Westchester County, NY, instead of proceeding another 20 feet or so to turn onto the Saw Mill River Parkway. The car became stuck on the tracks, and was hit by a northbound train a short time later. No one was injured, as the driver had run down the tracks to try to warn the train to stop, but the train could not stop in time. About 500 passengers were stranded for 2 hours, and train service from Grand Central Terminal was delayed for several hours, while they repaired damage to the electrified third rail.

The driver was from California and not familiar with the local roads, but the railroad crossing was very well marked and had crossing gates, which were up at the time (as the train didn't arrive until somewhat after the driver got stuck).

I've been through this crossing many times, and my impression is it is quite confusing to people exiting from the Saw Mill Parkway, but that for people ENTERING the Parkway, as this person was doing, the tracks are pretty obvious.

Full details here:

<http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20080103/NEWS01/801030409/1020/NEWS04>

and here:

<http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20080104/NEWS02/801040377/1020/NEWS04>

[Also noted by Edward Rice. Led astray by "GI Jane", the man is (or was) a computer consultant! PGN]

http://news.yahoo.com/s/ap/20080104/ap_on_fe_st/odd_gps_train_crash

***GPS in a tea shop anecdote**

<msb@vex.net (Mark Brader)>

Thu, 20 Dec 2007 04:59:10 -0500 (EST)

* From: "Richard Chambers" <richard.chambers7_NoSpam_@ntlworld.net>
* Newsgroups: alt.usage.english
* Subject: Re: Fings we was lernt rong in skool (Was Basrawis n all that cop)
* Message-ID: <eScaj.10711\$h35.10683@newsfe2-gui.ntli.net>
* Date: Wed, 19 Dec 2007 17:51:06 GMT

Philip Eden wrote

>>>

>>> Learning where places are in Geography.

>>

>> Quaintly out of date? Has King's Lynn become Peterborough, and

>> Peterborough Aberdeen, in the last x years?

>>

> I see the opposite effect. I had lunch with the head of school (of
> geography) at my old university (Brummagem) last year, and she
> was bemoaning the lack of interest most of her charges have in
> maps when they come up, and how difficult it now is to enthuse
> them when they are there. Maps, of course, are no longer called
> maps; they are now GIS (geographical information systems).
> We were both thoroughly sniffy about satnav: "I don't need satnav;
> I'm a geography graduate." Sad to say that sentiment doesn't apply
> to many (most?) recent geography graduates.

I have much the same feeling. I love maps, especially the new Ordnance Survey 2.5 inch = 1 mile series. Living in Leeds, we have the Dales, North York Moors, Peak District, Forest of Bowland, Yorkshire Wolds, Howardian Hills, and the Lake District, all within easy driving distance. To my wife's despair, I keep on buying Ordnance Survey maps for all these areas, but my collection is now nearing completion. GPS does not tell you where the good walks are. You need to be able to interpret the Ordnance Survey map if you want to plan a good walk for yourself. Furthermore, you need to know how to specify a Grid Reference point if you are going to use GPS to its full potential. I enjoy the mental challenge of finding my way by use of a map. GPS would rob me of that simple pleasure.

The following little story might be (i.e., probably is) an urban legend. My wife has a friend, who has a friend, who bought a GPS system for his car, and used it to go somewhere in Gloucestershire. On the way, he stopped off in Bourton on the Water for a cup of tea. Because GPS systems are worth quite a lot of money, and are easily removed, they are a sure reason for having your car broken into if you leave them on display. So, exactly as advised, he removed it, put it in his pocket, and started walking from the car park to find a tea shop. As he was walking towards the centre of the town, he suddenly heard a now-familiar voice saying "Turn left after 30 metres". He couldn't turn it off, so he just ignored it. "You've missed the turn". Then later: "Turn back, you must turn back". This instruction became annoyingly insistent. Eventually, he managed to turn it off, or at least, he thought he had. He went into a tea shop and ordered a pot of tea and some scones. "Turn back, you must turn round, then turn right after 100 metres".
>From time to time, the other customers in the tea shop were treated to further rather insistent directions while he drank his tea and ate his scone.

More GPS mishaps

<Paul Saffo <psaffo@mac.com>>
Thu, 10 Jan 2008 08:23:52 -0800

Not a new story, but a very nice writeup about the problem in the UK with GPS systems not knowing the appropriateness of roads for large trucks.

Mark Rice-Oxley, *The Christian Science Monitor*, 10 Jan 2008
<http://www.csmonitor.com/2008/0110/p20s01-woeu.html>

Satellite navigation systems send trucks down the wrong routes in Britain

Drivers end up rolling through towns on roads meant for a horse and cart. Can people please stop running into Ena Wickens's roof?

Mereworth, England

With its winding country lanes and parish church, its 18th-century cottages and sleepy allotments, life is gentle and agreeable in this bucolic southeast English village. Or at least it was until the truck drivers started coming through.

First there was the Slovenian driver en route to Wales with a load of paper who took an improbable detour and ended up wedging his juggernaut into a tiny lane. It was stuck for two days.

Then there were the 10-wheelers that wheezed their way up Butcher's Lane, a thin ribbon of a road constructed with horse and cart in mind. One made a mess of the roof on Ena Wickens's cottage, which lies flush to the lane. No sooner had it been repaired than another truck snorted its way up the roadway and crumpled part of the roof again.

"It's such a worry," says Ms. Wickens as she putters around the garden behind her cozy Jane Austen cottage. "This last time, it was lucky I was in, otherwise he would just have driven off. There is a sign at the bottom of the road saying 'Unsuitable for large vehicles,' but still they come."

Why, exactly, do they come? The answer is to be found in the satellite navigation kits (satnav for short) that are handy for getting motorists from one location to another, but not always judicious in selecting the most appropriate routes.

Legendary examples already exist of satnav equipment leading gullible drivers astray. There have been cars driving into streams, a woman who was directed the wrong way up a freeway, and even an ambulance crew that was diverted 200 miles by mistake.

There was the bus party looking forward to a day trip to Lille in northern France that was spirited off to the less fabulous Lille, Belgium, 100 miles away by mistake.

In Britain, satnav technology is generating a second, related problem of trucks plowing unwittingly into country lanes unsuitable for anything larger than small passenger vehicles.

One driver, for instance, stranded his 50 foot-wagon up a lane for three days in Ivybridge, southwest England, until a tractor could be found to tow it out. Another driver wedged a tractor-trailer on a bridge in the same part of the country that was finally released by cutting down hedges and trees. And then there was the coach operator who became stuck on a small roadway -- only to escape by driving through nearby fields.

Satellite navigation has turned one country lane in Wales into a virtual gill net, ensnaring almost every truck that comes along: One could only be

set free recently by knocking down a stone wall. And last month, a Lithuanian lorry driver was stuck for four days after his vehicle became wedged on a rural roadway more suitable for sheep than trucks.

Mereworth's unwanted encounter with modern navigation stems in part from an accident of geography. The hamlet lies close to a main freeway that runs from the port of Dover north to London and main transit routes to northern England.

Situated in Kent =96 the "garden of England" =96 Mereworth is a quaint mix of ancient and modern, an 18th-century church and castle and red-brick cottages alongside more modern detached homes. Tiny lanes thread their way improbably through hop fields and dwellings with no sidewalks. Most truckers barreling up the nearby freeway would probably have deep reservations about a set of directions that steered them into the village's serpentine streets. But not everyone is familiar with the back roads of Britain, nor always puts the right display screen on their dashboard.

"A lot of continental drivers are using systems which are not equipped for heavy vehicles," says Dennis Styles of Mereworth's parish council. "The cheaper models lead them down these narrow lanes. We have horse-and-cart roads from the early 1900s and they are now taking these huge vehicles" down them.

Villages up and down the country are howling about the sudden invasion of snorting trucks filling up tiny streets originally built for carriages. Some have even asked to be "wiped off the map."

In Wedmore, southwest England, the council wants urgent action to refine satnav software to make it more sensitive =96 and sensible. "It's happening on a daily basis," says council chairman John Sanderson. "We've had people's properties being damaged. There are no pavements, so big vehicles have to go close to properties. We get gridlock where police have had to come along and sort it out. When we talk to the HGV [heavy goods vehicle] drivers from the continent and ask them why they keep coming through, they say they have been sent by the satnav."

Mapping companies admit the technology is still in its infancy and acknowledge that improvements need to be made. "The road network is immense" says a spokesman for Tele Atlas, an international digital mapping company.

"GPS navigation is still a new technology, and the road network changes every year. So there's a constant updating process that needs to be done. What is happening is that haulier companies are using navigation devices that are specific to passenger cars."

Help may be at hand, though. Tele Atlas says it has launched a more sophisticated device for hauliers that can request what vehicle is being driven and then navigate them through the most appropriate route. The national mapping agency, Ordnance Survey, which produces road network data for satnav software companies, is refining its maps to show routes that big rigs should avoid. The aim is to provide a more intelligent picture of Britain's roads, which are used by more than 100,000 trucks a day.

"We want to get freight route maps recommended by all the local authorities into one consistent single format, agree on it, and make it available as part of our data," says Paul Beauchamp of Ordnance Survey.

He admits that the errant trucking problem has become worse in recent years. "There are more HGVs on the road than ever before, and more and more people are using satnavs," he says. "The more they are used, the higher the number of cases becomes."

But the trucking industry is wary of efforts to "redraw" the map to keep trucks off small roads. They warn that with the extraordinary growth in home deliveries, triggered principally by the rise in online shopping, big vehicles will still have to navigate small lanes.

"It's also worth saying that improved satnavs won't themselves solve all the problems," says Geoff Dossetter of the Freight Transport Association, an industry group that represents more than 200,000 truckers. "At the end of the day, it still comes down to the driver -- if he ignores the fact he's driving off a cliff or into a pond, it's his own fault more than the satnavs."

All of which means Ena Wickens will probably want to keep the name of her roofer handy.

Nightmare on VoIP Street

<Ed Ravin <eravin@panix.com>>

Wed, 9 Jan 2008 14:50:16 -0500

A friend of mine uses Vonage for her primary phone line. Their VoIP system gave her a nightmarish experience during the wee hours of December 15.

The problem started around midnight - her VoIP phone rang, and caller-ID showed it was a number local to her area, but she didn't recognize it. She answered, but there was no one on the line. Her phone rang again several minutes later - same caller-ID, again no one there. And a few minutes later, the phone rang again, same caller-ID, same nobody there.

Then her cell phone rang. The cell phone's caller-ID showed the same phone number as her VoIP phone did. Again, the line was dead when she answered it. Twice more in short order, the phantom caller rang her cell phone.

Now wide awake and rather disturbed, she went to her computer to look up the phone number of her putative persecutor. Google helpfully provided a reverse directory lookup - to a person with an Arabic-sounding name that she did not recognize. With the help of Mapquest, she found out that this unknown person lived only a few miles from her. Worried and feeling vulnerable, she was unable to get to sleep, thinking that a strange person in the neighborhood was calling both her home phone and cell phone for no apparent reason.

At 3 in the morning, her VoIP phone rings again - this time, the caller-ID says that her own cell phone is making the call! But the cell phone is turned off and is sitting on her nightstand. She finally smells the rat, and at 4 AM calls the Vonage customer support line. After a 30 minute wait, a polite but difficult-to-understand person explains that Vonage has been experiencing a problem with "phantom calls" and it should be resolved soon.

My friend had her Vonage account set up so that if her VoIP number was down, it would automatically forward calls to her cell phone. So Vonage's software PBX had her cell phone number on file, and it apparently went haywire and began placing calls to numbers in its database, and using other numbers in its database as the caller-ID.

The biggest risk here is believing what you see on your caller-ID display. Using computerized tools to compound your error and jump to the wrong conclusions is a close second. Then there's the well-known "mission creep" risk, where data supplied for one purpose is (mis) used for another. Even though the misuse was unintentional, it's a stark reminder that phone numbers are a special kind of data with real-world implications, especially when in the hands of buggy software that can make phone calls.

It took three days before Vonage sent my friend an email notice acknowledging the phantom calls. Apparently this incident was part of a much larger outage (the SIP of the iceberg?), as described here:

<http://www.dslreports.com/forum/r19627147-Vonage-outage~start=20>

and here:

<http://valleywag.com/tech/breakdowns/if-a-vonage-falls-in-the-woods-does-it-make-a-sound-334855.php>

✂ A risk of static analysis tools -- and refereeing

*<pgut001@cs.auckland.ac.nz (Peter Gutmann)>
Wed, 09 Jan 2008 20:04:07 +1300*

[This item is adapted, with permission, from a posting to another group. PGN]

Interesting anecdote: Some years ago a simple static code analysis tool was submitted to a conference. Two of the three reviewers, both of whom were extremely careful programmers, ran it on their own code just to see what would happen.

The tool produced 100% false positives (not 95, not 99, but fully 100%). As a result, the paper wasn't accepted.

The same paper was later submitted to another conference (where reviewers didn't try this), where it was accepted and won the best paper award.

[Possible] Moral: The sort of people who contribute to RISKS may not be

representative of programmers as a whole.

Bank gives money to fraudster posing as its chairman

<"David Dixon" <dgxon9@gmail.com>>

Thu, 10 Jan 2008 17:49:49 +0000

A fraudster walked into a branch of Barclays Bank (A major UK bank) posing as its chairman Marcus Agius and managed to walk out with 10,000 pounds (c. \$20,000). The conman is believed to have found Mr Agius' details online and persuaded call centre staff into issuing a Barclaycard (credit card) in his name. <http://news.bbc.co.uk/1/hi/business/7181741.stm>

REVIEW: "Managing Knowledge Security", Kevin C. Desouza

<Rob Slade <rmslade@shaw.ca>>

Fri, 14 Dec 2007 11:26:50 -0800

BKMAKNSE.RVW 20070927

"Managing Knowledge Security", Kevin C. Desouza, 2007, 0-7494-4961-6, U\$65.00/UK#32.50

%A Kevin C. Desouza secureknow.blogspot.com kev.desouza@gmail.com

%C 120 Pentonville Rd, London, UK, N1 9JN

%D 2007

%G 0-7494-4961-6 978-0-7494-4961-2

%I Kogan Page Ltd.

%O U\$65.00/UK#32.50 +44-020-7278-0433 kpinfo@kogan-page.co.uk

%O <http://www.amazon.com/exec/obidos/ASIN/0749449616/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0749449616/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0749449616/robsladesin03-20>

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

%P 200 p.

%T "Managing Knowledge Security"

Desouza is of the "competitive intelligence" community, so the "knowledge" of the title refers to special skills, processes, or other information that gives your business a particular advantage, and which is either unknown or in limited circulation elsewhere.

Chapter one provides some examples of thefts of intellectual property. The author also exhorts companies to classify and assign a value to their informational assets (with which advice I can only heartily concur). He goes on to describe the activities involved in spying on corporations, and notes the limitations of traditional security guards in this regard.

Chapter two explains how employees can be the greatest threat to the loss of institutional knowledge--and can also be the biggest asset in protecting it.

Considerations with regard to personal computing devices (such as laptops and advanced cell phones) for traveling executives are discussed in chapter

three. As well, there are suggestions on how to avoid being kidnapped, and some recommendations with respect to recycling paper and obsolete computer equipment. Chapter four looks at a range of the possible alliances between companies, and the ways that various problems related to intellectual property might occur as a result of those associations. Chapter five contains recommendations of diverse measures to limit physical access to corporate offices. Business continuity is addressed, in chapter six, from the perspective of loss of knowledge resources. (Oddly, there is little discussion of the higher levels of risk from social engineering inherent in such situations.) Basic information security practices, threats, and technologies are outlined in chapter seven.

The book presents an interesting viewpoint in regard to security, but does not seem to break any new ground. In terms of information security or classification, this work does not go beyond any standard security text such as the original edition of "Computer Security Basics" (cf. BKCMPSEC.RVW) or (ISC)2's "Official Guide" (cf. BKOITCE.RVW). With regard to social engineering, which one might consider a specialty of those in the "business intelligence" field, any of Ira Winkler's volumes, such as "Corporate Espionage" (cf. BKCRPESP.RVW) or "Spies Among Us" (cf. BKSPAMUS.RVW), has more detail and extensive suggestions. Desouza's work, clear and engaging as it is, is possibly an interesting additional outlook, but hardly a necessary addition or replacement.

copyright Robert M. Slade, 2007 BKMAKNSE.RVW 20070927
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 3

Tuesday 29 January 2008

Contents

- [Data entry error leads to incompatible transplant](#)
[Mark Brader](#)
- [London Heathrow plane crash](#)
[Colin Stamp](#)
- ["Butterfly Award": French Bank Says Trader Hacked Computers](#)
[Henry Baker](#)
- [Henhouses, guarding of, by foxes: Kerviel Kerfuffle](#)
[Steve Summit](#)
- [Problems with the German tax software "Magpie"](#)
[Debora Weber-Wulff](#)
- [Florida computer problems halt early voting](#)
[PGN](#)
- [The risks of upgrading software](#)
[Clive D. W. Feather](#)
- [Charter Cable deletes 14,000 e-mail accounts. No backups.](#)
[Danny Burstein](#)
- [IRS: Kansas City lost our tapes. Lots of personal info....](#)
[Danny Burstein](#)
- [Automated parking garage reopens](#)
[Rich Mintz](#)
- [Blue Screened Asphalt Jungle...](#)
[David Lesher](#)
- [Windows virus protection on NASA Linux machines](#)
[David Lesher](#)
- [Authors, pseudonyms, and software](#)
[Steven M. Bellovin](#)
- [Re: Metal structure beneath runway affects aircraft instruments](#)
[Roderick A Rees](#)
- [Re: Boeing 787 networking issues](#)
[Mark Siegel](#)
- [Re: Coffee Grounds Qantas](#)
[Brian Hayes](#)
- [Re: More GPS mishaps](#)
[Joel Maslak](#)
[Dag-Erling Smørgrav](#)

[Paul Saffo](#)

• [REVIEW: "Fuzzing", Michael Sutton/Adam Greene/Pedram Amini](#)

[Rob Slade](#)

• [Info on RISKS \(comp.risks\)](#)

✂ Data entry error leads to incompatible transplant

<msb@vex.net (Mark Brader)>

Thu, 24 Jan 2008 17:11:43 -0500 (EST)

It was revealed recently that in 2005 a kidney was transplanted in Liverpool, England, into a patient with the wrong blood type, due to an erroneous entry in the UK Transplant database. The error was noticed a few hours after surgery and the kidney was removed. The patient recovered successfully from the double surgery, but they're not saying what happened to the patient after that.

The error was apparently made at the Royal Liverpool and Broadgreen University Hospitals Trust, with UK Transplant merely recording the information. A spokesperson for the trust says that "A thorough investigation was concluded in 2006 and a series of improvements have been made" and there have been no more such incidents.

<http://www.liverpooldailypost.co.uk/liverpool-news/regional-news/2008/01/21/patient-given-wrong-kidney-transplant-64375-20374300/>

✂ London Heathrow plane crash

<Colin Stamp <Colin.Stamp@uk.ibm.com>>

Fri, 18 Jan 2008 12:22:32 +0000

All 136 passengers and 16 crew escaped from the British Airways flight BA038 from Beijing. Eighteen people were taken to the hospital with minor injuries. An airport worker told the BBC the Boeing 777 pilot (Peter Burkill, 43) said he had lost all power and had to glide the plane in to land. The worker also said the pilot had told him all the electronics had also failed. "He said he had no warning - it just went," the worker added. "It's a miracle. The man deserves a medal as big as a frying pan."

See the BBC Web Article:

<http://news.bbc.co.uk/1/hi/england/london/7194086.stm>

Colin Stamp, IBM United Kingdom Limited PO Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU

✂ "Butterfly Award": French Bank Says Trader Hacked Computers

<Henry Baker <hbaker1@pipeline.com>>

Sun, 27 Jan 2008 18:05:51 -0800

FYI -- If all else fails, blame it on the computer... Since this one trader may have singlehandedly upset the world's markets last week, I'd like to nominate him for the "Butterfly Award", which should be given to those whose actions are amplified by the nonlinearities in the world's systems in truly stupendous ways...

Societe Generale said Sunday that a trader who evaded all its controls to bet \$73.5 billion -- more than the French bank's market worth -- on European markets hacked computers and "combined several fraudulent methods" to cover his tracks, causing billions in losses. The bank says the trader, Jerome Kerviel, did not appear to have profited personally from the transactions and seemingly worked alone -- a version reiterated Sunday by Jean-Pierre Mustier, chief executive of the bank's corporate and investment banking arm. But, in a conference call with reporters, Mustier added: "I cannot guarantee to you 100 percent that there was no complicity." [Source: Jenny Barchfield and John Leicester, French Bank Says Trader Hacked Computers, Associated Press, 27 Jan 2008; PGN-ed, with memories of Nick Leeson and Barings Bank, [RISKS-16.87](#).]

Henhouses, guarding of, by foxes: Kerviel Kerfuffle

<Steve Summit <scs@eskimo.com>>

Sun, 27 Jan 2008 18:45:23 -0500

J rome Kerviel is being blamed for a \$7 billion loss at Soci t  G n rale in France. Evidently, before he became a trader, Kerviel worked in the bank's own internal fraud-prevention department, designing controls to catch suspicious trading activity. Allegations are emerging that he hacked the bank's computer systems -- i.e., those same controls -- as part of his alleged coverup.

Take the guy who designed the system to prevent questionable trades, then let him make trades. "What could possibly go wrong?"

<http://www.time.com/time/business/article/0,8599,1706661,00.html>

<http://www.washingtonpost.com/wp-dyn/content/article/2008/01/27/AR2008012700680.html>

[Later Update: A considerably more detailed account of Kerviel's alleged fraud, including the extent to which computers were involved:]

<http://www.nytimes.com/2008/01/28/business/worldbusiness/28bank.html?em&ex=1201669200&en=9787a96b4e941d12&ei=5087%0A> .

Problems with the German tax software "Magpie"

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

Thu, 17 Jan 2008 22:14:51 +0100

The Berliner Zeitung reports on 17 Jan 2008 on a problem with the German tax office's tax filing program "ELSTER" (Why on earth they call their software "magpie", especially when there is a German saying about the "thieving magpie" is anybody's guess).

<http://www.berlinonline.de/berliner-zeitung/print/politik/717364.html>

Seems the German tax system wasn't complicated enough, so they made a new rule that you can't take a deduction for travel to work unless you have to travel 21 kilometers or more each direction.

If you put in the true value when using ELSTER to submit your taxes online - such as 18 - the program returns an error and refuses to continue. If you put in a higher value than 21 (the journalist tested it with 30) then the program continues working on your taxes, but you just committed tax evasion by reporting more km than you really have.

The problem? If you just say "forget it" and skip this line, then you will have no chance to get money back from the government if this passage in tax law is struck down, which is quite probable, as many have submitted lawsuits against it.

The solution: file your taxes on paper again, make them type in all your values. Maybe then they will see that making such complicated rules confounds even their own software.

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/>

Florida computer problems halt early voting

*<"Peter G. Neumann" <neumann@csl.sri.com>>
Sat, 26 Jan 2008 13:32:41 PST*

What appears to have been a "total network failure" affected all Palm Beach County early-voting sites on 25 Jan 2008, four days before Florida's presidential primary election. Voter registration lists could not be accessed, which meant party affiliations and ballot choices could not be verified. [Source: UPI item, 25 Jan 2008]

The risks of upgrading

*<"Clive D. W. Feather" <clive@davros.org>>
Tue, 29 Jan 2008 15:22:01 +0000*

As a result of an upgrade to Vista in Ohio's Marietta High School computer systems, previously protected student information and photos were able to be accessed by unauthorized people. "It appears the students were interested in making changes to their photos in the school cafeteria system." The

photos and a student ID are used to verify charges for lunches, and officials suspected some students were manipulating the system to avoid paying for lunches. [Source: Marietta Times <<http://www.mariettatimes.com>>, PGN-ed]

Clive D.W. Feather +44 20 8495 6138 <http://www.davros.org>

✂ Charter Cable deletes 14,000 e-mail accounts. No backups.

<Danny Burstein <dannyb@panix.com>>
Thu, 24 Jan 2008 18:46:06 -0500 (EST)

(Note: there wasn't anything in either my Charter e-mail account or on their web page.)

Charter Communications officials believe a software error during routine maintenance caused the company to delete the contents of 14,000 customer e-mail accounts. There is no way to retrieve the messages, photos, and other attachments that were erased from inboxes and archive folders across the country on 21 Jan 2008. The company apparently deletes inactive accounts every three months. [Source: Jim Salter, Cable Co. Empties 14,000 E-Mail Accounts, Associated Press item, 24 Jan 2008; PGN-ed]

<http://www.newsday.com/technology/wire/sns-ap-charter-mistake,0,4378708.story>
<http://www.charter.com>

✂ IRS: Kansas City lost our tapes. Lots of personal info....

<Danny Burstein <dannyb@panix.com>>
Sat, 19 Jan 2008 22:16:30 -0500 (EST)

[Source: Lynn Horsley, KC faulted after probe of IRS tapes missing from City Hall, *The Kansas City Star*; PGN-ed]

A federal investigation of missing Internal Revenue Service tapes from City Hall in Kansas City has concluded that the city failed to follow 'proper safeguards for protecting federal tax return information.' That conclusion is contained in a heavily redacted report obtained recently by *The Kansas City Star* under a Freedom of Information Act request to the Treasury Department's inspector general for tax administration.

The inspector general's investigation stemmed from the disappearance of 26 IRS computer tapes containing taxpayer information. The tapes, which have never been found, are normally used by the city to help enforce collection of the 1 percent city earnings tax paid by people who live or work in Kansas City. ... The IRS has never said what information was on the tapes, how many taxpayers were affected, or whether those taxpayers would ever be notified about the missing information.

<http://www.kansascity.com/news/politics/story/451282.html>

Automated parking garage reopens

<Rich Mintz <richmintz@richmintz.com>>

Fri, 25 Jan 2008 09:26:30 -0500

The 314-space automated parking garage in Hoboken, New Jersey, near New York City, officially opened yesterday to local fanfare, in a ceremony marking the transfer of ownership from Unitronics (the garage's designer) to the City of Hoboken.

The garage actually opened in 2002, and there were numerous problems in the first two years, with three cars "dropped" in three years and vehicles trapped for hours or days at a time.

Video of the garage in action (courtesy of the Jersey Journal):

<http://www.youtube.com/watch?v=tcHvpi2OOK0>

Story from the Bergen Record, 25 Jan 2008:

<http://www.northjersey.com/news/transportation/14304872.html>

Story from the Jersey Journal, 25 Jan 2008:

<http://www.nj.com/news/jjournal/index.ssf?/base/news-1/1201245065129120.xml&coll=3>

Rich Mintz - richmintz@richmintz.com 201-217-8245 (desk), 646-708-5998 (cell)

Blue Screened Asphalt Jungle...

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

Mon, 14 Jan 2008 11:43:30 -0500 (EST)

<<http://www.engadget.com/2007/12/21/nyc-taxis-simply-running-mapping-app-over-unsecured-windows/>>

Those NYC Taxi & Limousine Commission mandated GPS+credit card+TV systems? Well, seems they run Windows, and [surprise!] they are, well.... hackable...

Will the warez community start awarding medallions soon? Does the open road bring new vistas of opportunity?

Windows virus protection on NASA Linux machines

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

Fri, 25 Jan 2008 19:54:45 -0500 (EST)

[I was told this story by an unSenior unAdminstration unOfficial; but I've already forgotten who it was..]

NASA Langley Research Center [LaRC] is now requiring all desktop Linux machines to be equipped with an antivirus program that detects and eliminates Windows viruses. Why? Apparently it is because there is an uncited NIST recommendation suggesting all desktop machines have virus scanners.

Of course, since some Linux machines may operate as mail servers or as file servers for Windows users, there may be causes for a virus scanner on the Linux server may be a good idea; it may be more efficient and easier to maintain a scanner there than on the client machines. But the average Linux machine does not do this, so detecting Windows viruses on them is superfluous.

The RISK? Why, anything you run on a computer can have security flaws, and anything that runs as root is that much more hazardous. A program which downloads virus signatures from a remote location then has the needed permissions to alter files based upon that data.

Now, on a Windows machine where viruses run rampant and where hourly patching seems the order of the day, that is a perfectly reasonable risk to take. On a Unix machine which does not suffer from those problems; running an antivirus program only adds risk but does not solve any actual problem.

Also, of course, we have the risk of people taking reasonable security guidelines and treating them as absolute mandates. Sadly, a lot of Federal agencies are prone to that activity.

[I wonder what LaRC is saying about OSX machines...? Further, I can see a dandy DoS attack scenario. Break into, or just buy the low bidder virus definition server company, and merely declare lots-a-files as:

Dangerous -- Must Destroy NOW

Or, use the root permissions you enjoy to zombify the machines. Sit back and enjoy the fun.]

✂ Authors, pseudonyms, and software

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Thu, 24 Jan 2008 03:39:49 +0000

I recently stumbled on this quote on a web page (http://www.sfreviews.net/lost_fleet_dauntless.html):

In an e-mail exchange, Henry explained to me the reasons for using a pseudonym for his newest opus. In addition to wanting to get away from the pigeonholing authors endure when they're known for writing one type of book, e.g. military science fiction, there's this: "The pen name was primarily driven by bookstore buying software. I've been caught (like so many others) in the decreasing orders death spiral. Based on prior sales, the chains order fewer copies, so they sell fewer, so they order even fewer, so they sell even fewer . . . The pen name short-circuits that

because the software just sees the pen name and doesn't assign any sales history to it."

I'm not sure if there's a word for how infuriating and depressing this is, that the fate of a writer's career is determined by software. Surely there have been armed insurrections over less. Okay, perhaps not, but there ought to be. After all, the notion of being consigned to oblivion by a computer seems a little too close to some of the bleaker visions of dystopian SF to me.

I think that latter paragraph sums it up nicely.

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

Re: Metal structure beneath runway affects aircraft instruments

<"Rees, Roderick A" <roderick.a.rees@boeing.com>>
Mon, 21 Jan 2008 07:52:55 -0800

(Re: Dixon, [RISKS-25.02](#))

The source of this problem was 13 locomotives provided to Britain by the USA under the Lease-Lend scheme. At the end of the Second World War, the U.S. did not want to have the locomotives returned, but under the legal terms of Lease-Lend, they could not be used after the war, nor could they be salvaged for scrap. They were therefore tipped into a water-filled hole at the end of a stub line in the Hounslow area of London, and buried. Years later (in the sixties, I believe) Heathrow was expanded, and came to include this forgotten railway graveyard. It was discovered by historical research when Heathrow wanted to put a new compass base there, and found that there was a significant magnetic anomaly.

Re: Boeing 787 networking issues ([RISKS-25.01](#))

<Mark Siegel <mark_siegel@cmail.sbcss.k12.ca.us>>
Tue, 08 Jan 2008 09:21:40 -0800

[Also Re: Malware and Auto Electronics (Klashinsky, [Risks 23.70/72](#))]

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

Re: Coffee Grounds Qantas (Wood, Re: [RISKS-25.02](#))

<Brian Hayes <bhayes@amsci.org>>

Tue, 15 Jan 2008 11:14:41 -0500

> 5. The galley drains in first class on OJM at BKK were blocked by coffee
> grounds.

Senior RISKS readers may remember the 1964 film "Fate Is the Hunter," based on an earlier book by Ernest K. Gann (who had been a pilot for American Airlines). It's the story of an aircraft crash investigation, where the cause turns out to be a cup of coffee spilled into a control console. Life imitates art. Fortunately, it's not death imitates art.

✂ Re: More GPS mishaps (Saffo, [RISKS-25.02](#))

<Joel Maslak <jmaslak@antelope.net>>

Mon, 14 Jan 2008 17:53:02 -0700

I can relate a personal experience, towing an RV trailer across the US with the help of satnav. Besides for some simply bad routing (it's idea of the quickest route between Amarillo, TX and Dallas, TX - both of which are in Texas - is via Oklahoma City, Oklahoma, which requires leaving and re-entering Texas. This route is several hours longer than the more direct route. But, that itself, is not particularly dangerous, except perhaps if CO2 emissions are considered. Rather, in Philadelphia, I saw first hand the result of the GPS routing my vehicle down a particularly unsuitable road in the Philadelphia suburbs. In the middle of this road was a one-lane iron bridge with a 3 ton (US) weight limit. My complete rig is about twice that weight, and the truck itself (a 3/4 ton Chevy diesel) is over 3 tons by itself - as I imagine many large SUVs are as well. I ended up backing up a long hill for about 3/4 of a mile, to reach a larger, more suitable road, rather than risk traveling over the bridge weighing twice as much as the bridge's capacity. The lesson? Check the maps and stick to major roads whenever possible - and when in doubt, talk to a local.

✂ Re: More GPS mishaps (Saffo, [RISKS-25.02](#))

<=?utf-8?Q?Dag-Erling_Sm=C3=B8rgrav?=> <des@des.no>>

Wed, 16 Jan 2008 15:46:17 +0100

> "It's also worth saying that improved satnavs won't themselves solve all the
> problems," says Geoff Dossetter ...

Dossetter is being too generous. It is **always** the driver's fault. I am not aware of any provision in the Vienna Convention on Road Traffic, nor in the traffic rules in force in the UK or any other country, which absolves the driver of responsibility for errors arising from the use of a faulty satellite navigation system (or a faulty paper map for that matter). Furthermore, there is no excuse for the driver not realizing that the road is too narrow or too poorly paved for his vehicle.

As far as I know, all automobile satnav systems, whether integrated or third-party, offer a disclaimer to that effect upon first use, sometimes even on every use.

[In Norway, foreign long-haul truckers, especially from Southern or Eastern Europe, are regularly involved in fatal accidents due to their ignorance - willful or otherwise - of Norwegian regulations and / or over-reliance on satellite navigation. Of course, said accidents are rarely fatal to the truckers, which may explain why they don't seem to care.]

✂ Re: More GPS mishaps ([RISKS-25.02](#))

<Paul Saffo <psaffo@mac.com>>

Fri, 18 Jan 2008 09:54:21 -0800

Well stated! It is so immensely practical that I doubt it has ever occurred to the local officials!

On Jan 18, at , Peter D. wrote:

> The article from the *Christian Science Monitor* about large trucks and
> narrow lanes was was appalling and funny (like much of comp.risks) but the
> problem is a solved one.

>

> What happens around here (Victoria, Australia) is that we don't like
> having trucks wedged tight under low bridges. So, we have a large sign
> that warns, "LOW CLEARANCE" and advises a maximum vehicle height. And
> soon after that a bright yellow steel girder hung by chains at the advised
> height. Most drivers are alert enough to stop when they hit the steel
> girder. It saves the bridge and does comparatively little damage to the
> truck.

>

> Vertical girders at the start of a narrow lane could easily do the
> analogous job.

✂ REVIEW: "Fuzzing", Michael Sutton/Adam Greene/Pedram Amini

<Rob Slade <rmslade@shaw.ca>>

Mon, 14 Jan 2008 15:42:32 -0800

BKFUZZNG.RVW 20071005

"Fuzzing", Michael Sutton/Adam Greene/Pedram Amini, 2007,
0-321-44611-9, U\$54.99/C\$68.99

%A Michael Sutton

%A Adam Greene

%A Pedram Amini

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

%D 2007
%G 0-321-44611-9 978-0-321-44611-4
%I Addison-Wesley Publishing Co.
%O U\$54.99/C\$68.99 416-447-5101 fax: 416-443-0948 bkexpress@aw.com
%O <http://www.amazon.com/exec/obidos/ASIN/0321446119/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0321446119/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/0321446119/robsladesin03-20>
%O Audience a+ Tech 2 Writing 1 (see revfaq.htm for explanation)
%P 543 p.
%T "Fuzzing: Brute Force Vulnerability Discovery"

In the foreword, H. D. Moore states that fuzzing is the submission, to a system, of miscellaneous inputs in order to find vulnerabilities, and that it is more art than science.

In the preface, the authors assert that, since it is important to have as many people as possible finding vulnerabilities in our applications, the book is written not only for researchers, but for the general public and those with no background in the idea and activity of fuzzing.

Part one provides background information and concepts. Chapter one outlines the three basic types of vulnerability discovery: white box, utilizing source code and other developer materials; black box, submitting inputs and observing the results; and gray box, using tools such as disassemblers and debuggers. A definition of fuzzing is attempted in chapter two, discussing boundary values analysis (submission of inputs that straddle the line between acceptable and improper), but notes that fuzzing goes beyond this level of activity. There is brief mention of mutation-basing (modification of input described as acceptable) and generation-basing (creation of test data from the specification of the format). Fuzzing methods are supposed to be the topic of chapter three, but it generally lists different types of programs (based on the types of applications they test). Different types of data representation are mentioned in chapter four. The requirements for successful fuzzing, discussed in chapter five, are basically the best possible understanding of the system under test, the ability to determine when an effect has been created, and care in recording attempts and results.

Part two examines a variety of application target types, and the automation of fuzzing activities. Chapter six lists some tools, and notes some factors in programming test generation programs. Subsequently, chapters follow a pattern of an initial discussion of a specific category of intended quarry (environment variables and arguments in chapter seven) and then automation of fuzzing for that purpose (environment parameters in chapter eight). The targets are Web applications (nine and ten), file formats (eleven, with automation for UNIX in twelve, and Windows in thirteen), network protocols (fourteen, fifteen, and sixteen), Web browsers (seventeen and eighteen), and in-memory fuzzing (nineteen and twenty).

Part three introduces advanced fuzzing technologies. Fuzzing frameworks, described in chapter twenty-one, are applications for specifying formats and generating ranges of test and probe input data to be used for submission to programs. It is difficult to find a consistent thread for chapter twenty-two, but the topic seems to have something to do with general programmatic approaches that may have promise for the automation of fuzzing.

While fuzzing can create failures, and therefore note the existence of faults, in a program, it cannot help us to identify vulnerabilities to be addressed unless we can distinguish the part of the application that is responsible for the malfunction. Chapter twenty-three explores this idea under the title of fuzzer tracking, or code coverage, and notes some of the utilities that can be of assistance, but doesn't do a good job of explaining the necessary functions and concepts. Intelligent fault detection, in chapter twenty four, is related to the material in twenty-two, although on a more generic level.

Part four is a kind of summary, with "Lessons Learned" (and the potential for the use of fuzzing in software development) in chapter twenty-five. The title "Looking Forward," in twenty-six, would normally lead the reader to expect some examination of future directions, but instead there is a list of some advanced fuzzing programs to close off the book.

This work does delineate the concepts involved in probing and testing of software through random or semi-random input submission. For those managing the software development process, these ideas are helpful, although the book may seem a trifle long to that audience. For those more directly involved in testing, the text may seem frustrating at times: either simplistic, for experienced testers, or not detailed enough, for quality assurance people just getting started in technical explorations. Still, this is the most complete volume in the field so far, easily exceeding Beaver's "Hacking for Dummies" (cf. BKHACKDM.RVW), Chirillo's "Hack Attacks Testing" (cf. BKHKATTS.RVW), or "The Software Vulnerability Guide" (cf. BKSUVLGD.RVW). Andrews' and Whittaker's "How to Break Web Software" (cf. BKHTBWSW.RVW) has a higher level of writing, but is more specialized, so Sutton, Greene, and Amini have provided a useful and more general guide.

copyright Robert M. Slade, 2007 BKFUZZNG.RVW 20071005
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 4

Saturday 2 February 2008

Contents

- [Transplant patient has NEW kidney removed after NHS computer blunder](#)
[Richard I. Cook](#)
- [Tachometer error caused 2005 runway overrun](#)
[Mark Brader](#)
- [Mideast submarine cable disruptions](#)
[David Leshner](#)
- [Empire State Building car e-interference mystery](#)
[David Chessler](#)
- [Technology Review: Stopping cars with microwaves](#)
[David Chessler](#)
- [Manufacturer Blames Bankruptcy on Failed ERP Implementation](#)
[Ken Dunham](#)
- [2008 meltdown margin player blames s/w for failure to complete trades](#)
[George Michaelson](#)
- [Fifth Amendment: Passphrase cannot be forced](#)
[David Leshner](#)
- [British software pirate sells GBP 12K package at 1/1000](#)
[Peter Mellor](#)
- [DTV vs USPS](#)
[Peter Zilahy Ingerman](#)
- [Voting Machine Usability Testing](#)
[Ken Dunham](#)
- [Impersonating armored car personnel](#)
[Craig Partridge](#)
- [Another public data loss in the UK](#)
[Robert Klemme](#)
- [Automated calling system glitch locks down school](#)
[Steve Eddins](#)
- [Re: Air Canada A319 upset](#)
[Peter Ladkin](#)
- [Re: Coffee Grounds Qantas](#)
[Preston de Guise](#)
- [Re: Metal structure beneath runway ...](#)
[Neil Youngman](#)
- [Hoist by one's own petard: data security: UK Child Benefits](#)

[Adrian Cherry](#)

• [REVIEW: "Software Testing Practice: Test Management", Spillner et al.](#)

[Rob Slade](#)

• [Info on RISKS \(comp.risks\)](#)

✂ **Transplant patient has NEW kidney removed after NHS computer blunder**

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

Thu, 24 Jan 2008 16:01:32 -0600

http://www.mailonsunday.co.uk/pages/live/articles/news/news.html?in_article_id=509289&in_page_id=1770

✂ **Tachometer error caused 2005 runway overrun**

<msb@vex.net (Mark Brader)>

Wed, 30 Jan 2008 22:36:27 -0500 (EST)

On May 18, 2005, a Jordanian Airbus A320 completed a flight (on behalf of a Spanish charter airline) from Fuerteventura, Spain, to Leeds Bradford Airport in England. After landing, it decelerated normally as far as a speed of 73 knots, but then the brakes on both sides failed almost completely. With runway running out and reverse thrust insufficient to stop, the pilot steered off the runway. At 22 knots the brakes reengaged, and the plane stopped safely without injuries.

The accident is covered by Report 6/2007 of the UK AAIB, which is available in PDF in sections under this page:

http://www.aaib.gov.uk/sites/aaib/publications/formal_reports/6_2007_jy_jar/jy_jar_report_sections.cfm?view=print

They say the failure was the result of "excessive wheel tachometer signal noise, caused by a bent tachometer driveshaft on each main landing gear assembly" combined with "inadequate fault tolerance within the brake control system". The tachometer is involved because that's how the Brake and Steering Control Unit (BCSU) tells whether the plane is skidding. But the tire and driveshaft could resonate at about the same frequency, causing the tachometer to produce electrical noise that in turn would cause the BCSU to malfunction and release the brakes to prevent a skid that was not happening.

The solution was to replace the driveshaft with a stronger one (solid instead of hollow), which would also have a different resonant frequency.

Mark Brader, Toronto, msb@vex.net

[Another item from me about something that happened in England in 2005! I just happened across this report while checking the AAIB site on the off-chance that there was news about the recent Heathrow incident.]

✂ **Mideast submarine cable disruptions**

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

Fri, 1 Feb 2008 02:12:16 -0500 (EST)

In what appears to separate incidents, two major submarine FO cables (FLAG Telecom and SEA-ME-WE 4) have been cut in the Middle East.

Dubai, Egypt, Saudi Arabia, Qatar, the United Arab Emirates, Kuwait, Bahrain, Pakistan, and India are all suffering badly. There's been much rerouting to trans-Pacific circuits.

The RISKS? Well first, in an amazing short period of time [TAT-1, the {copper} first transatlantic telephone cable was put into service in 1956; TAT-8, the first fiber cable was in 1988.] our civilization/economy has become highly dependent on photons & refined beach sand.

Second RISK: While cables are relatively safe in deep water, to be useful they must come ashore somewhere; and shallow water is where they are vulnerable. And ships also like those same shallows.

Cables are only REALLY redundant if they have nothing in common, and for reasons of geography, politics and history, they flock together in those same shallow port waters.

Alexander Harrowell made a sage comment on the NANOG list.

[Landing spots..] have historically been in the same strategic locations. Suez, Singapore, Cape Town; it's the strategic map of the British Empire. "Five strategic keys lock up the world", as Lord Fisher said. (Dover, Gibraltar, Singapore, Cape Town, and Suez).

I'm further reminded of Dan Charles' report on Relay, Maryland:
<<http://www.npr.org/templates/story/story.php?storyId=1030846>> where he discussed how wagon trains, telegraph, railroads, and now fiber... all Go West via the same route.

[See also a CNN report. PGN]

http://www.cnn.com/2008/WORLD/meast/01/31/dubai.outage/index.html?eref=rss_=_topstories

✶ Empire State Building car e-interference mystery (*NY Daily News*)

<David Chessler <chessler@usa.net>>

Tue, 29 Jan 2008 20:12:25 -0500

In addition to some of the reported incidents, there were several incidents in the Washington area some years ago in which digital PBXs interfered with air traffic control at National Airport (as it was then called).

http://www.nydailynews.com/news/2008/01/27/2008-01-27_empire_state_building_car_zap_mystery.html
http://www.nydailynews.com/img/2008/01/27/alg_empire-state.jpg

Several cars a day get bizarrely stranded in a five-block 'Bermuda Triangle'

near the Empire State Building.

http://www.nydailynews.com/img/2008/01/27/amd_valeev.jpg

In the shadow of the Empire State Building lies an "automotive Bermuda Triangle" - a five-block radius where vehicles mysteriously die. No one is sure what's causing it, but all roads appear to lead to the looming giant in our midst - specifically, its Art Deco mast and 203-foot-long, antenna-laden spire. "We get about 10 to 15 cars stuck near there every day," said Isaac Leviev, manager of Citywide Towing, the AAA's exclusive roadside assistance provider from 42nd St. to the Battery. "You pull the car four or five blocks to the west or east and the car starts right up."

"The lights work, the horn works, everything. But it won't start," Russell Valeev, a driver for Golden Touch Transportation said one recent evening as he sat in his 2005 Ford van with the hood propped open on E. 35th St., between Lexington and Park Aves. "It's my job. No money."

The 102-story building, at Fifth Ave. between 33rd and 34th Sts., has been home to broadcast equipment since its opening in 1931, when RCA installed an experimental TV antenna. Since the 9/11 attacks destroyed the twin towers, the building has regained its status as the leading transmission site for commercial broadcast outfits, with 13 TV and 19 FM stations mounting antennas on its spire.

The FCC said it has not received any complaints regarding interference affecting autos in midtown, and Empire State Building officials don't believe the claims. Yet some phantom transmission appears to cause the remote keyless entry systems of scores of car owners to go haywire and stop talking to their vehicles. [Source: Richard Weir, Empire State Building car zap mystery, *NY Daily News*, 29 Jan 2008; PGN-ed]

[The NY Daily News blog is replete with cases reported by affected drivers. You can add yours to the blog or report it to rweir@nydailynews.com. But by now it's familiar territory and no longer News. PGN]

Technology Review: Stopping cars with microwaves

<David Chessler <chessler@usa.net>>

Fri, 01 Feb 2008 18:11:31 -0500

Zapping the bad guys: Attached to the roof of this police car is a 200-pound electromagnetic system that can quickly bring an opposing vehicle to a stop. The system is six- to eight-feet long (antennae included) and almost three-feet wide. It works by sending out pulses of microwave radiation that disable the microprocessors that control the central engine functions of a car. Credit: Eureka Aerospace

http://www.technologyreview.com/files/13634/policecar_x220.jpg

Researchers at Eureka Aerospace are turning a fictional concept from the movie *2 Fast 2 Furious* into reality: they're creating an electromagnetic system that can quickly bring a vehicle to a stop. The system, which can be

attached to an automobile or aircraft carrier, sends out pulses of microwave radiation to disable the microprocessors that control the central engine functions in a car. Such a device could be used by law enforcement to stop fleeing and noncooperative vehicles at security checkpoints, or as perimeter protection for military bases, communication centers, and oil platforms in the open seas. [Source: Brittany Sauser, Stopping Cars with Radiation: A beam of microwave energy could stop vehicles in their tracks, MIT

Technology Review, 13 Nov 2007]

http://www.technologyreview.com/printer_friendly_article.aspx?id=19699

***Manufacturer Blames Bankruptcy on Failed ERP Implementation**

<"Ken Dunham" <kdunham@rogers.com>>

Wed, 30 Jan 2008 08:39:13 -0500

American LaFrance (ALF), a US manufacturer of fire trucks, has blamed a failed ERP implementation for its filing for bankruptcy this week. Coupled with "inventory not properly declared as obsolete", ALF incurred \$100 million in unanticipated costs, lengthy production delays, and problems servicing customers' existing trucks.

<http://www.americanlafrance.com/interior.asp?n=22>

A significant consequence to ALF's operational problems is fire departments across North America are apparently experiencing significant delays in obtaining spare parts and service for their front-line fire trucks, and new orders (most of which will be replacements for aging apparatus) are being delayed by months. This will undoubtedly result in apparatus (and possibly the associated companies of firefighters) being placed out of service more than usual, and/or use of older, less reliable reserve apparatus (which typically don't meet current safety standards).

Although problems with ERP implementations have caused a number of high profile business disruptions in recent years (eg Hersheys, HP) this is the first I've heard of a company blaming their bankruptcy on ERP. The RISKS involved in such large-scale IT projects are well known (especially to readers here), but unfortunately still occur all too often.

[For the benefit of readers who aren't accountants or lawyers, Chapter 11 is a US bankruptcy provision that allows a company to voluntarily declare bankruptcy, prepare a financial reorganization plan under the supervision of the bankruptcy court, and (hopefully) ultimately be discharged from bankruptcy as a viable concern.]

***2008 meltdown margin player blames s/w for failure to complete trades**

<George Michaelson <ggm@apnic.net>>

Fri, 1 Feb 2008 09:42:20 +1000

Tricom, a margin lending specialist in Australia was unable to complete its trades, and finalize settlements. the ASX had to declare a hold on its activities and close off the market without it. Everything was resolved by the next business day.

Tricom stated (according to the Australian Newspaper) that it was net positive, but s/w let it down and it couldn't complete the volume of processing required due to a new s/w system.

<http://www.australianit.news.com.au/story/0,24897,23142583-15306,00.html> suggests that the story is not that simple, the system was accepted under the 3 day burn-in test the ASX require, and that it will not form the main focus of any investigation.

I think we'll see quite a lot of software/computer-systems blame over triggers to sell, but this appears to be about scaling functions to close off, rather than automatic bet-the-market outcomes.

Interesting to think about what are the possible scaling functions in these kinds of systems. The average-to-peak difference could be immense, if you spread a range of people making smallish buys (by volume of event) spread over a long time, but then have a synchronization event which forces everyone to trigger SELL at the same time. It could be several decimal orders of magnitude variation in the transaction volumes, which makes capacity planning and even some data structure design quite important methinks...

✂ Fifth Amendment: Passphrase cannot be forced

*<"David Leshner" <wb8foz@panix.com>>
Tue, 18 Dec 2007 23:21:45 -0500 (EST)*

U.S. Magistrate Judge Jerome Niedermeier ruled that a man accused of transporting child pornography has a Fifth Amendment right to keep his password in his head, not give it to prosecutors.

In other words, the Fifth Amendment protects the right to keep passwords.

<http://www.volokh.com/files/Boucher.pdf>

✂ British software pirate sells GBP 12K package at 1/1000

*<MellorPeter@aol.com>
Wed, 16 Jan 2008 07:56:53 EST*

Michael Walton broke an encryption code in the AceCad software (a 3D modeling program for use in the construction of steel structures) which allowed him to make copies of it. He sold the copies for GBP 12 on eBay. The company has said that an AceCad licence costs between GBP 12,000 and 20,000. Walton, who reportedly had 80 identities on eBay, pleaded guilty to

copyright infringement and will be sentenced in February. The maximum term to which he might be sentenced is 10 years.

Precisely why he sold the package for less than 0.1% of its commercial value is not clear. The strength of the vendor's encryption has been questioned by some commentators. [Maybe he missed the K? PGN]

http://www.channelregister.co.uk/2008/01/15/uk_software_pirate_ebay/

Peter Mellor Tel/Fax: +44 (0)20 8459 7669

DTV vs USPS

<Peter Zilahy Ingerman <pzi@ingerman.org>>

Fri, 25 Jan 2008 17:30:21 -0500

The organization that has been set up to distribute set-top converter boxes (<http://www.dtv2009.gov>) uses a database that was purchased from the US Postal Service in order to determine whether the applicant address is a business or a residence. My address was erroneously classified as a business. The USPS has corrected the error in their data base, but the set-top people don't seem to understand that there can be errors in their database because it isn't current.

Voting Machine Usability Testing

<"Ken Dunham" <kdunham@rogers.com>>

Fri, 1 Feb 2008 12:34:09 -0500

Technology Review published results from usability (as opposed to security) reviews of voting machines, which find significant error rates due to user confusion.

<http://www.technologyreview.com/Infotech/20122/?nlid=850>

Ben Bederson <<http://www.cs.umd.edu/~bederson/>>, an associate professor at the Human-Computer Interaction Lab at the University of Maryland, was part of a team that conducted a five-year study <<http://www.brookings.edu/press/Books/2007/votingtechnology.aspx>> on voting-machine technology. Bederson says that machines should be evaluated for qualities beyond security, including usability, reliability, accessibility, and ease of maintenance. Bederson has designed a prototype of a user-friendly voting machine.

Whether electronic voting machines are under scrutiny for usability or security, many experts say that their design flaws call for reevaluation of the devices. Tadayoshi Kohno <<http://www.cs.washington.edu/homes/yoshi/>>, an assistant professor of computer science at the University of Washington, who has studied the security of several electronic systems, says, "My feeling of the electronic-voting community is that we started walking down a dark

alley, and we know that it's very dangerous. We know that at the end of the valley is a safe place. As a philosophical question, I have to ask, should we continue going down this dark alley, or should we step back and figure out some other way we want to go to safety?"

✂ Impersonating armored car personnel

<Craig Partridge <craig@aland.bbn.com>>

Thu, 17 Jan 2008 17:22:25 -0500

This seems to have suddenly become a popular (and sometimes successful) way to try to steal money. Someone impersonating a Brinks carrier got away with over \$100K in the DC area and it took some time for the bank to even realize it had been robbed.

<http://www.washingtonpost.com/wp-dyn/content/article/2008/01/10/AR2008011004339.html>

Another person wearing a uniform got into an apparently restricted area at a Brinks facility in Philadelphia and got his hands on \$640K but was caught trying to get out.

<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/01/17/national/a121606S03.DTL&tsp=1>

The stories don't have enough detail to understand fully how security was breached but it sounds, from both articles, as if a uniform alone suffices to identify someone. No ID checks?

✂ Another public data loss in the UK

<Robert Klemme <r.klemme@gmx.de>>

Sat, 19 Jan 2008 17:49:22 +0100

It happened again: a UK government institution lost quite a few data records of citizens. I won't bother to list the risks of leaving a laptop with unprotected data in a car; but again the major risk here is having people work with sensitive material who are either careless, uneducated or unaware of the sensitiveness of the data.

<http://www.timesonline.co.uk/tol/news/politics/article3213274.ece>

✂ Automated calling system glitch locks down school

<"Steve Eddins" <Steve.Eddins@mathworks.com>>

Thu, 31 Jan 2008 09:23:28 -0500

More than 2,000 people in Medford (Mass.) were called with an automated message: Their children were not in class. So many parents started arriving at Brooks Elementary School to check on their children that officials put

the place in lockdown. Superintendent Roy E. Belson said a telephone glitch occurred shortly after the district's automated calling system went through its update. Someone forgot to log out of the database before trying to send a message sometime before noon to the few parents whose children had been marked absent. [...] [One of the planned steps for preventing a recurrence is] posting a sign next to the phone system warning users to 'make sure you shut down the database before you go to message' mode." [Source: *The Boston Globe*, 31 Jan 2008]

http://www.boston.com/news/local/articles/2008/01/31/phone_glitch_hangs_up_schools/

✂ Re: Air Canada A319 upset (Ant, [RISKS-25.02](#))

<Peter Ladkin <ladkin@causalis.com>>

Tue, 15 Jan 2008 07:54:26 +0100

"Computer malfunction" and "flying manually" on an A319. What rot. Yes, I understand it is what the pilot said (or so it says on a note on an aviation forum cross-posted from another forum and supposedly written by a B757 first officer that was on the flight), but he has to say something to all the people in the back.

Here is a link to the incident report in the Transport Canada Civil Aviation Daily Occurrence Reporting System:

<http://www.pprune.org/forums/showpost.php?p=3828916&postcount=42>

They do not know if it was turbulence-related, system-related or both.

When there is an upset, the A320-series aircraft have a set of so-called "Abnormal attitude laws". You can check out the FCOM description of these and other flight control laws in section 1.27.30 at

<http://www.smartcockpit.com/pdf/plane/airbus/A320/systems/0010/>

or if you don't have time, a very brief comment at

<http://www.pprune.org/forums/showpost.php?p=3832144&postcount=60>

or a little more time for a "Noddy's Guide to Airbus Flight Control Laws" at

<http://www.pprune.org/forums/showpost.php?p=3832616&postcount=64>

I should warn that the "postcount" number on the links above may change as the forum is edited, which will send them to notes other than the ones I intend to reference, in which case one can simply search through the notes on the thread at <http://www.pprune.org/forums/showthread.php?t=307936> to recover the referenced posts.

Peter B. Ladkin Causalis Limited and University of Bielefeld, Germany
www.causalis.com www.rvs.uni-bielefeld.de

✂ Re: Coffee Grounds Qantas ([RISKS-25.02](#))

<Preston de Guise <pdeguise@gmail.com>>

Wed, 16 Jan 2008 11:19:21 +1100

Continuing from the story regarding a leaking coffee area causing a power outage on a Qantas jet last week, Australia's Sydney Morning Herald reported today that a former Qantas engineer has been charged with forging a maintenance engineer's license and maintaining jets without a license.

SMH reports that one of the aircraft he was alleged to have performed unlicensed maintenance on was VH-OJM, the Boeing 747-438 that suffered a power loss and made an emergency landing in Bangkok.

The risks of insufficient background checking for such high profile jobs (i.e., of the variety of "if this is done wrong, people can die") is obvious. One hopes Qantas revisits confirmation of correct credentials for all its engineering staff in light of this mishap.

The SMH story can be found at:

<http://www.smh.com.au/news/news/qantas-engineer-charged-with-forgery/2008/01/15/1200419845101.html>

Preston de Guise <pdeguise@gmail.com> +61 414 978 190 <http://www.anywebdb.com>

✶ Re: Metal structure beneath runway ... (Rees, [RISKS-25.03](#))

<Neil.Youngman <Neil.Youngman@youngman.org.uk>>
Wed, 30 Jan 2008 13:13:23 +0000

While this may be true, the original story (Dixon, [RISKS-25.02](#)) was about magnetic interference at London City Airport, not London Heathrow.

For those not familiar with London, there are a number of "London" airports. London City is very central and caters for short haul, mainly business traffic. London Heathrow is the main international hub and is situated on the Western fringes of Greater London, well away from the centre.

The other London airports (Gatwick, Luton, Stansted) are tens of miles outside the greater London area.

[Mistaken airport identification in Rees's item also noted by Mark Brader.
PGN]

✶ Hoist by one's own petard: data security: UK Child Benefits ([R-24.92](#))

<"Adrian Cherry, UK" <Adrian.Cherry@baesystems.com>>
Tue, 15 Jan 2008 09:42:45 -0000

Following up from "Whole of UK Child Benefit records on CD lost in the post"
<http://catless.ncl.ac.uk/Risks/24.92.html#subj3>

>Regarding the possibilities of fraud:
>

>The data includes: National insurance (NI) number Name, address and birth
>date Partner's details Names, sex and age of children Bank/savings account
>details ... quite useful for an identity fraudster, particularly the NI
>number. There is plenty of scope here for a fraudster to redirect payments.

I'm surprised that no mention has been made of one Jeremy Clarkson, an infamous celebrity motoring journalist. When the story broke about the loss of the Child Benefit Records on CD he rather rashly claimed that it was a storm in a tea cup, just a bit of scaremongering. To prove his point he published personal details and claimed there was nothing to fear. He is now 500 pounds poorer and a little wiser.

<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/01/07/nclarkson107.xml>
<http://www.guardian.co.uk/money/2008/jan/07/personalfinancenews.scamsandfraud>

At the time he wrote: "I have never known such a palaver about nothing. The fact is we happily hand over cheques to all sorts of unsavoury people all day long without a moment's thought. We have nothing to fear."

However, yesterday he told readers he had opened his bank statement to find a direct debit had been set up in his name and £500 taken out of his account.

"The bank cannot find out who did this because of the Data Protection Act and they cannot stop it from happening again," he said. "I was wrong and I have been punished for my mistake."

He added: "Contrary to what I said at the time, we must go after the idiots who lost the discs and stick cocktail sticks in their eyes until they beg for mercy."

REVIEW: "Software Testing Practice: Test Management", Spillner et al.

<Rob Slade <rmslade@shaw.ca>>
Thu, 24 Jan 2008 09:47:00 -0800

BKSTPTMN.RVW 20071110

"Software Testing Practice: Test Management", Andreas Spillner et al,
2007, 978-1-933952-13-0, U\$44.95

%A Andreas Spillner spillner@informatik.hs-bremen.de

%A Thomas Rossner thomas.rossner@imbus.de

%A Mario Winter winter@gm.fh-koeln.de

%A Tilo Linz tilo.linz@imbus.de

%C 26 West Mission St, Suite 3, Santa Barbara, CA 93101-2432

%D 2007

%G 978-1-933952-13-0 1-933952-13-X

%I Rocky Nook Inc.

%O U\$44.95 805-687-8727 fax 805-687-2204 joan@rockynook.com

%O <http://www.amazon.com/exec/obidos/ASIN/193395213X/robladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/193395213X/robladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/193395213X/robsladesin03-20>

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

%P 321 p.

%T "Software Testing Practice: Test Management"

This book is intended to assist candidates who are writing the exam for the International Software Testing Qualifications Board (ISTQB) Certified Tester.

Chapter one stresses the importance of software and software quality, and explains that the text is based on the ISTQB Certified Tester second ("Advanced") level, specifically the Test Manager module (excluding the topic of reviews). This chapter also presents an overview of the first ("Foundation") level as background. The tools and processes used to structure testing are outlined in chapter two. Testing is examined, in chapter three, in relation to the software life cycle. Problems with different development models are analyzed, but it is interesting that the complexity of the models is not covered as a risk factor. Criteria for a testing policy are discussed in chapter four. Chapter five mandates a formal test plan. The blueprint will be helpful for those who do not have a structure in place, but appears overly committed to items that are not inherently necessary for all trials. Controls to ensure and follow the progress of testing are detailed in chapter six. Chapter seven explains some of the common quality and process improvement models, and their implications for testing. Testing is used to detect faults or deviations in software, and chapter eight looks at the classification and handling of such issues. Chapter nine examines risk analysis with respect to software testing. The material follows most standard principles for risk management, and so is not wrong in any specifics, but the text fails to present helpful means for using this technique to best advantage. Various important skills that should be contained within the test team are listed in chapter ten. Test metrics are discussed, in chapter eleven, in an academic manner that is very similar to the style of chapter nine. In the same way, by attempting to apply a single process of evaluation to all test management software tools, the authors restrict the utility of chapter twelve. Chapter thirteen lists standards bodies, as well as some of the guidelines that relate to software development and evaluation.

The book reflects the certification, and one cannot fault it for that. However, if the authors had been willing to move beyond the overall coverage of principles, they might have produced a more useful work.

copyright Robert M. Slade, 2007 BKSTPTMN.RVW 20071110
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 5

Monday 18 February 2008

Contents

- [L.A. School payroll system's spectacular failure](#)
[Richard I. Cook](#)
- [FBI mistakenly receives supposedly protected e-mail](#)
[Steven M. Bellovin](#)
- [Canadian Government Mails Out Confidential Data](#)
[Ken Dunham](#)
- [JAL cabin crews sue over personal info](#)
[PGN](#)
- [JAL near miss on attempted takeoff](#)
[PGN](#)
- [Future of e-voting in doubt in Japan](#)
[PGN](#)
- [Computer Error Strands Tanker off Massachusetts](#)
[Lee Rudolph](#)
- [Bell Canada Data on 3.4 Million Customers Stolen](#)
[Ken Dunham](#)
- [Royal Canadian Mounted Police Censured for Privacy Violations](#)
[Ken Dunham](#)
- [Re: Lost Kansas City IRS tapes with personal info.](#)
[Danny Burstein](#)
- [Critics chuck MS 'friendly worm' plan on the compost heap](#)
[Chris Leeson](#)
- [Another BlackBerry Outage Caused by System Upgrade?](#)
[Ken Dunham](#)
- [Vulnerability info suppressed by criminals paying to hide it](#)
[Ken Dunham](#)
- [New GAO Report on IRS Information Security Pervasive Vulnerabilities](#)
[Diego Latella](#)
- [The GPS miracle](#)
[Rich Mintz](#)
- ['Woman Says Being Declared Dead Ruins Life'](#)
[PGN](#)
- [A reminder: Eric Sevareid's Law](#)
[Ken Knowlton](#)
- [Ah yes, just what you need!!!](#)

[David Lesher](#)

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

✶ L.A. School payroll system's spectacular failure (Re: [RISKS-24.84](#))

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

Wed, 13 Feb 2008 11:08:29 -0600

-- whither the U.S. National Healthcare IT Initiative?

[Source: "Payroll system beset from Day 1: Poor management, software failures and breakdowns in training led to a yearlong crisis at L.A. Unified." Joel Rubin, *Los Angeles Times*, 11 Feb 2008]

http://www.latimes.com/news/local/los_angeles_metro/la-me-payroll11feb11,1,4656862.story?page=1

Painful experience with Los Angeles' 95 million US\$ attempt to computerize its school payroll is reviewed in the referenced article. Predictable, of course, but, to quote an old protest song, "we were knee deep in the big muddy and the big fool said to push on." The spectacular failure is particularly remarkable because it involved what should have been a rather mundane project: the computerization of payroll for 36,000 employees. That such a project should go so badly wrong should, perhaps, make us more reluctant to embrace much larger efforts.

The present U.S. administration committed US\$100 million to a vaguely outlined project to catalyze the introduction of immediately available electronic medical records for healthcare in the U.S. The scale of the project is perhaps three to five orders of magnitude larger than the one that failed in LA but the sum committed to the endeavor is about the same. The efforts to introduce interoperable electronic medical records have been far more expensive and much less successful than anyone is willing to admit.

A private review of two major hospital systems showed that the overruns are on the order of 3 to 5 times (sic) the initially proposed price but also that the systems are delayed years beyond the plan horizon and the implementations are radically stripped-down versions of what had been proposed. Many of the high end features that were touted as bringing increased efficiency and safety to healthcare delivery have been scrapped or put off until later versions of the system. Senior management in these IT efforts are routinely replace every few years as schedules slip and costs increase. Somewhat surprisingly, hospital administrators remain optimistic regarding the future of these systems -- insisting that the problems encountered are the result of inevitable "growing pains" or narrowly technical flaws rather than inadequate planning, goal setting, design, or implementation. (One facility recognized that the project could not be made to work on the planned platform and essentially scrapped its entire effort and started over.) The similarities between the experiences with healthcare IT and the LA system's evolution are disturbing.

What is particularly troubling about the LA school system story is the willingness and ability of the system vendors and a few senior managers to

push forward despite many warnings that the project was far off course and out of control. Institutional needs and conflicts of interest created the problem and then sustained the fantasy that the system was going to work even as it was collapsing.

The scale of the healthcare IT initiative might be estimated like this. The LA system apparently spent over \$50 million before the failure became apparent -- this is for 36K employees or about \$1,400/employee. Taking the U.S. population at 300 million and assuming that the national effort is twice as efficient in implementation leads me to believe that about US\$20 billion will be spent before people realize that things have gone badly wrong. As a sanity check on these numbers, the system reviews described above indicate that a single facility can easily spend \$40 million in direct expenditures (just the hardware and software and associated IT people) before realizing that the IT system being built is going to fail. There are roughly 5000 U.S. hospitals, again giving a roughly US\$20 billion loss estimate. Of course, the mileage you get may vary.

Recommended reading:

Brooks FP. The Mythical Man-Month: Essays on Software Engineering (2nd Edition). Addison-Wesley, 336 pages. ISBN-10: 0201835959

FBI mistakenly receives supposedly protected e-mail

<"Steven M. Bellovin" <smb@cs.columbia.edu>>
Sun, 17 Feb 2008 13:35:16 +0000

Here's what I put in my blog:

A Technical Mistake

16 February 2008

<http://www.cs.columbia.edu/~smb/blog/2008-02/2008-02-16.html>

The Electronic Frontier Foundation

<<http://www.eff.org/deeplinks/2008/02/foia-document-shows-improper-fbi-access-entire-domains-email>>

has obtained an FBI document

<http://www.eff.org/files/090507_surge2.pdf> describing a mistake that was made in monitoring someone's email: the ISP sent the FBI all of the email for the entire domain, rather than just the suspect's email.

It isn't surprising that something like this can happen. Matt Blaze

<<http://www.crypto.com>> and I warned about configuration problems

<<http://www.crypto.com/papers/carnivore-risks.html>> in surveillance systems several years ago:

Needless to say, any wiretapping system (whether supplied by an ISP or the FBI) relied upon to extract legal evidence from a shared, public network link must be audited for correctness and must employ strong safeguards against failure and abuse. The stringent requirements for accuracy and operational robustness provide especially fertile ground for many familiar risks.

First, there is the problem of extracting exactly (no more and no less) the intended traffic.

The context then was Carnivore, but the problem is the same. On the same subject, Matt wrote

More seriously, I suspect that the meat (so to speak) of any meaningful analysis of Carnivore's security and behavior lies not in its core source code but rather in the parameters used when it is actually configured and installed.

In fact, errors by third parties are not uncommon. *The New York Times* report on this incident <http://www.nytimes.com/2008/02/17/washington/17fisa.html> makes it clear:

Past violations by the government have also included continuing a wiretap for days or weeks beyond what was authorized by a court, or seeking records beyond what were authorized. The 2006 case appears to be a particularly egregious example of what intelligence officials refer to as "overproduction" -- in which a telecommunications provider gives the government more data than it was ordered to provide.

The problem of overproduction is particularly common, F.B.I. officials said. In testimony before Congress in March 2007 regarding abuses of national security letters, Valerie E. Caproni, the bureau's general counsel, said that in one small sample, 10 out of 20 violations were a result of "third-party error," in which a private company "provided the F.B.I. information we did not seek."

From what has been released, the FBI did nothing wrong here. In fact, they say that they destroyed the unwanted (and unauthorized) emails when they noticed the problem. But mistakes /will/ happen. This is why I and others have warned <http://www.cs.columbia.edu/~smb/papers/j1lanFIN.pdf> about the dangers of too-close linkage to the telecommunications system: other plausible configuration errors could give malicious parties access to the network.

Surveillance is difficult. Complexity and interconnections make it dangerous, too.

[See Steve's blog for more. PGN]

Canadian Government Mails Out Confidential Data

*<"Ken Dunham" <kdunham@rogers.com>>
Tue, 5 Feb 2008 16:21:51 -0500*

Public Works and Government Services Canada (PWGSC), the procurement arm of the Canadian federal government, mailed out 138 CDs containing confidential government and commercial data in response to requests made under the Access

to Information Act. The confidential portions of the information were blacked out, but this was not done properly so anyone in possession of a CD can easily restore the confidential information. The root cause is apparently government -- mishandling of the new imaging software -- used to process information access requests (insufficient user training?).

The firms whose confidential commercial data has been compromised have been notified, but the government has refused to identify any of the recipients of the CDs on the basis that this would violate privacy laws. The Access to Information Act specifically exempts the government from civil liability for inadvertent disclosures made in good faith.

The government has asked the 138 recipients of the CDs to return them, but so far only 28 have done so.

Reported in the Globe and Mail:

<http://www.theglobeandmail.com/servlet/story/LAC.20080204.DISCS04/TPStory/>

✶ JAL cabin crews sue over personal info

*<"Peter G. Neumann" <neumann@csl.sri.com>>
Sat, 16 Feb 2008 10:50:17 PST*

Some 190 current and former cabin attendants of Japan Airlines Corp. and their union sued the airline and its largest labor union on 11 Feb 2008, claiming 150 items of personal information on 9800 employees -- including their DoB, home addresses, political beliefs, medical records, family status, physical descriptions, and internal job performance evaluations -- were collected without their consent, and seeking about 48 million yen in compensation. This was just recently discovered. [Source: Kyodo News, *The Japan Times*, 27 Nov 2007; PGN-ed]

<http://www.japantimes.co.jp/>

✶ JAL near miss on attempted takeoff

*<"Peter G. Neumann" <neumann@csl.sri.com>>
Sun, 17 Feb 2008 15:49:18 PST*

A Japan Airlines jet carrying 446 passengers and crew members started heading down a runway without permission while another JAL aircraft was still moving on the runway after landing at New Chitose Airport on 16 Feb 2008, but was stopped short of rear-ending the other plane just in time by an air traffic controller. The pilot reportedly misunderstood the controller, who was speaking in English. [Presumably within the standard subset used internationally.] [Source: JAL plane attempts takeoff without permission in Hokkaido after English language mix-up, *Japan Today*, 18 Feb 2008; PGN-ed]

<http://www.japantoday.com/jp/news/428379>

<http://www.yomiuri.co.jp/dy/national/20080217TDY01304.htm>

#Future of e-voting in doubt in Japan

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

Sat, 16 Feb 2008 10:50:17 PST

A bill designed to introduce electronic voting in national elections has been left up in the air due to worries about the system's reliability. The bill to revise the law on special provisions of the Public Offices Election Law has been carried over to the current Diet session at the House of Councillors after the House of Representatives passed it in the extraordinary Diet session. [...]

E-voting began in Japan in Feb 2002 for some local governments, and has expanded slowly since then, locally. Past difficulties have apparently caused questions of credibility. In one municipal election in July 2003, all servers went down, affecting Kani's 29 polling stations; the Japanese Supreme Court invalidated the election. Another election in Nov 2003 had problems with communications and servers. [Source: Discussion needed to ease fears about touch-screen machines, Ryota Akatsu, Yomiuri Shimbun Staff Writer, the *Daily Yomiuri, 3 Feb 2008, PGN-ed]

<http://www.yomiuri.co.jp/dy/national/20080208TDY04302.htm>

#Computer Error Strands Tanker off Massachusetts

<Lee Rudolph <lrudolph@panix.com>>

Tue, 12 Feb 2008 20:34:00 -0500 (EST)

The Coast Guard says a problem with the computers that control the 933-foot Catalunya Spirit's tanker's boilers caused a loss of power that left it adrift off Cape Cod. Some power has been restored to the switchboards. The tanker, carrying liquefied natural gas, is being towed to an anchorage about seven miles offshore for further troubleshooting. The tanker was heading from Trinidad and Tobago to Boston when it lost power early Monday about 45 miles off the Cape. [Source: Associated Press item, *The Boston Globe*, online, 12 Feb 2008]

Between the devil and the deep blue screen of death?

#Bell Canada Data on 3.4 Million Customers Stolen

<"Ken Dunham" <kdunham@rogers.com>>

Wed, 13 Feb 2008 09:55:28 -0500

Bell Canada announced that basic personal data for 3.4 million customers in Ontario and Quebec has been stolen, discovered in electronic form in a

Montreal home after a tip. The stolen subscriber data reportedly included names, addresses, telephone numbers, and services, but not financial information. However, roughly 5% of the phone numbers are unlisted, which may cause some consternation. [PGN-ed]

<http://www.reportonbusiness.com/servlet/story/RTGAM.20080212.wbelldata021=3/BNStory/Business/home>

✶ Royal Canadian Mounted Police Censured for Privacy Violations

<"Ken Dunham" <kdunham@rogers.com>>

Thu, 14 Feb 2008 08:29:30 -0500

The Privacy Commissioner of Canada has censured the Royal Canadian Mounted Police (RCMP), Canada's national police force, for maintaining large numbers of secret files in violation of both RCMP policy and Canadian law.

Summary: http://www.privcom.gc.ca/media/nr-c/2008/nr-c_080213_e.asp

Full report:

http://www.privcom.gc.ca/information/pub/ar-vr/rcmp_080213_e.pdf

Background:

http://www.privcom.gc.ca/media/nr-c/2008/nr-c_b-di_080213_e.asp

The RCMP has been struggling with criticism on a number of fronts recently, and this report is likely to strengthen calls for stronger governance and management oversight.

The RCMP have already committed to addressing the concerns raised by the Privacy Commissioner. The latter will be conducting a follow-up audit to verify compliance.

✶ Re: Lost Kansas City IRS tapes with personal info. (RISKS-25.03)

<Danny Burstein <dannyb@panix.com>>

Sat, 19 Jan 2008 22:16:30 -0500 (EST)

KC faulted after probe of IRS tapes missing from City Hall
Lynn Horsley, *The Kansas City Star*, 19 Jan 2008

"A federal investigation of missing Internal Revenue Service tapes from City Hall in Kansas City has concluded that the city failed to follow 'proper safeguards for protecting federal tax return information.' That conclusion is contained in a heavily redacted report obtained recently by The Kansas City Star under a Freedom of Information Act request to the Treasury Department's inspector general for tax administration. The inspector general's investigation stemmed from the disappearance of 26 IRS computer tapes containing taxpayer information. The tapes, which have never been found, are normally used by the city to help enforce collection of the 1 percent city earnings tax paid by people who live or work in Kansas City."

[and for good measure]

"The IRS has never said what information was on the tapes, how many taxpayers were affected, or whether those taxpayers would ever be notified about the missing information."

<http://www.kansascity.com/news/politics/story/451282.html>

✂ Critics chuck MS 'friendly worm' plan on the compost heap

<"Chris Leeson" <Chris.Leeson@atosorigin.com>>

Fri, 15 Feb 2008 16:07:21 -0000

(The Register)

http://www.theregister.co.uk/2008/02/15/ms_friendly_worm/

Microsoft are reportedly working on plans to distribute patches using techniques similar to those used by computer worms. Understandably, these plans are not popular amongst the security specialists.

The idea is that patches can be distributed within subnets to machines that are likely to be configured in a similar way. This hopes to reduce the load on download servers that currently take a huge hit when patches are released.

Of course, the process would be uncontrolled, and would never be secure enough for safe practical use.

(We have had the "benign virus" appear RISKS before, of course. If I recall correctly, Cliff Stoll posted about a similar idea by Fred Cohen in [RISKS-12.27](#). Chris)

<http://catless.ncl.ac.uk/Risks/12.27.html#subj13.1>)

✂ Another BlackBerry Outage Caused by System Upgrade?

<"Ken Dunham" <kdunham@rogers.com>>

Tue, 12 Feb 2008 10:34:47 -0500

BlackBerry messaging services were interrupted Monday afternoon (February 11) throughout North America due to an unspecified problem at the RIM data center in Canada through which all BlackBerry email messages are processed. Although RIM states the outage began at 3:30pm EST, this BlackBerry user also noticed message delays at various points earlier in the day. Jim Balsillie, RIM's co-CEO, speculated that the outage was caused by a system upgrade: "At the core virtually all these things tend to happen on service upgrades".

This latest outage follows on the heels of another widespread outage last

April, which was attributed to the introduction of a new feature that had been insufficiently tested.

Reported in the Ottawa Citizen and elsewhere:

<http://www.canada.com/ottawacitizen/news/story.html?id=3D23a3b21b-3d52-4714-b232-b7098c9f4996>
<<http://www.canada.com/ottawacitizen/news/story.html?id=3D23a3b21b-3d52-4714-b232-b7098c9f4996&k=3D8706>>
&k=3D8706=20

[Also reported by Mike Hogsett. PGN]

✂ Vulnerability info suppressed by criminals paying to hide it

<"Ken Dunham" <kdunham@rogers.com>>

Wed, 13 Feb 2008 10:07:35 -0500

The annual "X-Force" report, released on 12 Feb 2008 by Internet Security Systems, part of IBM Corp., says network and software vendors acknowledged 6,437 security flaws in 2007, down 5.4 percent from the prior year, but up from 4,824 the year before that. [Good news and bad news.] But the real bad news may be that a black market has emerged "that will pay up to \$100,000 (euro68,766) to computer whizzes" who find vulnerabilities and sell the information to criminal gangs eager to exploit them. Thus, it is profitable NOT to publicly report previously undetected flaws. [Source: Web security report says known vulnerabilities fall because criminals pay to hide them, Associated Press item; PGN-ed]

http://www.technologyreview.com/printer_friendly_article.aspx?id=20206
http://www.iss.net/documents/literature/x-force_2007_trend_statistics_report.pdf

✂ New GAO Report on IRS Information Security Pervasive Vulnerabilities

<Diego Latella <Diego.Latella@isti.cnr.it>>

Wed, 13 Feb 2008 17:18:45 +0100

On 8 Jan 2008 the GAO published a report that may be of interest for many RISKS readers:

GAO-08-211 Information Security: IRS Needs to Address Pervasive Weaknesses

<http://searching.gao.gov/query.html?charset=iso-8859-1&ql=&rf=2&qt=GAO-08-211&Submit=Search>

Dott. Diego Latella - Senior Researcher - CNR/ISTI, I56124 Pisa (ITALY)

<http://www.isti.cnr.it/People/D.Latella> - phone:+39 0503152982

[This is just one in a very long series of GAO reports on IRS computer problems. PGN]

✂ The GPS miracle

<Rich Mintz <richmintz@richmintz.com>>

Tue, 5 Feb 2008 11:50:49 -0500

All the anecdotes about how GPS has led people down the garden path, into lakes and rivers, 300 miles out of the way, etc., are entertaining -- I consume them hungrily. But is the situation they represent really that new, or really limited to technology?

The same thing can happen (and does) when people expect a printed map to be a perfect reflection of the real-world things (roads, etc.) it symbolizes, or to have complete information, or to be current. Some of the printed maps in my car don't show the directions of one-way streets, so "relying" on them can lead me around in circles. *None* of the printed maps in my car show the locations of things like "no left turn" signs, bridge ramps that are closed during rush hours, etc. And maps know even less about traffic conditions than GPS does (or can, at least in theory). Someone who drives frequently in the real world (or, for that matter, who does almost anything in the real world) constantly has to contend with incomplete or imperfect data, and constantly revise his or her mental map or action plan based on new information. That is as true for us as it is for zebras in the wild trying to keep from being eaten by lions.

With that as context, GPS navigation is nothing short of miraculous. To someone who doesn't understand the underlying science (and I am *almost* in that category, having only a basic conceptual grasp of how it works), it is like magic -- a magical black box that knows where you are, where you are going, and how to get there, almost without limitation. When I bought my basic no-frills consumer GPS navigation device six weeks ago, I was fully prepared for an experience that fell short of my expectations. I anticipated imprecision, the occasional inaccuracy, out-of-date road data. But no. The thing has worked exactly as advertised from the moment I took it out of the box in the parking lot of the store where I bought it.

In about 5,000 miles of driving, all across the congested New York region and up and down the Eastern Seaboard, *not once* has the system steered me wrong, aside from the two or three times that it was momentarily confused about my location on startup. *Not once* has it so much as instructed me to make an illegal turn, let alone an impossible one. Half a dozen times I have thought "it must be mistaken, I'm going to ignore it and turn here instead" -- on every such occasion, it was right and I was wrong. When I divert from the recommended route (for instance, because I as a human have knowledge about traffic conditions that makes an alternate route preferable), it notices what I am doing and recalculates a new route automatically according to my wishes in about eight seconds. The sole exception is that sometimes, in a complicated stack of highway ramps (as on the approach to the Brooklyn-Battery Tunnel in lower Manhattan), it momentarily gets confused about which level I'm on. But within a few seconds, it rights itself again.

At least in this relatively densely populated part of the United States, it appears to me to have *perfect* knowledge of every street, highway, ramp, and access road -- not *significant* knowledge, not *very good* knowledge, but *perfect* knowledge. I say that knowing that it cannot be literally

true, but for all practical purposes, to me it might as well be. And on top of that, it has a surprisingly complete and current database of business addresses and phone numbers (want a bagel right now in an unfamiliar neighborhood of Danbury, Connecticut? need to find a post office in a city you have never set foot in until 5 minutes ago? It can tell you where).

The device doesn't obviate the need to have common-sense overview knowledge of unfamiliar areas before heading into them ("if the GPS device stopped working, what road would I ask directions to?"), nor the need to pay attention to make sure that the real world conforms with the map on the screen. But I would say that since getting the device, my driving paradigm has permanently changed. I still carry a stack of maps and atlases in the car, but now I only look at them when I'm heading somewhere completely new for the first time. I leave the device on all the time, even when I'm not heading anywhere in particular, so I have an overview map of my surroundings right in front of me -- which has frequently led to interesting detours I never would have thought to make without it. I go anywhere I like, in any direction, and never worry about getting lost. I freely detour from my planned route whenever I feel like it, even in completely unfamiliar areas, secure in the knowledge that I can easily find my way back (or find a more efficient route from the stopover to my ultimate destination). It is nothing short of miraculous.

[Reminder: RISKS is always short on success stories, so I am happy to run this one. PGN]

✂ 'Woman Says Being Declared Dead Ruins Life'

<"Peter G. Neumann" <neumann@csl.sri.com>>
Sat, 16 Feb 2008 7:10:36 PST

News Story - WSMV Nashville
<http://www.wsmv.com/news/15315424/detail.html?taf=nash>

✂ A reminder: Eric Sevareid's Law

<Ken Knowlton <KCKnowlton@aol.com>>
Wed, 6 Feb 2008 12:13:28 EST

(Lest we forget:)

"The chief cause of problems is solutions."
Eric Sevareid, 1970

✂ Ah yes, just what you need!!!

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

Mon, 11 Feb 2008 10:47:14 -0500 (EST)

Forwarded message:

> From: <ntisa77@yahoo.com.au>
> To: <wb8foz@panix.com>
> Subject: I've visited your website <http://www.csl.sri.com/~risko/risks.txt>
> Date: Mon, 11 Feb 2008 23:58:42 +1100
>
> Hi,
>
> We've seen your website at <http://www.csl.sri.com/~risko/risks.txt>
> and we love it!
>
> We see that your traffic rank is 0
> and your link popularity is 0.
> Also, we see that you are online since <Online since>.
>
> With that kind of traffic, we will pay you up to \$4,800/month
> to advertise our links on your website.
>
> If you're interested, read our terms from this page:
> <http://www.contactthem.ws/hit.php?s=10&p=2&w=102122>
>
> Sincerely,
>
> Ngaupokoina Isamaela
> The ContactThem Network
> 61395628930

Why am I reminded of the line from Animal House:

"And as for you, you don't even HAVE a grade point average! Zero point zero"

[David, Ngaupo obviously wants to be your Auto-Mate manager. PGN]



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 6

Monday 25 February 2008

Contents

- [Securing The Wrong Spaces: A Lesson](#)
Paul Ferguson via Gregory Hicks
- [Software problem at London Heathrow Terminal 4 affects baggage](#)
Peter Mellor
- [YouTube outage blamed on Pakistan](#)
Amos Shapir
- [One way not to conduct Internet voting](#)
Peter Kaiser
- [Being declared dead ruins life](#)
Andrew Koenig
- [New RFID ticketless bus system in Brisbane goes live... with glitches](#)
George Michaelson
- [US Treasury "TreasuryDirect" Web site security enhancements](#)
Jonathan Kamens
- [EU money for 4 small businesses IT risk mgmt pilot](#)
Patrick O'Beirne
- [Cold Boot Attacks on Disk Encryption](#)
Jacob Appelbaum
Declan McCullagh
- [Illegal drag race kills eight](#)
John Curran
- [Free-to-download password cracker](#)
Peter Mellor
- [Re: the GPS miracle](#)
Steven M. Bellovin
- [Info on RISKS \(comp.risks\)](#)

✉ Securing The Wrong Spaces: A Lesson

<Gregory Hicks <ghicks@cadence.com>>
Thu, 21 Feb 2008 01:41:57 -0800 (PST)

-- Begin Forwarded Message --

From: "Paul Ferguson" <fergdawg@netzero.net>

Date: Thu, 21 Feb 2008 07:08:58 GMT

Excerpt from techdirt.com.

A brand new Japanese warship that apparently has the country's latest and greatest radar system, was unable to spot a fishing boat in its path, leading to a collision and two missing fishermen. This is raising all sorts of questions about the quality of the radar system, but some are saying that the collision was really due to human error and that the radar system is designed more to watch out for missiles in the air, rather than ships below it.

That's a fair enough response, but does point out that vulnerabilities come from all directions -- and you can make the best system in the world, but if it's looking for the wrong thing, it won't stop something bad from getting through. It does seem rather ironic to set this ship up to be the best in the world at spotting threats from the sky -- and forget to include a decent system to find threats right next to it in the sea.

Link: <http://techdirt.com/articles/20080219/021718291.shtml>

There is a great security lesson to be learned here -- if you're focused on securing only a subset of the entire threat landscape, the insecurities will generally occur in the places you're not focusing on.

Focus on the Big Picture.

"Fergie", a.k.a. Paul Ferguson, Engineering Architecture for the Internet
fergdawg(at)netzero.net ferg's tech blog: <http://fergdawg.blogspot.com/>

[Gregory Hicks, Cadence Design Systems, 555 River Oaks Pkwy, San Jose,
CA 95134 408.576.3609]

*** Software problem at London Heathrow Terminal 4 affects baggage**

<MellorPeter@aol.com>

Thu, 21 Feb 2008 19:44:45 EST

On 19 Feb 2008, the British Airports Authority (BAA) warned passengers via its website that a software problem was causing a reduction in baggage handling capacity. <http://www.heathrowairport.com/> (According to the same website, the system is now fully operational.)

British Airways (BA) went one better and warned passengers via its website that long-haul passengers who turned up with check-in bags would not be allowed to fly! This ban affected economy class only. (Of course. What did you expect?) http://www.britishairways.com/travel/home/public/en_gb (An update on BA's website dated 21st February also announces that the system has been reinstated.)

BA's ban extended to transfer passengers. Precisely what a long-haul passenger who transferred to a BA flight at T4 already laden with hold baggage was supposed to do, was not explained.

Source of story:

http://www.theregister.co.uk/2008/02/20/heathrow_software_glitch/

Peter Mellor; Mobile: 07914 045072; email: MellorPeter@aol.com
Telephone and Fax: +44 (0)20 8459 7669

#YouTube outage blamed on Pakistan

<Amos Shapir <amos083@hotmail.com>>

Mon, 25 Feb 2008 17:21:11 +0200

Pakistan's attempts to block access to YouTube have been blamed for a near global blackout of the site on Sunday. Full story at:

<http://news.bbc.co.uk/1/hi/technology/7262071.stm>

(This looks like a misguided attempt to change DNS routing).

#One way not to conduct Internet voting

<Peter Kaiser <djc@resiak.org>>

Tue, 19 Feb 2008 23:18:05 +0100

Democrats Abroad, the US Democratic Party's organization for its members living outside the USA, sends delegates to the party's nominating convention. This year Democrats Abroad held a "Global Primary" to select the delegation's candidate. People could vote in person in a few places, but the intention was for most of the voting to be over the Internet.

Howard Dean, Democratic Party chair, said that the party would be observing the process closely, because it would be significant if Democrats Abroad held a secure, well-run election over the Internet.

But the "Global Primary" wasn't secure or well-run.

To begin with, registration to vote over the Internet was managed on unsecured web pages, an extraordinarily basic error. I brought this to the attention of a party official immediately; to her credit, she brought the objection up to the national organization, which responded that it didn't matter, because the actual voting would be secure. That's a serious lack of understanding: if registration isn't secure, then voting isn't secure because the registree's information can be hijacked. That information is also the kind that's used for identity theft.

Voting was supposed to be secure because it required a "ballot number" and PIN. These were distributed by email. Oops! Someone who could capture or

eavesdrop the outgoing mail stream delivering that information could own the vote in its entirety. Someone who could eavesdrop the mail coming to a particular address could steal that vote.

Then there was the actual process of voting, which was handled (on secured Web pages) by a third-party company. I observed a vote. After supplying the "ballot number" and PIN, the voter was informed that his browser lacked an essential plugin which would have to be installed before the process could continue. The "plugin" was Java. The voter was on a slow, expensive dialup line which would have made it very painful to find and download the software, but luckily I happened to have the Java installer with me, and I started it up.

Oops! The voter was using a Windows account without the privilege to install that software. The sketchy voting instructions indicated nothing about what would happen if the voter had to interrupt the process. Was the sign-in for one time only? If the user stopped the browser, would the process time out and give him another chance to vote later? There was no way to know: it was certain only that the process couldn't continue until the browser could use Java, and the user hadn't the privilege to install the software. In the event, I used Windows "run as" to install Java from the administrative account, and the voter was able to carry the voting process to the end. Could most users have done this? I doubt it.

The vote itself was interesting, because along with the legitimate candidates it presented some who had formally withdrawn their candidature -- e.g., John Edwards, and there was no indication what to do about that. What happened to votes for non-candidates? No way to know. And why can't an Internet vote be kept current as of when it begins by simply not presenting non-candidates?

Near the end of the process, after submitting his vote, the voter was given the choice of quitting or printing out a page showing his vote. Democrats Abroad had encouraged people to print out their votes, but it's hard to imagine why, since the special vote-printing popup page indicated clearly that it wasn't binding. So why bother?

There are well-known risks at every stage of the episode, so I repeat: that whole process was neither secure nor well-run; moreover, its collection of personal information using unsecured Web pages exposed participants to the risk of information theft, and delivering notionally secure information by email is painfully bad judgment. The episode proves nothing except that well-intentioned people continue to make elementary but serious errors in designing and setting up processes that must be safe at every step if they are to be meaningful.

Perhaps someone will bring this up to Mr Dean. My mail to the Democratic National Committee hasn't been answered.

✉ Being declared dead ruins life (Re: [RISKS-25.05](#))

<"Andrew Koenig" <ark@acm.org>>

Tue, 19 Feb 2008 09:54:46 -0500

That item reminds me of something that happened many years ago.

I had two colleagues who I'd rather not name, as you'd surely recognize them. One of them had the habit of letting (paper) mail pile up in his inbox for a week or two, then dealing with it all at once. The other was a bit of a practical joker, who one day took all of the mail piled up in the inbox, wrote "DECEASED" on each piece, and put in the outbox.

I am told that it took many months to sort out the resulting mess.

✶ New RFID ticketless bus system in Brisbane goes live... with glitches

<"George Michaelson" <ggm@pobox.com>>

Sat, 23 Feb 2008 15:47:11 +1000

Brisbane has deployed an RFID based ticketless smartcard bus system its calling the 'go' card. The integrated travel system is described at http://en.wikipedia.org/wiki/TransLink_%28South_East_Queensland%29 And the ticketing system provider is Cubic http://en.wikipedia.org/wiki/Cubic_Transportation_Systems%2C_Inc.

The system has been under test in the northern part of the network, and will be deployed citywide on Monday the 25th. Its actually already live, its just the card supply/distribution issue which is formally released next week.

The system demands you cardswipe on and off, and computes journey values, and inter-system transfers. It uses GPS in buses and ferries, and station boundaries. From my observations, the system uses GPS quite heavily, and the drivers have a low level of engagement (at this time at least) in the system, concentrating on the (hopefully fewer) cash paying fares.

I got myself and my son a card, and we found it was live on friday, so used it.

From one days use, I had one problem, for 2 journeys. One was that because the bus uses GPS, and bus drivers in extremis stop at non-scheduled stops, but the readers are designed to not enable card operations except either when commanded by the driver, or at scheduled stops, it was not able to cardswipe me off. (presumably, after driver training, they will know how to enable this).

The second was that having not been recorded off, yet getting on another bus inside 5 minutes, while I was carded off the first bus by the system, it refused to consider it a legal transfer, and recorded two journeys, one for the maximum fare. Refund pending, 10 day turnaround, after I rang in.

There is a third fault, recorded in local newspapers: the system doesn't work in underground stations without driver override, presumably because

the GPS can't work. Again, resolved after training, if they command/override.

The system already had a 'upgrade day' failure when an attempted test at a few locations accidentally took down a major portion of the network for railway stations.

My observation: Any new system is going to have glitches, but from my experience, failure for a random singleton is a bit of a worry. At least my son had a perfect score on his one. Operator training would have resolved my problem, if its still lacking 2 days before official launch, you have to worry that the refund phone desk is going to melt down next week. So if I take the best case, from 2 sample individuals for 4 journey instances on 8 buses, thats still 12% failure. On a lightly loaded system (both of us were the only card users for our journeys)

I could complain that the system uses simply AWFUL warning messages such as "card reader not in service" when the bus is moving, rather than something human-centric such as "bus in motion: swipe off disabled" (or something) -the system as a whole is quite obviously working, the readers should not be implying they are dysfunctional.

But more worryingly, the systems designers seem to be making some system design mistakes here. Humans and Human systems ARE NOT BLACK BOXES. So by designing a system with GPS, which attempts to forbid fare dodges by refusing to card off except at scheduled stops, they have taken two very useful 'side effect' behaviours out of the bus system: getting off the bus at non-scheduled stops, and getting off the bus between stops. Both are very common, both are until now entirely normal for many users of the system but both are apparently outside their system design plan and both have a strong financial penalty if the driver now doesn't (or can't) command/override the system. And designing a system with GPS, but which can't work in underground stations, when the system has at least two, with several more in planning, seems odd.

Thirdly, it seems unfortunate that they can card me off the first bus when I card on the second, but can't short-circuit the excess fare reclaim. I'm trying to understand the likelihood that what that represents is an attempted gaming of the system, vs a legitimate user who is continuing their trip. I would have expected that it was within the system loss tolerances to at least try to start it preferencing the good case. Instead of which, if you don't register online, and audit your card, you can wind up losing quite significant amounts of money if the journey you don't card 'off' on has a high maximum value. For instance, the stop I did get off on, and the stop I did get on the next bus were within 150m of each other. I wonder if the GPS precision has been dialed up too high? (nobody should care about bus journeys under 150m, and the same card being used inside 30min inside 150m distance looks to ME like a valid event)

I still laud Brisbane Transport for doing this. Integrated ticketing is wonderful, as anyone who has used the Hong Kong system, or any of the worldwide 'Oyster' card deployments which I believe followed on from it. By comparison Sydney transport has just imploded on a smartcard contract, and their bus operator is buying up surplus ex-Brisbane driver-operated ticket

consoles, to expand the pre-RFID/smartcard system.

On the more security-conscious level, bus passengers who use the system, and register the card (you have to, to claim refunds or ensure against cardloss, which can hold up to \$AU 200 in value) are now positionally accurate when on a bus to within 10m, which presumably has some Philip-K-Dick manifestation for the (police)man amongst us.

✈ US Treasury "TreasuryDirect" Web site security enhancements

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

Tuesday, January 29, 2008 8:06 PM

The US Treasury offers www.TreasuryDirect.gov for purchasing and managing a portfolio of securities issued by the Federal government.

They've made some effort over time to make the site secure, and they've recently been beefing up security. I'd like to share details about two of their new security features.

When you log into the site, it asks you for your account number and your password. However, you can't type your password. Instead, you are presented with a "virtual keyboard" whose keys have been scrambled, such that you have to hunt around for the characters in your password and click them one by one in order to enter it.

Above the keyboard, it says, "A virtual keyboard, with keys that display in random order, is available to deter others from learning your password."

The words "virtual keyboard" are a link, which pops up the following text (from

<http://www.treasurydirect.gov/indiv/help/TDHelp/help_ug_274-SecFeaturesProtectAcctLearnMore.htm>

<http://www.treasurydirect.gov/indiv/help/TDHelp/help_ug_274-SecFeaturesProtectAcctLearnMore.htm>) when you click on it:

Virtual Keyboard: The virtual keyboard is one of many new security features introduced in TreasuryDirect as part of our on-going commitment to heightened password and account security to protect our customers' investments. The advantage of using the virtual keyboard, with keys that display in random order each time you log in, is that others are deterred from learning your password and Access Card information.

When Java-Script is enabled, each time you arrive at the "Access your TreasuryDirect Account" page to log in, you will be presented with this virtual keyboard to enter your password. You'll use your mouse with the virtual keyboard to enter the letters, numbers, and special characters that are contained in your password.

If you have received your Access Card, you'll also use the virtual keyboard to enter your Access Card values.

(More about the Access Card in a minute.)

To enter my password with this new keyboard, I must move my mouse slowly over it, search for each of the characters in my password, and pause over each one while I click it and then look at and count the number of characters in the password field to confirm that the last one was entered correctly. Then I have to do it all over again because I made at least one mistake the first time. All this on a "keyboard" in full view of anyone who can see my screen.

It is unfathomable to me how the people who designed this feature could possibly think that it is more secure than typing a password on a keyboard.

Now, about those "Access Cards". A few weeks ago, I got email from the Treasury notifying me that they were going to be sending me an access card which would be required in the future for accessing my account. About a week ago, they sent me a separate email message notifying me that the card would be arriving very soon, and I should contact them if I did not receive it within ten days. They also said that shortly after I received the card, I would no longer be able to log into the site without it.

The card itself has a bar code, a nine-digit decimal serial number, and a grid with ten columns labeled A through J and five rows labeled 1 through 5. At the intersection of each row and column is a random letter or number, for a total of fifty. Once the access card is enabled for my account, after I enter my username and password, the site will display a drop-down list with several serial numbers, only one of which is actually mine, and with three grid coordinates (e.g., "C2"). To finish logging in, I will have to select the correct serial number and then enter (using the virtual keyboard) the three characters corresponding to the displayed grid coordinates. A demonstration of how this works can be viewed at <http://www.treasurydirect.gov/indiv/help/TDTutorial/tutorial.htm> <<http://www.treasurydirect.gov/indiv/help/TDTutorial/tutorial.htm>>.

I don't know whether this technology was purchased from a third party or invented by the Treasury. It's an interesting attempt to implement inexpensive two-factor authentication. It's better than nothing, but it's obviously useless at preventing illicit access by people who are in physical proximity to the account owner, since they can simply sneak a photocopy of the card when the owner isn't looking.

✂ EU money for 4 small businesses IT risk mgmt pilot

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

Thu, 21 Feb 2008 10:11:00 +0000

http://www.enisa.europa.eu/pages/micro_enterprises_pilot.htm

Building information confidence with micro enterprises
Pilots for the introduction of Risk Management process

ENISA issues a call to identify potential pilots to participate in a Risk

Management promotion activity. The selected pilots will be financially supported by ENISA with maximum 20000 euros to install Risk Management within their IT infrastructure and perform an initial Risk Assessment. The selection criteria are stated below (see Background).

Potential pilots are requested to use the attached form to send information relevant to their organisation and to the scope of a possible Risk Management introduction project. Proposals can be sent to ENISA until 29 Feb 2008.

Main criteria for the pilots are their size, sector and geographical spread among different areas of Europe. In order to select potential pilots ENISA will use the following selection criteria:

With the pilot ENISA wants to support small and micro enterprises in the introduction of Risk Management The potential pilot can be performed in cooperation with a multiplier organisation that guarantees the inclusion of multiple small/micro enterprises (i.e., small SMEs) The benefits from the pilot for the participating enterprises must be evident The pilot will maximise inclusion of multiple stakeholders (e.g. dissemination potential) The pilot consists of a group of small/micro organisations building up a network (e.g. part of a supply chain, independent members of a distributed structure etc.) The subject of the pilot must be the available ENISA material or alternatively an existing good practice in the area of Risk Management in Europe The pilot activity will be defined in some detail (plans, participants).

Patrick O'Beirne, Systems Modelling Ltd. <http://www.sysmod.com/>
(+353)(0) 5394 22294

*** Cold Boot Attacks on Disk Encryption (via Dave Farber's IP)**

*<Jacob Appelbaum <jacob@appelbaum.net>>
February 21, 2008 12:34:09 PM EST*

With all of the discussions that take place daily about laptop seizures, data breach laws and how crypto can often come to the rescue, I thought the readers of IP might be interested in a research project that was released today. We've been working on this for quite some time and are quite proud of the results.

Ed Felten wrote about it on Freedom To Tinker this morning:
<http://www.freedom-to-tinker.com/?p=1257>

"Today eight colleagues and I are releasing a significant new research result. We show that disk encryption, the standard approach to protecting sensitive data on laptops, can be defeated by relatively simple methods. We demonstrate our methods by using them to defeat three popular disk encryption products: BitLocker, which comes with Windows Vista; FileVault, which comes with MacOS X; and dm-crypt, which is used with Linux. The research team includes J. Alex Halderman, Seth D.

Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten."

"Our site has links to the paper, an explanatory video, and other materials."

"The root of the problem lies in an unexpected property of today's DRAM memories. DRAMs are the main memory chips used to store data while the system is running. Virtually everybody, including experts, will tell you that DRAM contents are lost when you turn off the power. But this isn't so. Our research shows that data in DRAM actually fades out gradually over a period of seconds to minutes, enabling an attacker to read the full contents of memory by cutting power and then rebooting into a malicious operating system."

Our full paper with videos and photos can be found on the Princeton website: <http://citp.princeton.edu/memory/>

Re: Cold Boot Attacks on Disk Encryption (via Dave Farber's IP)

<Declan McCullagh <declan@well.com>>
February 21, 2008 3:57:43 PM EST

The paper published today makes some pretty strong claims about the vulnerabilities of Microsoft's BitLocker, Apple's FileVault, TrueCrypt, Linux's dm-crypt subsystem, and similar products.

So I put the folks behind it to a test. I gave them my MacBook laptop with FileVault turned on, powered up, encrypted swap enabled, and the screen saver locked.

They were in fact able to extract the 128-bit AES key; I've put screen snapshots of their FileVault bypass process here:
http://www.news.com/2300-1029_3-6230933-1.html

And my article with responses from Microsoft, Apple, and PGP is here:
http://www.news.com/8301-13578_3-9876060-38.html

Bottom line? This is a very nicely done attack. It's going to make us rethink how we handle laptops in sleep mode and servers that use encrypted filesystems (a mail server, for instance).

Archives: <http://www.listbox.com/member/archive/247/=now>
RSS Feed: <http://www.listbox.com/member/archive/rss/247/>

Illegal drag race kills eight

<"Curran, John" <John.Curran@mms.gov>>
Tue, 19 Feb 2008 13:30:00 -0500

Last weekend an illegal drag race in the Washington, DC suburbs ended in tragedy when a car (not involved in the race) plowed into a crowd of people who had gathered to watch the race. This column from the **Baltimore Sun** puts an interesting light on the idea of risks for those who routinely take part in something like the race.

The writer spoke to a scientist who specializes in risk perception. The key remark from the piece:

"Peters is a research scientist who specializes in risk perception, a psychologist who works for a think tank called Decision Research that studies, basically, why people do what they do. I had called seeking wisdom on why someone - or many someones, as it turns out - would gather on a dark, desolate highway in the middle of the night and wander onto it to watch people drive like maniacs.

Peters had seen news reports of the crash, and was struck by the seemingly festive nature of the gathering, until it turned fatal, that is.

"Everyone's out there, it seems like it's good old-fashioned fun, it's a very party-like atmosphere," she said. "There's the familiarity of it - people had done this before, and it had never been a problem before."

Peters said it's that familiarity that makes even the obviously risky - walking onto a thoroughfare, after two fast and furious cars have screamed past you - seem like perfectly normal behavior."

http://www.baltimoresun.com/news/local/bal-md.marbella19feb19_0,2107578.column

John Curran, OMM Program IT Security Manager, CISSP, CISM, IAM 703-787-1712

[See also The Psychology of Risks, Dr. Leonard S. Zegans, in the December 2007 Inside Risks column in the **Communications of the ACM**.

<http://www.csl.sri.com/neumann/insiderisks07.html#211>]

✂ Free-to-download password cracker

<MellorPeter@aol.com>

Mon, 25 Feb 2008 09:59:59 EST

If this is as good as it purports to be, let's hope that only the white-hats use it!

RainbowCrack is a general propose implementation of Philippe Oechslin's faster time-memory trade-off technique. In short, the RainbowCrack tool is a hash cracker. A traditional brute force cracker try all possible plaintexts one by one in cracking time. It is time consuming to break complex password in this way. The idea of time-memory trade-off is to do all cracking time computation in advance and store the result in files so called "rainbow table". It does take a long time to precompute the

tables. But once the one time precomputation is finished, a time-memory trade-off cracker can be hundreds of times faster than a brute force cracker, with the help of precomputed tables.

<http://www.antsight.com/zsl/rainbowcrack/index.php>

Peter Mellor; +44 (0)20 8459 7669 MellorPeter@aol.com

Re: the GPS miracle (Mintz, [RISKS-25.05](#))

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Tue, 19 Feb 2008 04:28:57 +0000

I'm glad it's worked for you. I find that it *usually* works well for me. However, mine -- purchased just 2.5 months ago -- tried to steer me through dead-end streets twice on a single drive within 20 miles of my house in New Jersey... The first time, I decided to see if the Dead End sign was wrong. It wasn't; the GPS was.

The other thing I noticed -- from getting it wrong a couple of times -- is that at complex intersections or where two possible turns are very close to each other, it's very easy to misunderstand which turn it wants you to make. I doubt there's any good technical solution to that short of a heads-up display showing the route it wants you to take, overlaid on reality.

It is great, and I still use it. But I'm much less sanguine about the correctness of its database.

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



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 7

Saturday 1 March 2008

Contents

- [Risks of Leap Years and Dumb Digital Watches](#)
[Mark Brader](#)
 - [Risks of Leap Years and Dumb Airline Software](#)
[PGN](#)
 - [\\$1.2 billion up in smoke](#)
[Paul Saffo](#)
 - [Southeast Florida Massive Power Outage](#)
[Steven J. Greenwald](#)
 - [FL power failure triggered by human error](#)
[Lauren Weinstein](#)
 - [Competent? We can't even archive our own e-mail reliably!](#)
[Jim Horning](#)
 - [DreamHost Accidentally Bills Customers \\$7,500,000](#)
[Dan Jacobson](#)
 - [IT Project Failure Blog](#)
[Ken Dunham](#)
 - [Is the "law of unintended consequences" biting W3C DTD reference?](#)
[George Michaelson](#)
 - [Pakistan, YouTube, Google, and No Simple Answers](#)
[Lauren Weinstein](#)
 - [Re: YouTube outage blamed on Pakistan](#)
[R A Lichtensteiger](#)
[Richard Grady](#)
[Jay R. Ashworth](#)
 - [Cold Boot Attacks: Vulnerable While Sleeping](#)
[Ed Felten via Monty Solomon](#)
 - [Citibank needs a clue](#)
[Rich B. Astaird](#)
 - [Re: Hoist by one's own petard: data security: UK Child Benefits](#)
[Merlyn Kline](#)
 - [REVIEW: "Better Ethics Now", Christopher Bauer](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Risks of Leap Years and Dumb Digital Watches

<msb@vex.net (Mark Brader)>

Fri, 29 Feb 2008 03:15:30 -0500 (EST)

All right now, how many people reading this:

[1] saw a previous version of this message in [RISKS-6.34](#), 13.21, 17.81, 20.83, and/or 23.24?

[2] 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

[3] *hadn't realized it yet*?

Personally, I first remembered it was time for my quadrennial posting and only then that I therefore needed to reset my own watch...

Mark Brader, Toronto, msb@vex.net

✂ Risks of Leap Years and Dumb Airline Software

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

Sat, 1 Mar 2008 8:15:24 PST

Passengers using United Airlines' Easy Check-In were unable to print out boarding passes for several hours on Friday 29 Feb 2008. This was not a problem four years ago, and apparently came as a surprise to UAL.

[Source: A short AP item spotted in the *San Francisco Chronicle* this morning. PGN-ed]

✂ \$1.2 billion up in smoke

<Paul Saffo <psaffo@mac.com>>

Fri, 22 Feb 2008 22:04:35 -0800

There is something deeply obscene about the idea of a \$1.2 billion plane to begin with, but the thought of it burning up only brings to mind what myriad other, better purposes that money could have been put to... p

B-2 Stealth Bomber Crashes on Guam, The Associated Press, 23 Feb 2008

A B-2 stealth bomber crashed [on 23 Feb 2008] at an air base on Guam, but both pilots ejected safely and were in good condition, the Air Force said. It was the first crash of a B-2 bomber.

The accident occurred 11 days after a Navy plane crashed into the ocean about 20 miles northeast of Guam's Ritidian Point. Four aircrew members ejected from the EA-6B Prowler electronic warfare aircraft and were rescued

by helicopter.

Southeast Florida Massive Power Outage

<"Steven J. Greenwald" <sjg6@gate.net>>

Tue, 26 Feb 2008 18:19:41 -0500

PGN asked me to write up something regarding the Southeast Florida power outage because of my location (North Miami). I don't really know much more than what the new media have reported, but I can give some local anecdotal accounts.

According to my UPS software, power failed today (February 26, 2008) at 13:09:12. This jibes with news media accounts of power failing at 9 minutes after 1pm.

Million of people lost power (I heard 2.3 million at one point).

I first heard that the two Turkey Point nuclear reactors just south of Miami (Key Biscayne National Park area) shut down as well as the two coal plants at the same site. This peaked my interest, especially because we have no coal powered plants at that site (we do have two gas powered plants at that site, in addition to the two nuclear reactors). I have yet to get in touch with a contact that works for Florida Power & Light (FPL) at that site (he monitors the endangered salt water crocodile population that thrives at the Turkey Point site).

Later reports stated that a total of 8 power plants shut down. I don't know specifics, but heard that the other 3 nuclear plants in the state did not shut down (Crystal River (1), and Port Saint Lucie (2)). Miami's mayor reported "It was not sabotage" early on (I congratulate him on his technical expertise). Recently (approximately 17:10) FPL has reported that the failure got caused by a substation equipment failure in the western part of Miami-Dade county (the Everglades?).

Huge sections of Miami-Dade county endured long blackouts (as I write this about 800,000 "customers" still have no power). Broward county (just north of us) endured many surges, and outages occurred as far north as Daytona (according to the news media) and as far south as the Florida Keys.

Many people evacuated high-rise office buildings in downtown Miami. The Wachovia building (44 stories) currently serves as the news media focus, as people had to walk down 44 flights of stairs (some in high heels; office workers in tall buildings might want to keep backup sneakers by their workstations). Why a building like that does not have backup power remains a great mystery to me. Many felt thankful they did not get stuck in elevators.

Traffic lights went out across the country causing massive traffic problems that still have not gotten resolved as I write this (17:25). Again, I wonder why the traffic lights do not have backup power.

Most businesses gave employees the rest of the day off, which I suppose just exacerbated the traffic snarls. The county schools kept students on-site. Our train system failed, and the country has finally sent school buses to the stations to move the people.

Many people eating lunch had problems paying, and many restaurants had to add up bills manually, which evidently caused some problems due to innumeracy and computer issues.

My fiancée, Laura Corriss, who works at Barry University (Miami Shores), reports that they never lost power and did not suspend classes. Her brother Michael reported that power went out on Miami Beach.

Our friend Myfanwy James who works at a law office on the 14th floor of a building in the Brickell area (near downtown Miami) reports that they lost power so she took the emergency elevator down (the building has a generator) and went home. She reported a lot of traffic snarls, but nothing else.

Another friend, Vivian Marthell (a local artist specializing in the intersection of art and technology/science), reports that in her area (downtown Miami) the expressway appeared totally backed up. Expressway totally backed up. Vivian, an all-around smart person, asked me, "You know the old Emergency Broadcast System? Why can that get done using wireless technology so that we could find out about these things faster, and get updates?" I must give Viv total credit for this idea (I have not heard it before); if anyone wishes to contact her feel free to send me a note and I will put you in touch.

Another contact reports that school children in a South Miami school got evacuated because their classrooms had no windows (no light, air, etc.).

I have nothing else to report, but now it starts to get dark.

FL power failure triggered by human error

*<Lauren Weinstein <lauren@vortex.com>>
Fri, 29 Feb 2008 17:54:46 -0800 (PST)*

A field engineer was diagnosing a switch that had malfunctioned. Without authorization, he disabled two levels of relay protection. This affected 26 transmission lines and 38 substations. [PGN-ed]

<http://www.cnn.com/2008/US/02/29/florida.outage/index.html?iref=mpstoryview>

Competent? We can't even archive our own e-mail reliably!

*<"Jim Horning" <Jim.Horning@sparta.com>>
Wed, 27 Feb 2008 13:20:18 -0800*

A former White House technology manager told the committee that the Bush administration's e-mail system "was primitive and the risk that data would be lost was high." More than 1000 days worth of e-mail has vanished.

[PGN-ed]

[Try <http://horning.blogspot.com>. The *WashPost* URL moved.]

✂ DreamHost Accidently Bills Customers \$7,500,000

<Dan Jacobson <jidanni@jidanni.org>>

Thu, 07 Feb 2008 04:03:17 +0800

<http://blog.dreamhosters.com/2008/01/15/dreamhost-accidently-bills-customers-7500000/>

The billing glitch happened when Josh was manually running the billing script for the last two weeks. Instead of inputting the billing date as 2007-12-31, he ran the script for 2008-12-31...

✂ IT Project Failure Blog

<"Ken Dunham" <kdunham@rogers.com>>

Tue, 12 Feb 2008 12:09:37 -0500

Michael Krigsman maintains a blog on ZDNet summarizing a wide range of IT project failures: <http://blogs.zdnet.com/projectfailures/>

✂ Is the "law of unintended consequences" biting W3C DTD reference?

<George Michaelson <ggm@apnic.net>>

Sat, 9 Feb 2008 14:48:26 +1000

The blog

http://www.w3.org/blog/system/2008/02/08/w3c_s_excessive_dtd_traffic says that badly written software which doesn't cache, or work out what it doesn't need, is fetching the DTD reference that everyone points at the W3C, around 130,000,000 times a day, or 350Mbps of resources.

Does this remind anyone of the time the home-box vendors put a university's NTP server address in firmware? except this time, (and I don't really mean this, but it is in my mind...) the W3C sort-of did it to themselves..

The blogs mention remediation such as relocating the URL to paths more amenable to anycast or other distribution methods. Doubtless this will solve itself in time.

✶ Pakistan, YouTube, Google, and No Simple Answers (Re: [RISKS-25.06](#))

<Lauren Weinstein <lauren@vortex.com>>

Tue, 26 Feb 2008 17:29:57 -0800 (PST)

[From Network Neutrality Squad (www.nnsquad.org)]

The Pakistan/YouTube story brings together a number of different elements that touch on Network Neutrality (and what I might call "content neutrality") in various ways that are useful to examine further, even though we may stray away from the central network neutrality focus momentarily.

First, I'll offer a comment regarding my use of the term "religious zealots" relating to take-down demands at YouTube. No quibbling -- as far as I'm concerned anyone who wishes to block the entire planet from seeing material that one religious group feels is distasteful or blasphemous (for religious reasons) is a zealot. It makes no difference if we're talking about any of the world's major religions or the "Slackers" at the Church of the SubGenius -- the same standards apply.

Now, if a country wants to *try* block their population from certain Internet materials, that may be their right, however ineffective such efforts will ultimately be (<http://lauren.vortex.com/archive/000229.html>).

But when those efforts impinge on the rights and access of everyone else, we enter an unacceptable situation. In the case of Pakistan's disrupting YouTube routes globally, I'm perfectly willing to accept the explanation that this was a combination of error and fundamental routing vulnerabilities. The latter in particular is a topic for another time.

But the fact that Google reportedly pulled down the video in question that triggered this entire situation is of much greater concern. The fact that this video could be seen as violating particular YouTube rules is notable, but questions of the equality, "neutrality," and global impact of those very rules are of even more import.

I appreciate -- in fact I applaud -- the need for Google to be responsible with their sites' contents. But we repeatedly see a double standard in this regard that is increasingly difficult to fathom.

If you show up at Google with a DMCA take down order, you generally get a rapid response. This is understandable -- DMCA is the law -- at least at the moment.

But it's far less clear why Google should permit religious demands to (attempt) to censor material globally as reportedly occurred in this situation. Pakistan's laws and religious sensibilities don't trump the rest of the world's rights, nor should any country have a veto over what other countries' populations can access.

This situation is made all the more perplexing by Google's routine refusal in most cases to act in instances of *individuals* being defamed or

otherwise damaged by Web sites that prosper solely on the basis of high-ranking Google search results. I've made a number of past proposals relating to this area (e.g. "Search Engine Dispute Notifications: Request For Comments" - (<http://lauren.vortex.com/archive/000253.html> and linked items), plus I've previously discussed how Google has made an initial step in a relevant positive direction relating to news sources ("Google Takes First Key Step Toward Search Dispute Resolutions" - <http://lauren.vortex.com/archive/000267.html>).

However, for the vast majority of conventional (non-news source) Web pages in Google search result listings, concerned parties have no effective mechanism to comment or otherwise flag results to indicate that serious disputes are in progress, so they effectively have no recourse.

This then is the dichotomy. Certain classes of content and complaints result in action from Google, and others simply do not.

What's particularly depressing about this situation is that -- in my opinion -- Google appreciates that this is a problem, but feels that they can't risk really dealing with it. In fact, I've discussed some of these issues face-to-face with various Google folks (especially in the context of my "Urgent Call For a Google At-Large Public Ombudsman" - (<http://lauren.vortex.com/archive/000251.html>) and I've come away with the strong impression that they felt both sympathetic and impotent in this instance.

Google impotent? A contradiction in terms? Not really. My sense is that they are very concerned that if they opened the door broadly to these kinds of complaints, they'd be flooded with aggrieved parties and be essentially paralyzed as a result.

I definitely do agree that there are serious scalability issues that impact on these matters, but I don't feel that these issues present intractable problems, and I don't consider the alternative of the status quo to be acceptable.

However, these are all of course decisions for Google to make, and my effective influence over events up at the Googleplex is nil.

What this all boils down to is that these are complex situations with few clear-cut, off-the-shelf answers waiting to be plucked. But we can try to work our way through them to the best of our abilities, and ideally with as little animosity and as much good will as possible.

Lauren Weinstein, NNSquad Moderator

Re: YouTube outage blamed on Pakistan (Shapir, [RISKS-25.06](#))

<R A Lichtensteiger <rali@tifosi.com>>
Mon, 25 Feb 2008 19:15:56 -0500

It was a local route leaked into the global BGP mesh.

AS 17557 (PKTELECOM-AS-AP Pakistan Telecom) announced a route for the netblock YouTube is in and was sinking the traffic locally. Except that the BGP announcement of the routes "leaked" out to their upstream provider, PCCW. From PCCW, it spread, and therefore lots of places saw that as a shorter route to the YouTube servers than the legitimate announcement.

According to reports I've seen, the YouTube/Google engineering staff tried to override the announcement on that netblock by announcing a pair of specific (/25) routes for the same block. That didn't work out because most network providers filter out announcements for space smaller than a /24.

The risk and lesson? "Trust, but verify," of course.

Had PCCW implemented filters on inbound BGP announcements and limited it's downstreams to only those netblocks it has, this wouldn't have happened.

The network of networks is built on trust; it has to be, because the whole point to the thing is to push management out toward the edges and decentralize the system. But there +are+ safety valves -- places you can examine the incoming data and sanity check it. PCCW didn't. How many other's don't either? And how many of them are having engineering conferences right now trying to make sure they aren't the next cause of a high profile outage like this one?

Only time will tell.

[Noted by others. For example, Anthony DeRobertis suggested "A quick visit to routeviews.org's bgplay shows the mistake fairly clearly."
<http://bgplay.routeviews.org/bgplay/>

Andrew Pam cited

<http://arstechnica.com/news.ars/post/20080225-insecure-routing-redirects-youtube-to-pakistan.html>

Tore A. Klock recommended a writeup by Danny McPherson here on what (most likely) happened:

<http://asert.arbournetworks.com/2008/02/internet-routing-insecurity-pakistan-nukes-youtube/>
PGN]

✉ Re: YouTube outage blamed on Pakistan (Shapir, [RISKS-25.06](#))

<Richard Grady <richard@richbonnie.com>>
Mon, 25 Feb 2008 19:52:21 -0800

The referenced story <http://news.bbc.co.uk/1/hi/technology/7262071.stm> says

"The government has valid reason for that, but they have to find a better way of doing it. If we continue blocking popular websites, people will stop using the Internet."

Perhaps that is the real agenda. Block all the good sites, and the people will give up using the Internet.

[Fat chance. PGN]

✂ Re: YouTube outage blamed on Pakistan (Shapir, [RISKS-25.06](#))

<"Jay R. Ashworth" <jra@baylink.com>
Tue, 26 Feb 2008 16:16:39 -0500

The Pakistani PTT was *apparently* using BGP advertisements to hijack YouTube's IP address range, and redirect it to some in-country machines that displayed a message saying that YouTube was Baaaaad.

Alas, those announcements, which shouldn't have been leaked *out* of the Pakistani Autonomous System (AS 17557), and then shouldn't have been permitted to leak *into* any of their upstreams... did.

Here's regular RISKS contributor Steve Bellovin's take on it:

<http://www.cs.columbia.edu/~smb/blog/2008-02/2008-02-24.html>

It has a link at the very bottom to a much more in-depth treatment from BGP-watchers Renesys:

http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube.shtml

RISKS? Well, the top one I see is people saying "oh, it's just YouTube." What happens next time, when it's not YouTube, it's eTrade?

This one was very probably just sloppy network engineering. That doesn't mean the next one *won't* be an attack. Just because hoofbeats usually mean horses, don't forget that there *are* zebras out there. (That is the original intent of the medical quote, in case you ever wondered...)

Jay R. Ashworth, Ashworth & Associates, St Petersburg FL jra@baylink.com
<http://baylink.pitas.com> <http://photo.imageinc.us> +1 727 647 1274

✂ Cold Boot Attacks: Vulnerable While Sleeping (Ed Felten)

<Monty Solomon <monty@roscom.com>>
Fri, 29 Feb 2008 17:32:06 -0500

[From Ed Felten's blog 26th Feb 2008 <http://www.freedom-to-tinker.com/?p=1258>]
(Re: [RISKS-25.06](#))

Our research on cold boot attacks on disk encryption has generated lots of interesting discussion. A few misconceptions seem to be floating around, though. I want to address one of them today.

As we explain in our paper, laptops are vulnerable when they are "sleeping"

or (usually) "hibernating". Frequently used laptops are almost always in these states when they're not in active use - when you just close the lid on your laptop and it quiets down, it's probably sleeping.

When a laptop goes to sleep, all of the data that was in memory stays there, but the rest of the system is shut down. When you re-open the lid of the laptop, the rest of the system is activated, and the system goes on running, using the same memory contents as before. (Hibernating is similar, but the contents of memory are copied off to the hard drive instead, then brought back from the hard drive when you re-awaken the machine.) People put their laptops to sleep, rather than shutting them down entirely, because a sleeping machine can wake up in seconds with all of the programs still running, while a fully shut-down machine will take minutes to reboot. [...]

✂ Citibank needs a clue

<Rich B. Astaird>
Fri, 29 Feb 2008

I just dug an e-mail from Citibank out of the Spam folder. I know it's really them because they have my full name and the last four digits of my card number listed inside. It was a very "Important Message":

Dear Rich B. Astaird,

As a current Citi Cardmember, you know your security is our top priority. But we also want to make sure you receive emails containing important information from us.

Don't let Citi messages be filtered out by your e-mail provider - add our "from addresses" to your address book.

Follow these 3 simple steps:

1. Open your e-mail address book
2. Add a contact or "add new contact"
3. Enter `citicards@info.citibank.com` and click Save

As reported previously in RISKS, some banks don't seem to have a clue about how to use email securely. Or, in this case, how to keep their email out of the Spam folder. It's not: just ask Mr. SpamAssassin what not to do:

```
> Content analysis details: (5.1 points, 5.0 required)
>
> pts rule name          description
> -----
> 3.1 RCVD_IN_NJABL_SPAM  RBL: NJABL: sender is confirmed spam source
>                          [216.35.62.93 listed in combined.njabl.org]
> -0.0 SPF_HELO_PASS     SPF: HELO matches SPF record
> 0.0 HTML_MESSAGE       BODY: HTML included in message
> 2.0 FROM_EXCESS_BASE64  From: base64 encoded unnecessarily
```

A quick check on the IP address (bigfootinteractive.com, a company known for its bulk mailings and spammer-like behavior), shows it is also listed in the SORBS and CSMA blacklists. Let's see, if I were Citibank, and wanted to stop my mail from getting flagged as spam, would I (a) stop outsourcing my email to a company with a reputation for spamming, or (b) send vaguely-worded email to my customers in the hope that it will convince them to whitelist my return address?

The worst-case RISK is that people who use a provider where such instructions actually work will follow them, and then every phishing email trying to steal their Citibank credentials will sail right through.

Way to go, Citibank!

Very truly yours,

(not) Rich B. Astaird

Re: Hoist by one's own petard: data security: UK Child Benefits

<"Merlyn Kline" <merlyn@zynet.net>>

Tue, 5 Feb 2008 09:30:23 -0000

(Cherry, [RISKS-25.04](#))

> I'm surprised that no mention has been made of one Jeremy Clarkson, ...

Perhaps not mentioned because it bears no real relevance. The UK direct debit system is set up so that anybody who is empowered to create direct debits can do so with no more than the information that, as Clarkson originally said, is published on every cheque we write (among other places). The system is designed to make it easy for companies such as utilities to set up direct debits. The security is in the careful vetting by the banks of the companies so empowered, and the guarantee that the banks make to their customers: that if a direct debit is ever used to take money from your account without your permission, they will refund it without question. Clarkson could presumably avail himself of the benefit of this guarantee if he so chose. It probably serves him better not to do so in this case.

What has happened here is that the charity which has received the money has either over-stepped the line of its own direct debit agreement with the bank, or has had its own security compromised in some way which has nothing to do with Clarkson's publication of his bank details (or, indeed, the loss of Child Benefit records). Under the circumstances I suppose it seems churlish to all concerned to go after the charity, as would otherwise normally happen.

So Clarkson was right first time round and to have so publicly reversed his position does not seem well.

REVIEW: "Better Ethics Now", Christopher Bauer

<Rob Slade <rmslade@shaw.ca>>

Mon, 25 Feb 2008 12:04:05 -0800

BKBEEETNO.RVW 20071118

"Better Ethics Now", Christopher Bauer, 2005, 978-0-9765863-3-3,
US\$21.99/C\$29.99

%A Christopher Bauer chris@bauerethicsseminars.com

%C 1604 Burton Ave., Nashville, TN 37215

%D 2005

%G 0-9765863-3-9 978-0-9765863-3-3

%I Aab-Hill Business Books

%O US\$21.99/C\$29.99 615-385-3523

%O <http://www.amazon.com/exec/obidos/ASIN/0976586339/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0976586339/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0976586339/robsladesin03-20>

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

%P 171 p.

%T "Better Ethics Now: How to Avoid the Ethics Disaster You Never
Saw Coming"

A note on the title page of the book states that the text is intended to educate and entertain in regard to ethics, and that the material is neither comprehensive nor tested. (It is ethical to let the reader know that, although my initial reaction was that the "entertain" aspect might have been a bit of an abdication of the author's responsibilities to the readers.) The introduction asserts that the focus of the work is on how a lack of personal responsibility creates the foundation for corporate ethical disasters, and that having individuals improve their own ethical standards will enhance the integrity of the company. There is, of course, something to this, although it does fly in the face of a great many studies identifying the "tone at the top" as the major determinant of corporate ethical standards.

Chapter one notes that ethical breaches in companies have serious financial ramifications, and reiterates the position that assessing your own morals will improve those of the company, primarily by forcing you to determine if the normal business behaviour you are asked to follow is ethical. (This does tie back to the issue of "tone at the top": if your ethics stand up to scrutiny and you feel comfortable in your working environment, the tone is probably OK.) Ethics are guiding principles, chapter two tells us. It isn't just following (or even breaking) rules, says chapter three. Chapter four seems to repeat this last, in slightly different wording, properly taking issue with the subject of "compliance," which has become something of a buzzword and panacea in recent years. Using cute expansions of "ethics" as an acronym, chapter five tentatively introduces the idea of personal responsibility and decision. A simple tool for personal assessment is described in chapter six. Chapter seven examines the issues of reporting or otherwise dealing with ethical violations that you discover.

Chapter eight moves the discussion to the corporate level, noting the importance of policy statements, processes, and procedures. Ethical behaviour involves achieving positive actions, we are told in chapter nine, rather than merely avoiding negative ones. Chapter ten does promote the importance of the "tone at the top," noting that sometimes you, as an employee, may need to walk away from an intolerable situation. Chapter eleven suggests that those in management and leadership need to communicate ethics directly and openly. The idea that the moral standards of each employee are important is again stressed in chapter twelve. Proper ethics are not always easy, says chapter thirteen. Chapter fourteen repeats encouragement to be proactive about promoting ethics, and suggests various procedures for the corporation.

There are other books on ethics, and business ethics as well. Johnson's "Computer Ethics" (cf. BKCOMPETH.RVW) is a classic and Tavani's "Ethics and Technology" (cf. BKETHTECH.RVW) adds depth and intellectual rigour. Bauer's work is very different: there is little academic or conceptual background, but the brevity and practicality of the work may make it more suitable for the general work environment. While it doesn't add much to the debate, it could certainly be used for training and the promotion of ethical standards, and is probably more accessible for the general population of employees and managers.

copyright Robert M. Slade, 2007 BKBEETNO.RVW 20071118
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 8

Friday 14 March 2008

Contents

- [Wind Power Risks](#)
Charles Wood
- [FBI Found to Misuse Security Letters](#)
lynn via Dave Farber's IP
- [RFID hack could crack open 2 billion smart cards](#)
Sharon Gaudin
- [Nasty scanner attack: AccuBasic malware](#)
PGN
- [Hacking a pacemaker](#)
Gadi Evron
- [More on pacemaker risks](#)
PGN
- [Stopping cars with microwaves](#)
Matthew D. Healy
- [It's too easy to access the "off" switch](#)
Robert P Schaefer
- [UK ISPs to sell users' private browsing information](#)
Mike Scott
- [TSA can't believe MacBook Air is a real laptop; owner misses flight](#)
Paul Saffo
- [Deja Vu all over again](#)
Andrew Koenig
- [CAPTCHA attacks](#)
Monty Solomon
- [Safari "beachball" black on black](#)
Richard A. O'Keefe
- [Risks of Leap Years and Dumb Digital Watches](#)
Clive D. W. Feather
Amos Shapir
- [USENIX Announces Open Access to Conference Proceedings](#)
Lionel Garth Jones
- [Info on RISKS \(comp.risks\)](#)

✶ **Wind Power Risks**

<"Charles Wood" <j.charles.wood@gmail.com>>

Mon, 3 Mar 2008 08:03:47 +0900

It is now becoming more common to hear of wind power caused outages. The outages are either a loss of service because the wind has stopped blowing or, surprisingly, because there is too much wind.

These problems were not so apparent when the percentage of wind power was low compared to the overall capacity, and in particular to rapid response generators such as hydro.

It seems that wind power has become too successful and the engineering required to integrate it into different grids has lagged behind. In particular, the correct balance is not being achieved between wind power capacity in a region and the available replacement power sources - transmission and local non-base load sources.

A recent outage in Texas illustrates the low wind example. An *IEEE Spectrum* article by Peter Fairley explains the overload scenario.

The Texas outage on February 27 as reported by Reuters:

<http://www.reuters.com/article/domesticNews/idUSN2749522920080228?feedType=RSS&feedName=domesticNews&rpc=22&sp=true>

"Electric Reliability Council of Texas (ERCOT) said a decline in wind energy production in west Texas occurred at the same time evening electric demand was building as colder temperatures moved into the state.

The grid operator went directly to the second stage of an emergency plan at 6:41 PM CST (0041 GMT), ERCOT said in a statement.

System operators curtailed power to interruptible customers to shave 1,100 megawatts of demand within 10 minutes, ERCOT said. Interruptible customers are generally large industrial customers who are paid to reduce power use when emergencies occur."

The IEEE article on power surges from wind farms is at

<http://spectrum.ieee.org/feb08/5943> and the key paragraph is this:

Wind-farm installation in Europe grew an estimated 38 percent last year, up from 19 percent in 2006, bringing the total capacity to about 67 gigawatts (roughly the equivalent of 20 to 25 standard-size nuclear power plants). At those rates, European grid operators report, windmill construction is outstripping growth in transmission capacity. The result is that in wind-farm-rich countries such as Germany and Denmark, high winds cause large and unanticipated power flows that saturate the grids of neighboring nations. In recent years this has forced grid operators to curtail scheduled transfers of power between grids. In 2008, the grid operators warn, the unanticipated power flows could overload lines anywhere from the Czech Republic to the Netherlands.

✶ FBI Found to Misuse Security Letters (From Dave Farber's IP)

<lynn [lynn@ecgincc.com]>

Fri, 14 Mar 2008 9:36

<http://www.washingtonpost.com/wp-dyn/content/article/2008/03/13/AR2008031302277.html?hpid=topnews>

FBI Found to Misuse Security Letters; 2003-06 Audit Cites Probes of Citizens
Justice Department official Glenn A. Fine testifies about his probe of
national security letters. (Dennis Cook -- Associated Press)

Dan Eggen, *The Washington Post*, 14 Mar 2008

The FBI has increasingly used administrative orders to obtain the personal records of U.S. citizens rather than foreigners implicated in terrorism or counterintelligence investigations, and at least once it relied on such orders to obtain records that a special intelligence-gathering court had deemed protected by the First Amendment, according to two government audits released yesterday.

The episode was outlined in a Justice Department report that concluded the FBI had abused its intelligence-gathering privileges by issuing inadequately documented "national security letters" from 2003 to 2006, after which changes were put in place that the report called sound.

A report a year ago by the Justice Department's inspector general disclosed that abuses involving national security letters had occurred from 2003 through 2005 and helped provoke the changes. But the report makes it clear that the abuses persisted in 2006 and disclosed that 60 percent of the nearly 50,000 security letters issued that year by the FBI targeted Americans. [...]

Archives: <http://www.listbox.com/member/archive/247/=now>

RSS Feed: <http://www.listbox.com/member/archive/rss/247/>

[See also

<http://www.reuters.com/article/topNews/idUSN0563517120080305>

PGN]

✶ RFID hack could crack open 2 billion smart cards (Sharon Gaudin)

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

Fri, 14 Mar 2008 14:43:13 PDT

Sharon Gaudin, *Computerworld*, 14 Mar 2008

A student at the University of Virginia has discovered a way to break through the encryption code of RFID chips used in up to 2 billion smart cards used to open doors and board public transportation systems.

Karsten Nohl, a graduate student working with two researchers based in

Germany, said the problem lies in what he calls weak encryption in the MiFare Classic, an RFID chip manufactured by NXP Semiconductors. Now that he's broken the encryption, Nohl said he would only need a laptop, a scanner and a few minutes to get the cryptographic key to an RFID door lock and create a duplicate card to open it at will.

And that, according to Ken van Wyk, principal consultant at KRvW Associates, is a big security problem for users of the technology.

"It turns out it's a pretty huge deal," said van Wyk. "There are a lot of these things floating around out there. Using it for building locks is the biggy, especially when it's used in sensitive government facilities - and I know for a fact it's being used in sensitive government facilities."

Van Wyk told Computerworld that one European country has deployed military soldiers to guard some government facilities that use the MiFare Classic chip in their smart door key cards. "Deploying guards to facilities like that is not done lightly," he added. "They recognize that they have a huge exposure. Deploying guards is expensive. They're not doing it because it's fun. They're safeguarding their systems." He declined to identify the European country.

Manuel Albers, a spokesman for NXP Semiconductors, said the company has confirmed some of Nohl's findings. However, he said there are no plans to take the popular chip off the market.

"The MiFare chip was first introduced in 1994. At the time, the security level was very high," he said in an interview. "The 48-bit key lengths for encryption was state of the art."

Albers added that the company has other, more secure chips in its product portfolio these days, but the MiFare Classic is a relatively inexpensive, entry-level chip. Anyone needing a highly secure smart card should make sure there's layered security and not just depend on the chip's encryption, he said.

"We have to start this discussion, really, at the level where we differentiate between the security level the chip provides and the additional security features an entire card provides. You're dealing with a layered security system, like strands to a rope," said Albers, noting that between 1 billion and 2 billion smart cards with this MiFare Classic-type chip have been sold. "As long as there's demand for this product [and] system integrators saying this product is good enough for their platforms, we will continue to offer it."

Albers noted that NXP recently released MiFare Plus, which is backward-compatible with the MiFare Classic while offering better security. He said the company did not release the updated chip because of Nohl's findings, but it did use some of his information when designing it.

"The problem is the card and the card reader," said Nohl. "They speak the same cryptography language that is flawed. Both need to be replaced. There is a lot of infrastructure to be replaced. The encryption is not standard. It's weak. It uses two short keys."

While Albers said "the majority" of the smart cards with this chip are used as bus or subway cards, both van Wyke and Nohl said the real problem lies in the cards that are used as door locks.

"I don't think people want to steal other people's bus tickets," said Nohl. "But think about chemical waste storage buildings or military facilities. The stakes are a lot higher. If you break in, you don't get a \$2 bus ticket, but [you get] whatever is in that warehouse. These cards are used around the world to secure high-level buildings. All these applications will suffer as soon as somebody with criminal intent finds the details that we have."

Nohl explained that since the MiFare Classic smart cards use a radio chip, he can easily scan them for information. If someone came out of a building, carrying a smart card door key, he could walk past them with a laptop and scanner in a backpack or bag and scan their card. He also could walk past the door and scan for data from the reader.

Once he's captured information from a smart card and the card reader on the door, he would have enough information to find the cryptographic key and duplicate a smart card with the necessary encryption information to open the door.

How long would it take him to capture the necessary information? About two minutes, he said.

Van Wyk thinks Nohl might be humble in his estimate. "He says it would take him two minutes to crack it? Two minutes? I'd like to know what he did with the other minute and 55 seconds," he said. "It is so easy to crack most of that stuff. I don't think it's general to RFID, but there are a lot of RFID implementations that haven't done this very well. You could do RFID well, but it turns out that not many vendors are."

✂ Nasty scanner attack: AccuBasic malware

*<"Peter G. Neumann" <neumann@csl.sri.com>>
Wed, 12 Mar 2008 22:07:20 PDT*

http://voter.engr.uconn.edu/voter/Reports_files/seeA-tamperEVoting.pdf

In this paper we present a security assessment of the Diebold AccuVote Optical Scan voting terminal (AV-OS), a popular OS terminal currently in wide deployment anticipating the 2008 Presidential elections. The assessment is developed using exclusively reverse-engineering, without any technical specifications provided by the machine suppliers. We demonstrate a number of security issues that relate to the machine's proprietary language, called AccuBasic, that is used for reporting election results. While this language is thought to be benign, especially given that it is essentially sandboxed by the firmware to have only read access, we demonstrate that it is powerful enough to (i) strengthen known attacks

against the AV-OS so that they become undetectable prior to elections (and thus significantly increasing their magnitude) or, (ii) to conditionally bias the election results to reach a desired outcome. Given the discovered vulnerabilities and attacks we proceed to discuss how random audits can be used to validate with high confidence that a procedure carried out by special purpose devices such as the AV-OS has not been manipulated. We end with a set of recommendations for the design and safe-use of OS voting systems.

During our own experimentation we found that the bytecode language offers a wealth of functions that can be potentially exploited by an attacker. In particular, we will demonstrate a time-bomb attack in which the bytecode checks the date and time in order to decide whether the election has begun. An attack utilizing such code can retain proper behavior in pre-election testing, in which the machine is verified by comparison with hand counted ballots, while behaving improperly during the actual election.

✂ Hacking a pacemaker

<Gadi Evron <ge@linuxbox.org>>
Wed, 12 Mar 2008 03:45:19 -0500 (CDT)

Almost a year ago I gave a talk at the CCC Camp in Germany I called "hacking the bionic man". It even made Wired, in some fashion.
<http://blog.wired.com/27bstroke6/2007/08/will-the-bionic.html>
<http://events.ccc.de/camp/2007/Fahrplan/events/2049.en.html>

In the talk, among other things such as the DNA and scripting languages, medical doctors and reverse engineers... was about cybernetic hacking. I gave some predictions, some for 2 years, others 40 years. Some again were pure science fiction. I was wrong on the 2 years, it's here.

Today, this came up in the news (hat tip to Paul Ferguson on the funsec mailing list):
http://www.nytimes.com/2008/03/12/business/12heart-web.html?_r=1&oref=slogin

" The threat seems largely theoretical. But a team of computer security researchers plans to report Wednesday that it had been able to gain wireless access to a combination heart defibrillator and pacemaker.

They were able to reprogram it to shut down and to deliver jolts of electricity that would potentially be fatal . if the device had been in a person. In this case, the researcher were hacking into a device in a laboratory. "

✂ More on pacemaker risks

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

Fri, 14 Mar 2008 14:48:31 PDT

"Security and Privacy of Implantable Medical Devices," Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H. Maisel, IEEE Pervasive Computing, January 2008.

<http://www.secure-medicine.org/PervasiveIMDSecurity.pdf>

"Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel, IEEE Symposium on Security and Privacy, May 2008. <http://www.secure-medicine.org/icd-study/icd-study.pdf>

✂ Stopping cars with microwaves (Re: [RISKS-25.07](#))

<"Matthew D. Healy" <mdhealy@sprynet.com>>

Thu, 28 Feb 2008 08:45:15 -0500 (EST)

My father has a pacemaker wired to his heart and is therefore required to stay away from things like domestic microwave ovens. What might happen to him if this device were used to stop a perpetrator in his vicinity?

✂ It's too easy to access the "off" switch.

<"Schaefer, Robert P \{(US SSA)\}" <robert.p.schaefer@baesystems.com>>

Wed, 12 Mar 2008 9:13:04 PDT

from boingboing:

Teen pranksters switch off San Francisco's electric buses
(Posted by Cory Doctorow), 11 Mar 2008

Destiny sez, "San Francisco is now stymied by 'bus tampering.' Their new electric 'hybrid' buses have an on/off switch -- which, unfortunately, 'can be accessed easily through an unlocked panel on the outside of the bus.' 'When that happens, the drivers can't accelerate, they lose radio contact with dispatchers and the interior lights on the buses go out.' Teenage pranksters then pelt the immobile buses with rocks." Link (Thanks, Destiny!)

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/03/07/BAOKVF1E8.DTL&tsp=1SF>

✂ UK ISPs to sell users' private browsing information

<"mike scott" <mike@scottsonline.org.uk>>

Sat, 08 Mar 2008 10:20:59 -0000

Three major UK ISPs apparently are in advanced talks with a company called Phorm, intending to let Phorm monitor all unsecured web traffic to and from their users. The expressed intent is to offer an "improved browsing experience" through better targeted web advertising, and anti-phishing protection - thereby "improving" one's internet security. One, BT, has already trialed the system.

The ISPs and Phorm are remarkably coy about the system, and Phorm in particular appears to have offered inconsistent explanations of how it all works. However, it does appear clear that this system provides access for a private company to an unprecedented amount of data that even the UK government is not permitted (at least without a court order). Phorm promise faithfully not to record information such as bank details or telephone numbers :-)

Phorm claim the data is summarized and anonymized; regular readers of RISKS will I'm sure be aware that true anonymization is exceedingly difficult - and in fact this scheme would give ready access to identities should anyone take the trouble. Quite apart from being a breach of trust by the ISPs involved, it appears to drive a coach, horses and a whole army through protection offered by assorted UK legislation, including the Data Protection Act, Computer Misuse Act, Regulation of Regulatory Powers Act, etc, etc. It will if nothing else provide a central point for cracking to obtain information about these ISPs' users.

The proposed system has been mentioned in passing in the media - who regrettably seem to have accepted without further investigation Phorm's assurances that there's no privacy issue. They've not even noticed that the so-called "opt-out" won't stop the data scanning, just the ads.

Oh, did I forget to mention Phorm used to be 121Media, of rootkit and PeopleOnPage fame? And involves servers outside the EU, in China in particular? I think there's not so much a RISK, more of a CERTAINTY that this will go pearshaped.

References:

http://www.phorm.com/isp_partners/

<http://www.oix.com/index.html>

<http://www.badphorm.co.uk>

http://www.theregister.co.uk/2008/02/29/phorm_roundup/

<http://www.techdirt.com/articles/20080218/024203278.shtml>

<http://www.guardian.co.uk/technology/2008/mar/06/internet.privacy>

(and note that the Guardian has signed up with phorm for the targeted ads scheme)

http://www.theregister.co.uk/2008/02/27/bt_phorm_121media_summer_2007/

(and so on...)

[BTW this issue affects virginmedia, BT and talktalk in the UK - around 10 million people iirc. Other ISPs are waiting to jump on the bandwagon. Talktalk seem to be backpedaling, and may be making it opt in, although there is still major doubt about what /exactly/ is happening.]

<http://www.scottsonline.org.uk> lists incoming sites blocked because of spam

mike@scottsonline.org.uk Mike Scott, Harlow, Essex, England

✂ TSA can't believe MacBook Air is a real laptop; owner misses flight

<Paul Saffo <paul@saffo.com>>
Mon, 10 Mar 2008 10:44:30 -0700

(I doubt this story is true, but still it is too good not to pass on -p)

TSA can't believe MacBook Air is a real laptop, causes owner to miss flight; posted 10 Mar 2008 by Darren Murph

<http://www.engadget.com/2008/03/10/tsa-cant-believe-macbook-air-is-a-real-laptop-causes-owner-to/>

The TSA has been known to take issue with products designed in Cupertino before, but for one particular traveler, it was Apple's thinnest laptop ever that caused the latest holdup. Upon tossing his ultra-sleek slab of aluminum underneath the scanner, security managed to find enough peculiarities to remove it from the flow, pull it aside and wrangle up the owner for some questions. Apparently, the TSA employee manning the line was flabbergasted by the "lack of a drive" and the complete absence of "ports on the back," and while hordes of co-workers swarmed to investigate, the user's flight took off on schedule. Thankfully, said owner was finally allowed to pass through after some more in-the-know colleagues explained in painfully simple terms what an SSD was, but the poor jet-setter most definitely paid the price for trying to slip some of the latest and greatest under the sharp eyes of the TSA (and cutting it close on time, of course).

✂ Deja Vu all over again

<"Andrew Koenig" <ark@acm.org>>
Wed, 27 Feb 2008 12:54:54 -0500

Yet another example of a major company sending e-mail that looks like phishing in E-mail from Paypal:

Dear Andrew Koenig,

Now you can pay with PayPal at all your favorite shopping sites, even when it's not an option at checkout. Use the new PayPal Plug-in to:

- * Shop securely anywhere online
- * Fill out shipping forms in 1 click.
- * Save your receipts to review anytime

Install in seconds - download for free and start Shopping today!

The words "download for free" are a hyperlink, and when I hover the cursor over it, I learn that it is a link to

<http://email1.paypal.com/u.d?xxxxxxx=nnn>, where the x represents

various letters and digits and the n's represent digits.

So unless email1.paypal.com is somehow now part of the PayPal domain, this appears to be a legitimate solicitation disguised as a phishing attempt.

As I remarked last time, they appear to be trying to train their customers to fall for phishing scams. What on earth could they be thinking?

✂ CAPTCHA attacks

<Monty Solomon <monty@roscom.com>>
Mon, 10 Mar 2008 10:29:16 -0400

Yahoo's CAPTCHA Security Reportedly Broken
January 17, 2008 06:00 PM

<http://www.informationweek.com/news/showArticle.jhtml?articleID=205900620>

Streamlined anti-CAPTCHA operations by spammers on Microsoft Windows Live Mail
Feb 6 2008 1:37PM

<http://www.websense.com/securitylabs/blog/blog.php?BlogID=171>

Google's CAPTCHA busted in recent spammer tactics
Feb 22 2008 4:52PM

<http://www.websense.com/securitylabs/blog/blog.php?BlogID=174>

✂ Safari "beachball" black on black

<"Richard A. O'Keefe" <ok@cs.otago.ac.nz>>
Fri, 7 Mar 2008 17:41:55 +1300

My G4 PowerMac was replaced by an intel-Mac this week. I had a number of problems, notably browsers not coping with links to PDFs. My sysadmin fixed all this, but we thought she hadn't, because in Safari, when you link on a PDF link, it opens up a black window, and then while it is fetching the document, it spins a black "daisy" that has replaced the old beachball. If you know it is there, you can just see it, but if you don't know to expect it, you will never notice it. Black information on a black background? Not what I'd expected from Apple.

✂ Risks of Leap Years and Dumb Digital Watches (Brader, [RISKS-25.07](#))

<"Clive D. W. Feather" <clive@on-the-train.demon.co.uk>>
Mon, 3 Mar 2008 15:04:30 +0000

On reading [Mark Brader's post], I checked to discover that my watch was a day ahead. But not because it wasn't the smarter kind. On the contrary, it

understands that 29 Feb occurs one year in four [almost], but was set to the wrong year in the cycle! Perhaps you need to run this posting next year.

As a user interface risk: I haven't figured out how to find the right year on my watch other than by cycling through the months and checking whether it accepts February 29th then, once it does, stepping through the months again.

Clive D.W. Feather <http://www.davros.org> +44 20 8495 6138 clive@davros.org

Re: Risks of Leap Years and Dumb Digital Watches ([RISKS-25.07](#))

<Amos Shapir <amos083@hotmail.com>>

Mon, 3 Mar 2008 17:35:56 +0200

I have 3 clocks, each of different generation, and each has its set of bugs:

* My watch is a pocket analog one, its date has to be set 5 times a year (by turning the crown).

* My bedside clock is 1980-vintage big red LED digital (best for displaying time at night). It doesn't know about Feb. 29, so its date display has to be set once every 4 years (by running around the year - it has a "fast forward" button but no way to step down).

* The latest acquisition is an LCD clock which also shows the year number, so it can figure out leap days; it might have a problem in 2100, if it lasts that long. It sets itself by listening to a radio time signal, so theoretically it should never have to be set at all, but every now and then it glitches and displays a wrong time, date or year; the difference is always a power of 2 in one of the digits, which looks like it's getting the data in some sort of BCD format, without any checksum or sanity check (which is not news on RISKS). I wonder how many critical installations are using the same chip.

USENIX Announces Open Access to Conference Proceedings

<Lionel Garth Jones <lgj@usenix.org>>

Thu, 13 Mar 2008 13:53:15 -0700

USENIX is pleased to announce open public access to all its conference proceedings.

This significant decision will allow universal access to some of the most important technical research in advanced computing. In making this move USENIX is setting the standard for open access to information, an essential part of its mission.

USENIX could not achieve such goals without the support and dedication of its membership. We urge you to encourage others to join USENIX. Membership

helps us present over 20 influential conferences each year and offer open access to the technical information presented there.

USENIX conference proceedings can be found at:

<http://www.usenix.org/publications/library/proceedings/>

Questions? Contact papersinfo@usenix.org.

[This is a wonderful step in the pursuit of open access to information, PGN]



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 9

Thursday 27 March 2008

Contents

- [Billion-dollar IT failure at Census Bureau](#)
[eekid](#) via [David Farber](#)
- [A Heart Device Is Found Vulnerable to Hacker Attacks](#)
[Barnaby Feder](#) via [Monty Solomon](#)
- [FL power outage NERC updates](#)
[Catherine M Horiuchi](#)
- [Vandals halt some hybrid buses using external 'off' switch](#)
[Rick Damiani](#)
- [Flight Service Software Crashes; Pilot Briefings Delayed](#)
[Gabe Goldberg](#)
- [Substantial supermarket breach affects millions](#)
[Robert Heuman](#)
- [Man arrested by mistake over phone system bug](#)
[Rick Damiani](#)
- [Hoax on Craigslist causes duped victims to steal property](#)
[Mark Brader](#)
- [Payment by fingerprint disappears](#)
[Jon Van and Becky Yerak](#) via [Paul Saffo](#)
- [Cute e-mail leak](#)
[Steve Summit](#)
- [Search engine bait?](#)
[Steve Schafer](#)
- [Info on RISKS \(comp.risks\)](#)

✂ Billion-dollar IT failure at Census Bureau (eekid via IP)

<David Farber <dave@farber.net>>
Mon, 24 Mar 2008 17:50:06 -0700

Why is anyone surprised. I spent many years on NRC (National Research Council) study groups looking at Social Security, IRS, FAA and various DoD software procurements. They were all in serious troubles usually due to very poor procurement processes; endlessly changing requirements; poor software

management etc. BUT it still goes on and on and on. Try reading some of the NRC reports. They are informative and sad. DF

From: eekid@aol.com [eekid@aol.com]
Sent: Monday, March 24, 2008 5:03 PM
Subject: Billion-dollar IT failure at Census Bureau

Billion-dollar IT failure at Census Bureau
Posted by Michael Kringsman @ 7:51 pm
<http://blogs.zdnet.com/projectfailures/?p=660>

US Census Bureau faces cost overruns up to \$2 billion on an IT initiative replacing paper-based data collection methods with specialized handheld devices for the upcoming 2010 census. The Bureau has not implemented longstanding Government Accountability Office (GAO) recommendations and may therefore be forced to scrap the program. Harris Corp., the contractor associated with this incompetently managed initiative, was awarded a \$600 million contract to develop the handhelds and related software.

In March 5, 2008 testimony before the Senate, Commerce Secretary Carlos M. Gutierrez said: "There is no question that both the Census Bureau and Harris could have done things differently and better over the past couple of years."

On the same date, Census Bureau Director, Steve H. Murdock, added:

I cannot over-emphasize the seriousness of this problem. My colleagues and I recognize that we must move quickly to address this problem, and implement solutions. While we still have an enormous challenge in front of us, I am confident that we are close to defining and implementing a strategy that will ensure a successful 2010 Census.

The GAO characterized the handheld initiative, known as the Field Data Collection Automation (FDCA) program, as follows:

Of the \$11 billion total estimated cost of the 2010 Census, the Census Bureau planned (as of 2007) to spend about \$3 billion on automation and information technology in order to improve census coverage, accuracy, and efficiency. Among other things, the Bureau is planning to automate many of its planned field data collection activities as a way to reduce costs and improve data quality and operational efficiency.

The GAO report, dated March 8, 2008, added:

In October 2007, GAO concluded that without effective management of key risks, the Field Data Collection Automation (FDCA) program responsible for the devices faced an increased probability that the system would not be delivered on schedule and within budget or perform as expected. The magnitude of these problems is not clear. [T]he Bureau has not performed recommended analysis or provided sufficient information to provide a level of confidence in its \$11.5 billion life-cycle cost estimate of the decennial census. The Bureau has not itemized the estimated costs of each component operation, conducted sensitivity analysis on cost drivers, or provided an explanation of significant changes in the assumptions on which these costs

are based. Together, these weaknesses and actions raise serious questions about the Bureau's preparations for conducting the 2010 Census.

Computer World blogger, Frank Hayes, summarized the situation succinctly, "The fancy custom handhelds might work. But if they don't, the Census Bureau will use paper instead."

THE IT PROJECT FAILURES ANALYSIS

Managing an \$11 billion initiative is a daunting task and unforeseen problems are inevitable. Nonetheless, the GAO, going back to January, 2005, repeatedly identified significant procurement, management, and operational risks associated with this project. For reasons unknown, the Census Bureau chose not to follow these recommendations.

The following table summarizes significant project issues identified by the GAO:

Billion dollar IT mismanagement at Census Bureau

How does a failure of this magnitude arise? Clearly, Census Bureau management is ineffective at properly and efficiently executing the organization's basic mandate. A detailed analysis would probably reveal hidden agendas; conflicts of interest; good intentions gone bad; inexperienced, lazy, and incompetent management; lack of controls; and plain old poor judgment. I believe these deeply ingrained issues are symptomatic of fundamental problems shared by both Bureau leadership and line management.

My recommendation: The GAO must conduct a formal inquiry into two specific areas:

1. It should investigate and analyze the management policies and procedures that allowed this situation to develop and persist over the course of several years. We must understand why program controls didn't prevent this huge waste of dollars.
2. It should perform a detailed (and I mean exhaustive) investigation of Harris Corp.'s role. Let an unbiased panel determine what percentage of the billion-dollar waste Harris caused and force the company to pay direct restitution for that amount.

Until the government holds contractors and their agency sponsors accountable, massive failures will continue and more money will be flushed down the drain.

Archives: <http://www.listbox.com/member/archive/247/=now>

RSS Feed: <http://www.listbox.com/member/archive/rss/247/>

A Heart Device Is Found Vulnerable to Hacker Attacks

<Monty Solomon <monty@roscom.com>>

Sat, 15 Mar 2008 00:58:46 -0400

Barnaby J. Feder, *The New York Times*, 12 Mar 2008

<http://www.nytimes.com/2008/03/12/business/12heart-web.html?ex=1363060800&en=ccf7bc417ed75bfb&ei=5090>

To the long list of objects vulnerable to attack by computer hackers, add the human heart. The threat seems largely theoretical. But a team of computer security researchers plans to report Wednesday that it had been able to gain wireless access to a combination heart defibrillator and pacemaker. They were able to reprogram it to shut down and to deliver jolts of electricity that would potentially be fatal - if the device had been in a person. In this case, the researcher were hacking into a device in a laboratory. The researchers said they had also been able to glean personal patient data by eavesdropping on signals from the tiny wireless radio that Medtronic, the device's maker, had embedded in the implant as a way to let doctors monitor and adjust it without surgery.

The report, to published at www.secure-medicine.org, makes clear that the hundreds of thousands of people in this country with implanted defibrillators or pacemakers to regulate their damaged hearts - they include Vice President Dick Cheney - have no need yet to fear hackers. The experiment required more than \$30,000 worth of lab equipment and a sustained effort by a team of specialists from the University of Washington and the University of Massachusetts to interpret the data gathered from the implant's signals. And the device the researchers tested, a combination defibrillator and pacemaker called the Maximo, was placed within two inches of the test gear. ...

FL power outage NERC updates

<Catherine M Horiuchi <cmhoriuchi@usfca.edu>>

Mon, 03 Mar 2008 01:10:31 -0800

Five days before the Florida outage, the North American Electric Reliability Corporation (the electric industry's "self-regulatory" watchdog) issued a press release reporting its CEO's address to the National Transmission Delivery Forum. He stated: "We are operating the grid closer to the edge than ever before." This in context of need to improve the transmission system to support initiatives for more wind power (intermittent load) and micro-generation (distributed load)

<http://www.nerc.com/~filez/pressreleases.html>

The preliminary cause of the 02/26/2008 disturbance has been categorized as human error: a single mistake by a single worker at a single substation.

Florida Power & Light President Olivera said, "We don't know why the employee took it upon himself to disable both sets of relays."

<http://www.cnn.com/2008/US/02/29/florida.outage/index.html>

This type of systemic problem due to tight coupling and lack of resilience we've seen in other high-reliability, highly-engineered systems (TMI; two shuttle losses; arguably, the 17th Street Canal failure during Hurricane

Katrina and even the recent beef recall.) Yet it appears difficult for some engineers/managers to publicly acknowledge that humans are guaranteed to make mistakes, and computers are also guaranteed to fail, given enough potential instants in which to fail. Or, to advocating systems with less potential for these failures.

In Florida, "Changes to safeguard against future human error already have been implemented."

<http://www.floridatoday.com/apps/pbcs.dll/article?AID=/20080301/NEWS01/803010334/1006/news01>

So, almost before the NERC investigation is started, the "fix" is already in place. How likely is it that these changes will have their own unintended consequences? (Something as simple as, say, errors due to worker fatigue, if whatever shortcuts workers were taking to complete tasks in allotted time are no longer available.)

Note strong similarities between the Florida disturbance and the 12/08/1998 power outage in San Francisco ([RISKS-20.11](#)) affecting 456,000 customers, also a "human error" causality, where two worker events "directly" precipitated the outage:

1) A transmission construction crew working on the #2 115kV bus, Section D at the San Mateo substation, failed to remove protective grounds that had been installed as a safety measure while the crew was working on the bus section.

2) Before energizing the bus section at the conclusion of this construction work, a PG&E transmission substation operator failed to engage the protective relays.

www.cpuc.ca.gov/Published/Graphics/24197.PDF

An inability to perfectly correct operations is illustrated by PG&E's subsequent outages in 2005 and 2007. Commented PG&E spokesperson Darlene Chiu after the July 2007 outage: "The problem began when breakers in the utility's transmission service opened for an unknown reason. Every time workers attempted to close those breakers to restore service, it caused voltage fluctuations."

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/07/24/BAG9NR67253.DTL&tsp=1>

Workers tried doing what they expected to work, but it didn't. Even after the power was back on, the spokesperson reported the breakers opened "for an unknown reason." That is, it may be impossible to figure out why automated systems are acting in a particular manner within the very small space of time before automated systems take further pre-programmed actions, thereby enlarging a power outage. This impossibility can be characterized as "human error."

Transmission grid operations are increasingly complex and at the same time increasingly interconnected, suggesting systemic failure and "normal" accidents will continue to occur at regular intervals. Plan accordingly.

Cathy Horiuchi, University of San Francisco
(formerly of the Sacramento Municipal Utility District)

✂ Vandalism halts some hybrid buses using external 'off' switch

<"Rick Damiani" <rick@patongroup.com>>

Sat, 15 Mar 2008 21:45:34 -0700

"Muni drivers have reported over the last couple of weeks that people have been shutting down the power on their buses by flipping a switch that can be accessed easily through an unlocked panel on the outside of the bus. When that happens, the drivers can't accelerate, they lose radio contact with dispatchers and the interior lights on the buses go out. The power loss does not affect the brakes."

Details here:

<http://www.sfgate.com/cgi-bin/article.cgi?f=3D/c/a/2008/03/07/BAOKVF1E8.DTL&tsp=1SF>

An external power switch like this is a good thing if the bus is involved in a serious collision. Rescue workers would naturally be leery of approaching a severely damaged vehicle equipped with batteries big enough to move a bus. Sounds like they made it a bit too easy to get to.

Rick Damiani, Applications Engineer, The Paton Group California: (310)429-7095

✂ Flight Service Software Crashes; Pilot Briefings Delayed

<Gabe Goldberg <gabe@gabegold.com>>

Tue, 18 Mar 2008 14:51:39 -0400

Lockheed Martin computer programmers are trying to figure out why a planned software upgrade to FS21 caused the system to crash late Tuesday night. /AVweb/ received a tip from a former briefer in Michigan that the system went down at about 0100Z. A spokeswoman for Lockheed Martin told /AVweb/ that when they realized the FS21 upgrade was "unstable," they reverted to the backup system known as AISR (Aeronautical Information System Replacement). "It provides the same type of information as FS21 but it's in disparate sources so it takes a little longer for the briefing. In the morning, queue times were several minutes, but by around 11 a.m. they were in the single digits."

Lockheed Martin posted an alert on its *Web site* <<http://www.afss.com/>> indicating that calls to 800-WX-BRIEF may be delayed until the problem is resolved. A notice posted to the Web site on March 9 indicated that the software upgrade was being done to "provide improvements to the service we provide especially in PIREP processing with a more efficient mask for obtaining the data from the pilot, among other items." The FAA has agreed to provide Congress with a *status report*

http://www.avweb.com/avwebflash/news/FAA_to_Congress_FSS_Needs_Work_197253-1.html

every 90 days on Lockheed Martin's performance in managing the FSS contract. The next one is expected to be delivered at the end of April.

Gabriel Goldberg, Computers and Publishing, Inc. (703) 204-0433
3401 Silver Maple Place, Falls Church, VA 22042 gabe@gabegold.com

#Substantial supermarket breach affects millions

<RsH <robert.heuman@alumni.monmouth.edu>>
Tue, 18 Mar 2008 18:00:15 -0400

Once more with feeling. A lack of precise information, but again an exposure that need not have happened.

On Tue, 18 Mar 2008 15:18:20 GMT, "Security Wire Daily"
<SearchSecurity@lists.techtarget.com> wrote:
.....
SearchSecurity.com: Security Wire Daily
Breaking security news, the latest industry developments and trends
March 18, 2008
.....

HANNAFORD BREACH ILLUSTRATES NEED TO HAVE A SURVIVAL PLAN
Bill Brenner, Senior News Writer

A serious data breach at the Hannaford Bros. Co. supermarket chain exposed as many as 4.2 million credit and debit card numbers to identity fraud.

In a statement released Monday on the Maine-based Hannaford website, President and CEO Ronald Hodge said the company had contained an intrusion of its computer network that resulted in the theft of customer credit and debit card numbers. <http://go.techtarget.com/r/3288677/1421272>

R. S. (Bob) Heuman <robert.heuman@alumni.monmouth.edu>

#Man arrested by mistake over phone system bug

<"Rick Damiani" <rick@patongroup.com>>
Fri, 14 Mar 2008 20:51:20 -0700

An interesting take on the risk of believing what 'the computer says' without doing any additional investigation is here:
<http://thedailywtf.com/Articles/Youll-Need-to-Come-Downtown.aspx>

Short summary:

Homicide detectives, looking at the incoming calls to a murder victim (a drug dealer), find many of them are coming from '520-833-0000'. Steve McDowan pays the bill for that number, so naturally the detectives really want to talk to Steve. When they pick him up at work, Steve tells them that the number is his son's number. The detectives tell Steve about the murdered

drug dealer on their way to pick up his son. Everybody goes downtown. Steve's son denies making the calls, and finally gets the police to let him look up his call record at the phone company web site. Not seeing the outgoing calls there, the detectives call the phone company. From the original article:

"They called customer service, got transferred around several times, waited the requisite forty minutes on hold, and finally a tier-3 tech support technician answered the phone.

"Yes," the younger officer said into the speakerphone, "I'm investigating a homicide here and need to know, why are some outgoing calls not recorded for 520-833-0000? We have a record of the incoming calls from that number... could someone be hacking into your computers or something"

"Ha," the technician snorted, "no. This happens sometimes. If the calling party blocks their caller ID, it'll show up as 520-833-0000 instead of ten-zeros. We're working on it!"

The two detectives glared at each other, flabbergasted. "We're uhh," the older officer stumbled, "we'd like to thank you for coming down, and apologize for any, umm, inconvenience." The ride back was much less awkward... at least, for Steve and his son."

It's interesting how over-reliance on computers caused the problem (detectives chasing the wrong person), but using them correctly (Steve's son and the phone company technician) saves the day.

Rick Damiani, Applications Engineer, The Paton Group California: (310)429-7095

Hoax on Craigslist causes duped victims to steal property

*<msb@vex.net (Mark Brader)>
Mon, 24 Mar 2008 16:22:49 -0400 (EDT)*

[To make a long story short, two bogus ads offered a horse and other belongings of Robert Salisbury, a contractor in Jacksonville, Oregon, to anyone who would take them. Unsuspectingly, he returned home to find many people carting off his stuff. *Seattle Times*, 24 Mar 2008; PGN-ed]

http://seattletimes.nwsourc.com/html/localnews/2004302237_webhoax24m.html

Payment by fingerprint disappears

*<Paul Saffo <paul@saffo.com>>
Fri, 21 Mar 2008 08:40:59 -0700*

Jon Van and Becky Yerak, Troubled biometrics firm disables scanners at Jewel
Chicago Tribune, 21 Mar 2008 [PGN-ed]

www.chicagotribune.com/business/chi-fri-pay-by-touch-mar21,0,1005086.story

Jan Bledsoe was shocked Thursday to learn she can no longer just swipe her finger across a screen at the local Jewel store to buy her groceries because the bankrupt company behind the technology no longer will process such transactions. Solidus Networks Inc., a provider of payment processing, is no longer operating its biometrics unit. The firm's failure prompted some financial analysts to question whether technology that relies on biological information to identify a customer is ready for the market's mainstream.

"Commercial biometrics is inevitable," said Paul Saffo, a Silicon Valley-based trend forecaster. "There are huge risks, but it's just so cheap and convenient, people won't be able to resist it. Whenever Americans face a choice between privacy and convenience, they always choose convenience."

jonvand2@gmail.com

byerak@tribune.com

Copyright 2008, Chicago Tribune

Cute e-mail leak

<Steve Summit <scs@eskimo.com>>

Mon, 24 Mar 2008 00:32:05 -0400

Companies unclear on the concept of reciprocity love to use the convenience of e-mail to send you and me messages but then deny us the convenience of replying, often insisting we use some web-based form instead. To drive home the message, the one-way mail will often come from (or have replies directed to) a bogus address in a domain name such as "donotreply.com".

Since 2000, the domain name "donotreply.com" has been owned by a guy named Chet Faliszek. You can just imagine the kind of mail he gets there.

Details at http://blog.washingtonpost.com/securityfix/2008/03/they_told_you_not_to_reply.html.

Choice excerpts:

"...many of the misdirected e-mails amount to serious security and privacy violations. In February, Faliszek began receiving e-mails sent by [a bank in] New Jersey. Included in the message were PDF documents detailing every computer the bank owned that was not currently patched against the latest security vulnerabilities."

"With the exception of extreme cases... Faliszek says he long ago stopped trying to alert companies about the e-mails he was receiving. It's just not worth it: Faliszek said he is constantly threatened with lawsuits from companies who for one reason or another have a difficult time grasping why he is in possession of their internal documents and e-mails."

[Also noted by Jim Reisert, with additional quotes. PGN]

✂ Search engine bait?

<Steve Schafer <steve@fenestra.com>>

Sat, 08 Mar 2008 22:35:10 -0500

Go to one of these web sites:

<http://www.inpcars.com>

<http://www.healthek.com>

<http://www.toolsmet.com>

Choose one of the displayed categories at random and click the link. (Some of the categories are empty, so you may need to try more than one.)

Read the descriptions of the products.

At first glance, it appears that the descriptions are very poor English translations (of who knows what source language). But a closer look reveals that that's not what's happening, and that they are in fact crafted by taking a genuine English description (from a manufacturer's site, perhaps?) and then applying a randomized thesaurus-based word replacement algorithm.

For example, I found a product where it was clear that the original adjective used in the descriptions of a pair of related products was "quiet." It had been replaced in one case by "reserved," and in the other by "taciturn."

In one description, the word "bulb" (as in "light bulb"--the product was a lamp) had been replaced by "scaly bud"; in another, the word "mouth" was replaced by "oral fissure."

This is similar to the paraphrasing and euphemisms that you sometimes see in spam email offers for various drugs, etc., but I've never seen a spam email take it to the level of these sites.

So what's going on? If you click one of the "More Info" links, you first have to pass through a captcha barrier, and then you are taken to a page with links to eBay and Amazon.com, and occasionally some other sites. The links are typically only vaguely (if at all) related to the item you've requested "more info" about.

Who is this company that's gaming the eBay Affiliates and Amazon.com Associates programs? That's a difficult question to answer. The pages themselves are completely devoid of any kind of identifying information. A WHOIS search on the domain names reveals that the domain owners are hiding behind an anonymizer service based in the Netherlands.

Why the weird parallel-universe descriptions? It's obviously search engine bait (after all, that's how I found the sites in the first place). But why go to so much trouble? I don't know if there's something special about the replacement words and phrases that makes them rank highly, or it's just a

tactic to avoid copyright issues.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 10

Tuesday 1 April 2008

Contents

- [A modest proposal for the improvement of Daylight Saving](#)
[Tony Finch](#)
- [A Current Affair: Lauren Weinstein, Inside Risks, CACM April 2008](#)
[PGN](#)
- [Chaos Computer Club publishes Minister's fingerprint - and more](#)
[Peter Houppermans](#)
- [DST transition time mismatches](#)
[Tony Finch](#)
- [Mini-Y2K fears over Aussie daylight saving change](#)
[Max Power](#)
- [NYPD erases crime statistics for February 29](#)
[Ed Ravin](#)
- [More flights canceled as Heathrow remains in chaos](#)
[Alan Cowell via David Farber's IP](#)
- [Heathrow: The risks of hubris](#)
[Diomidis Spinellis](#)
- [GPS Errors are riskier than you may imagine: consider Liability-Critical Applications](#)
[Bern Grush](#)
- [Re: Securing The Wrong Spaces: A Lesson](#)
[Rick Damiani](#)
- [Re: Arrest over phone system bug: Trailing zeroes](#)
[Graham Reed](#)
- [Re: Thieves become victims?](#)
[stanley](#)
- [Info on RISKS \(comp.risks\)](#)

✉ A modest proposal for the improvement of Daylight Saving

<Tony Finch <dot@dotat.at>>

Tue, 1 Apr 2008 06:24:00 +00:52

At this time of year we enjoy the twice annual collection of stories about problems caused by time zone adjustments. DST is a cunning way of getting

people to adjust their habits to make better use of sunlight when it is available. We know from the turbulent history of DST in the USA that people will not make this adjustment without external influence, or if they do they will not do so with consistent start and end dates or indeed any regard for the inconvenience of those around them. (See David Prerau's book, "Saving the Daylight".)

So DST is beneficial provided it is applied consistently over a reasonably large area. However it is a crude and arbitrary mechanism. It offends those who think time should be a matter of natural philosophy, not of politics. It is a great inconvenience to us technologists when the politicians cannot stop themselves from messing around with the schedule. It causes many problems when the clocks suddenly jump by an hour twice a year.

I believe there is a way to enjoy the benefits of DST while avoiding these drawbacks. The essential idea is that our clocks should be set using sunrise as a benchmark instead of noon. This is an entirely scientific way of adjusting our clocks (and therefore our habits) to seasonal conditions, so it is immune to political fiddling. Our clocks would run fast by about a minute a day in the spring, and slow by a minute or two a day in the autumn, so there would be no unpleasant disruptions to our sleep. If we forget to make an adjustment we won't be embarrassingly early or late.

It is obviously not sensible for clocks in Land's End and John O'Groats to tell different times just because of their differing latitudes. Therefore, just as we use standard longitudes to define our time zones, we would use standard latitudes to define sunrise time. Let us use the time of sunrise at the tropic of cancer, 23.44 degrees north, as our standard. The difference between this time and that latitude's latest sunrise, 06:44, gives us an offset to add to our zone's standard time. This adjustment varies smoothly between nothing in January and an hour and a half in June, giving us even more evening sunlight to enjoy. Southern countries would use the same mechanism, but with the tropic of capricorn as their standard latitude.

Some will argue that it is inconvenient to adjust one's watch every day for most of the year. We were happy enough to do so with mechanical watches in the past, so I don't think this is a big deal, and lazy people can probably get away with adjusting theirs once a week. I also see it as an opportunity for innovative new intelligent clocks and watches. There may be slightly more difficulty checking relative times when communicating between northern and southern sunrise time zones, but the time difference tables will only be about 40 times larger. It is also a great way for geophysicists to remain involved in timekeeping after leap seconds are abolished.

I recommend this proposal to you, and hope that it is as successful as William Willett's idea one hundred years ago.

f.anthony.n.finch <dot@dotat.at> <http://dotat.at/>

✂ A Current Affair: Lauren Weinstein, Inside Risks, CACM April 2008

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

Tue, 1 Apr 2008 00:03:00 GMT

The April 2008 issue of the *Communications of the ACM* includes an important Inside Risks article by Lauren Weinstein. (It is of course subject to CACM copyright, so I won't reproduce his article here, but suggest that it is worth reading.) It is online on my Inside Risks website:

<http://www.csl.sri.com/neumann/insiderisks08.html#214>

✶ Chaos Computer Club publishes Minister's fingerprint - and more

<Peter Houppermans <phobos@pobox.com>>

Sun, 30 Mar 2008 14:23:23 +0200

The last publication of the Chaos Computer Club (CCC) has published a fingerprint of the Interior Minister Wolfgang Schäuble (quoting the oft-heard mantra "if you have nothing to hide you should have nothing to fear"), together with a tongue in cheek "collection album" page where readers can fill in fingerprints of other ministers if they manage to collect them.

<http://www.ccc.de/updates/2008/schaubles-finger> (sorry, only in German).

The CCC didn't stop there: for good measure they also repeat their 2004 guide in both English and German on how to lift fingerprints and use them as your own, complete with links to videos of the process and how it has been used to defeat a pay-by-fingerprint system of a German supermarket chain.

http://www.ccc.de/biometrie/fingerabdruck_kopieren?language=de (German)

http://www.ccc.de/biometrie/fingerabdruck_kopieren?language=en (English)

The usual "we'll sue you" noises are already being heard, which highlights interesting questions about the fingerprints you leave behind..

✶ DST transition time mismatches

<Tony Finch <dot@dotat.at>>

Fri, 28 Mar 2008 12:31:28 +0000

The following cartoon makes an amusing observation about the recently increased mismatch between European and American DST schedules.

<http://www.telegraph.co.uk/money/graphics/2008/03/28/calex28.gif>

f.anthony.n.finch <dot@dotat.at> <http://dotat.at/>

✂ Mini-Y2K fears over Aussie daylight saving change

<Max Power <dist23@juno.com>>

Thu, 27 Mar 2008 16:58:52 -0700

My view has been and always will be:

Australia & NZ should totally abandon Daylight Savings Time (DST).

DST has no place in Australasia because most of Australia and NZ are Semitropical or Temperate -- with the corresponding reduced variation in sunrise and sunset times. The only region of Australasia that may even be nominally affected by this change are the NZ provinces South of Canterbury (where Christchurch is, South Island).

As part of the this region's attempts to reduce its carbon (CO2) output, a policy of reasonable workplace scheduling needs to be instated. With the abolition of Australia's "Work Choices" and some minor tweaks to NZ employment contracts laws -- this can be done without disenfranchising anyone.

As a matter of state policy, the Australia & NZ "Free Trade Agreement" (FTA) and the "Uniform Commercial Code" (UCC) needs to be amended to abolish DST, as it creates a "NONUNIFORM competitive environment." Using DST is probably more responsible for the loss of global competitiveness in Australasia, as it creates totally unnecessary work in the commercial and governmental sectors -- and needlessly endangers people's lives.

I hope the new Rudd government issues a Y2036/Y2038 compliance law that forces the Federal and State governments to Audit their systems and gradually impose compliance benchmarks as time goes on. The Unix/POSIX time problem will negatively impact Australia's (and NZ's) global competitiveness if it is allowed to remain unfixed.

Max Power, CEO, Power Broadcasting HireMe.geek.nz

Mini-Y2K fears over Aussie daylight saving change // By ASHER MOSES - SMH

| Friday, 28 March 2008

<http://www.stuff.co.nz/4454030a28.html>

The decision to extend daylight saving in south-eastern Australia could create a mini-Y2K by putting the internal clocks on computers, smartphones and corporate servers out of sync.

From this year on, daylight saving in NSW, Victoria, ACT, Tasmania and South Australia will end a week later than usual on the first Sunday in April and, with the exception of Tasmania, recommence three weeks earlier on the first Sunday in October.

The change was intended to harmonise daylight saving dates across the country and give Australians more daylight hours, which in turn benefits the environment by reducing evening electricity use.

Many electronic devices with internal clocks are set to adjust automatically for daylight saving but, as a result of the recent date changes, the adjustments this year will be incorrect.

The fallout for regular consumers could include missed meetings or appointments, but corporations face bigger headaches as their internal servers, fleets of BlackBerry devices and automated systems such as payroll, stock trading and manufacturing are operating under the old daylight saving regime.

Clocks must therefore be adjusted manually or via software updates from the device makers.

A similar issue occurred in the United States last year when daylight saving was changed to kick in three weeks earlier and end a week later. At the time The New York Times reported it would cost public companies \$US350 million to make computer fixes to deal with the changes.

Microsoft has issued an advisory to users of its Windows, Outlook and Windows Mobile products recommending they download an update from microsoft.com.au that will synchronise computer clocks with the daylight saving changes.

"The synchronisation [issue] is not exclusive to Microsoft products. It affects all devices that update automatically according to the old daylight saving schedule," Microsoft's customer and partner experience director, Hugh Jones, said.

IDC analyst Liam Gunson said widespread problems could occur if people were not made aware of the issue and did not take action to fix it.

He said the same problems were predicted in New Zealand last year when daylight saving changes were made but no serious problems eventuated.

"It was really just a matter of education and people knowing that they need to download a certain patch or look at their IT systems and it appears that most people did," he said.

The issue has been likened to the Y2K or millennium bug, albeit on a far smaller scale and with less serious consequences.

Y2K caused chaos leading into the new millennium as it was feared computer systems, which stored years as only two digits, would be unable to recognise dates from 2000 onwards.

Governments spent hundreds of billions of dollars working to fix the problem, with computer engineers predicting doomsday scenarios such as that critical finance and electricity industries would stop operating and planes would fall out of the sky.

However, when the year 2000 finally arrived, there were no major computer disasters. There is debate over whether this was a result of the immense preparation for Y2K or people overstating the seriousness of the problem.

#NYPD erases crime statistics for February 29

<Ed Ravin <eravin@panix.com>>

Wed, 19 Mar 2008 17:34:31 -0400

The Village Voice reports that the New York City Police Department's "CompStat" report for the 9th Precinct shows zero homicides in 2008. In spite of Tina Negrón having been murdered in an East Village supermarket on February 29, 2008:

You have to go to the fine print - an asterisk at the bottom of the stats - to get what's kind of an explanation: "Crime figures for February 29, 2008 ... were excluded to ensure accurate comparisons."

Negrón wasn't the only victim who was victimized again by the stats. A total of 248 felonies, including two murders, occurred citywide on February 29. But they were excluded from the CompStat analysis - the NYPD's method of tracking seven "major" crime categories (murder, rape, robbery, felonious assault, burglary, car theft, and grand larceny). [...]

The NYPD press office's top CompStat guru didn't return several phone calls from the Voice. But according to published reports in 2004, the NYPD stopped counting Leap Day statistics in 2000. Attributing the reasons to an unnamed police spokesman, a Daily News story explained that Leap Day is withheld from CompStat because "adding the extra day ... could show an unreliable increase in crime in comparison with the prior weeks and months and cause changes in deployment when it is not really necessary."

Full story at:

http://www.villagevoice.com/news/0812_The-NYPD-Ignores-Leap-Day-Crimes,381244,2.html

The cooked statistics from the NYPD for the 9th Precinct are viewable here:

http://nyc.gov/html/nypd/downloads/pdf/crime_statistics/cs009pct.pdf

[note that the footnote that crime stats for Leap Day were excluded does not appear in that PDF, but it does appear on other CompStat reports at the same web site]

See also my post in [RISKS-13.69](#) describing how the NYPD played computer games with a performance metric in their 911 dispatch system, and [RISKS-24.28](#) on much more blatant (and unauthorized) rigging of the crime statistics in a different precinct by a high-ranking cop who wanted to improve his numbers.

Crime statistics have been used as political bludgeons for years in NYC and it's not surprising that the NYPD takes every step possible to avoid looking bad. I wonder what crimes happened on February 29, 2000, that prompted that policy change in the first place?

[Also noted by Danny Burstein, who noted that other big cities (such as LAPD) include leap-day numbers. PGN]

More flights canceled as Heathrow remains in chaos [IP]

<David Farber <dave@farber.net>>

Fri, 28 Mar 2008 15:12:09 -0700

More flights canceled as Heathrow remains in chaos

By Alan Cowell The New York Times

Friday, March 28, 2008

British Airways canceled dozens of flights at Heathrow's glittery new Terminal 5 on Friday as its staff struggled for the second day with state-of-the-art technology that was supposed to hasten check-in procedures and make flying a pleasure.

The hitches since the terminal opened to passengers on Thursday were "definitely not British Airways' finest hour," the airline's chief executive, Willie Walsh, said as he offered a personal, public apology for disrupting the travel plans of thousands of people.

British Airways canceled almost 70 flights on Thursday, after a day of delays caused by baggage handling problems. On what was supposed to be the first full day of operations at Terminal 5, many flights took off with their holds empty, carrying passengers with just cabin baggage.

Some passengers slept overnight in the steel-and-glass terminal - reviving precisely those images of delay and decline in British aviation that British Airways said it would banish with the opening of the new terminal.

As a result, Walsh said, about 36 flights out of Terminal 5 - mainly short-haul and domestic - were canceled in advance Friday to ease pressure on staff members dealing with unfamiliar procedures and systems.

Walsh said there had been "problems in the car parks, airport areas, computer glitches and the baggage system."

About the prospects for the weekend, he said Friday: "I would expect some disruption tomorrow, but I think it will become better as we become accustomed to the building and the quirks of the systems."

Travelers arriving early Friday confronted what one traveler, Tony Pascoe, 35, called chaos as they stood in line for several hours only to be told their flight had been canceled.

"It was chaotic," he told Britain's Press Association, "Everyone who had been queuing were annoyed and a lot of jostling and arguing started. Then the desk just crashed so everyone stood there.

"It is diabolical. I am a frequent traveler and this is the worst experience

ever - it is absolutely shocking."

"This is a public relations disaster at a time when London and the U.K. are positioning themselves as global players," said David Frost, director general of the British Chambers of Commerce. "We can only hope that this will provide a wake-up call as we gear ourselves up to host the Olympics in 2012."

Heathrow is one of the world's busiest airports, handling about 67 million passengers a year. The new terminal - reserved exclusively for use by British Airways - was designed to counter the airport's image as an unpleasant place for travelers. The building cost about \$8.7 billion and has 10 miles of baggage-conveyor belts supposed to carry up to 12,000 items of luggage an hour. But the baggage system has been at the heart of the start-up problems.

Other airlines, excluded from Terminal 5, took some delight in claiming to pick up business from British Airways as travelers switched to carriers operating out of Heathrow's older terminals.

And a private aviation company, Netjets, said in a statement that the number of people seeking private business flights had risen by 88 percent over a 24-hour period as "travelers sought to bypass the chaos of the opening of Terminal 5 at Heathrow."

<http://www.iht.com/articles/2008/03/28/europe/heathrow.php>

Archives: <http://www.listbox.com/member/archive/247/=now>

✈ Heathrow: The risks of hubris

<Diomidis Spinellis <dds@aueb.gr>>

Sat, 29 Mar 2008 12:14:43 +0200

I assume other comp.risks contributors will by now have provided the details and the background regarding the problems of Heathrow's terminal 5: the parking sign snags, the baggage processing backlog, the canceled flights, and the resulting chaos. A related interesting angle is an email that British Airways circulated to its customers on the day of the terminal's opening. Here are some notable excerpts, as highlighted by a colleague who brought this to my attention:

Dear Mr [...],

Five and a half years ago the building of our new home began in our most visionary project to date. Today we opened the doors. There is no more waiting... Terminal 5 welcomes you.

*At Terminal 5 everything has been streamlined and designed to make your

journey through the terminal calm and relaxed.* And this morning we saw all the planning fall into place.

The next time you fly in to, or on from Terminal 5, *you'll experience for yourself how all the planning and careful design has fallen into place.* The arrivals Gates are conveniently located to minimise your walk from the plane and if you're transferring to another flight, Flight Connections is so smooth, you'll be through in 20 minutes.

A state-of-the-art baggage system, a shopping concourse that rivals London's West End, and an array of tempting restaurants, bars and cafes to choose from, you'll discover nothing has been overlooked to ensure *your time at Terminal 5 is spent in a most relaxing and enjoyable way.* [...]

In this case the risk is that the making of grandiose claims about yet-to-be-established performance can easily backfire.

Diomidis Spinellis - Athens University of Economics and Business
<http://www.dmst.aueb.gr/dd>

✈ GPS Errors are riskier than you may imagine:

<"Bern Grush" <bgrush@skymetercorp.com>>
Sun, 23 Mar 2008 02:16:14 -0400

consider Liability-Critical Applications

re: <http://catless.ncl.ac.uk/php/risks/search.php?query=gps>

I note, after searching this RISKS database of items on "GPS", that a considerable number of observations from your writers re GPS errors are actually errors in the mapping data bases that are used in navigation system applications (e.g., automotive navigation), rather than a GPS positioning error due to signal errors per se. This distinction may not be interesting when you are lost in your car, but it is critical in other applications.

GPS position estimates have inherent errors (generally of a couple of meters in "open sky" circumstances, but possibly 100s of meters on some occasions due to "non-line-of sight multipath error" in especially built-up urban areas. Some GPS-Auto-Nav users will have noted temporary errors such as their position being displayed on the wrong road. The difficulty is more subtle than writers surmise. There are indeed errors in the maps being used. Even if a map is correct when installed in your device, roads change. But at any one moment how can you be sure an error is in the positioning estimate or on the map. You really need to rely on signage if it is available.

But worse than all this is that we are on the cusp of deploying GPS-based road-tolling systems, the majority of which will depend on map-matching algorithms to determine which road you are on or which "cordon" you are in to calculate a charge. These tolling systems will be subject to error for the same fundamental two reasons signal errors and map errors.

The risk here is that tens of companies are building and tens of municipalities and tens of counties are considering investing in GPS-tolling systems that will critically rely on map-matching.

Considering that the very first such system (Germany) cost far in excess of Euro 10⁹, these companies, cities and countries are about to put many, many billions at risk. Any decent lawyer could cobble together a class action suit to defeat charges based on map-matching. They only need your collection of emails to show negligent system design.

Bern Grush, Chief Scientist | skymetercorp.com
desk +1 416 673 8406 | cell +1 647 218 8600

✉ Re: Securing The Wrong Spaces: A Lesson (Ferguson, [RISKS-25.06](#))

<"Rick Damiani" <rick@patongroup.com>>
Sat, 15 Mar 2008 18:14:56 -0700

This isn't actually a design flaw or oversight. Naval vessels (like every other ocean-going ships) are equipped with surface search radar, but naval vessels often don't use it. RADAR emissions can be detected at twice the distance they can 'see', so a warship running it's surface search RADAR is both broadcasting it's position and telling everyone how far away they can stay and not be detected. That's often not the most useful thing a warship could do.

The real failure here was undoubtedly much more complex than simply not running the RADAR though. The underway watch team charged with safe operation of the ship (i.e. those actually involved in navigation and maneuvering) on a military vessel usually includes a couple of dozen people, including several equipped with nothing more sophisticated than binoculars and a sound-powered phone. That all of them missed seeing the boat until they hit it speaks less of electronic failures and more of some kind of systemic personnel issue.

Rick Damiani, Applications Engineer, The Paton Group, California: (310)429-7095

✉ Re: Arrest over phone system bug: Trailing zeroes ([RISKS-25.09](#))

<Graham Reed <greed@pobox.com>>
Thu, 27 Mar 2008 20:31:20 -0400

The "trailing zeros" bug Rick Damiani wrote about in [RISKS 25.09](#) reminded me of a similar, but fortunately far less intrusive, problem a friend of mine had with his ADSL connection.

I had recommended the ISP I had recently begun using, and he'd happily signed up and got his modem and router configured and working

perfectly... well, mostly perfectly. A few web sites, without any apparent relation, just wouldn't work when he went to them with his new DSL account. Switching back to the old account, everything was fine. (And I'd thought PPPoE could never have a benefit.)

Since I'd recommended the ISP, I was on the hook here, especially since my connection had been, and continues to be, quite reliable.

So I did the usual pings and traceroutes and didn't notice anything other than the usual "ICMP is scary" lossage. No two of the failing web sites seemed to be network-ologically related, so it didn't look like a particular carrier having issues with that ISP... and, anyway, I could get to all of them--via the same hops.

In desperation, we went into his router's set-up. It didn't feel like a Path MTU discovery problem, but I was out of ideas. Then I noticed the IP address of his modem: x.y.z.0/32. A perfectly legitimate host address for a point-to-point connection.

So we called up the ISP's support desk, and told the guy there what was happening and my suspicion about the "trailing 0" being a problem. It wasn't wrong, but it was the only thing odd I could see. The guy at the ISP agreed, right down to the "it's not wrong but it's unusual" feeling, and assigned a new IP with a non-zero final octet to my friend. Sure enough, all the missing web sites turned up.

My guess was that some providers were dumping packets purporting to be from a /24 network address, making the assumption that an all-zeroes final octet must mean the packet is spoofed. Which is fine for /24 all the way up to /31. But for anything else, you're at RISK of having a legitimate host address junked.

/24 is common. Really, really common. But we all know the RISKS that arise when we treat "common" as if it was "only". You can't tell what my address structure is; even before CIDR, I was regularly working in subnetted class A space, and our netmasks never left the building.

(Either that, or someone had heard the old saw that "auditors reject any line item that ends in 5 or 0.")

🔪 Thieves become victims?

<stanley@peak.org>

Thu, 27 Mar 2008 18:35:48 -0700 (PDT)

In [RISKS-25.09](#), Mark Brader wrote a submission with the subject: "Hoax on Craigslist causes duped victims to steal property." A demonstration of how making the "long story short" changes the story completely. [PGN-ed and oversimplified; don't blame Mark.]

The victim was not unsuspecting when he returned home. He had received a

phonecall while away from home from someone about the horse, which was in much better shape than it should have been had it been abandoned. While driving home, he passed several people with truckloads of property he knew was his. When stopped and told they had his property, they ignored him. When he arrived home, he found more people, some of whom showed him a printout of the craigslist entry as proof that they could steal his property, and many of them drove off with more of his stuff, after being told they were stealing.

There were no "duped victims". The victim cannot, by definition, steal his own property. Those who stole were dupes, but they aren't the victims here in any reasonable sense of the word. The people who got the property profited.

The local sheriff has already gone on record as saying that those who took the property face criminal charges if caught, but have been given an opportunity to return what they took with no questions asked.

Let's not allow technology cloud the ethics and results. Sometimes dupes are the victims, as in 419 scams, but here the victim was the fellow whose property was stolen. Those who were presented with a "too good to be true" opportunity this time are the thieves, and could have prevented a lot of damage had they simply called the fellow whose stuff they wanted to take to make sure.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 11

Wednesday 9 April 2008

Contents

- [Crossed wires cited in recent UAL skidding incidents](#)
[Monty Solomon](#)
- [Unanticipated GPS risk: foreign translations](#)
[Paul Schreiber](#)
- [Census to scrap handheld computers for 2010 count](#)
[Bob Schaefer](#)
- [Boston city complaint line lags](#)
[Donovan Slack](#) via [Monty Solomon](#)
- [Indiana school district wipes out high school grades](#)
[Danny Burstein](#)
- [Re: Search engine bait?](#)
[Martin Ward](#)
- [Another genuine mail that looks like a phish](#)
[Andy Piper](#)
- [Nissan GT-R sports car recognizes racetrack coordinates and aftermarket parts](#)
[Clark Family](#)
- [REVIEW: "Security Data Visualization", Greg Conti](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

✉ Crossed wires cited in recent UAL skidding incidents

<Monty Solomon <monty@roscom.com>>
Tue, 1 Apr 2008 09:11:28 -0400

Crossed wires cited in recent skidding incidents
Two United A320s went off runway in recent months after wheels locked up
<http://www.msnbc.msn.com/id/23887919/>

[For inspections of MD-80 wheel-well wiring, American Airlines canceled more than 500 flights on 8 Apr, and 1000 flights on 9 Apr. PGN]

✂ Unanticipated GPS risk: foreign translations

<Paul Schreiber <shrub@mac.com>>

Tue, 8 Apr 2008 00:10:56 -0700

I just discovered this problem:

<<http://paulschreiber.com/blog/2008/04/08/lost-in-translation/>>

In English, when reading numbers out loud, one often chunks the numbers into smaller groups. For example, when reading the phone number 555-1212, one would say five five five, one two one two, not five hundred fifty-five, one thousand two hundred and twelve.

Similarly, one would call Interstate 280 interstate two eighty, not interstate two hundred and eighty.

Toyota's Prius GPS does this. It's an example of good design -- speak the language your customers speak.

However, this falls apart when you switch the Prius over to French. Exit 420 becomes exit quatre (4) vingt (20). The problem? In most parts of the French-speaking world, 80 is also pronounced quatre vingts (four twenties).

In this case, you have to listen to your GPS and read the screen to be sure you take the right exit.

✂ Census to scrap handheld computers for 2010 count

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

Thu, 3 Apr 2008 13:48:11 PDT

Yet another computer related project over budget and behind schedule.

[thanks to Bob Schaefer.]

http://www.nextgov.com/nextgov/ng_20080403_9574.php

✂ Boston city complaint line lags

<Monty Solomon <monty@roscom.com>>

Sun, 6 Apr 2008 23:29:37 -0400

Donovan Slack, *The Boston Globe*, 6 Apr 2008

City complaint line lags;

Despite Menino's vow, a system to track citizen calls is still years away

When Boston officials rolled out their ambitious plans for a citizen complaint tracking system like the ones that are commonplace in cities

across the country, Mayor Thomas M. Menino announced, "The city's changing, and my administration has to change, too."

Nearly two years later, the administration has not changed much, leaving Boston far behind other cities such as New York, Chicago, Baltimore, and even Somerville and Hartford - and leaving untold numbers of citizen complaints by the wayside.

City officials have spent \$2 million. They've hired outside consultants. They've bought furniture and telephones for a complaint call center in City Hall, and painted the room a pale shade of blue. But senior officials say it could be nearly two more years and \$2 million more before the administration has a citywide system to keep track of residents' complaints about everything from burned out street lights to missed trash pickups. ...

http://www.boston.com/news/local/articles/2008/04/06/city_complaint_line_lags/

✂ Indiana school district wipes out high school grades

<Danny Burstein <dannyb@panix.com>>

Tue, 1 Apr 2008 19:45:40 -0400 (EDT)

from the school's website of Evansville, Indiana

"... The Evansville Vanderburgh School Corporation recently experienced a hardware malfunction with its AS400 computer server resulting in a loss of student grades...

" Following scheduled maintenance on March 27, 2008, disk errors occurred. After working with IBM engineers around the clock to mitigate data loss, the engineers determined that due to an unfortunate and very rare combination of hardware problems and backup configuration settings, all student grade book assignment data for the current grading period is no longer in the system. Harrison, North and Bosse High Schools and Harwood Middle School - all on the six-week grading period - lost four weeks of individual assignment grades that had been posted."

rest: <http://www.evscschools.com/>

[Also noted by Jim Reisert.

http://news.yahoo.com/s/ap/20080401/ap_on_re_us/grades_gone_1

PGN]

✂ Re: Search engine bait? ([RISKS-25.09](#))

<Martin Ward <martin@gkc.org.uk>>

Fri, 28 Mar 2008 10:40:49 +0000

> Read the descriptions of the products.

> ... they are in fact crafted by taking a genuine English description (from
> a manufacturer's site, perhaps?) and then applying a randomized
> thesaurus-based word replacement algorithm.

My guess is that the changes are designed to make each page look different,
so as to avoid being marked down for having many similar pages.

martin@gkc.org.uk <http://www.cse.dmu.ac.uk/~mward/>
G.K.Chesterton web site: <http://www.cse.dmu.ac.uk/~mward/gkc/>

Another genuine mail that looks like a phish

<Andy Piper>

Thu, 03 Apr 2008 10:17:31 +0100

Yesterday I received an invitation from TaxCalc to purchase the new 2008
version [for those in the US, the UK tax year starts April 6th]:

"We are delighted to inform you that TaxCalc 2008 is available for immediate
download."

It goes on:

"Go to

<http://response.pure360.com/_act/link.php?mId=A833682651665220042396&tId=7258777>www.taxcalc.com
to order now." plus assorted other links where the URL is not actually the
same as the supplied text.

Which to me looks like a phishing attempt more than anything else. It seems
though that pure360.com is a marketing organization that handles this sort
of thing for a number of companies and the mail is in fact genuine. I'm
guessing that if I click through the link [I'm not going to!] I will end up
at taxcalc.com eventually, but why do they even do this? Why not just put up
the real URL if I am going to end up there anyway?

I sent a mail to pure360 CC'ing the taxcalc sales team, and to their credit
they (taxcalc) gave me a call within the hour, although I didn't get the
impression they were going to do anything about it. The call was
clever/disturbing as well - I never gave my number out in my mail, and I
used a different mail address from the one I have registered with them; they
must have deduced who I was from the "phish"-link and looked up my number in
their records.

Now I am really paranoid. The link above clearly identifies me individually,
am I giving out something to RISKS that puts me at even more RISK?! so
I click through the link and end up at a taxcalc login page. Clearly some
form of sanity has prevailed.

The RISK, as always, is how can we expect to educate the public when
reputable companies do things like this. Maybe they need to look at some

basic material such as Dr Seuss' Internet guide - "One phish, two phish - red phish, blue phish" ...

Nissan GT-R sports car recognizes racetrack coordinates and

<Clark Family <cclark@ix.netcom.com>>

Tue, 04 Mar 2008 14:58:56 -0800

aftermarket parts

Apparently the Nissan Corp. has ruined the fun of aftermarket tuners on the latest GT-R high performance street sportscar in Japan. The ECU is set on a hair trigger and balks at many aftermarket performance upgrades as well as non-factory installed tires and wheels through the run-flat detectors.

But more ominously, the onboard navigation system watches your speed via GPS and recognizes popular racetrack locations. You must scroll through a series of menus and agree to disable the 180kph (111mph) speed limiter. Then after thrashing it on the track, you must take it for a \$1000 Nissan High Performance Center safety check or the warranty is void.

Big Brother is your co-pilot.

REVIEW: "Security Data Visualization", Greg Conti

<Rob Slade <rmslade@shaw.ca>>

Tue, 08 Apr 2008 10:21:38 -0800

BKSCDTVS.RVW 20071124

"Security Data Visualization", Greg Conti, 2007, 978-1-59327-143-5,
U\$49.95/C\$59.95

%A Greg Conti www.gregconti.com

%C 555 De Haro Street, Suite 250, San Francisco, CA 94107

%D 2007

%G 978-1-59327-143-5 1-59327-143-3

%I No Starch Press

%O U\$49.95/C\$59.95 415-863-9900 fax 415-863-9950 info@nostarch.com

%O <http://www.amazon.com/exec/obidos/ASIN/1593271433/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/1593271433/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/1593271433/robsladesin03-20>

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

%P 244 p.

%T "Security Data Visualization: Graphical Techniques for Network
Analysis"

Data visualization is very valuable. It is, however, difficult to perform properly in many situations: interpretation of data into graphics can be extremely useful, but it is often difficult to determine how best to present the information, and in the same way

that proper visualization can be tremendously helpful, the wrong choice can be terrifically misleading. Conti somewhat avoids this issue in the introduction, since all he claims for the book is inspiration.

Chapter one provides a number of data visualization and user interface examples. Some simple data visualization experiments in chapter two show a few interesting ideas that can be explored with text and simple graphics files, as well as comparative images as simple processing is pursued. The port scan data displays suggested in chapter three don't seem to work quite as well. Similarly, chapter four looks at vulnerability scanning, but the recommendations presented don't appear to add much of value in displaying the data. Slightly better results seem to be obtained using real Internet data in chapter five, since some notion of the implications of the information can be taken from the illustrations. Chapter six contains a number of examples of impressive visualization of security data, but there is limited discussion as to how to determine the best means of displaying data of different types. The aspects of creation of visualizations, for firewall logs, is dealt with in chapter seven, and with IDS (Intrusion Detection System) data in eight. Chapter nine discusses ways of attacking visualizations, usually by injecting spurious data. General principles for building visualization systems are in chapter ten. Chapter eleven turns to areas for additional research on the topic in the future. Chapter twelve lists references and resources.

The book is pretty, and it may provide inspiration. However, it probably won't provide an awful lot of assistance in getting your data effectively visualized.

copyright Robert M. Slade, 2007 BKSCDTVS.RVW 20071124
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 12

Tuesday 22 April 2008

Contents

- [Industrial Control Systems Killed Once, Will Kill Again](#)
[Ryan Singel](#)
 - [GPS leads a bus astray](#)
[David Caley](#)
 - [Neighbor's data shows up in my browser](#)
[borborugmus](#)
 - [Oklahoma Dept of Corrections Website URLs contain raw SQL](#)
[Jim Garrison](#)
 - [Real-time spying on credit card holders](#)
[Nick Brown](#)
 - [Larger Prey Are Targets of Phishing](#)
[John Markoff](#) via [Monty Solomon](#)
 - [Aer Lingus economy 5-euro flights to the US after test data leaked to web](#)
[Patrick O'Beirne](#)
 - [Gone in 60 seconds: Spambot cracks Live Hotmail CAPTCHA](#)
[Emil Protalinki](#) via [Monty Solomon](#)
 - [Bouncing Merrily Along](#)
[Peter B. Ladkin](#)
 - [The 10,000 web sites infection mystery solved](#)
[Bojan Zdrnja](#) via [Monty Solomon](#)
 - [Re: Census to scrap handheld computers for 2010 count](#)
[Derek P. Schatz](#)
 - [Re: Search engine bait?](#)
[Randall Roberts](#)
 - [Re: Another genuine mail that looks like a phish](#)
[Gregory Hicks](#)
 - [Re: Nissan GT-R sports car and GPS](#)
[Peter Houppermans](#)
[JTaylor](#)
 - [2008 IEEE Symposium on Security and Privacy](#)
[Yong Guan](#)
 - [REVIEW: "Computer Security: Principles and Practice"](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

Industrial Control Systems Killed Once, Will Kill Again (Ryan Singel)

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

Fri, 11 Apr 2008 5:10:42 PDT

On 10 Jun 1999 a 16-inch diameter steel pipeline operated by the now-defunct Olympic Pipeline Co. ruptured near Bellingham, Washington, flooding two local creeks with 237,000 gallons of gasoline. The gas ignited into a mile-and-a-half river of fire that claimed the lives of two 10-year-old boys and an 18-year-old man, and injured eight others.

Wednesday, computer-security experts who recently re-examined the Bellingham incident called its victims the first verified human casualties of a control-system computer incident. They argue that government cybersecurity standards currently under debate might have prevented the tragedy. ...

Following the 1999 incident, a nearly three-year investigation by the National Transportation Safety Board concluded that multiple causes contributed to the deadly conflagration, including pipeline damage inflicted by construction workers years earlier, and a misconfigured valve.

But the factor that intrigues Joe Weiss (Applied Control Solutions) and Marshall Abrams (MITRE) is a still largely unexplained computer failure that began less than 30 minutes before the accident and paralyzed the central control room operating the pipeline, preventing workers from releasing pressure in the line before it hemorrhaged.

With support from the U.S. National Institute of Standards and Technology, Weiss and Abrams pored over public government records on the incident, looking at it through the lens of a pending cybersecurity standard called NIST 800-53. The duo concluded that the requirements in the standard would have prevented the explosion from occurring. ...

Security experts and government investigators have long warned that the complex networks controlling critical infrastructures like the power grid, and gas and oil pipelines, were not built with security in mind -- a point driven home by several incidents of the systems failing. In January 2003, the Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant and disabled a safety-monitoring system for nearly five hours. Later that year, a software bug in a General Electric energy-management system contributed to a cascading power failure that cut off electricity to 50 million people in eight states and a Canadian province. [Source: Ryan Singel, Wired.com, Threat Level: Privacy, Security, Politics and Crime Online, blog 9 Apr 2008; PGN-ed]

<http://blog.wired.com/27bstroke6/2008/04/industrial-cont.html>

GPS leads a bus astray

<David Caley <dcaley@marchex.com>>

Thu, 17 Apr 2008 13:31:29 -0700

Another instance of directions from a GPS navigational device overriding common sense:

A police report said the driver of a charter bus (11' 8") carrying 22 students told police he was following directions from a global positioning device prior to a crash into a pedestrian overpass that was too low (9' clearance). [Source: Seattle, KIRO TV, 17 Apr 2008]
<http://www.kirotv.com/news/15912549/detail.html>

Neighbor's data shows up in my browser

<borborugmus <borborugmus@gmail.com>>
Sun, 13 Apr 2008 20:51:12 -0400

This weekend I was doing some last-minute work on my taxes, using TurboTax Deluxe tax software. TurboTax has an online site, ItsDeductible.com, that you can go to in order to get help in determining the value of non-monetary charitable deductions you've made.

I had been to the ItsDeductible site once or twice in the past, and had had a little trouble logging in. So I went to a section on the site to try and change my login name, which I had made much too long. I started to type in my current information, and when I typed in the first letter of my first name, the auto-complete function put in the name "Jason" instead of my name. That seemed very strange, because I am the only person who ever uses this computer, and my name is not Jason.

I changed it back to my own first name, and typed in my last name. Then I tabbed to the address field. As I typed in the first digit of my 3-digit house number, the house number and street name of my next-door-neighbor showed up in the auto-complete list! Since I know these neighbors, and know that the homeowner's first name is "Jason", I next moved back up to the "Last name" field of the form. I typed in the first letter of what I know is Jason's last name. And Jason's last name came up in the auto-complete list!

There seems to be some way that my next-door-neighbor's information got into my PC. They always have their wireless internet on, but my wireless reception is usually disabled. I really don't know how this could have happened. Of course, since the problem showed up while I was doing my taxes, I am even more paranoid about what information of mine might have been swapped between households.

I tried to make the problem repeat after a reboot, but was unable to duplicate the login screen. I also checked my "Identity Safe" passwords from Norton, and see that only my own information is saved for that web site. The browser I used was Firefox, but I can't find a way to see how it has stored its auto-complete section.

✘ Oklahoma Dept of Corrections Website URLs contain raw SQL

*<Jim Garrison <jhg@jhmg.net>>
Tue, 15 Apr 2008 11:56:14 -0500*

The Oklahoma DOC published a web interface where the URL contained the SQL query executed to retrieve the data to be reported. Thus, any knowledgeable user could execute general SQL queries against a database containing large amounts of personal information -- including UPDATE statements (!) It was taken down only after management was shown that THEIR personal information was available.

<http://thedailywtf.com/Articles/Oklahoma-Leaks-Tens-of-Thousands-of-Social-Security-Numbers,-Other-Sensitive-Data.aspx>

✘ Real-time spying on credit card holders

*<Nick Brown <Nick.BROWN@coe.int>>
Fri, 11 Apr 2008 12:40:53 +0200*

Business Week reports that Mastercard is to launch a new service which will, among other things, allow the payer of a corporate or other card to receive real-time alerts as to what the card is being used for.

http://www.businessweek.com/magazine/content/08_16/b4080031217154.htm

The risks are left as an exercise for the reader...

✘ Larger Prey Are Targets of Phishing (John Markoff)

*<Monty Solomon <monty@roscom.com>>
Wed, 16 Apr 2008 08:53:03 -0400*

An e-mail scam aimed squarely at the nation's top executives is raising new alarms about the ease with which people and companies can be deceived by online criminals. Thousands of high-ranking executives across the country have been receiving e-mail messages this week that appear to be official subpoenas from the United States District Court in San Diego. Each message includes the executive's name, company and phone number, and commands the recipient to appear before a grand jury in a civil case.

A link embedded in the message purports to offer a copy of the entire subpoena. But a recipient who tries to view the document unwittingly downloads and installs software that secretly records keystrokes and sends the data to a remote computer over the Internet. This lets the criminals capture passwords and other personal or corporate information. Another

piece of the software allows the computer to be controlled remotely. According to researchers who have analyzed the downloaded file, less than 40 percent of commercial antivirus programs were able to recognize and intercept the attack.

The tactic of aiming at the rich and powerful with an online scam is referred to by computer security experts as whaling. The term is a play on phishing, an approach that usually involves tricking e-mail users - in this case the big fish - into divulging personal information like credit card numbers. Phishing attacks that are directed at a particular person, rather than blasted out to millions, are also known as spear phishing.

The latest campaign has been widespread enough that two California federal courts and the administrative office of the United States Courts posted warnings about the fake messages on their Web sites. Federal officials said they stopped counting after getting hundreds of phone calls from corporations about the messages. At midday on 15 Apr 2008, one antispam company, MX Logic, said in a Web posting that its service was still seeing at least 30 of the messages an hour.

[Source: John Markoff, *The New York Times*, 16 Apr 2008; excellent long article, PGN-ed]

<http://www.nytimes.com/2008/04/16/technology/16whale.html?ex=1365998400&en=208591045a06cdf&ei=5090>

✶ Aer Lingus economy 5-euro flights to the US after test data

<"Patrick O'Beirne" <pob@sysmod.com>>
Fri, 18 Apr 2008 14:43:40 +0100

leaked to web

Aer Lingus blamed a technical fault for Wednesday's error, which saw up to 300 people book 5-euro business-class flights to the US. However, the airline will provide economy-class seats to the customers who made the reservations between 7.30am and 9am, when a promotional fare test webpage was mistakenly put up live. [The flights of course were not 5 euro but about 150 euro each when taxes and charges were added. PO'B] [Source: RTE news; PGN-ed]

<http://www.rte.ie/news/2008/0418/aerlingus.html>

Patrick O'Beirne, Systems Modelling Ltd.

<http://www.sysmod.com/> (+353)(0) 5394 22294

✶ Gone in 60 seconds: Spambot cracks Live Hotmail CAPTCHA

<Monty Solomon <monty@roscom.com>>
Wed, 16 Apr 2008 08:05:12 -0400

Emil Protalinski, 15 Apr 2008

Internet users are quite familiar with the Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), a quick method that verifies whether or not the user trying to sign up is a person or a bot. A picture with swirled, mangled, or otherwise distorted characters is displayed and the user then types in the correct letters or numbers. Thus far, the system has worked well to slow down malicious bots, but recently the groups behind such software have made significant strides. A security firm is now reporting that the CAPTCHA used for Windows Live Mail can now be cracked in as little as 60 seconds.

Back in early February, a group cracked Windows Live Hotmail's CAPTCHA. A few weeks later, Gmail's version followed suit. In just over a month's time, some anti-spam vendors were forced to completely block the domain for the popular service as bots signed up for thousands of bogus accounts and began to flood the tubes with e-mail advertisements for lottery tickets and watches. The close proximity of the two cracks has done everything but sealed CAPTCHA's fate.

To make matters worse, Websense Security Labs is now reporting that the method for getting around Windows Live Mail's CAPTCHA has been improved to the point that a bot can decipher the text and make a guess in less than six seconds, on average. Windows Live Hotmail's Anti-CAPTCHA automatic bot, which hooks itself into Internet Explorer on a victim's machine, has a success rate of about 10-15 percent. That means that it takes up to one minute for a single bot to create a new account. ...

<http://arstechnica.com/news.ars/post/20080415-gone-in-60-seconds-spambot-cracks-livehotmail-captcha.html>

✶ Bouncing Merrily Along

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

Tue, 22 Apr 2008 09:04:10 +0200

We recently reconfigured our mail SW and for a couple of days I got a few hundreds of rejected-mail bounce messages. My e-mail address has been forged by spammers for years and these bounces came from handling such fraudulent messages.

No one in this world, so far as I know -- and I have searched the records for years, and employed agents to help me -- has ever lost money by underestimating the intelligence of the great masses of the mail system administrators. And I can't be the first to have observed that. So I am prepared to believe that there are at least a few hundred admins out there who have never heard of spam and fraudulent "From:" lines.

But many if not most of these messages came from machines that either advertised themselves as spam filters, or showed that the message had passed through spam filters!

One could make it a legal offence to reply to the "From:" address of a message one had classified as spam. It likely wouldn't curb the phenomenon,

but it would ensure a steady flow of cash to the state, which could then redistribute it amongst Internet infrastructure providers.

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

[NOTE: neumann and risks From: addresses have been widely forged in the past few weeks. PGN]

✂ The 10,000 web sites infection mystery solved

<Monty Solomon <monty@roscom.com>>

Mon, 21 Apr 2008 10:49:21 -0400

Published: 2008-04-16,

Last Updated: 2008-04-16 19:14:00 UTC

by Bojan Zdrnja (Version: 3)

Back in January there were multiple reports about a large number of web sites being compromised and serving malware. Fellow handler Mari wrote the initial diary at <http://isc.sans.org/diary.html?storyid=3834> .

Later we did several diaries where we analyzed the attacks, such as the one I wrote at <http://isc.sans.org/diary.html?storyid=3823> . Most of the reports about these attacks we received pointed to exploitation of SQL Injection vulnerabilities.

Yesterday, one of our old friends, Dr. Neal Krawetz, pointed us to another site hosting malicious JavaScript files with various exploits. While those exploits where more or less standard, we managed to uncover a rare gem between them - the actual executable that is used by the bad guys in order to compromise web sites.

While we had a general idea about what they do during these attacks, and we knew that they were automated, we did not know exactly how the attacks worked, or what tools the attackers used. The strategy was relatively simple: they used search engines in order to find potentially vulnerable applications and then tried to exploit them. The exploit just consisted of an SQL statement that tried to inject a script tag into every HTML page on the web site.

The utility we recovered does the same thing. The interface appears to be in Chinese so it is a bit difficult to navigate around the utility, but we did some initial analysis of the code (which is very big) to confirm what it does. ...

<http://isc.sans.org/diary.html?storyid=4294>

✂ Re: Census to scrap handheld computers for 2010 count ([RISKS-25.11](#))

<"Schatz, Derek P" <Derek.P.Schatz@boeing.com>>

Wed, 9 Apr 2008 17:47:58 -0700

And what would be the likelihood that the handheld computers could be re-used for the 2020 Census? Would the vendor still support the more than 10-year-old hardware at that time? How many RISKS subscribers are still using 10+ year old computers?

The risk: Spending gigantic wads of money on something that will be obsolete before it can be used even a second time?

Re: Search engine bait? ([RISKS 25.09](#))

<"Randall Roberts" <randall.roberts@eds.com>>

Thu, 10 Apr 2008 12:12:05 -0500

This might be a simple captcha hacking operation. Well designed captchas are hard to break programmatically, so people put up stuff like this to get people to do the work for them.

Randy Roberts, Global Network Security Capability EDS, Security & Privacy Service Line, MD 354 4000 North Mingo Road Tulsa, OK 74116 +1 918 939-4844

[Also noted by Joseph Gwinn. PGN]

Re: Another genuine mail that looks like a phish (Piper, [RISKS-25.11](#))

<Gregory Hicks <ghicks@cadence.com>>

Wed, 9 Apr 2008 20:35:22 -0700 (PDT)

Let's just say this: If you're running a marketing campaign for some company, you'd want to have some way of collecting metrics that allow you to go back to the sponsoring company and say "Look, we got you this many qualified leads. Of these, this many bought your product. So you owe us \$X plus \$Y as a bonus..."

Anyway, that is why a company will send you an e-mail, expect you to click a link and end up at the client company's website.

Re: Nissan GT-R sports car and GPS (Clark, [RISKS-25.11](#))

<Peter Houppermans <peter@houppermans.com>>

Thu, 10 Apr 2008 12:49:29 +0200

If the onboard navigation system was designed by TomTom it will probably ask

you all these questions whilst you're driving. TomTom appears to have decided in Navigator 6 that certain things like setting up a data link for traffic information are important enough to divert your attention from the road, and there's no disabling that question. It would be nice if someone added an 'adult' mode where you can take some of those decisions yourself again, and just once instead of every time..

Tomtom have a watchdog idea too, and the potential flaws in both this and the Nissan approach are identical: a flawed map or analysis will make a mess of the conclusion. In the case of Tomtom, maps include in some places speed limit information which is in itself not such a bad idea.

The idea went off the cliff by making display modifications based on the speed data. When you exceed the "map limit", the speed indicator goes red. When you go WELL over the speed limit it starts blinking, not normal-inverse but visible-invisible, at approx a 1Hz frequency.

In other words, for a precise speed indication you may have to take your eyes off the road for a full second in the worst possible conditions. Duh. Oh, and no way to disable that feature either.

But no fears of Big Brother speed limits via GPS: not only did I find the speed limit data far from accurate, even when corrected there's another fly in the ointment: variable limits.

In various countries, multiple speed limits are deployed, adjusted according to situation (snow, pollution, accidents etc). Which speed limit do you store?

All I'm waiting for now is a government imposed feature where speeding drivers will be automatically diverted into the nearest traffic jam..

Re: Nissan GT-R sports car and GPS (Clark, [RISKS-25.11](#))

<<jtayNOSPAMlor@hfdONTSENDMESPAMx.andara.com>>
Thu, 10 Apr 2008 12:10:54 GMT

> Then after thrashing it on the track, you must take it for a \$1000 Nissan
> High Performance Center safety check or the warranty is void.

GPS jammers cost less than \$100. Does the car work if it can't get a GPS fix?

2008 IEEE Symposium on Security and Privacy

<"Peter G. Neumann" <neumann@csl.sri.com>>
Fri, 18 Apr 2008 23:35:46 PDT

PROGRAM:

<http://www.ieee-security.org/TC/SP2008/oakland08.html>

May 18-21, 2008, The Claremont Resort
Berkeley/Oakland, California, USA
Claremont Hotel Group Rate Deadline: April 25, 2008

Contact: Yong Guan <guan@iastate.edu>

REVIEW: "Computer Security: Principles and Practice",

<Rob Slade <rmslade@shaw.ca>>

Mon, 14 Apr 2008 12:34:38 -0800

William Stallings/Lawrie Brown

BKCMSCPP.RVW 20080204

"Computer Security: Principles and Practice", William Stallings/Lawrie Brown, 2008, 978-0-13-600424-0

%A William Stallings williamstallings.com/CompSec/CompSec1e.html

%A Lawrie Brown

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

%D 2008

%G 0-13-600424-5 978-0-13-600424-0

%I Prentice Hall

%O 800-576-3800 416-293-3621 +1-201-236-7139 fax: +1-201-236-7131

%O <http://www.amazon.com/exec/obidos/ASIN/0136004245/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0136004245/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0136004245/robsladesin03-20>

%O Audience i+ Tech 2 Writing 3 (see revfaq.htm for explanation)

%P 798 p.

%T "Computer Security: Principles and Practice"

I am woefully laggard in getting this review out, particularly since I reviewed the text in process, last fall, and therefore have to declare a possibility of bias.

The preface states that the book is intended as the text for a one- or two-semester course in computer security. The work is also addressed to professionals as a basic reference. In that latter regard it may come up short, missing elements of infrastructure, fire protection, investigation, forensics, and being rather weak in terms of architecture and business continuity planning.

There is a rather interesting chapter zero in the volume (it and chapter one are presumably "part zero," which is sound computing theory, but somewhat bemusing in a book) laying out the structure of the text, as well as pointing to the technical resource and course Website, noted above. Chapter one defines fundamental security terms and concepts from various sources. The list is comprehensive, but, given sometimes conflicting positions, little attempt is made to analyze, integrate, or unify the material. There is an excellent set

of references and a solid set of questions and problems, as well as a brief appendix addressing security standards and documents.

Part one involves computer security technology and principles. Chapter two introduces cryptographic tools. The basic ideas of cryptography are presented, but one must go to other chapters and appendices for details and usage of the technology. This structure is unusual in cryptographic literature, but the new perspective may demonstrate somewhat stale abstractions in a fresh way. It is rather odd that the coverage of authentication, in chapter three, does not note the IAAA model of Identification, Authentication, Authorization, and Accountability. Access control, in chapter four, is limited to data access. (The authors also follow the original paper describing Role-Based Access Control as a form of mandatory access control, even though RBAC is now frequently used in discretionary access control environments.) Chapter five's discussion of database security emphasizes the theoretical aspects of that specialty. Intrusion detection is introduced in chapter six. Malicious software is given a scholarly, rather than practical, treatment in chapter seven, but the content is more accurate than is usual even in the security literature. Denial of service attacks are addressed in chapter eight. Chapter nine's review of firewalls concentrates, almost exclusively, on stateful inspection, and the material on intrusion prevention systems repeats, to a large extent, chapter six. Trusted computing and multilevel security, in chapter ten, are discussed in terms of formal security models and security architecture.

Part two deals with software security, with chapter eleven being devoted to the topic of buffer overflows, and the other software subjects covered comprising chapter twelve.

Part three contains topics the authors consider to be management issues. These are (in order through chapters thirteen to eighteen), physical and infrastructure security, human factors (primarily policy and awareness concerns), auditing security management and risk assessment, security controls (plans and procedures), and legal and ethical aspects.

Part four details cryptographic algorithms, and the material is as good as one might expect from the author of "Cryptography and Network Security" (cf. BKCRNTSC.RVW). Symmetric encryption and message confidentiality, illustrated by the Data Encryption Standard and the advanced Encryption Standard, is the topic of chapter nineteen. Asymmetric cryptography and hashes are in twenty.

Part five turns to Internet security. Some Internet security protocols and standards are listed in chapter twenty-one. A detailed look at Kerberos leads off chapter twenty-two's examination of authentication applications.

Operating systems security is the subject of part six, with a look at the Linux model in chapter twenty-three, and Windows in twenty-four.

Appendices at the end of the book provide information on number theory, pseudorandom number generation, projects for teaching security, standards and standards organizations, and the TCP/IP protocol suite.

Of the various domains of information systems security, there is limited material in regard to the security implications of various aspects of computer hardware and architecture, the formation of an architectural model for security design, and business continuity planning. Otherwise, however, the coverage is quite comprehensive, much more so than in other course texts such as Gollman's excellent but now aging "Computer Security" (cf. BKCOMPSC.RVW), Bishop's rather abstract "Computer Security: Art and Science" (cf. BKCMSCAS.RVW), and Stamp's interesting, but sometimes spotty, "Information Security: Principles and Practice" (cf. BKINSCPP.RVW). Anderson's "Security Engineering" (cf. BKSECENG.RVW) is, of course, not only a solid text, but also a useful professional reference, and Stalling and Brown might wish to examine the practical issues dealt with in that work. A range of editions of the "Information Security Management Handbook" (cf. BKINSCMH.RVW) would have similar overview, and more detail, but hardly in a single volume. There is also the "Official (ISC)² Guide to the CISSP Exam" (cf. BKOIGTCE.RVW), and now the "Official (ISC)² Guide to the CISSP CBK," but Stalling and Brown's work, while less broad and detailed, is more academically rigorous.

copyright Robert M. Slade, 2008 BKCMSCPP.RVW 20080204
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 13

Sunday 27 Apr 2008

Contents

- [Hack into Obama campaign site exploited a coding flaw](#)
[Jordan Robertson](#) via [Joseph Lorenzo Hall](#)
- [Hacking a rival smart card?](#)
[Robert P. Schaefer](#)
- [Face scans for air passengers to begin in UK this summer](#)
[Brian Randell](#)
- [30th Spamiversary](#)
[Brad Templeton](#) via [Mike Hogsett](#)
- [Re: Bouncing Merrily Along](#)
[Paul Karger](#)
- [Re: Real-time spying on credit card holders](#)
[Ron Garret](#)
- [Re: Neighbor's data shows up in my browser](#)
[Paul D. Smith](#)
[Erik Mooney](#)
- [Re: GPS leads a bus astray](#)
[Roger Scrafford](#)
- [Re: Nissan GT-R sports car and GPS](#)
[Chris Kantarjiev](#)
[Dag-Erling Smørgrav](#)
[Dag-Erling Smørgrav](#)
[Peter Houppermans](#)
[Dag-Erling Smørgrav](#)
- [Info on RISKS \(comp.risks\)](#)

✉ Hack into Obama campaign site exploited a coding flaw

<[Joseph Lorenzo Hall \[joehall@gmail.com\]](mailto:joehall@gmail.com)>

Thursday, April 24, 2008 10:46 AM

(Jordan Robertson)

[Via Dave Farber's IP distribution. PGN]

A simple flaw in the coding of Senator Barack Obama's Web site led to a hacking switcheroo of presidential proportions just days before the Pennsylvania primary. Some supporters who tried to visit the community blogs section of Obama's site started noticing late last week they were being redirected to Senator Hillary Rodham Clinton's official campaign site. Security researchers said a hacker exploited a so-called "cross-site scripting" vulnerability in Obama's Web site to engineer the ruse.

Netcraft Ltd. said the hacker injected code into certain pages in the section -- code that was then executed when subsequent visitors tried to view the community blogs section. The vulnerability has since been fixed. ... [Jordan Robertson, The Associated Press, 23 Apr 2008; PGN-ed]
<http://www.washingtonpost.com/wp-dyn/content/article/2008/04/23/AR2008042302976.html>

Joseph Lorenzo Hall, UC Berkeley School of Information <http://josephhall.org/>

✂ Hacking a rival smart card?

<"Peter G. Neumann" <neumann@csl.sri.com>>
Thu, 24 Apr 2008 14:14:51 PDT

From Reuters via Robert P Schaefer

A computer hacker testified on Wednesday that News Corp's NDS unit hired him to develop software to reverse-engineer a rival's smart card. Was the purpose to pirate?

<http://www.reuters.com/article/technologyNews/idUSN2334980420080424?pageNumber=3D1&virtualBrandChannel=0>

✂ Face scans for air passengers to begin in UK this summer

<Brian Randell [Brian.Randell@ncl.ac.uk]>
Friday, April 25, 2008 8:05 AM

[Via Dave Farber's IP distribution. PGN]

Owen Bowcott, *The Guardian*, 25 Apr 2008
Face scans for air passengers to begin in UK this summer;
Officials say automatic screening more accurate than checks by humans

A face recognition system will scan faces and match them to biometric chips on passports. Airline passengers are to be screened with facial recognition technology rather than checks by passport officers, in an attempt to improve security and ease congestion. Unmanned clearance gates will be phased in to scan passengers' faces and match the image to the record on the computer chip in their biometric passports.

Border security officials believe the machines can do a better job than humans of screening passports and preventing identity fraud. The pilot

project will be open to UK and EU citizens holding new biometric passports.

But there is concern that passengers will react badly to being rejected by an automated gate. To ensure no one on a police watch list is incorrectly let through, the technology will err on the side of caution and is likely to generate a small number of "false negatives" - innocent passengers rejected because the machines cannot match their appearance to the records.

They may be redirected into conventional passport queues, or officers may be authorised to override automatic gates following additional checks.

Ministers are eager to set up trials in time for the summer holiday rush, but have yet to decide how many airports will take part. If successful, the technology will be extended to all UK airports. ...

Full story at:

<http://www.guardian.co.uk/business/2008/apr/25/theairlineindustry.transport>

School of Computing Science, Newcastle University, Newcastle upon Tyne, NE1 7RU, UK <http://www.cs.ncl.ac.uk/people/brian.randell> +44 191 222 7923
IP Archives RSS Feed: <http://www.listbox.com/member/archive/rss/247/>

✉ 30th Spamiversary

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

Fri, 25 Apr 2008 14:05:35 PDT

[Thanks to Mike Hogsett for noting this event, and Brad Templeton for recording it.]

What is allegedly the very first spam message was sent roughly 30 years over the ARPANET:

<http://www.templetons.com/brad/spamreact.html#msg>

In seeing this, Mike was amused because he works with some of the people it was addressed to, of whom a few are still at SRI:

NEUMANN@SRI-KA, GARVEY@SRI-KL, MABREY@SRI-KL, WALDINGER@SRI-KL and some of whom are retired:

ENGELBART@SRI-KL, NIELSON@SRI-KL, GOLDBERG@SRI-KL

(I am always amused when some of these old ARPANET addresses show up in today's incarnations of spam.)

Also somewhat before Mike's time, Geoff Goodfellow, Ron Kunzelman, Dan Lynch, and many others at SRI were instrumental in the evolution of the ARPANET.

Also included in the enormous enumerated TO: list (historically interesting in itself by not having been suppressed!) are Bill English (who was the catalyst for much of Doug Engelbart's innovations being transitioned from SRI to PARC), Dave Farber, Irv Jacobs, Bob Metcalfe, Jon Postel (who by then had moved from SRI to ISI), three Sutherlands, and Lauren Weinstein, to name

just a few.

Happy Birthday, Spam! Sorry I cannot wish you many happy returns.

[Error corrected in archive copy. PGN]

Re: Bouncing Merrily Along (Ladkin, [RISKS-25.12](#))

<Paul Karger <karger@watson.ibm.com>>

Wed, 23 Apr 2008 09:23:13 -0400

Making it a legal offence to reply to the "From:" address of a message one had classified as spam would be disastrous. Many overly-ambitious spam filters classify legitimate email as spam. In particular, there is one spam filter that regularly classifies email from family members as spam, even though the email itself is quite legitimate and contains no evil attachments. Until there are perfect spam classifiers (which is likely never), such a legal requirement would criminalize responding to legitimate, but miss-classified emails. (Yes - I've tried to get the spam filter in question fixed, but it hasn't happened yet.)

Re: Real-time spying on credit card holders (Brown, [RISKS-25.12](#))

<Ron Garret>

Wed, 23 Apr 2008 23:13:46 -0700

> The risks are left as an exercise for the reader...

I've been reading RISKS for a looooong time. I'm not quite as paranoid as they come, but I'm close, and I don't see the problem. In fact, this seems like a pretty good idea to me, not so much because it allows bosses to spy on their employees (though that doesn't seem altogether unreasonable) but because this kind of closed loop could put a serious dent in credit card fraud. The source of nearly all credit card fraud is the fact that under the current protocols, the information used in one transaction can be used to conduct a different transaction. Adding a closed loop through a node over which the card holder has actual control (like an email account or a cell phone) eliminates this problem. The only reason IMO the card companies have not done this sooner is that they have been able to fob the problem off on the merchants.

Perhaps Mr. Brown would be so kind as to elucidate exactly what he thinks the RISKS are?

Re: Neighbor's data shows up in my browser (borborugmus, [RISKS-25.12](#))

<"Paul D. Smith" <paul_d_smith@hotmail.com>>

Wed, 23 Apr 2008 08:26:11 +0100

How about the following explanation. Both neighbours use the same ISP and power off their networks. when they power up, the ISP assigns Jason's DHCP address to the OP and then the tax site maps that IP address (previously used by Jason) and provides Jason's details to the OP.

This would be a really scary ignorance of the way in which the Internet works!

Re: Neighbor's data shows up in my browser (borborugmus, [RISKS-25.12](#))

<Erik Mooney <erik@dos486.com>>

Wed, 23 Apr 2008 11:32:14 -0500

This is easily explainable by server-side IP tracking, so you can rest easy on "Jason" hacking your computer. It's quite likely the server noticed a hit from an IP address that matched a recent login from Jason. (Either an exact match, or similar within a few subnet bits.) So it helpfully preloaded the auto-complete list to speed the login process for Jason. After your reboot, the most recent hit from that IP or subnet was no longer Jason, so Jason's information was no longer preloaded.

The privacy risk does exist, but would seem fairly minimal. Name and address are hardly secrets, so the only thing you learned was that he has a computer and used TurboTax online. A View Source on the HTML might have dispelled any further concerns about leaking Jason's info to you or your info to anyone else from the same IP address or subnet.

Re: GPS leads a bus astray (Caley, [RISKS-25.12](#))

<"Roger Scrafford" <roger.scrafford@gmail.com>>

Wed, 23 Apr 2008 16:20:05 -0700

Last year my Significant Other Martha and I were at the end of a California vacation, driving south from Calistoga to Oakland in our GPS-equipped rental car. All went well until the pleasant female GPS voice told us to take a certain exit. It didn't look right, but I thought, "Why not? We have time, and we might see something new."

I took the exit, as did the car behind me.

I was directed down some very suburban side streets which were clearly not going to be taking us anywhere near the Oakland airport.

The car stayed behind me.

Finally the car honked because I had slowed to try to figure out where I

was, and what might have gone wrong. I pulled over, and as he roared past me, honking again, I could hear the driver shout something about "tourists."

I continued on, following the GPS route, which now brought me back to the starting point of the misdirection.

"Turn right," said the GPS. To do so would have taken me around the same suburban loop.

Just as I turned left (against the advice of the GPS) I noticed that the car which had once been following us, and which had honked and whose driver had shouted, was now sitting curbside, its occupants shouting and waving arms in frustration, arguing about which of them had made this terrible mistake.

Though I have no proof, I believe they had the same in-car GPS that we had, and received the same erroneous directions. But we used our heads, and were soon on our way back to Oakland on a road we knew would actually take us there. For all I know, the other car is still looping around that obscure California neighborhood, blindly following the instructions of the GPS.

Re: Nissan GT-R sports car and GPS (Clark, [RISKS-25.11](#))

<Chris Kantarjiev <cak@dimebank.com>>

Tue, 22 Apr 2008 18:07:14 -0700

I've spent the last two years looking at map data from vendors across the world trying to understand if they have decent speed limit data. They don't. Last time I ran the numbers, NAVTEQ provided "observed" speed limit data on less than 10% of the US street segments. TeleAtlas is worse. You don't want to hear how bad the EMEA data are. For the most part, the best you can do is choose a speed limit based on the class of road (limited access, expressway, arterial, etc.)

Most US States have speed limits that vary by vehicle type - for example, class A trucks may only drive 55 on freeways even if the road speed limit is listed as 65. That's in California (and many other states), but there are exceptions, sometimes on a per-road basis (the Ohio Turnpike comes to mind, and Texas has even more arcane rules).

Real-time conditions aren't even under consideration ... though the infrastructure to deliver the condition information is improving!

Re: Nissan GT-R sports car and GPS (Taylor, [RISKS-25.12](#))

<Dag-Erling Smørgrav <des@des.no>>

Wed, 23 Apr 2008 11:05:15 +0200

> Does the car work if it can't get a GPS fix?

Modern car navigation systems (such as the TomTom Go 920) have accelerometers in addition to a GPS receiver. The primary purpose of these accelerometers is to allow the system to function in tunnels and deep valleys, but they should also nullify the effect of a GPS jammer, unless of course the jammer is in a car that's driving on the same road, in the same direction, at the same speed as you are.

Re: Nissan GT-R sports car and GPS (Houppermans, [RISKS-25.12](#))

<Dag-Erling Smørgrav <des@des.no>>

Thu, 24 Apr 2008 09:59:17 +0200

> [... SEE 25.12. PGN]

With all due respect, this is preposterous.

First of all, the speed limit warning is one of a series of safety features that can be enabled and disabled, and last I checked they were all disabled by default. When they were first introduced in a software update some months ago, I deliberately enabled the speed limit warning and the menu restrictions.

Second, if you do enable it, there is an audible warning when you go above ~110% of the local speed limit. The default sound is a soft triple chime that repeats at an interval of about 30 seconds (I've never timed it, it just feels that way)

Third, there is a hysteresis, so that if you cross from a section with a higher speed limit into a section with a lower speed limit, TomTom will wait a bit for you to reduce your speed before the speed indicator goes red and the audible alarm goes off.

Fourth, if you are going more than 10% over the speed limit - which is when it starts blinking - you'd better be watching the road and not your satnav or I wouldn't want to be on the same road as you. In fact, TomTom has another safety feature you can enable that blanks the screen when you go above a certain speed.

Fifth, regarding misleading speed limit information, *use your eyes* - how on earth did you cope before you got your satnav? - and use TomTom's map correction feature to report the error. I concede that it doesn't handle variable limits, though, and it is a problem in Oslo, where I live, albeit a minor one - there is only one road where the speed limit varies on a daily or intra-daily basis, and two where it varies on a seasonal basis.

Sixth, when you've driven a few miles with your TomTom, you should have a pretty good idea of the magnitude and sign of the error on your car's built-in speedometer (mine is 8%, and unless there is something wrong with your car, it is always positive, i.e. you are going slower than the speedometer indicates), so incorrect speed limit information in your satnav shouldn't be a problem - provided you pay attention to the signage so you

know when it's incorrect.

Personally, I don't find the blinking annoying at all - once I enabled it, I adapted very quickly so that I now see in my peripheral vision when it's on and when it's off, and I don't have to stare at it to read the speed.

✉ Re: Nissan GT-R sports car and GPS (Smørgrav, [RISKS-25.1](#))³

<Peter Houppermans <peter@houppermans.com>>

Thu, 24 Apr 2008 13:10:00 +0200

We differ of opinion on a number of points.

It starts with an apparent assumption that all TomTom versions are equal, which is not the case. I was talking about Navigator 6 on Symbian (further named N6) - my fault for not clearly identifying it because it alters the discussion somewhat (and it means another risk has been identified, version delta).

Further, note that I'm not **relying** on the speed limit feature - it actually gets in my way :-)

> I deliberately enabled the speed limit warning and the menu restrictions.

I didn't deny the original useful intention. It's especially handy when abroad and when you're in a different system of measurements (miles vs kilometers) - but claiming a feature isn't a problem because you can switch it off misses the point somewhat. And in my version it cannot be disabled. Speed indication comes with limit "feature", like it or not.

New risk: different implementation per version. In N6, the speed tolerance in N6 is limit + 5 km, with the disco effect starting at limit + 10 km (where limit = what TomTom derives from the supplied maps). N6 also lacks the audible alarm, but I started this discussion talking about the speed indication and what the alarm "feature" does to it - not that I'm somehow reliant on the limit information (if anything, I'd be happy if I could disable it).

> TomTom will wait a bit for you to reduce your speed before the speed
> indicator goes red and the audible alarm goes off.

And this affects the discussion in which way?

> In fact, TomTom has another safety feature you can enable that blanks the
> screen when you go above a certain speed.

Available in N6. I think we're on the level with road sharing - I would be worried about a driver relying on an external, unaudited and unaccredited piece of equipment with data in need of improvement as primary means to comply with speed limits, instead of using a speedometer that require formal type approval before vehicle use. And let's hope the radio stays off :-)

My point is exactly that there is very little time to take in data when driving (side and rear mirror scan, speedo, fuel status, children) so the last thing a device should do is obstruct information. If one insists on blinking then use at least a method that doesn't deny or delay information, especially if this feature isn't optional.

[...] I already observed I'm not that interested in the limit data (it presently seems to get in the way :-).

The map correction feature is another fun feature. It leads me to suspect it's maybe a good idea to avoid any new road layouts for a while because drivers may be distracted entering map changes, potentially resulting in a higher than usual accident risk.. Joking aside, the only way I can see that work sensibly is if it's a one-button feature which simply sends the current GPS location to the surveyors for review (i.e. uses the traffic link, for example). That would ensure the quality of the input, because the whole map sharing concept has IMHO some entertaining potential too.

As a matter of fact, if you file a map issue with TomTom this is exactly what happens. You identify an issue, and they appear to queue a location survey to re-acquire the information, which assures the quality. And sell you a new map :-).

I think my reasons for why I want the speed facility are slightly immaterial to the discussion, but FYI, it merely serves as extra calibration data for me as a driver as I use multiple vehicles in various countries, it's not a primary source of information.

> Personally, I don't find the blinking annoying at all ...

Well, AFAIK blinking fell into programming disrepute (other than for severe alarms and Hollywood movies) somewhere around the times VT100s were introduced. It appears we need to re-chlorinate the gene pool because it keeps popping up. Blinking, as it were..

It's also not a major issue (after all, I'm still using the software :-), merely a fine example of how the best intentions get waylaid by not thinking something through and sufficiently testing it in the field. I see the same issue with map share - I'm sure creative use will appear at some point.

I just hope it can be disabled..

Re: Nissan GT-R sports car and GPS (Houppermans, [RISKS-25.13](#))

*<Dag-Erling Smørgrav <des@des.no>>
Thu, 24 Apr 2008 15:54:40 +0200*

When the "restricted menus" feature is enabled and the car is moving, most menu choices - including map correction - are disabled.

There is an option to have a button on the screen that you hit to mark the location so you can enter the correction later. I don't like it, as it clutters the screen; instead, I either make a mental note to enter the correction later, or pull over and enter it right away.

You get twelve months of free updates for every map you buy.

There is also an option to update your map with unverified corrections, in which case you immediately get any correction that has been reported by multiple users. I'm not sure what the cutoff is, and I'm not sure how quickly speed limit corrections are made available; they seem to be processed manually, unlike simpler changes (one-way streets, blocked streets, intersections converted to roundabouts or vice versa...)



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 14

Friday 2 May 2008

Contents

- [U.S. Customs computer system fails nationwide](#)
[PGN](#)
 - [Protecting Yourself From Suspicionless Searches While Traveling](#)
[Jennifer Granick via Monty Solomon](#)
 - [Air marshals' names tagged on 'no-fly' list](#)
[Audrey Hudson via Monty Solomon](#)
 - [Italy posts salary details on web](#)
[Amos Shapir](#)
 - [Tot dies after Internet 911 call fails to reach dispatchers](#)
[Tony Toews](#)
 - [Canadian Human Rights Commission investigator hijacks woman's Internet connection](#)
[Kelly Bert Manning](#)
 - [Microsoft anti-encryption toolkit](#)
[David Lesher](#)
 - ["Default Password" exploits still work](#)
[William Nico](#)
 - [Protecting credit card holders](#)
[Kearton Rees](#)
 - [Police officer uses real witness statement as template document](#)
[Identity withheld by request](#)
 - [False alarm guaranteed after 7 years](#)
[Daniel P.B. Smith](#)
 - [Facial recognition in airports... please say it's April 1st.](#)
[Fred Cohen](#)
 - [Re: Face scans for UK air passengers](#)
[Peter Houppermans](#)
 - [Re: 30th Spamiversary](#)
[Amos Shapir](#)
 - [Re: Real-time spying on credit card holders](#)
[Nick Brown](#)
 - [Blown to Bits, Abelson/Ledeen/Lewis](#)
[PGN](#)
 - [Info on RISKS \(comp.risks\)](#)
-

#U.S. Customs computer system fails nationwide

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

Thu, 1 May 2008 9:52:37 PDT

The CNN Wire reported on 30 Apr 2008 that a nationwide computer failure shut down terminals at U.S. Customs entry points. However, a backup system on laptops appears to have worked, instituted after previous system failures (e.g., 18 Aug 2005, [RISKS-24.02](#)).

#Protecting Yourself From Suspicionless Searches While Traveling

<Monty Solomon <monty@roscom.com>>

Thu, 1 May 2008 22:22:29 -0400

Protecting Yourself From Suspicionless Searches While Traveling
Posted by Jennifer Granick, 1 May 2008

The Ninth Circuit's recent ruling (pdf) in *United States v. Arnold* allows border patrol agents to search your laptop or other digital device without limitation when you are entering the country. EFF and many civil liberties, travelers' rights, immigration advocacy and professional organizations are concerned that unfettered laptop searches endanger trade secrets, attorney-client communications, and other private information. These groups have signed a letter asking Congress to hold hearings to find out what protocol, if any, Customs and Border Protection (CBP) follows in searching digital devices and copying, storing and using travelers' data. The letter also asks Congress to pass legislation protecting travelers' laptops and smart phones from unlimited government scrutiny.

If privacy at the border is important to you, contact Congress now and ask them to take action!

In the meantime, how can international travelers protect themselves at the U.S. border, short of leaving their laptops and iPhones at home? ...

<http://www.eff.org/deeplinks/2008/05/protecting-yourself-suspicionless-searches-while-t>

#Air marshals' names tagged on 'no-fly' list

<Monty Solomon <monty@roscom.com>>

Wed, 30 Apr 2008 09:05:22 -0400

Some federal air marshals have been denied entry to flights they are assigned to protect when their names matched those on the terrorist no-fly list, and the agency says it's now taking steps to make sure their agents are allowed to board in the future. [Source: Audrey Hudson, *Washington Times*, 29 Apr 2008]

<http://www.washingtontimes.com/apps/pbcs.dll/article?AID=/20080429/NATION/782525487/1001>

Italy posts salary details on web

<Amos Shapir <amos083@hotmail.com>>

Thu, 1 May 2008 17:27:21 +0300

"There has been outrage in Italy after the outgoing government published every Italian's declared earnings and tax contributions on the Internet."

Apparently this was not a bug, but intentional. In any case, the full details of every Italian's income and tax returns were posted without warning on the Net for anyone to see, for at least 24 hours. (BBC report)

<<http://news.bbc.co.uk/1/hi/world/europe/7376608.stm>>

Tot dies after Internet 911 call fails to reach dispatchers

<Tony Toews <tony@granite.ab.ca>>

Wed, 30 Apr 2008 23:30:58 -0600

18-month-old Elijah Luck died on 29 Apr 2008 after his aunt called 911 from the family's Comwave VoIP phone at home in in Coventry, but an ambulance reportedly took more than half an hour to arrive -- with the call center being slow in transferring the call to the Calgary dispatch.

<<http://www.canada.com/calgaryherald/news/story.html?id=3cb08a17-9abf-4a50-9665-51a15732df5d&k=39015>>

[Also noted by Mark Brader. No guarantees on longevity of URLs. PGN]

http://www.ctv.ca/servlet/ArticleNews/print/CTVNews/20080501/voip_911call_080501/20080501/?hub=TopStories&subhub=PrintStory
http://calsun.canoe.ca/News/Columnists/Platt_Michael/2008/05/02/5448331-sun.php

Canadian Human Rights Commission investigator hijacks woman's Internet connection

<bo774@freenet.carleton.ca (Kelly Bert Manning)>

Sun, 27 Apr 2008 16:40:10 -0400 (EDT)

A woman caught up in a mysterious Internet hijacking scandal that has sparked a federal privacy investigation into the Canadian Human Rights Commission says she was shocked, angry and confused at suddenly finding herself publicly associated with white supremacists. ... In response to a subpoena, Bell Canada linked Jadewarr to Ms. Hechme's personal Internet account, and provided her address and telephone number at the public hearing. [Source: Colin Perkel, Internet hijacking 'disturbing', says Ottawa woman, Canadian Press, 27 Apr 2008

<http://www.theglobeandmail.com/servlet/story/RTGAM.20080427.whijacknet0427/BNStory/National/home>

Luckily for Ms. Hechme the Human Right of Privacy is protected by a different Federal Commission in Canada.

Microsoft anti-encryption toolkit

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

Thu, 1 May 2008 16:11:13 -0400 (EDT)

Subject: Microsoft Helps Law Enforcement Get Around Encryption - New York Times

X-URL: http://www.nytimes.com/idg/IDG_852573C4006938808825743900804723.html?ref=technology&pagewanted=print

Microsoft Helps Law Enforcement Get Around Encryption, 30 Apr 2008

The growing use of encryption software like Microsoft's own BitLocker by cyber criminals has led Microsoft to develop a set of tools that law enforcement agents can use to get around the software, executives at the company said.

Microsoft first released the toolset, called the Computer Online Forensic Evidence Extractor (COFEE), to law enforcement last June and it's now being used by about 2,000 agents around the world, said Anthony Fung, senior regional manager for Asia Pacific in Microsoft's Internet Safety and Anti-Counterfeiting group. Microsoft gives the software to agents for free. ...

Miscellaneous thoughts:

00) Who says it's only "cyber criminals" using file encryption; and [what we used to think of was..] law enforcement using such tools? Note Fung's group's title.

01) This reminds me of Spy vs. Spy; except where both sides work for the same side. It brings in all the issues the NSA has faced over the decades: ("Do we plug this hole now; or will Boris see we did, and stop using their version of X?")

Who is MSFT's real customer; the user or the LE/FI community? How long before Redmond gets pressured to weaken BitLocker because COFEE can't help? What will their response be?

10) Wigglers, a faux-use mouse designed to forestall a screen-saver activation, have been around for a while. How long until some encryption code author puts a random pop-up interrogation into their code? I.e. even if the system is ""busy"" it suddenly asks for a response, a simple CAPTCHA. When it gets a wrong answer, it stops and demands the full pass-phrase. [Another approach would be to immediately demand same when a new device is found by the OS.]

11) We are seeing more laptops & phones being searched and/or confiscated by DHS at US borders. I suspect many multinational corporations will sacrifice

an encrypted laptop rather than reveal its contents.

100) Will shortcoming of COFEE et.al. push the legal system into a major test case of coerced passphrase release? ["Give up your password or rot in jail?"]

May you live in interesting times.

✂ "Default Password" exploits still work

<William Nico <nico@mcs.csueastbay.edu>>
Mon, 28 Apr 2008 14:16:42 -0700 (PDT)

An article in the Contra Costa Times 26 April under the headline "1,500 gallons of gas swiped" [\[http://www.contracostatimes.com/lafayette/ci_9057588?nclick_check=1\]](http://www.contracostatimes.com/lafayette/ci_9057588?nclick_check=1) implies that the thief/thieves used an access code on the pumps, which had not been changed from the manufacturer's default, to keep the volume of pumped gas from being reported. Here are a couple of paragraphs excerpted from the article:

"... Between March 31 and April 7, he [the proprietor] noticed large disparities between what his fuel counters were showing and what was actually sloshing around in his station's underground storage tanks. ...
"He contacted police and soon figured out that someone had unlocked a panel on one of the pumps and punched in a code on an internal key pad. The code disables the pump from requiring remote authorization to activate. The authorization system is legitimately used to cut off gas flow and allow maintenance workers to clean valves. ... "... someone versed in fuel pump maintenance was a likely culprit, since a lay person or even a station owner like himself lacks the technical knowledge to pull off such a feat. ...
"[The proprietor] installed reinforced locks in his underground storage tanks and entered a new authorization code inside the fuel pumps -- changing it from a default code entered by the pump manufacturer, which is why he suspects the thief had trade knowledge."

William R. Nico, California State University East Bay Hayward, CA 94542-3092
www.mcs.csueastbay.edu/~nico (510)885-3386 Math. and Comp. Science Emeritus

✂ Protecting credit card holders

<<kearton.rees@bt.com>>
Tue, 29 Apr 2008 14:45:26 +0100

A BBC consumer programme "Watchdog" reported recently (28 Apr 2008) on cases where credit card companies' computer based fraud detection systems were disabling users cards when they detected unusual, and possibly fraudulent, spending patterns. However, all the users concerned were on holiday abroad (New York, South Africa & Rome) and left stranded with little or no money

it then took four or five days and a lot of effort to get the cards re-enabled. In some case this caused the users to have to cancel significant chunks of a 'holiday of a life-time'. In one case the bank *had* tried to contact the user by sending an e-mail to his home address, whilst he was stuck in New York with no money.

The bank's responses were essentially that these systems were there to protect their users from fraud and that users should let their banks know when they are likely to be going somewhere different so that such situations can be avoided. However, the cancellations had happened to some users despite doing this. It seems the decisions were made solely by the computers with no recourse to the users' branch manager (for example) or to any information provided by the user on their whereabouts.

The banks mentioned seemed to only be prepared to pay a small amount of compensation (100 pounds max for the situations in the programme), nothing near what it cost some users to call their bank's customer services from South Africa. (Being able to contact the banks' customer services departments easily from abroad was another sore point.)

The main learning point is that you should always take several different means of paying when you go abroad.

British Telecommunications plc Adastral Park, Martlesham, Ipswich, UK, IP5 3RE
Kearton.Rees@bt.com | www.btbrand.bt.com

✂ Police officer uses real witness statement as template document

<[Identity withheld by request]>
Mon, 28 Apr 2008

I was recently the victim of a (very minor) assault. This was reported to the police, and in due course I went to the police station to provide a formal witness statement. The officer charged with making the statement said that, to save time, he would type up the statement as I gave it rather than writing it down by hand and then typing it up later. He then led me into a computer room, much as one would find in a school or university for use by the students (indeed, some of the notices on the wall seemed to imply that the room was often used for training courses but happened to be vacant at that time) and logged in to Windows. He then opened up a folder with a large number of MS Word documents and clicked on one to open it. Initially I assumed that this was a template file, but when it appeared on the screen it didn't appear to have the blank spaces and "WRITE WITNESS' NAME HERE" phrases that one would expect. Intrigued, I looked closer and saw that the text appeared to be a witness statement about another assault that had happened about a week before mine. This was confirmed when the officer asked me not to look at the text at the bottom of the screen, because it was a private witness statement about another crime.

The officer then set about typing up my witness statement thus: he added several blank lines at the beginning of the document and then began cutting

and pasting sentences or sometimes whole paragraphs from the bottom half (the old statement) to the top half (my statement). After pasting each section in, he went over it changing the details as appropriate. The reason he gave for doing this was that he wanted to make sure that he had included all the necessary sections and formulaic wording so that it would be acceptable in court. Once he had finished taking my statement, he chose 'Save As' and entered a filename, saving it in the same folder. All the file names were prepended with a date (presumably he had not discovered, or not been allowed to use, the 'sort by date' option).

I would say "The RISKS are obvious", but given recent discussion I feel I ought to attempt to enumerate them.

1. I was shown the personal data of another victim. Of course, I looked away as soon as I suspected it was not just an "example crime" (which was before he told me that it was real) but others might not have been so scrupulous.
2. As featured in previous RISKS bulletins, Word files can sometimes retain data that had supposedly been deleted. If the witness statement is sent electronically to the other parties in the case, they too may be able to extract confidential information about the case used as a template (and perhaps the one used as a template for that file, and so on).
3. I have used a similar editing method in the past when writing less important documents such as homework assignments, and in my experience it is very easy to accidentally omit a section or leave it unchanged from the previous version. Especially in the case of omitting a section, this error could then propagate to subsequent statement files and potentially invalidate several pieces of evidence.
4. The file was kept under the old name (but not saved) until the end of the interview (which lasted over an hour). If there had been a power cut or system crash, the file would presumably have been lost. Conversely, if the file had been saved accidentally, or even autosaved, presumably the old statement would have been overwritten.

I prefer to remain anonymous to protect the officer involved from being made a scapegoat for what are obviously, at least to a certain extent, institutional failings. I will however name the police force involved: Cambridgeshire Police [England].

False alarm guaranteed after 7 years

*<"Daniel P.B. Smith" <usenet2006@dpbsmith.com>>
Sun, 27 Apr 2008 19:56:37 -0400*

Last night I was awakened at 2 a.m. by an alarm beeping every thirty seconds. A few minutes of stumbling around trying to find the high-pitched, hard-to-localize sound revealed it to be our Kidde Nighthawk carbon monoxide detector. Its digital display was reading "Err." It was not showing a low

battery condition, but just to be sure, I replaced the batteries, to no avail. I then took the unit down and looked for directions on the back. A sticker on the back said "UNIT ERROR: Intermittent audible alarm every 30 seconds. Refer to User's Guide for details."

Was there any cause for concern? Well, probably not, since this obviously was not the ALARM CONDITION, signaled by a different pattern of beeps. On the other hand, it is human nature to ignore real warnings through wishful thinking (radar echoes at Pearl Harbor in 1941 must be incoming __American_ planes). I didn't want to make that mistake, so I decided I should at least check the User's Guide... but could I find it? Not likely. I was wide awake by now, so I figured I might as well try to download it from the manufacturer's website. Among other things, if I had enough mental clarity to do this it would prove to me that I wasn't anoxic. I found it, downloaded it, and in the "unit malfunction" section I learned that

"Seven years after initial power up, this unit will 'chirp' every thirty seconds to indicate that it is time to replace the alarm. The unit will not detect CO in this condition."

Since the sticker on the back showed it was assembled in November, 2000, I figured that the mystery was solved, took the batteries out, went back to sleep, and replaced the unit the next day.

Apart from this planned obsolescence being "very convenient," as the Church Lady used to say, the RISK is of confusing users just in a situation where things should be as clear and unambiguous as possible.

Was there really not enough room on the back of the device itself to note that it would beep and show "Err" seven years after installation? And was it really impossible to program a different message than "Err" for the seven-year expiration condition?

✶ Facial recognition in airports... please say it's April 1st.

*<Fred Cohen <fred.cohen@all.net>>
Mon, 28 Apr 2008 04:00:22 -0700*

[Re: Face scans for air passengers to begin in UK this summer (Brian Randell), [RISKS-25.13](#)]

> Officials say automatic screening more accurate than checks by humans

True enough. Assuming the goal is to match a face to a known face. People are notoriously terrible at this. To do better is not that hard today. But, presumably, that's not what the guards do - match a face to a face. If they did, I would never get through any airport anywhere. My hair is shorter and grayer, my face is thinner, I don't have a mustache anymore, and I am slowly balding. But I don't think that's what they are there to do - at least not exclusively.

> But there is concern that passengers will react badly to being rejected by
> an automated gate. To ensure no one on a police watch list is incorrectly
> let through, the technology will err on the side of caution and is likely
> to generate a small number of "false negatives" - innocent passengers
> rejected because the machines cannot match their appearance to the
> records.

"False negative"? False rejection or false positive or false detection is more like it. Given that the system is designed to detect mismatches, it is a "false negative" when it fails to detect a mismatch. A false negative would be allowing someone through when they should not go through.

> They may be redirected into conventional passport queues, or officers may
> be authorised to override automatic gates following additional checks.

Seems to me like this is no better than randomly picking off one in 20 passengers for more detailed scrutiny.

> Ministers are eager to set up trials in time for the summer holiday rush,
> but have yet to decide how many airports will take part. If successful,
> the technology will be extended to all UK airports. ...

So they want to do it when there are lots and lots of passengers instead of when the traffic is light and delays relatively short. That way when it fails it will be a huge disaster instead of a small one?

Will the passengers have to frown to get on a plane now? I predict they will be frowning anyway with all of the security crap they will have to go through.

Fred Cohen, 572 Leona Drive, Livermore, CA 94550 1-925-454-0171
<http://all.net/> Join <http://tech.groups.yahoo.com/group/FCA-announce/join>

Re: Face scans for UK air passengers ([RISKS-25.13](#))

<Peter Houppermans <peter@houppermans.com>>
Sun, 27 Apr 2008 21:08:55 +0200

The last time I renewed my passport I got the new EU issue, with facial RFID embedded. It imposed huge quality demands on the passport picture, and I can only assume there is somewhere a check comparing old with new (would be a bit daft otherwise).

However, I noted immediately that:

(a) The scanning equipment had not arrived at the issuing embassy. Thus, no final check to see if the chip actually worked, and AFAIK there's no data on field failure rates yet.

(b) There did not appear to be any shielding for the chip as the U.S. passports have. So principally the EU passport creates an extra risk for

me in hostile areas, which is an interesting take on my human rights..

There is, however, a flipside to this lack of shielding. Given (a) above, and given that I occasionally work with broadcast equipment it is not inconceivable my jacket has already passed through the beam of a microwave transmitter whilst dangling off my bag.

Oops..

✉ Re: 30th Spamiversary ([RISKS-25.13](#))

<Amos Shapir <amos083@hotmail.com>>

Thu, 1 May 2008 17:22:13 +0300

It is interesting to note that among the reactions to this first spam (those quoted in the article, anyway) only Richard Stallman had recognized the features which would in time make the net great: the ability to focus messages to specific well selected groups of people, as well as the inherent freedom of expression. IMHO this shows the difference between visionaries and high-talkers.

✉ Re: Real-time spying on credit card holders (Garret, [RISKS-25.13](#))

<Nick Brown <Nick.BROWN@coe.int>>

Fri, 2 May 2008 10:14:49 +0200

> Perhaps Mr. Brown would be so kind as to elucidate exactly what he thinks
> the RISKS are?

Unfortunately his e-mail address did not appear, so I'll reply to the list. I apologise if this is redundant, but I guess maybe some other people asked themselves the same question.

Here are some of the risks which I thought of within a few minutes of reading the original article:

* Real-time financial transaction data being sent "by e-mail", as if e-mail guaranteed either delivery of the message (full mailbox, spam filter badly configured) or that only the intended recipient of the mail would see it. The first of those means that the person paying for the service may well not get it (with potentially hilarious consequences in the form of lawsuits, as experts try to prove to a court exactly where an e-mail got lost); the second means that the information may be retransmitted to a number of "interested" parties ("hey Martha, I thought Joe was in Cleveland, turns out he's in New York" - yeah, negotiating a takeover, and trying to do it quietly). At one site with which I am very familiar and which I have no reason to believe is untypical, there is a complete parallel network of information between the administrative assistants of directors who have delegate access to their bosses' e-mail. (This gets

particularly interesting when someone changes jobs and their delegation privileges are forgotten.)

* Overreaction by managers, especially since the corporate culture of a company which signs up for this service is unlikely to be particularly laid-back when it comes to expenses. Example: I'm on my way to the airport and I find I've left my ticket at home. No big deal, it's fully refundable, I'll charge another one to the company card and we'll sort out the refund when I return. Only the meeting is in somewhere "nice", and when my boss gets the ticket, he decides I'm taking my wife (etc.) along and cancels the card while I'm in the air.

The bottom line is that if you're going to give employees a company card, you have to have the procedures and accountability in place to control its usage after the fact. If you're worrying that your staff may charge a \$400 dinner contrary to policy, don't give them the card. Maybe the junior executive charging that meal had to do so because the CEO got a big call from Tokyo halfway through the meal. But the credit card terminal only has room to enter "Tip", not "note to corporate finance".

Perhaps Ron works for a nicer organisation than many other people. I ran the above paragraphs past a couple of colleagues and they both smiled knowingly.

Nick Brown, Strasbourg, France.

PS: And, of course, there's our oldest friend, plain simple programming and operational errors. A field shifts by one while someone at Mastercard is reorganising chunks of their database in Excel and hey presto, someone at Google gets a copy of someone at Microsoft's expenses.

Blown to Bits, Abelson/Ledeen/Lewis

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

Tue, 29 Apr 2008 14:29:43 PDT

Keep an eye out for this book:

Hal Abelson, Ken Ledeen, Harry Lewis

Blown to Bits:

Your Life, Liberty, and Happiness after the Digital Explosion

Addison Wesley, June 2008

"There is no simpler or clearer statement of the radical change that digital technologies will bring, nor any book that better prepares one for thinking about the next steps." Lawrence Lessig (from the cover)



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 15

Friday 16 May 2008

Contents

- [No-flies on you?](#)
[PGN](#)
- [Gone in 60 seconds: Spambot cracks Live Hotmail CAPTCHA](#)
[Emil Protalinski via Monty Solomon](#)
- [Hacker leaks 6 million Chileans' records](#)
[Amos Shapir](#)
- [Dilbert site wants to install a widget](#)
[William Ehrich](#)
- [Used hardware containing sensitive data](#)
[Tony Harminc](#)
- [88,000 hospital patient records stolen in NYC](#)
[Danny Burstein](#)
- [UK CCTV used to create a music video](#)
[Forest Mars](#)
- [QWERTYUIOOPS](#)
[Charles C. Mann](#)
- [Post Office changes 100 SF addresses](#)
[Rob McCool](#)
- [PO-boy](#)
[Peter Zilahy Ingerman](#)
- [Debian OpenSSL Predictable PRNG Toys](#)
[H D Moore via Monty Solomon](#)
- [Debian OpenSSL Vulnerability](#)
[Monty Solomon](#)
- [How not to use SSL](#)
[Nickee Sanders](#)
- [A risk for those that own Digital photo frames](#)
[Identity withheld](#)
- ['Peel and Stick' Tasers Electrify Riot Control](#)
[Paul Saffo](#)
- [Risks of Be-clowning Yourself at Computerized Speeds, Internationally](#)
[R.G. Newbury](#)
- [REVIEW: "Geekonomics: The Real Cost of Insecure Software", David Rice](#)
[Rob Slade](#)
- [Info on RISKS \(\[comp.risks\]\(#\)\)](#)

✂ No-flies on you?

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

Thu, 15 May 2008 10:01:17 PDT

The *NYTimes* on 15 May 2008 has an editorial (We'll Have to Check, Sir) noting that the no-fly list is still populated with names that cause too many false positives. [We've mentioned Senator Edward Kennedy and everyone named David Nelson here before.] One airline reports 9,000 false hits every day, according to DHS head Michael Chertoff. He is proposing each would-be flier provide airlines with his/her date of birth (which would cut down extensively on bogus hits -- but ONLY if the person's DoB was given accurately AND if the birthdate of the actual terrorist were known!). The terrorist watch list now contains more than 900,000 names. TSA estimates that 15,000 people have actually managed to get their own names off the list, although the process is reportedly "frustratingly slow".

✂ Gone in 60 seconds: Spambot cracks Live Hotmail CAPTCHA

<Monty Solomon <monty@roscom.com>>

April 16, 2008 8:05:12 AM EDT

[Source: Emil Protalinski, ArsTechnica, 15 Apr 2008]

Internet users are quite familiar with the Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), a quick method that verifies whether or not the user trying to sign up is a person or a bot. A picture with swirled, mangled, or otherwise distorted characters is displayed and the user then types in the correct letters or numbers. Thus far, the system has worked well to slow down malicious bots, but recently the groups behind such software have made significant strides. A security firm is now reporting that the CAPTCHA used for Windows Live Mail can now be cracked in as little as 60 seconds.

Back in early February, a group cracked Windows Live Hotmail's CAPTCHA. A few weeks later, Gmail's version followed suit. In just over a month's time, some anti-spam vendors were forced to completely block the domain for the popular service as bots signed up for thousands of bogus accounts and began to flood the tubes with e-mail advertisements for lottery tickets and watches. The close proximity of the two cracks has done everything but sealed CAPTCHA's fate.

To make matters worse, Websense Security Labs is now reporting that the method for getting around Windows Live Mail's CAPTCHA has been improved to the point that a bot can decipher the text and make a guess in less than six seconds, on average. Windows Live Hotmail's Anti-CAPTCHA automatic bot, which hooks itself into Internet Explorer on a victim's machine, has a success rate of about 10-15 percent. That means that it takes up to one minute for a single bot to create a new account. ...

<http://arstechnica.com/news.ars/post/20080415-gone-in-60-seconds-spambot-cracks-livehotmail-captcha.html>

Hacker leaks 6 million Chileans' records

<Amos Shapir <amos083@hotmail.com>>

Mon, 12 May 2008 19:17:58 +0300

"A computer hacker in Chile has published confidential records belonging to six million people on the Internet, officials say."

Full story at: <http://news.bbc.co.uk/2/hi/americas/7395295.stm>Amos Shapir

Dilbert wants a widget

<William Ehrich <ehrich@mninter.net>>

Mon, 05 May 2008 09:31:16 -0500

The Dilbert site (www.dilbert.com) wants me to install a special 'widget' to let me see their cartoons. That rings all my alarm bells. Even if honest and safe, it seems a bad precedent.

Like some other sites, they want an e-mail address which would presumably get a corresponding entry in my spam filter.

Used hardware containing sensitive data

<"Tony Harminc" <tony@harminc.net>>

Fri, 9 May 2008 16:13:18 -0400

There have been plenty of stories of used laptops and hard drives containing confidential data, and my impression is that even the non technical people I know now understand this risk when disposing of old hardware. But recently I picked up two items at the local Goodwill store for \$5 each; a home-style DSL router/NAT box, and a burglar/fire alarm panel, evidently removed during a renovation. Both have user manuals available online, and both contained easily readable data that would provide at least the basis for a denial of service attack, and possibly much more.

Although the router was password protected, a particularly bad (but documented) design allows for access to be regained and the existing password to be discovered, all through the browser interface. The router also contained a PPPoE userid and password, and a first name - quite possibly enough for some social engineering, and probably enough to log in to the PPPoE provider and cause trouble. I have seen a number of similar boxes at the same Goodwill, presumably as people change their home networks

to WiFi and can't think of anything to use the old unit for.

The alarm panel, not a consumer product exactly, but still well documented online, had an account identifier both on a sticker inside and programmed in, and primary and backup numbers for the box to call. In my experience alarm companies will, not unreasonably, respond to alarms from even a closed or delinquent account, since the potential liability for them is very much higher if they fail in error to respond to a real call than if they notify the emergency services and let them attend at the last known address just in case.

Risks: Try to give your old hardware a good home, and risk annoyance or worse.

✂ 88,000 hospital patient records stolen in NYC

<danny burstein <dannyb@panix.com>>
Sun, 4 May 2008 13:42:54 -0400 (EDT)

"Computer equipment stolen from an administrative office in Clifton (a neighborhood in Staten Island, NYC) in December contained personal information from 88,000 patients that have been treated at Staten Island University Hospital. After four months with no arrests, hospital administrators are just now beginning the process of sending out letters to patients whose names, Social Security and health insurance numbers were contained in computer files on a desktop computer and a backup hard drive stolen Dec. 29 from the hospital's finance office at 1 Edgewater Plaza."

http://www.silive.com/news/index.ssf/2008/04/stolen_computer_contained_info.html

This case is a bit different from the standard RISKS story, inasmuch as it's based on a traditional physical theft, and from inside a working office, rather than a car. But it does go to show that the old risks are still around.

(There's a side issue of the hospital taking four months before notifying the public, which may actually be in violation of NYS law and federal regs.)

✂ UK CCTV used to create a music video

<Forest Mars <lostjournals@gmail.com>>
May 12, 2008 7:00:42 PM EDT

[From Dave Farber's IP distribution, in response to Frode Hegland, U.K. turns CCTV, terrorism laws on pooping dogs

"The United Kingdom has the most surveillance cameras per capita in the world. With the recent news that CCTV cameras do not actually deter crime, how can the local town councils justify the massive surveillance program? By going after pooping dogs."]

I don't know what is going on with the UK, it's like they're using 1984 as an installation guide.

In case anyone missed this clever turning of the tables, however, here's the story of a music band who not being able to afford to produce their video, performed in front of 80 of the estimated 13 million (public) surveillance cameras in UK, and then got the footage by filing a request under UK's Data Protection Act.

<http://www.arsgeek.com/?p=3961>

Link includes the finished video.

"The Get Out Clause are an upcoming UK band who are currently unsigned. They took a brilliant and I'm sure soon to be much copied method to producing their own video. Unable to hire a production crew for a standard 1980's era MTV music video, they performed their music in front of 80 of the 13 million CCTV "security" cameras available in England, including one on a bus.

They then used Britain's Data Protection Act to request the footage that was shot of them. Grab some decent and inexpensive video editing tools (say. . . an iMac) and presto! They got themselves a unique and in my opinion quite interesting music video."

QWERTYUIOOPS

<ccmann@comcast.net (Charles C. Mann)>
Mon, 05 May 2008 05:06:36 +0000

[From Dan Farmer's list. PGN]

My laptop is on its way to decrepitude, so I've been thinking about looking around for a replacement. I always figured I should just buy a big company's machine, as they're a commodity, and just look for the cheapest price for what I want, since they're all basically the same. Apparently this logic is flawed. Apparently Dell has just released a laptop in which the arrangement of keys on the keyboard is mistaken:

<http://www.flickr.com/photos/jacobgordon/2455618195/in/photostream/>

Fortunately for us in the US, this just affects their European models. But still, it's kind of amazing.

Post Office changes 100 SF addresses

<Rob McCool <robm@robm.com>>
Thu, 8 May 2008 15:06:21 -0700 (PDT)

The US Postal Service has changed the address of 100 people in San Francisco. According to the story, the problem arises because at one end of the street in question, the name is "La Playa", and at the other it is "Great Highway" -- and where the split is between them depends on whose map you are looking at.

The article does a pretty good job of diving into the implications of this, and the risks, including the technical problems that can happen such as GPS units not being updated with the "latest" decision about what name this street has.

A Post Office spokesperson was quoted as saying that the decision to eliminate one of the ambiguous street names for these addresses was based on a database upgrade: "The legal address of the area in question is La Playa. We are required to deliver to the legal address. We understand that some residents have been using the Great Highway address for decades, but at some point we updated our database and (La Playa) is what is in our database."

✂ PO-boy

*<"Peter Zilahy Ingerman, PhD" <pzi@ingerman.org>>
Sun, 11 May 2008 18:45:14 -0400*

My street address is 40 Needlepoint Lane. When I tried to use it on the Amtrak web site as a mailing address, it was rejected as being a post office box. Discussion with Amtrak's Internet Help Desk revealed that this is a known problem: the software that detects/disallows post office boxes simply looks for an adjacent "po" in the address! UGH!

✂ Debian OpenSSL Predictable PRNG Toys

*<Monty Solomon <monty@roscom.com>>
Thu, 15 May 2008 23:26:18 -0400*

H D Moore, Metasploit

The Bug

On May 13th, 2008 the Debian project announced that Luciano Bello found an interesting vulnerability in the OpenSSL package they were distributing. The bug in question was caused by the removal of the following line of code from md_rand.c

```
MD_Update(&m,buf,j);  
[ .. ]  
MD_Update(&m,buf,j); /* purify complains */
```

These lines were removed because they caused the Valgrind and Purify tools to produce warnings about the use of uninitialized data in any code that was

linked to OpenSSL. You can see one such report to the OpenSSL team here. Removing this code has the side effect of crippling the seeding process for the OpenSSL PRNG. Instead of mixing in random data for the initial seed, the only "random" value that was used was the current process ID. On the Linux platform, the default maximum process ID is 32,768, resulting in a very small number of seed values being used for all PRNG operations.

The Impact

All SSL and SSH keys generated on Debian-based systems (Ubuntu, Kubuntu, etc) between September 2006 and May 13th, 2008 may be affected. In the case of SSL keys, all generated certificates will be need to recreated and sent off to the Certificate Authority to sign. Any Certificate Authority keys generated on a Debian-based system will need be regenerated and revoked. All system administrators that allow users to access their servers with SSH and public key authentication need to audit those keys to see if any of them were created on a vulnerable system. Any tools that relied on OpenSSL's PRNG to secure the data they transferred may be vulnerable to an offline attack. Any SSH server that uses a host key generated by a flawed system is subject to traffic decryption and a man-in-the-middle attack would be invisible to the users. This flaw is ugly because even systems that do not use the Debian software need to be audited in case any key is being used that was created on a Debian system. The Debian and Ubuntu projects have released a set of tools for identifying vulnerable keys. You can find these listed in the references section below. ...

<http://metasploit.com/users/hdm/tools/debian-openssl/>

Debian OpenSSL Vulnerability

<Monty Solomon <monty@roscom.com>>

Thu, 15 May 2008 23:26:18 -0400

DSA-1571-1 openssl -- predictable random number generator

Date Reported: 13 May 2008

Affected Packages: openssl

Vulnerable: Yes

Security database references: In Mitre's CVE dictionary: CVE-2008-0166.

More information:

Luciano Bello discovered that the random number generator in Debian's openssl package is predictable. This is caused by an incorrect Debian-specific change to the openssl package (CVE-2008-0166). As a result, cryptographic key material may be guessable.

This is a Debian-specific vulnerability which does not affect other operating systems which are not based on Debian. However, other systems can be indirectly affected if weak keys are imported into them.

It is strongly recommended that all cryptographic key material which has been generated by OpenSSL versions starting with 0.9.8c-1 on Debian systems is recreated from scratch. Furthermore, all DSA keys ever used on affected Debian systems for signing or authentication purposes should be considered compromised; the Digital Signature Algorithm relies on a secret random value used during signature generation. ...

<http://www.debian.org/security/2008/dsa-1571>

✂ How not to use SSL

<Nickee Sanders <njsanders@ihug.co.nz>>

Sun, 4 May 2008 09:05:45 +1200

I fly to Paris next week. A couple of days ago I booked a shuttle into the city itself. This is a company I have used before and I was happy to use them again. They must have a manual reservations process, because although one can "book" and pay on the web, the confirmation e-mail doesn't arrive until up to 24 hours later. Because of this I like to keep the confirmation webpage loaded in my browser until the e-mail arrives.

This time around, I had to restart my machine before I got the e-mail. So I went back into my browser history on the off-chance that reloading the page would show enough details about the transaction.

This worked better than I'd expected. There was my name, my confirmation num-...hey, hang on...isn't that a different confirmation number from the original one? Yup, I was right. What the heck?

I immediately went to the URL...and found to my utter amazement, that after the "<https://>" and the domain name, were the entire details of my transaction, including my credit card number, expiry date, and the 3 digits off the back of the card.

sigh...

Of course I was charged a second time with the page reload, but this is obviously not the first time this has happened and the folks handled the situation very well. But way to go to completely defeat the point of SSL!

✂ A risk for those that own Digital photo frames

<[Identity withheld]>

Mon, 5 May 2008

Mocmex, an insidious computer virus that collects passwords for online games, recognizes and blocks antivirus activity from over 100 vendors, and also evades Microsoft security and firewalls. It hides itself in photo frames. [Source: Deborah Gage, *San Francisco Chronicle*, 15 Feb 2008]

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/02/15/BU47V0VOH.DTL&type=business>

[Old item, but we had not noted it before. PGN]

✶ 'Peel and Stick' Tasers Electrify Riot Control

<Paul Saffo <paul@saffo.com>>

Wed, 14 May 2008 06:44:49 -0700

I'll bet someone figures out countermeasures to this real fast...

Source: 'Peel and Stick' Tasers Electrify Riot Control
Company's New Converter Kit Turns Shields into Shockers
Noah Shachtman, WiReD BLOG Network, 14 May 2008 [PGN-ed]
<http://blog.wired.com/defense/2008/05/pretty-soon-cop.html>

Pretty soon, cops won't just be packing stun guns. They'll be carrying electrically-charged riot shields, zapping their unruly without unholstering their weapons. That is, if the folks at Taser International have their way. The company just introduced the "Taser Shield Conversion Kit featuring the Taser Repel Laminate Film Technology." The kit "features a peel and stick perforated film, power supply and necessary conversion equipment. This laminate becomes electrified providing a powerful deterrent to protect officers and keep suspects or rioters at bay." What could possibly go wrong?

[See Noah's blog for the Rest of the Story. PGN]

✶ Risks of Be-clowning Yourself at Computerized Speeds, Internationally

<"R.G. Newbury" <newbury@mandamus.org>>

Tue, 06 May 2008 01:02:49 -0400

So I received a phish mail...my (non-existent) account at the Bank of Montreal has been suspended... yada yada nada...

Obviously a phish from a Microsoft script-kiddy as the entire URL is visible in text

For your safety we have decided to suspend your access.

You will need to verify your identity.

http://www.simforce.net.au/helen_peng/REN/administrator/includes/js/bmologon.php?

Customer Service, Bank of Montreal.

So I decided to visit the root system. Turns out, they design and build websites. All Microsoft websites. Lotsa flash and flashy motion and loud audio. And no e-mail address for a contact, only a flash (in the old sense of the word) web-contact page. Which of course, does not work with Firefox and Fedora. Same thing for the client system which lives further down the

URL chain. Wanna see a directory listing of Helen Peng's directory. Go right ahead. So I can't tell them they have been screwed, in more ways than once. Maybe they will notice the extra server load and the high traffic levels serving one particular page which they don't actually know about? Ya think? Geoff

REVIEW: "Geekonomics: The Real Cost of Insecure Software", David Rice

<Rob Slade <rmslade@shaw.ca>>
Mon, 05 May 2008 11:37:09 -0800

BKGKNMCS.RVW 20080207

"Geekonomics: The Real Cost of Insecure Software", David Rice, 2008,
0-321-47789-8, U\$29.99/C\$32.99
%A David Rice david@geekonomicsbook.com
%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario M3C 2T8
%D 2008
%G 0-321-47789-8 978-0-321-47789-7
%I Addison-Wesley Publishing Co.
%O U\$29.99/C\$32.99 416-447-5101 800-822-6339 bkexpress@aw.com
%O <http://www.amazon.com/exec/obidos/ASIN/0321477898/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0321477898/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/0321477898/robsladesin03-20>
%O Audience n+ Tech 2 Writing 3 (see revfaq.htm for explanation)
%P 362 p.
%T "Geekonomics: The Real Cost of Insecure Software"

In the preface, the author states that the only pre-requisite for reading the book is a "hint of curiosity." This is because the work explores the issue of insecure and unreliable software from a sociological and economic perspective, rather than giving the topic a purely technical examination.

Rice's book is readable, informative, and makes important points. I enjoyed it. Normally such an assessment comes at the end of the review, but I want to state this up front, because, in the remainder of the commentary contains a number of critical comments. For the most part, though, these apply to components that Rice has not included, and which would tend to support his contention, rather than detract from it.

Chapter one repeats a lot of the material in the preface, sometimes in greater detail. Rice compares software with cement, in terms of the infrastructure of modern society, and also introduces the economic concepts of incentives and utility. The emphasis, in the analysis of software flaws, is on intrusions and networking, but the examples cited concentrate on concerns of reliability, rather than intrusions, somewhat weakening the overall argument. The lack of software standards, and the fact that unregulated markets militate against quality and safety, are addressed in chapter two. The text also specifically explores the problems involved in the ubiquitous practice of patching software faults. Rice's reasoning on the matters, while generally sound and extremely convincing, does have some

odd quirks. For example, he repeats the widely held belief that building secure software in the first place must necessarily be more expensive, or companies would be doing it. (A relevant counter-example in the world of non-computer technology would be that of refrigerator doors. For years fridge door latches were a danger to children when old fridges were abandoned. Children playing around the fridges could enter them, and then become locked inside. It was only after appliance companies were forced to change the door locking mechanisms that they turned to magnetic closures--and found that not only were those mechanisms safer, but also cheaper and more energy efficient. Thus, companies may sometimes need to be forced into practices that may actually be to their advantage. Overall, consideration of such additional elements only serve to strengthen Rice's basic premise that insecure software is unnecessarily costly.)

In chapter three, Rice notes the extremely low rate of prosecution for computer crimes, and moves from there to the statement that professional cybercrime is not just a criminal matter, but that the issue of software unreliability is of concern for national, and even international, economic security. He concentrates, again, on software vulnerabilities, failing to fully assess investigative weaknesses (and the economic pressures preventing law enforcement agencies from hiring and retaining trained forensic staff), the inherent risks of information warfare (to the attacker as well as the target), and the difficulty of establishing and validating trust relationships. He correctly identifies the problem with paying bounties for vulnerabilities (which many have forgotten). Noting the deleterious effect of allowing visible dilapidation to go unrepaired, he asserts that the invisible imperfections of software are even more important, but his argument appears incomplete.

After reiterating the point that speed of innovation and time-to-market is important to software developers, chapter four appears to lose focus, finally seeming to make the point that we need some kind of licensing for software development. Chapter five's review of tort law tends to overshadow the more significant message that software developers enjoy an unparalleled immunity from lawsuits, and thus have no motivation to produce software of high quality. Various characteristics of open source software, and related development processes, are used to point out, in chapter six, differing economic forces both for and against software reliability.

Near the beginning of chapter seven Rice admits that he proposes no ultimate answers to the question of code quality. He does, however, list arguments that can be used to start further discussion on the possible approaches to revise the incentive environment in order to promote quality software. The list of potential approaches includes allowing the "free market" to deal with the problem (in other words, do nothing), promote litigation, license software engineers, create standards, or impose some form of vulnerability tax on developers.

Towards the end of chapter seven, the author states that "[t]his book has argued, no matter how imperfectly, that incentives are key to changing the story of software." Despite my minor quibbles, Rice's case is solid, and his thesis is important. This work should be required reading for all involved in matters of technology policy, from managers and security professionals responsible for application development, to politicians. If

this publication is successful enough, the publisher might have an incentive to ask the author to update his text for a second edition, at which time Rice might tighten up his arguments and include some of the missing bits. Then this book should be required reading for all developers and programming students.

copyright Robert M. Slade, 2008 BKGKNMCS.RVW 20080207
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 16

Thursday 22 May 2008

Contents

- [Betting glitch spurs calls for reform](#)
[Will Oremus via PGN](#)
- [Animal tricks, take n+1](#)
[Jeremy Epstein](#)
- [Ants and Computers](#)
[Gene Wirchenko](#)
- [F.B.I. Says the Military Had Bogus Computer Gear](#)
[John Markoff via Monty Solomon](#)
- [Another undeleted/deleted Document - "Krolls Associates"](#)
[Danny Burstein](#)
- [Don't phlash that dwarf - hand me the pliers!](#)
[John Leyden via Randall](#)
- [Geolocation software risks](#)
[Mickey Coggins](#)
- [Shopping centers tracking cell phones](#)
[PGN](#)
- [China's All-Seeing Eye](#)
[EEkid via Dave Farber](#)
- [Re: Real-time spying on credit card holders](#)
[Curt Sampson](#)
- [Microsoft security advice for sale](#)
[Peter Houppermans](#)
- [Old-Style Pumps Balk At \\$4-a-Gallon Gas, Too](#)
[Nick Miroff via Monty Solomon](#)
- [Clueless in France](#)
[Pete Kaiser](#)
- [PayPal XSS Vulnerability Undermines EV SSL Security](#)
[Paul Mutton via Monty Solomon](#)
- [More GPS Mishaps](#)
[Gene Wirchenko](#)
- [Re: UK CCTV used to create a music video](#)
[Chris Drewe](#)
- [Re: Dilbert wants a widget](#)
[Bill Bumgarner](#)
- [Re: Debian OpenSSL Predictable PRNG Toys](#)

[Jim Horning](#)

• [Re: Securing The Wrong Spaces: A Lesson](#)

[David E. Price](#)

• [Info on RISKS \(comp.risks\)](#)

✂ "Betting glitch spurs calls for reform"

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

Thu, 22 May 2008 14:22:45 PDT

An unidentified bettor at Bay Meadows Race Track (which closed forever on 10 May 2008) apparently put down 1300 one-dollar quick-pick superfecta bets on the Kentucky Derby. Not one of the computer-generated tickets included the eventual winner, Big Brown. After being prodded by the California Horse Racing Board on 7 May 2008, the betting machine vendor Scientific Games discovered that its software was dropping the last horse in the field from quick-pick choices on all 7,000 of its Bet Jet machines nationwide. They "couldn't say" how long this had been happening, as they had "no way" of auditing past usage. It was also unclear whether this was an intentional scam from which anyone was profiting, or just a screw-up.

Incidentally, Scientific Games was the vendor whose equipment was used in the Breeders' Cup wild-card Autotote Pick-6 insider scam (RISKS-33,38,39).

[Source: Will Oremus, *Palo Alto Daily News*, 21 May 2008; PGN-ed]

✂ Animal tricks, take n+1

<"Jeremy Epstein" <Jeremy.Epstein@softwareag.com>>

Fri, 16 May 2008 10:11:45 -0400

One of the oldest recurring themes in RISKS is the damage animals can do to computer systems, generally indirectly by cutting off electricity supplies. Cf. [RISKS-4.02](#), 8.75, 16.30, 19.96, 20.87, and probably a bunch of others.

We're now moving from mammals (especially squirrels) down the food chain, and closer to the equipment itself - several recent reports of ants in south Texas getting in to electronic equipment. Computerworld [1] quotes an exterminator as saying "ants shorted out three computers that were running a pipeline that brought chemicals into the plant. The ants took down two computers last year and one in 2006, affecting flow in the pipeline each time... If you open a computer, you would find a cluster of ants on the motherboard and all over. You'd get 3,000 or 4,000 ants inside, and they create arcs."

[1]

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9086098&source=NLT_SEC&nid=38

[An arc for these little guys would be *ancillary*. It would need to be a

No-Ways Arc, a pun that I reused in the title of the first item in [RISKS-4.02](#), recalling Bob Ashenhurst's spoofed page in Rick Gould's PhD thesis on bridge switching circuits that delved into no-ways arcs and two-terrible subgiraffes in relay graphs with bidirectional current paths. I couldn't resist recalling that 51 years later. PGN]

Ants and Computers

<Gene Wirchenko <genew@ocis.net>>

Fri, 16 May 2008 10:18:52 -0700

This article tells of a non-indigenous species of ant causing in Texas:

<http://www.itbusiness.ca/it/client/en/CDN/News.asp?id=48425>

They are shorting out various forms of equipment including computers. Here is the text of the article:

A flood of voracious ants is heading straight for Houston, taking out computers, radios and even vehicles in their path. Even the Johnson Space Center has called in extermination experts to keep the pests out of their sensitive and critical systems.

The ants have been causing all kinds of trouble in five Texas counties in and around the Gulf Coast. Because of their sheer numbers, the ants are short circuiting computers in homes and offices, and knocking systems offline in major businesses. When IT personnel pry the affected computers open, they find the machines loaded with thousands of ant bodies.

"These ants are raising havoc," said Roger Gold, professor of entomology at Texas A&M University in College Station. "They're foraging for food and they'll go into any space looking for it. In the process, they make their way into sensitive equipment."

The ants have been dubbed Crazy Raspberry ants after Tom Raspberry, owner of Budget Pest Control in Pearland, Texas. He first tackled this particular type of ant back in 2002. Since then, the problem has only escalated.

Raspberry said the ants have caused a lot of trouble for one Texas chemical company in particular. Not wanting to name the company, he said the ants shorted out three different computers that were running a pipeline that brought chemicals into the plant. The ants took down two computers last year and one in 2006, affecting flow in the pipeline each time.

"I think they go into everything and they don't follow any kind of structured line," said Raspberry. "If you open a computer, you would find a cluster of ants on the motherboard and all over. You'd get 3,000 or 4,000 ants inside and they create arcs. They'll wipe out any computer."

The Johnson Space Center called in Raspberry a month or two ago in an attempt to keep the ants out of their facilities. Too late. Raspberry said he's found three colonies at the NASA site, but all have been small enough to

control.

"With the computer systems they have in there, it could devastate the facility," said Raspberry. "If these ants got into the facility in the numbers they have in other locations, well, it would be awful. I've been in this business for 32 years and this is unlike anything I've ever seen. Anything. When you bring in entomologists from all over the United States and they're in shock and awe, that shows you what it's like."

The Johnson Space Center referred all questions about the ants to Raspberry.

The ants, which are tiny and reddish, aren't native to Texas. Officials believe they came off a ship from the Caribbean, said Paul Nester, a program specialist with the Texas AgriLife Extension Service. They were first spotted about six years ago. Gold said in the last few years they've spread in a radius of about 50 miles. And now they're moving into Houston, the fourth-largest city in the country.

"Fifty miles might not seem like a lot until you realize they're moving into Houston," said Gold. "It could really affect a lot of people's lives."

A big problem here, noted Nester, is how quickly their numbers are multiplying.

A queen fire ant, long a problem in Texas, can lay as many as 1,000 eggs a day, he said. The Crazy Raspberry ants are thought to be as prolific. However, an ant mound normally has one queen. The new ants have many queens so they're able to multiply their ranks that much more quickly. They also don't go to the trouble of building ant hills. They simply nest under anything they can find -- a log, a tire or a pet's water bowl -- and then they quickly move on as they spread further into the state.

Nester said the ants swarmed into trucks at a shipping company, shorting out the radios and even the vehicles themselves.

Gold said the ants got into an engine compartment at a sewage treatment plant and shorted out the pumps so they couldn't move the sewage out. He added that they've also overrun a subdivision and caused a lot of electrical damage to houses there.

Part of the problem is that exterminators have found it nearly impossible to kill the ants. Oh, you can kill some of them - the first wave, maybe. However, there are so many more ants coming behind them, that the first wave falls dead in the insecticide and the subsequent waves merely walk on the dead bodies, keeping themselves out of the poison and safe from harm.

Gold warned people not to spray pesticide inside their computers and to simply call in the professionals to prevent mixing up poisonous concoctions or storing the potentially harmful partly used insecticides."

F.B.I. Says the Military Had Bogus Computer Gear (John Markoff)

<Monty Solomon <monty@roscom.com>>

Sat, 17 May 2008 20:12:53 -0400

[Source: John Markoff, *The New York Times*, 9 May 2008]

Counterfeit products are a routine threat for the electronics industry. However, the more sinister specter of an electronic Trojan horse, lurking in the circuitry of a computer or a network router and allowing attackers clandestine access or control, was raised again recently by the F.B.I. and the Pentagon.

The new law enforcement and national security concerns were prompted by Operation Cisco Raider, which has led to 15 criminal cases involving counterfeit products bought in part by military agencies, military contractors and electric power companies in the United States. Over the two-year operation, 36 search warrants have been executed, resulting in the discovery of 3,500 counterfeit Cisco network components with an estimated retail value of more than \$3.5 million, the F.B.I. said in a statement.

The F.B.I. is still not certain whether the ring's actions were for profit or part of a state-sponsored intelligence effort. The potential threat, according to the F.B.I. agents who gave a briefing at the Office of Management and Budget on Jan. 11, includes the remote jamming of supposedly secure computer networks and gaining access to supposedly highly secure systems. Contents of the briefing were contained in a PowerPoint presentation leaked to a Web site, Above Top Secret.

A Cisco spokesman said that the company had investigated the counterfeit gear seized by law enforcement agencies and had not found any secret back door. ...

<http://www.nytimes.com/2008/05/09/technology/09cisco.html?partner=rssuserland&emc=rss&pagewanted=all>

✶ Another undeleted/deleted Document - "Krolls Associates"

<Danny Burstein <dannyb@panix.com>>

Wed, 21 May 2008 11:16:06 -0400 (EDT)

While the story is a bit vague on details as to the format/program of the original e-mailed document, we've all seen this before:

James Doran, KROLL EXPOSES CLIENT INFO, *NY Post*, 4 May 2008

Inspector Clouseau is alive and well - and he appears to be working for Kroll Associates.

The corporate spies, who are supposed to specialize in unearthing - and keeping - company secrets, last week announced the conclusion of a four-month long investigation into the North Carolina State Highway Patrol.

While the 47-page report appeared to be run of the mill, "meta data" buried in the electronic document named three Texas-based oil and gas exploration companies - Panther Bayou Energy, Bayou Bend Petroleum and Cymraec Resources, which has recently changed its name to Vermillion - and seven executives related to the companies.

On the subject line of the should-have-been-deleted information are the words "Due Diligence Investigation" - corporate-speak for the type of spying carried out by Kroll and others when a company is considering a takeover or a merger.

[snippety snip, rest at:]

http://www.nypost.com/seven/05042008/business/kroll_exposes_client_info_109385.htm

Phlashing attack thrashes embedded systems (John Leyden)

*<Randall Webmail <rvh40@insightbb.com>>
May 21, 2008 4:18:00 PM EDT*

[Don't phlash that dwarf - hand me the pliers!]

John Leyden, Phlashing attack thrashes embedded systems, **The Register**, 21 May 2008 [PGN-ed] <http://www.theregister.co.uk/2008/05/21/phlashing/>>

A security attack that damages embedded systems beyond repair was demonstrated for the first time in London on Wednesday. The cyber-assault thrashes systems by abusing firmware update mechanisms. If successful, the so-called phlashing attack would force victims to replace systems.

The attack was demonstrated by Rich Smith, head of research for offensive technologies and threats at HP Systems Security Lab, at the EUsecWest security conference in London on Wednesday. Smith told Dark Reading that such as "permanent denial of service" attack could be carried out remotely over the Internet.
http://www.darkreading.com/document.asp?doc_id=154270&WT.svl=news1_1

Geolocation software risks

*<Mickey Coggins <risks@int.ch>>
Sun, 18 May 2008 22:53:40 +0200*

I'm sure this is not news to any RISK readers that are somewhat familiar with global IP addressing, but may be of interest to those that are not.

There are several companies that sell databases or access to databases that attempt to map an IP address to a geographic location. This seems to be done for reasons such as localizing advertising, and limiting access to data based on the person's country.

When they get the mapping wrong in their database, it can be problematic for the owner of the IP address. I ran across an exchange on the support form of one such company here:

<http://forums.geobytes.com/viewtopic.php?t=5022>

Apparently the design of their software does not allow them to correctly attribute classless IP addresses smaller than a /24.

The risk here is that their customers are getting wrong results from the database queries, without any indication. I'll leave the possible effects of these wrong results as an exercise for the reader.

✂ Shopping centers tracking cell phones

<"Peter G. Neumann" <neumann@csl.sri.com>>
Mon, 19 May 2008 14:05:31 PDT

[Thanks to Lauren Weinstein for spotting this one. PGN]

Slashdot <<http://yro.slashdot.org/article.pl?sid=08/05/18/1838222>> notes an article in the *Times* of London on a tracking device by a company called Path Intelligence that tracks the whereabouts of cell phones within shopping centers.

<http://technology.timesonline.co.uk/tol/news/tech_and_web/article3945496.ece>

✂ China's All-Seeing Eye

<EEkid@aol.com [EEkid@aol.com]>
Monday, May 19, 2008 12:02 AM

[From Dave Farber's IP list]

"Over the past two years, some 200,000 surveillance cameras have been installed throughout the city. Many are in public spaces, disguised as lampposts. The closed-circuit TV cameras will soon be connected to a single, nationwide network, an all-seeing system that will be capable of tracking and identifying anyone who comes within its range -- a project driven in part by U.S. technology and investment. Over the next three years, Chinese security executives predict they will install as many as 2 million CCTVs in Shenzhen, which would make it the most watched city in the world."

"The end goal is to use the latest people-tracking technology -- thoughtfully supplied by American giants like IBM, Honeywell and General Electric ... to identify and counteract dissent before it explodes into a mass movement like the one that grabbed the world's attention at Tiananmen Square."

"The mergers made L-1 a one-stop shop for biometrics. Thanks to board

members like former CIA director George Tenet, the company rapidly became a homeland-security heavy hitter. ... L-1 can legally supply its facial-recognition software for use by the Chinese government."

"I get to the customs line at JFK, watching hundreds of visitors line up to have their pictures taken and fingers scanned. In the terminal, someone hands me a brochure for "Fly Clear." All I need to do is have my fingerprints and irises scanned, and I can get a Clear card with a biometric chip that will let me sail through security. Later, I look it up: The company providing the technology is L-1."

http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye/

Re: Real-time spying on credit card holders (Brown, [RISKS-25.14](#))

<Curt Sampson <cjs@cynic.net>>

Tue, 6 May 2008 14:30:14 +0900

[Relating to the "risks" of real-time e-mail notification of credit card transactions]

- > * Real-time financial transaction data being sent "by e-mail", as if e-mail
- > guaranteed either delivery of the message....
- > ...
- > * Overreaction by managers...and cancels the card while I'm in the air.

While these are both certainly "risks," I think that this particular analysis of the situation is pretty poor: it's nowhere near a balanced risk assessment that will help someone less knowledgeable about these things to make a decision, or give us good reason to suggest to the credit card company that they change or discontinue the service.

So let's look at these two points in that light, shall we?

First, e-mail certainly is not guaranteed delivery. Should we really want guaranteed real time delivery, we need a better mechanism. Perhaps a leased line to a terminal in the cardpayer's office? Or a have a human telephone the cardpayer every time the card is used. Both are pretty expensive, and unlikely to be implemented. The cheapest alternate and practical solution I can think of would be to assign an office worker to check the current card transactions on the card's web site on, say, a half-hourly basis, which is still pretty expensive.

Assuming e-mail has a 90% success rate for delivery, which option serves the cardpayer best in preventing fraud: assigning staff to check the website hourly, enabling the e-mail but having a 10% chance that they'll miss a transaction, and thus, a smaller chance that they'll miss a fraudulent transaction, or doing nothing, with the certainty that they'll not get real-time notification of a fraudulent transaction? It depends on the situation, of course, but I'd wager that for a vast majority, the e-mail option provides the best cost-benefit ratio.

Note that one might even disable the notifications while someone's traveling (when you're likely to see a lot of them), and use them only one the cardholder is not travelling, when transactions are far more likely to be fraudulent (assuming the card is used only for travel).

So my vote on this side of things: an excellent feature, use it as necessary, and do keep in mind that you might miss an e-mail, so have a backup plan to deal with a fraudulent translation for which you don't get an e-mail notification.

Well, I could go on to the other point, but I think that this provides a reasonable example of how we should be doing risk analysis, and a good contrast to the, "Oh no! There are risks!" school of post that I see here from time to time.

Curt Sampson +81 90 7737 2974 <http://www.starling-software.com>

Microsoft security advice for sale

<peter@houppermans.com>

Sat, 17 May 2008 17:34:24 +0200 (CEST)

Words fail me..

On the few Windows systems I have left, I always check what Windows update wants to install (proved a good strategy during the "Windows Genuine Advantage" disaster). This hour's suggested patch was a "GDI+ scanner".

Being the curious sort, I followed the link

<<http://go.microsoft.com/fwlink/?LinkId=33568>> and guess what?

It links straight into a Microsoft Word document - in .docx format..

[Eric Rachner noted "Yeah, whoever posted that document should've been more thoughtful. In the meantime, you don't have to purchase Office -- just download the free .docx reader from Microsoft.]

Old-Style Pumps Balk At \$4-a-Gallon Gas, Too

<Monty Solomon <monty@roscom.com>>

Sat, 17 May 2008 03:29:21 -0400

[Source: Nick Miroff, *The Washington Post*, 16 May 2008]

Like a lot of small-scale entrepreneurs, Cathy Osborne worries that she'll go out of business if fuel prices rise above \$4 a gallon. Not because she won't be able to buy gas at that price, but because she won't be able to sell it.

The old mechanical gas pumps with scrolling dials at her country store in Fauquier County lack the gears to go beyond \$3.99 a gallon. State inspectors shut down her diesel pump several months ago when the fuel topped the \$4 mark, so now all that's left are two pumps dispensing 87-octane gasoline, set at \$3.75 -- and climbing. ...

<http://www.washingtonpost.com/wp-dyn/content/article/2008/05/15/AR2008051503756.html>

✶ Clueless in France

<Pete Kaiser <djc@resiak.org>>

Tue, 20 May 2008 08:10:17 +0200

Order broadband from France Telecom. You will get web access to your account information; the details of your order, for instance, are on a page like this:

<http://suivicommande.francetelecom.com/...{number N}>

The information on this page includes your name, the address where the service is installed, your access code, account number, telephone number, and of course what (they think) you ordered and what its status is.

N+1 also works, but for someone else's order. And so forth.

It is staggeringly irresponsible to put this kind of information on unsecured pages, especially with public consecutive transaction numbers in the URL. They do a lot on unsecured pages, or pages with a mix of secured and unsecured frames that come from different domains.

And they also got our order wrong.

✶ PayPal XSS Vulnerability Undermines EV SSL Security (Paul Mutton)

<Monty Solomon <monty@roscom.com>>

Sat, 17 May 2008 11:06:44 -0400

[Source: Paul Mutton, netcraft, 16 May 2008]

A security researcher in Finland has discovered a cross-site scripting vulnerability on paypal.com that would allow hackers to carry out highly plausible attacks, adding their own content to the site and stealing credentials from users.

The vulnerability is made worse by the fact that the affected page uses an Extended Validation SSL certificate, which causes the browser's address bar to turn green, assuring visitors that the site - and its content - belongs to PayPal. Two years ago, a similar vulnerability was discovered on a different page of the PayPal site, which also used an SSL certificate. ...

http://news.netcraft.com/archives/2008/05/16/paypal_xss_vulnerability_undermines_ev_ssl_security.html

More GPS Mishaps

<Gene Wirchenko <genew@ocis.net>>

Sun, 18 May 2008 22:34:46 -0700

This week's (May 18, 2008) News of the Weird has under Recurring Themes two items about GPS mishaps. (<http://www.newsoftheweird.com/>)

[Click on 05-18-08 if it is no longer the current column, scroll down to recurring themes, and this is what PGN found:]

Navigation System On, Brain Off: Brad Adams, 52, crashed his charter bus (carrying two dozen high school softball players, who had to be sent to a hospital) into a pedestrian bridge in Seattle's Washington Park Arboretum in April (bus: 11 feet, 8 inches high; bridge, 9 feet, 0 inches). Adams said he missed warning signs because he was busy following the navigation system. [Seattle Times, 4-17-08]

Five days after that, in King's Lynn, England, a Streamline taxi minibus had to be pulled from the River Nar after the driver, who said he was obediently following the navigation system instructions, drove straight into the water. [Lynn News, 4-23-08]

Re: UK CCTV used to create a music video ([RISKS-25.15](#)).

<"Chris D." <e767pmk@yahoo.co.uk>>

Wed, 21 May 2008 21:36:08 +0100

Blatant opinion from a Brit: it feels like either '1984', or an Internet-era version of 1970s East Germany... It's a bit difficult to sort through the media hype, but apart from the world's biggest DNA sample database, allegedly some local authorities have experimented with garbage containers incorporating RFID chips, so that they can track down errant citizens who failed to sort their 6 types of plastics for recycling. Just this week (May 20th) it was widely reported that laws are being proposed requiring telecomms companies and ISPs to supply the Home Office (interior ministry) with all telephone traffic and web surfing details and copies of e-mails handled; potential data volumes are noted as a concern (what a surprise). And coming soon (maybe) -- ID cards! <https://www.ips.gov.uk/>, follow links. There's a strong tradition here that "the gentleman in Whitehall [Government offices] knows best", so opposition has been limited to grumbles and moans.

> Unable to hire a production crew for a standard 1980's era MTV music
> video, they performed their music in front of 80 of the 13 million CCTV
> "security" cameras available in England

Funnily enough, a humorist in a newspaper some years ago suggested making a movie this way -- you've heard of `cinema verite', so he proposed `cinema securite'...

Chris Drewe, Essex County, UK.

Re: Dilbert wants a widget (Ehrich, [RISKS-25.15](#))

<Bill Bumgarner <bbum@mac.com>>

Fri, 16 May 2008 15:31:49 -0700

The new Dilbert site design is abysmal. It is a flash based behemoth that takes a long time to load, is slow, and generally crowds the page with useless garbage.

In other words, every bit the design product of a group of people working in an environment that Dilbert so effectively pokes fun of.

In response to the unbelievably loud set of complaints about the "new and improved" design, a "fast" page was made available:

<http://www.dilbert.com/fast>

Re: Debian OpenSSL Predictable PRNG Toys

<"Horning, Jim" <Jim.Horning@sparta.com>>

Mon, 19 May 2008 14:46:10 -0700

"Random" and "haphazard" are not synonyms.

The assumption that uninitialized memory actually contains *random* values, rather than merely values *that the writer of the code does not know how to predict* is a highly dubious one. I have used systems where the values of uninitialized variables were totally predictable. I don't know which open source operating systems randomize the contents of memory when allocating it and which do not, but anyone who cares about the results of the OpenSSL package really ought to.

I hope that someone is checking out the predictability of all the non-Debian PRNG results?

Re: Securing The Wrong Spaces: A Lesson (Damiani, [RISKS-25.10](#))

<"David E. Price, SRO, CHMM" <price16@ltnl.gov>>

Tue, 20 May 2008 11:00:33 -0700

Actually, because of the effects of the inverse square law, given an equally

sensitive radar on the other end they can be detected at 4 times the distance they can 'see', not twice the distance. (A RISK of simple math?)

Senior Safety Analyst
(Nuclear, Chemical, Biological, and Explosives Accident/Safety Analyses)

[typo corrected in archive copy. PNG]



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 17

Friday 30 May 2008

Contents

- [Wrong patient gets appendix removed, software to blame](#)
[Rex Sanders](#)
- [E-Voting Banned by Dutch Government](#)
[Udo de Haes](#)
- [Don't phlash that dwarf -- hand me the pliers!](#)
[John Leyden](#)
- [Firmware-based phone vulnerabilities](#)
[David Magda](#)
- [A Low-cost Attack on a Microsoft CAPTCHA](#)
[Jeff Yan and Ahmad Salah El Ahmad via Monty Solomon](#)
- [SYN attack from RIAA contractor](#)
[David Leshner](#)
- [Random and haphazard are not synonyms](#)
[Andrew Koenig](#)
- [An iTunes file database problem Apple will never fix](#)
[Max Power](#)
- [Microsoft's Masters: Whose Rules Does Your Media Center Play By?](#)
[Greg Sandoval](#)
- [Fundraising that is too Excel-lent to report](#)
[Mark Brader](#)
- [On-line registration for College Reunion 2008](#)
[F John Reinke](#)
- [Why not set the pump to half price and post a sign?](#)
[Daniel P. B. Smith](#)
- [Re: Securing The Wrong Spaces: A Lesson](#)
[John Sullivan](#)
[Bill Hopkins](#)
- [An account of the Estonian Internet War](#)
[Gadi Evron](#)
- [Info on RISKS \(comp.risks\)](#)

Wrong patient gets appendix removed, software to blame

<Rex Sanders <rsanders@usgs.gov>>

Fri, 23 May 2008 10:26:57 -0700

Software incompatibility was part of a chain of events leading to the wrong patient getting an appendectomy.

News story:

http://www.santacruzsentinel.com/ci_9356389

Original report:

<http://www.cdph.ca.gov/certlic/facilities/Documents/HospitalAdministrativePenalties-2567Forms-LNC/2567DominicanHospital-SantaCruz-Event-QQGN11.pdf>

or

<http://preview.tinyurl.com/49u49w>

E-Voting Banned by Dutch Government

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

Fri, 23 May 2008 12:36:38 PDT

[via Natarajan Shankar]

Udo de Haes, Andreas, InterGovWorld.com (21 May 2008)

The Netherlands has banned the use of electronic voting machines in future elections due to concerns that the technology was too vulnerable to eavesdropping. "Developing new equipment furthermore requires a large investment, both financially and in terms of organization," according to the Ministry of Internal Affairs. "The administration judges that this offers insufficient added value over voting by paper and pencil." The Dutch government also banned voting printers, which were criticized by a group of experts led by Bart Jacobs, a professor at Radboud University in Nijmegen, over similar security concerns. The Netherlands will make use of electronic vote counting, and will conduct tests to improve its effectiveness. The local activist group "Wij vertrouwen stemcomputers niet" (We don't trust voting computers), led by computer hacker Rop Gonggrijp, declared the decision a victory for those who want verifiable election results.

Don't phlash that dwarf -- hand me the pliers!

<David Chessler <chessler@usa.net>>

Sat, 24 May 2008 21:19:01 -0400

[From johnmacsgroup]

Phlashing attack thrashes embedded systems

John Leyden, *The Register*, 21 May 2008

<http://www.theregister.co.uk/2008/05/21/phlashing/>

A security attack that damages embedded systems beyond repair was demonstrated for the first time in London on Wednesday. The cyber-assault thrashes systems by abusing firmware update mechanisms. If successful, the so-called phlashing attack would force victims to replace systems.

The attack was demonstrated by Rich Smith, head of research for offensive technologies and threats at HP Systems Security Lab, at the EUsecWest <<http://www.eusecwest.com/agenda.html>> security conference in London on Wednesday. Smith told Dark Reading that such as "permanent denial of service" attack could be carried out remotely over the Internet. <http://www.darkreading.com/document.asp?doc_id=154270&WT.svl=news1_1>

Theoretically the attack could be both more effective (as the damage caused would be harder to recover from) and cheaper than conventional denial of service attacks, which typically rely on hackers paying to rent control of a network of compromised PCs.

The PhlashDance approach relies on exploiting frequently unpatched vulnerabilities in embedded systems, such as flaws in remote management interfaces, to get access to a system. That alone wouldn't be enough, but because firmware updates are seldom secured, the possibility exists of making an update that effectively trashes a system.

Smith is calling on vendors to authenticate the mechanism as one way of defending against such attacks. He is demonstrating a tool to search for vulnerabilities in firmware, as well as an attack mechanism to corrupt vulnerable firmware at EUsecWest.

There's no record of such an attack even occurring and other security watchers are skeptical over whether crackers could make money - the main motive for denial of service attacks - from such an approach. Both H D Moore of Metapolit fame and the Hack a Day blog reckon that exploiting vulnerabilities to plant malware in firmware is a far more insidious and dangerous type of attack than simply destroying systems. Another presentation at EuSecWest will demonstrate a proof of concept rootkit capable of covertly monitoring and controlling Cisco routers. The Cisco IOS rootkit software was developed by Sebastian Muniz, of Core Security. <<http://www.hackaday.com/2008/05/20/phlashing-denial-of-service-attack-the-new-hype>>

Firmware-based phone vulnerabilities

<David Magda <dmagda@ee.ryerson.ca>>
Wed, 28 May 2008 13:56:03 -0400 (EDT)

There are some phones that have complicated software (iPhone, Nokia S60 line), but even "firmware-based" phones now have security issues:

- > This vulnerability allows remote attackers to execute arbitrary code on
- > vulnerable Motorola RAZR firmware based cell phones. User interaction is
- > required to exploit this vulnerability in that the target must accept a
- > malicious image sent via MMS.

>

- > The specific flaw exists in the JPEG thumbprint component of the EXIF
- > parser. A corrupt JPEG received via MMS can cause a memory corruption
- > which can be leveraged to execute arbitrary code on the affected device.

<http://www.zerodayinitiative.com/advisories/ZDI-08-033/>

http://www.theregister.co.uk/2008/05/28/razr_security_jpg/

✂ A Low-cost Attack on a Microsoft CAPTCHA

<Monty Solomon <monty@roscom.com>>

Mon, 12 May 2008 08:02:37 -0400

Jeff Yan, Ahmad Salah El Ahmad
School of Computing Science, Newcastle University, UK
{Jeff.Yan, Ahmad.Salah-El-Ahmad}@ncl.ac.uk

Abstract: CAPTCHA is now almost a standard security technology. The most widely used CAPTCHAs rely on the sophisticated distortion of text images rendering them unrecognisable to the state of the art of pattern recognition techniques, and these text-based schemes have found widespread applications in commercial websites. The state of the art of CAPTCHA design suggests that such text-based schemes should rely on segmentation resistance to provide security guarantee, as individual character recognition after segmentation can be solved with a high success rate by standard methods such as neural networks. In this paper, we analyse the security of a text-based CAPTCHA designed by Microsoft and deployed for years at many of their online services including Hotmail, MSN and Windows Live. This scheme was designed to be segmentation-resistant, and it has been well studied and tuned by its designers over the years. However, our simple attack has achieved a segmentation success rate of higher than 90% against this scheme. It took on average ~80 ms for the attack to completely segment a challenge on a desktop computer with a 1.86 GHz Intel Core 2 CPU and 2 GB RAM. As a result, we estimate that this Microsoft scheme can be broken with an overall (segmentation and then recognition) success rate of more than 60%. On the contrary, its design goal was that "automatic scripts should not be more successful than 1 in 10,000" attempts (i.e. a success rate of 0.01%). For the first time, we show that a CAPTCHA that is carefully designed to be segmentation-resistant is vulnerable to novel but simple attacks. Our results show that it is not a trivial task to design a CAPTCHA scheme that is both usable and robust. ...

http://homepages.cs.ncl.ac.uk/jeff.yan/msn_draft.pdf

✂ SYN attack from RIAA contractor

<David Lesher <wb8foz@8es.com>>

Thu, 29 May 2008 15:08:24 -0400

MediaDefender is a company that works for the RIAA/MPAA to thwart the distribution of copyrighted materials over P2P networks. Apparently, over the weekend, they SYN flooded servers hosting seeds for Revision3's BitTorrent-distributed programs.

Revision3's CEO Jim Louderback explains the SYN flood attack and MediaDefender's role in it in a really well written blog post:

<http://revision3.com/blog/2008/05/29/inside-the-attack-that-crippled-revision3>

FYI: Revision3 is an ad-supported online TV network that distributes original programming via podcast, streaming, and BitTorrent, among other methods. BitTorrent and SYN flooding are explained in Louderback's post.

#Random and haphazard are not synonyms

*<Andrew Koenig <ark@acm.org>>
Fri, 23 May 2008 10:54:33 -0400*

Jim Horning's note ([RISKS-25.16](#)) about uninitialized memory reminds me of something that happened to me nearly 40 years ago.

At the time I was in college and working as a student consultant at the computer center. Another student came in with a problem: A comparison in his program wasn't working as he thought.

This program was in 360 assembly language, using a single-pass assembler with the wonderful name of SPASM. 360 machine language includes a bunch of instructions to work with sequences of characters that can range from 1 through 256 characters. This particular student was exploiting this feature in a way that was breathtakingly clever or naive -- or both.

He had several Boolean flags in his program. He used three bytes to represent each flag, setting those bytes to the EBCDIC values of "SAM" or "XYZ" to represent true or false. Moreover, he did not bother to initialize these flags, figuring that they would start out with random values. In other words, if he wanted a flag to start out as false, he would assume it was true if its value was "SAM", trusting that the probability that it would be "SAM" by chance would be small enough to be zero for practical purposes. Similarly, if wanted a flag to start out as true, he would assume that it was false if its value was "XYZ".

What he did not count on was that this single-pass assembler assembled his program in the same memory that it subsequently used to run it--so that one of his variables would always start out with "SAM" as its initial value.

I never did figure out why he didn't use the assembly language's initialization feature.

✂ An iTunes file database problem Apple will never fix

<Max Power <dist23@juno.com>>

Mon, 26 May 2008 00:39:19 -0700

An iTunes file database problem Apple will never fix: podcast files that are not deleted do not moved out of their original directory ... and iTunes has other poor podcast directory disk capacity tracking issues.

In one case iTunes showed I had no "National Nine News" files, but the directory had about 1gb worth of video files. This memory and file tracking problem is more severe with video files, but audio files may have the same problem if they are not MP3 files. At its worse iTunes could tell users it has no files, but your hard disk could be full of podcasts. This is not an iTunes library issue. I am fairly certain that iTunes counts only podcasts you have not deleted in its disk capacity tracking text below the podcast list. More people need to provide more detail about this long-standing iTunes bug.

My system Vista: podcasts stored on a FAT32 drive OSX systems probably have this same flaw, as it is a User Interface problem (high-level code vs low-level edge code that interfaces with the OS).

Max Power, CEO, Power Broadcasting, SA HireMe.geek.nz

✂ Microsoft's Masters: Whose Rules Does Your Media Center Play By?

<Monty Solomon <monty@roscom.com>>

Fri, 23 May 2008 07:47:20 -0400

Posted by Danny O'Brien, 19 May 2008

While its customers are still puzzling over why Vista Media Center is suddenly refusing to record over-the-air NBC digital TV, Microsoft has come out with an astounding admission, courtesy of Greg Sandoval at CNet News:

"Microsoft included technologies in Windows based on rules set forth by the (Federal Communications Commission)," a Microsoft spokeswoman wrote in an e-mail to CNET News.com. "As part of these regulations, Windows Media Center fully adheres to the flags used by broadcasters and content owners to determine how their content is distributed and consumed."

Microsoft's statement shines light on how Microsoft expects Media Center to behave. If this is the company's explanation for what users are seeing when attempting to record digital NBC broadcasts over-the-air, then Microsoft is saying Vista obeys the broadcast flag: a requirement rejected by courts and Congress. ...

<http://www.eff.org/deeplinks/2008/05/microsofts-masters-whose-rules-does-your-media-cen>

Fundraising that is too Excel-lent to report

<msb@vex.net (Mark Brader)>

Mon, 26 May 2008 18:01:29 -0400 (EDT)

* From: Greg Goss <goss@gossg.org>
* Newsgroups: alt.fan.cecil-adams
* Subject: Democratic fundraising overwhelms FEC computers
* Date: Mon, 26 May 2008 12:07:09 -0600

What is the difference when you have a quarter million people signing checks for \$200 instead of 200 people signing checks for a quarter million?

Your fundraising report to the government becomes unwieldy.

http://politicalwire.com/archives/2008/05/26/democratic_fundraising_strains_fec_computers.html

[The FEC is at the same time both Overwhelmed and Underwhelming. PGN]

For other reports, browse on
Obama fundraising report spreadsheet excel

On-line registration for College Reunion 2008

<"r@rcc" <reinkefj@reinke.cc>>

Tue, 27 May 2008 07:53:46 -0400

Here's an attempt to bootstrap an authentication process. Argh! Everyone is an InfoSec expert.

Wonder if I can sign up everyone I know? Maybe I can order a Ferrari? If they are this lame, I can NOT imagine what the site security is like!

This is a real email from one of 'my' schools.

Argh!

You can't make this stuff up!

fjohn

*** begin quote ***

From: The Alumni Relations Team [mailto:alumni@zzzzz.edu]

Sent: Friday, May 16, 2008 5:19 PM

To: yyyyy

Subject: NEW: On-line registration for zzzzz College Reunion 2008!

Dear yyyyy

zzzzz College is launching a new payment gateway that will further ensure that using your credit card on our Web site is both secure and protected. On-line safety is our main concern, whether you register for a class or event, make a gift or purchase an item. Please use our Web site knowing that you will always be provided with the best possible means of using your credit card in a safe and secure on-line environment.

In order take advantage of the feature to register for Alumni Reunion Weekend (<http://www.zzzzz.edu/reunion>), you are being sent your Campus Wide Identification Number. This will serve as your "User ID". Your initial pin number will be your birth date, entered as six digit number (ex.021458). After you have entered this information on the link provided below to the registration page, you may change your log on information to a more familiar configuration.

USER ID:
000761932

PIN:
(your 6 digit birth date in the form of MMDDYY - i.e. Feb 14 1958 would be 021458)

To Register for Reunion Weekend 2008:

1. Access the new Self Service Payment Gateway:
<https://self-service.zzzzz.edu>
(If you experience a "website security certificate" notification, select "allow" as prompted)
2. Enter your User ID and pin (provided above)
3. Select the Alumni Services tab
4. Select Reunion 2008
5. Follow prompts to complete your registration with credit card

These measures ensure all of us that your personal information remains private. Thank you for your continued support of the College. We look forward to seeing you on Reunion Weekend!

Warmest regards,
xyz, Director of Alumni Relations

[Literals PGN-ed to hinder filtering.]

✶ Why not set the pump to half price and post a sign?

<"Daniel P. B. Smith" <dpbsmith@verizon.net>>
Sun, 25 May 2008 11:32:34 -0400

Monty Solomon quoted a Washington Post article about a gas-station operator

who fears going out of business because her mechanical pumps can't be set to more than \$3.99 a gallon.

The reporter doesn't explain why she couldn't do what was done on a widespread basis the last time something like this happened.

On 23 May 1979, *The New York Times* reported that "New York State gave dealers emergency permission to meter by the half-gallon. The change is designed to allow more of them to charge more than \$1 a gallon and thus encourage them to stay open.... By allowing machines to charge by half-gallons, the technical limit would be doubled, to \$1.99 8/10 a gallon."

My recollection is that at the time, in other cases, operators simply set the pumps to register half the actual price, and posted conspicuous signage stating the actual prices and noting the customer would be charged twice the total registered by the pump registered.

I'm no lawyer, and certainly can't speak to weights and measures law in every state, but I find it hard to believe that an station owner taking such an action in good faith would get in serious trouble.

[Big surprise. This is what is happening. Lots of items submitted on this "problem". PGN]

Re: Securing The Wrong Spaces: A Lesson (Damiani, [RISKS-25.10](#))

<John Sullivan <john@kanargh.force9.co.uk>>
Sun, 25 May 2008 17:34:14 +0100

(The original piece was in [RISKS-25.06](#).)

Assuming your transmitter emits a specific strength RF pulse, and your receiver can detect anything more powerful than some (lower) strength pulse, the inverse square law will help determine the maximum path length between transmitter and receiver that still allows detection.

Having determined this length, but assuming perfect reflectors where necessary, whether the path is looped back on itself to reach the position of the original transmitter (enemy at distance X, path length 2X), or layed straight to reach the enemy receiver (enemy at distance 2X, path length 2X) shouldn't make a difference.

Re: Securing The Wrong Spaces: A Lesson (Price, [RISKS 25.16](#))

<"Bill Hopkins" <whopkins@wmi.com>>
Tue, 27 May 2008 14:33:48 -0400

Picking nits off nits, re: target detection vs. radar source detection:

It's actually much more than four times the distance. Only a tiny fraction of the incident signal is reflected by the target, so we are talking about orders of magnitude, not small integer ratios.

Given that, the limit on detecting someone else's threat detection radar is limited more by the geometry of surface-to-surface signals on a sphere than distance effects on signal strength.

The lesson of the original post holds, that systems to detect military threats may not (indeed, may be designed not to) detect civilian bystanders.

✂ An account of the Estonian Internet War

<Gadi Evron <ge@linuxbox.org>>

Tue, 20 May 2008 09:30:40 -0500 (CDT)

About a year ago after coming back from Estonia I promised I'd send in an account of the Estonian "war". The postmortem analysis and recommendations I later wrote for the Estonian CERT are not yet public.

A few months ago I wrote an article for the Georgetown Journal of International Affairs, covering the story of what happened there, in depth. The journal owns the copyright so I had no way of sending that along either. I wasn't about to email saying "go buy a copy".

Mostly silly articles kept popping up with misguided to wrong information about what happened in Estonia, and when an Estonian student was arrested for participating, some in our community even jumped up to say "it was just some student". Ridiculous.

This is the "war" that made politicians aware of cyber security and entire countries scared, NATO to "respond" and the US to send in "help". It deserved a better understanding for that alone, whatever actually happened there.

I was there to help, but I just deliver the account. The heroes of the story are the Estonian ISP and banking security professionals and the CERT (Hillar Aarelaid and Aivar Jaakson).

Apparently the Journal made my article available in PDF form by a third party:

Battling Botnets and Online Mobs

Estonia's Defense Efforts during the Internet War

URL: <http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf>

It is not technical, I hope you find it useful.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 18

Tuesday 3 June 2008

Contents

- [Fire at The Planet takes down thousands of websites](#)
[Gene Wirchenko](#)
- [UK power rationing causes fires and false fire alarms](#)
[Alistair McDonald](#)
- [Beware of Error Messages At Bank Sites](#)
[Brian Krebs via George Sherwood](#)
- [Still even more lost data](#)
[Gene Wirchenko](#)
- [Mass exploitation with Adobe Flash](#)
[Monty Solomon](#)
- [Risks in Instant Runoff Voting](#)
[PGN](#)
- [Arkansas Election Officials Baffled by Machines that Flipped Race](#)
[PGN](#)
- [Spelling checker runs amok in Pennsylvania high-school yearbook](#)
[Al Stangenberger](#)
- [Full Disclosure and why Vendors Hate it](#)
[Jonathan A. Zdziarski via Monty Solomon](#)
- [Re: An iTunes file database problem Apple will never fix](#)
[Alistair McDonald](#)
- [Re: Wrong patient gets appendix removed, software to blame](#)
[PGN](#)
- [REVIEW: "Secure Programming with Static Analysis", Chess/West](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

✉ Fire at The Planet takes down thousands of websites

<Gene Wirchenko <genew@ocis.net>>
Mon, 02 Jun 2008 08:29:35 -0700

A fire at The Planet's data center in Houston TX on 31 May 2008 was blamed on a faulty transformer. About 9,000 servers and 7,500 customers were

affected by the outage over the weekend. B3ta.com (a high-profile British comedy site) is a notable casualty. [Power was restored on 2 Jun. PGN]
http://www.theregister.co.uk/2008/06/01/the_planet_houston_data_center_fire/

UK power rationing causes fires and false fire alarms

<Alistair McDonald <alistair@inrevo.com>>
Fri, 30 May 2008 10:54:04 +0100 (BST)

As an introduction, the domestic electricity supply in the UK is generally very good, with no brownouts - outages are very rare. I realise that this contrasts with the supply in some other countries. This means that when power does fail here, we're sometimes not ready for it.

This week, The Sizewell B nuclear electricity generating station in Suffolk, UK went offline, and was followed shortly afterward by a coal-fired electricity generating station, Longannet in Fife, also going offline. The nuclear reactor went offline when a failsafe was triggered by a faulty reading on a control panel.

The loss of capacity was worsened when several smaller generation facilities went offline for periods of time during the next few hours.

The National Grid took measures to protect the supply, by lowering supply voltages and eventually shutting off supply to parts of the nation. Details at http://www.theregister.co.uk/2008/05/29/blighty_leccy_crisis/

However, the Teeside *Evening Gazette* notes that there were many false fire alarms over a wide area of the country due to the power outages, and at least one real fire (although the reported "power surge" cause may not be related to the power failure).

<http://www.gazettelive.co.uk/news/teeside-news/2008/05/28/n-plant-shutdown-blacks-out-tees-84229-20984943/>

As the UK's electricity supply is expected to be outstripped by demand in the next few years, incidents like these may increase.

<http://www.independent.co.uk/news/business/news/utility-giant-rwe-warns-of-uk-electricity-shortages-526919.html>

Alistair McDonald, InRevo Ltd (<http://www.inrevo.com>) Tel 07017 467 396
Author of the SpamAssassin book: (<http://www.packtpub.com/spamassassin/>)

Beware of Error Messages At Bank Sites: Brian Krebs

<George Sherwood <sherwood@testcover.com>>
Tue, 03 Jun 2008 19:43:12 +0000

Computer Security: Beware of Error Messages At Bank Sites
Brian Krebs's blog at *The Washington Post* website

If you own or work at a small to mid-sized business, and are presented with

an error message about data synchronization or site maintenance when trying to access your company's bank account online, you might want to give the bank a call: A criminal group that specializes in deploying malicious software to steal banking data is presenting victims with fake maintenance pages and error messages as a means of getting around anti-fraud safeguards erected by many banks.

Dozens of banks now require business customers to log in to their accounts online using so-called "two factor authentication" methods, which generally require the customer to enter something in addition to a user name and password, such as a random, one-time-use numeric code generated by a key fob or a scratch-off pad.

But one of this past year's most prolific cyber gangs -- which targets virus-laden e-mail attacks against specific individuals at small to mid-sized businesses -- has devised a simple but ingenious method of circumnavigating these security measures. When a victim whose PC is infected with their data-stealing malware attempts to log in at a banking site that requires two-factor authentication, the fraudsters modify the display of the bank site in the victim's browser with an alert saying "please allow 15 to 30 minutes for your request to be synchronized with our server."

By intercepting the victim's password along with the one-time code -- and assuring that the victim will never be able to use that one-timecode -- the thieves can quickly use the one-time code to log in as the victim and proceed to drain the bank account.

http://blog.washingtonpost.com/securityfix/2008/06/beware_of_error_messages_at_ba_1.html?nav=rss_blog

[See Brian's outstanding blog, which notes the case of a fake error message inserted by malware during May 2008 in a spoof of the U.S. Tax Court, and further discussion. PGN]

Still even more lost data

*<Gene Wirchenko <genew@ocis.net>>
Sun, 01 Jun 2008 15:06:27 -0700*

Bank of New York Mellon Corp. officials last week confirmed that a box of unencrypted data storage tapes holding personal information of more than 4.5 million individuals was lost more than three months ago by a third-party vendor during transport to an off-site facility. [Source: Computerworld, 30 May 2008]

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9091318&source=rss_news50

Note the incredibly sophisticated encrypted technique. It is so sophisticated that Eudora does not recognise it as a word.

✂ Mass exploitation with Adobe Flash

<Monty Solomon <monty@roscom.com>>

Thu, 29 May 2008 23:19:43 -0400

Alerts, Security Labs, 29 May 2008

Threat Type: Malicious Web Site / Malicious Code

Websense Security Labs ThreatSeeker technology has detected thousands of web sites infected with the recent mass JavaScript injection that exploits a vulnerability in Adobe Flash (CVE-2007-0071) to deliver its malicious payload. This attack has been previously mentioned in ISC and Adobe's blog.

This vulnerability is not a 0-day, and users with the latest version of Flash Player (version 9.0.124.0) are safe. However, there are still many on older versions of Flash that are unaware of this mass web infection and are susceptible to this drive-by attack. An update to the latest version of Flash Player is highly recommended. ...

<http://securitylabs.websense.com/content/Alerts/3096.aspx>

✂ Risks in Instant Runoff Voting

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

Fri, 30 May 2008 11:35:03 PDT

Runoff elections are expensive, which has led to various approaches to avoiding them by having voters express priorities among the various candidates. However, an important paper by Kenneth Arrow (RAND Corp, 1948) provides mathematical evidence that no voting system that ranks preferences among more than two candidates can guarantee logically fair nonparadoxical results.

A nice example of a "winner-turns-loser" paradox with Instant Runoff Voting (IRV) is given by William Poundstone, *Why Elections Aren't Fair (And What We Can Do About It)*, Hill & Wang, 2008, by considering hypothetically what might have happened in the 1991 Louisiana governor's race if IRV had been used. I oversimplify slightly (and ignore the political positions that might have made this logical!):

34% of the voters were for Edwin Edwards, 32% for David Duke, 27% for Buddy Roemer. Under IRV, Roemer would have been eliminated, and his votes reallocated -- which could have resulted in Edwards winning.

Suppose Edwards managed to have swung 6% of Duke's voters to have switched to Edwards. Then Duke would have been eliminated, and the reallocation could have resulted in Roemer being the winner.

There's a nice review article on Poundstone's *Gaming the Vote*, and Spencer Overton's *Stealing Democracy: The New Politics of Voter Suppression*, Norton,

2008, in *The Nation*, 2 Jun 2008, written by Peter C. Baker.

<http://www.thenation.com/doc/20080602/baker>

Arkansas Election Officials Baffled by Machines that Flipped Race

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

Fri, 30 May 2008 10:49:31 PDT

Source: Kim Zetter <kzetter@gmail.com>, 29 May 2008 [PGN-ed]

<<http://blog.wired.com/27bstroke6/evoting/index.html>>

Bruce Haggard, an election commissioner in Faulkner County, Arkansas, is baffled by a problem that occurred with two voting machines in this month's general state elections. The machines allocated votes cast in one race <http://www.thecabin.net/stories/052408/loc_0524080001.shtml> to an entirely different race that wasn't even on the electronic ballot. The problem resulted in the wrong candidate being declared victor in a state House race. "I don't understand how it could possibly happen," Haggard told Threat Level. [It is easy to NOT UNDERSTAND if you haven't been reading RISKS for the past 20 years, or not been paying attention to the media coverage. PGN]

The problem occurred with two touch-screen voting machines made by Election Systems & Software, which were the only machines used in Faulkner County's East Cadron B voting precinct.

Haggard says the night before the election, officials noticed that the electronic ballot on two machines slated to be used at East Cadron B was missing the State House District 45 race. So officials printed up paper ballots to be used just for that race in that precinct.

Voters cast electronic ballots on the voting machines for other races, then cast paper ballots for the District 45 race. At the end of the day, Dr. Terry Fiddler (D) had beat Linda Tyler (D) for the House seat with 794 votes to Tyler's 770. But a post-election examination revealed that despite the fact that the electronic ballots on the two machines at the East Cadron B precinct didn't display the District 45 race, the machines recorded votes for that race anyway.

After some examination, officials determined that the machines had taken votes that were actually cast in a different race -- the Cadron Township Constable race -- and given them to the non-existent District 45 race instead. Luckily, Haggard says officials were able to determine this is where the votes came from because the touch-screen machines produce a voter-verifiable paper audit trail.

Those paper trails showed correctly that there was no District 45 race on the ballot and, thus, that there were no votes cast on the machines for the District 45 race. But memory cards taken from inside the machines, showed that the machines recorded votes in the District 45 race. Officials were able to determine that those District 45 votes actually belonged to the Cadron Township Constable race because the same number of votes that were

allocated to the District 45 race in the memory cards matched the number of votes that voters had cast in the Cadron Township Constable race, which appeared on the voter-verifiable paper audit trail.

``Somehow the recording software had tabulated it into the wrong race, Thank goodness for the paper trail. We went to the paper trail and could show how people actually voted."

Haggard doesn't have a clue how the switch could have happened but says that it was either a problem with the ballot definition file that election officials created before the election that tells the machines where to allocate votes or in the voting machine software itself.

Once the bogus votes in District 45 were subtracted from the totals, Fiddler lost 51 votes in the race, showing that Tyler had actually won the House seat. [...]

This is not the first time that ES&S voting systems have had vote-flipping problems. In Ohio during last November's general election ES&S tabulation software flipped the vote totals <<http://blog.wired.com/27bstroke6/2007/11/votes-flipped-i.html>> for two candidates. Officials noticed the problem when they compared the vote totals produced from the memory cards to the totals that appeared on paper printouts from the machines.

ES&S machines in Ohio also had a separate problem last November when voters, among them the secretary of state, reported that their machine had dropped a candidate's name from the race <<http://blog.wired.com/27bstroke6/2008/03/the-mysterious.html>> and displayed a gray bar in his place.

ES&S machines were also at the center of the controversy over the 13th Congressional District race in Florida in 2006 when more than 18,000 ballots cast in Sarasota County showed no vote cast in the CD-13 race after hundreds of voters had complained that the machines failed to respond to their touch. An investigation by the Government Accountability Office indicated that the machines likely weren't to blame in that case, though critics have questioned the thoroughness of that investigation.

See also:

- * Votes Flipped in Ohio Race that Used E-voting machines
<<http://blog.wired.com/27bstroke6/2007/11/votes-flipped-i.html>>
- * Ohio's Election Portends Trouble
<<http://www.wired.com/science/discoveries/news/2006/10/71999>>
- * Report: Magnet and PDA Sufficient to Change Votes on ES&S Voting Machine
<<http://blog.wired.com/27bstroke6/2007/12/report-magnet-a.html>>

✂ Spelling checker runs amok in Pennsylvania high-school yearbook

<Al Stangenberger <forags@nature.berkeley.edu>>

Mon, 02 Jun 2008 12:57:08 -0700

Middletown Area High School's yearbook listed Max Zupanovic as "Max Supernova," Kathy Carbaugh as "Kathy Airbag" and Alessandra Ippolito as "Alexandria Impolite," just to name a few. The mistakes were found on four of the yearbook's 176 pages, co-editor Amanda Gummo said.

Ed Patrick of Taylor Publishing, which printed the book, said his company is responsible for the errors and will provide free stickers printed with the correct names. "It happens all the time, every year," Patrick said. "Look at any yearbook in the country." [Source: AP news, 2 Jun 2008]
<http://apnews.myway.com/article/20080602/D91222D01.html>

[Another example of blind acceptance of a spelling-checker's suggestions. I do think the publisher's comment about it "happening all the time" is a little unprofessional. AS]

[My yearbooks generally had zero defects (except for my college freshman yearbook -- which included a fictitious student named Duke Miasma. But then that was a feature, and not a defect. And that was before spelling checkers, when people learned how to spell. PGN]

Al Stangenberger, Center for Forestry, Univ. of California at Berkeley
145 Mulford Hall # 3114, Berkeley, CA 94720-3114 (510)642-4424

Full Disclosure and why Vendors Hate it: Jonathan A. Zdziarski

<Monty Solomon <monty@roscom.com>>
Sat, 31 May 2008 15:35:59 -0400

Jonathan A. Zdziarski, May 2008

I did a talk recently at O'Reilly's Ignite Boston party about the exciting iPhone forensics community emerging in law enforcement circles. With all of the excitement came shame, however; not for me, but for everyone in the audience who had bought an iPhone and put something otherwise embarrassing or private on it. Very few people, it seemed, were fully aware of just how much personal data the iPhone retains, in spite of the fact that Apple has known about it for quite some time. In spite of the impressive quantities of beer that get drunk at Tommy Doyle's, I was surprised to find that many people were sober enough to turn their epiphany about privacy into a discussion about full disclosure. This has been a hot topic in the iPhone development community lately, and I have spent much time pleading with the different camps to return to embracing the practice of full disclosure.

The iPhone is shrouded in secrecy on both sides - Apple (of course) uses their secrets to instill hype (and gloss over many otherwise obvious privacy flaws), while the iPhone development community uses their secrets to ensure they can exploit future versions of the firmware to find these flaws (along with all the other fun stuff we do). The secrets on both sides appear to

have not only hurt the product, but run the risk of devolving an otherwise amazing device into the next surveillance fear. With the military and federal agencies testing the iPhone for possible use, some of the long-held secrets surrounding the iPhone even run the risk of affecting national security. ... <http://www.zdziarski.com/papers/fulldisclosure.html>

✂ Re: An iTunes file database problem Apple will never fix (R-25.17)

<"Alistair McDonald" <alistair@inrevo.com>>

Mon, 2 Jun 2008 08:59:01 +0100 (BST)

I'm surprised this item appeared in RISKS. It appears to be a generalised complaint about iTunes software; there is no evidence of a dialogue with Apple (so how can Max say "never"?) plus nothing specific in terms of version numbers or details of how to reproduce the problem.

I suspect that if there was a general flaw in iTunes that caused disk space to be retained, that such a defect would be well publicised. A quick search on google returns only problems with the wrong detection of iPod capacity.

The piece finishes with a vague conjecture that because this is a UI problem, it must exist on both OSX and windows platforms. How the location of the defect was tracked to the UI code, and how it affects OSX is, apparently, left as an exercise for the reader.

The risk? Just because someone knows the list submission address does not make their submissions valid.

Alistair McDonald, InRevo Ltd (<http://www.inrevo.com>) Tel 07017 467 396

✂ Re: Wrong patient gets appendix removed, software to blame

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

Fri, 30 May 2008 13:26:04 PDT

(Sanders, [R 25 17](#))

[For those of you who did not dig it out, here is the text, for the RISKS archives.]

Software incompatibility was part of a chain of events leading to the wrong patient getting an appendectomy. The mistake occurred on 14 Nov 2007, when two female patients were scheduled for computed tomography, or CT scans. The first patient underwent an appendectomy that evening because of the CT results. But the surgery was unnecessary. The next day, a radiologist discovered the patient's CT scan was actually that of a second patient. However, the patient's information had already been entered into the computer system for the CT scan. After the second patient's scan was completed, a radiology technician noted the error, removed the first patient's information and entered information on the second patient. When

the first patient's information was deleted from the computer in the scan room, it was not deleted from the computer system used by the radiologist. ``This was due to an incompatibility of the software between the two systems."`

REVIEW: "Secure Programming with Static Analysis", Chess/West

<Rob Slade <rmslade@shaw.ca>>

Mon, 02 Jun 2008 11:49:44 -0800

BKSCPWSA.RVW 20080219

"Secure Programming with Static Analysis", Brian Chess/Jacob West, 2007, 978-0-321-42477-8, U\$49.99/C\$61.99

%A Brian Chess

%A Jacob West

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

%D 2007

%G 978-0-321-42477-8 0-321-42477-8

%I Addison-Wesley Publishing Co.

%O U\$49.99/C\$61.99 416-447-5101 800-822-6339 bkexpress@aw.com

%O <http://www.amazon.com/exec/obidos/ASIN/0321424778/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0321424778/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0321424778/robsladesin03-20>

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

%P 587 p. + CD-ROM

%T "Secure Programming with Static Analysis"

Part one is an introduction to software security and static analysis. The authors define static analysis as any means of assessing the programming or code without executing the program. Chapter one states that defensive programming (coding in such a way as to deal with unexpected submissions) will protect against errors, but possibly not against a deliberate adversary, and that adding security features to an application will not necessarily make for a secure program. There is a general outline of various types of software problems, and the advantages of using static analysis early in the development process. Chapter two describes the different types of static analysis and their uses. How to use static analysis as part of overall code review is covered in chapter three. Chapter four details the internal structures and functions of static analysis.

Part two examines software problems that have been all too common in our application environment. Chapter five looks at the right and wrong ways to handle input. The ubiquitous buffer overflow gets two chapters: six discusses string issues, while seven deals with integer (particularly counter and pointer) situations. Error and exception handling is detailed in chapter eight.

Special application environments and requirements make up part three. The Web is handled, in a generic manner, in chapter nine. Chapter ten

specializes in XML (eXtensible Markup Language) and Web services. Privacy, personally identifiable information, and pseudorandom number generation all get put into chapter eleven. The special issues of privileged programs and processes are noted in chapter twelve.

Part four demonstrates static analysis in practice. This is a set of instructions for using the Fortify Code Analyzer and Audit Workbench programs, which are provided on the CD. Chapter thirteen is for Java, and fourteen for the C language. (Since the rest of the book has been detailed, helpful, and quite free of taint of bias, this final sales pitch seems acceptable.)

Code review and analysis gets mentioned in other works on secure programming, but this guide goes into technicalities that can be of considerable use to the developer. Chess and West have also made a very solid case that static analysis is a more effective way to find highly significant faults, and correct them earlier in the process. I commend this both to developers, and to those in security who need to better manage a secure development process.

copyright Robert M. Slade, 2008 BKSCPWSA.RVW 20080219
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 19

Sunday 8 June 2008

Contents

- [Control-Alt-SCRAM; update reboots nuke plant](#)
[Brian Krebs](#) via [David Leshner](#)
 - [Sensor error caused \\$1.4 bill B2 crash!](#)
[David A. Fulghum](#) via [Paul Saffo](#)
 - [UK bank takes 9 months to combine computer systems](#)
[Peter Mellor](#)
 - [Online registration for US visa waiver scheme from August 2008](#)
[Donald Mackie](#)
 - [The ID Divide: Peter Swire and Cassandra O Butts](#)
[Monty Solomon](#)
 - [ISP Secretly Added Spy Code To Web Sessions: Ryan Singel](#)
[Monty Solomon](#)
 - [Advice from HM Revenue & Customs on NI number fraud](#)
[Peter Mellor](#)
 - [Stanford employees' data on stolen laptop](#)
[PGN](#)
 - [Sometimes the computer is right...](#)
[David Hollman](#)
 - ["She'll never fail to stop at a railroad crossing ever again"](#)
[Jeff Rosen](#) via [Mark Brader](#)
 - [Experts Revive Debate Over Cellphones and Cancer](#)
[Tara Parker-Pope](#) via [Monty Solomon](#)
 - [Re: Risks in Instant Runoff Voting](#)
[Richard Gadsden](#)
 - [Re: Fire at The Planet takes down thousands of websites](#)
[Paul Czyzewski](#)
 - [Re: Whose Rules Does Your Media Center Play By?](#)
[Steve Wildstrom](#)
 - [Re: Beware of Error Messages At Bank Sites](#)
[Paul Czyzewski](#)
 - [Re: An iTunes ... problem Apple will never fix](#)
[Henry Baker](#)
[Max Power](#)
 - [Info on RISKS \(comp.risks\)](#)
-

#Control-Alt-SCRAM; update reboots nuke plant

<David Lesher <wb8foz@panix.com>>

Thu, 5 Jun 2008 17:47:22 -0400 (EDT)

Brian Krebs, *The Washington Post*, 5 Jun 2008

<http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958_pf.html>

A nuclear power plant in Georgia was recently forced into an emergency shutdown for 48 hours after a software update was installed on a single computer. The incident occurred on March 7 at Unit 2 of the Hatch nuclear power plant near Baxley, Georgia. The trouble started after an engineer from Southern Company, which manages the technology operations for the plant, installed a software update on a computer operating on the plant's business network.

The computer in question was used to monitor chemical and diagnostic data from one of the facility's primary control systems, and the software update was designed to synchronize data on both systems. According to a report filed with the Nuclear Regulatory Commission, when the updated computer rebooted, it reset the data on the control system, causing safety systems to errantly interpret the lack of data as a drop in water reservoirs that cool the plant's radioactive nuclear fuel rods. As a result, automated safety systems at the plant triggered a shutdown. ...

#Sensor error caused \$1.4 bill B2 crash!

<Paul Saffo <paul@saffo.com>>

Fri, 6 Jun 2008 18:53:02 -0700

[ouch! Reminds me of an early error with the Airbus fly-by-wire system that ended up with a controlled flight into terrain bec of a computer problem. -p]

Forgotten Lesson Caused B-2 Crash, 6 Jun 2008

David A. Fulghum/Aerospace Daily & Defense Report

Crews and maintainers never formally recorded information on a vulnerability involving the B-2's air pressure sensors and the simple workaround crews came up with to mitigate it, a crucial omission that set the stage for a Feb. 23 B-2 crash in Guam.

Aircrews and maintenance teams learned about the sensors' susceptibility to moisture during a Guam deployment in 2006. They also discovered that turning on the 500-degree pitot heat would quickly evaporate the water and the flight computer would receive normal readings.

But the information was not formally 'captured' in maintenance or lessons-learned publications, said Maj. Gen. Floyd Carpenter, president of the accident investigation board and vice commander of 8th Air Force. The

result was that by the 2008 deployment, the information was passed on by word of mouth so that "some people knew about it and some people did not," he said during a Pentagon briefing June 5. Crews never encountered the problem at the bomber's home base of Whiteman Air Force Base, Mo.

Earlier incident

Earlier in the 2008 deployment, another B-2 had reached 70 knots in its takeoff roll when abnormal indications caused the pilot to abort. The aircraft taxied back to maintenance, the moisture was evaporated with pitot heat and the mission continued without incident.

But on Feb. 23, calibration of the sensors was done without turning the sensor heaters on. The skewed information from three of the 24 air pressure sensors on the Spirit of Kansas fed distorted information into the flight control computer. When the aircraft reached 130 knots, the computer thought it was at the 140-knot takeoff speed and rotated for takeoff.

The sensors also indicated the bomber was in a nose-down attitude so it commanded a rapid pitch up that reached 30-31 degrees before the pilots could correct and stop the climb at an altitude of about 80 feet. The effects of the low takeoff speed and high angle of attack caused the B-2's speed to deteriorate until the aircraft stalled and began a roll to the left, when its left wing tip struck the ground. At that point the pilots ejected (Aerospace DAILY, March 28).

The aircraft's remains were boxed and will be sent to the U.S., where the cockpit, seats and hatches will be used for training.

Additional information, including the crash investigators report and video, is posted on Air Combat Command's Web site at <http://www.acc.af.mil/aibreports/>.

<http://www.aviationweek.com/aw/generic/story.jsp?id=3Dnews/B-2060608.xml&headline=3DForgotten%20Lesson%20Caused%20B-2%20Crash&channel=3Ddefense>

[Also noted by Gabe Goldberg. PGN]

UK bank takes 9 months to combine computer systems

<MellorPeter@aol.com>

Fri, 6 Jun 2008 20:25:28 EDT

The system in use by building societies* for some older types of account involves a "pass book" to record transactions. With computer systems universally in use, the counter clerk no longer writes each transaction into the book by hand, but inserts the book into a printer. The system keeps track of which line on the page the previous transaction was printed on and prints the next transaction immediately below it.

Over the last 6 months or so I have found that the transactions in my pass

book are frequently overprinted on top of the previous transaction (or transactions, if I made more than one on the previous visit). When this happened again today (6th June) I asked the clerk why.

My building society (the Abbey: now a bank) merged last September with a Spanish financial institution which forced a new computer system onto it. I noticed that there was frequent chaos at the time with the system being down or running slowly. According to the clerk, the overprinting is a related problem, and is due to there being effectively two systems working in parallel, since the roll-out of the new system is not yet complete (or the merger of the two computer systems is not complete). Which system you get depends on which branch you visit, so the system at the Stevenage branch "remembers" the last transaction I made _in Stevenage_ and prints over any more recent transactions that I made at one of the branches in London, and vice versa!

* I won't go into details about what a "building society" is, for non-UK readers. Suffice it to say that they are rather like banks, and over the past few years, most of them have actually turned themselves into banks.

Peter Mellor <MellorPeter@aol.com> +44 (0)20 8459 7669

✶ Online registration for US visa waiver scheme from August 2008

<Donald Mackie <donald@iconz.co.nz>>

Wed, 4 Jun 2008 19:49:07 +1200

The US has a visa waiver scheme for visitors from a number of countries (including NZ). Citizens of those countries do not need to apply for a visa to visit the US up to 90 days. They currently complete an I94 form on the plane and are admitted (after screening) with appropriate visitor stamp in their passports. A new scheme has been announced that will require prospective visitors to register online. The website will be online from August and the system will be compulsory from January. There is a fuss in the media here (http://www.nzherald.co.nz/section/1/story.cfm?c_id=1&objectid=10514241) over the requirement to register 72 hours before travel, a problem for people making urgent business or family visits. A spokesperson on the radio today said that there will be mechanisms to address those situations, which is fine. Only one commentator has so far expressed anxiety about the greater risk which is that of security around personal information submitted to such a site. The spokesperson also said that people will be able to update their travel details online, only increasing my concerns about security. Bear in mind that the current I94 includes DOB, passport number etc. Risks self evident.

✶ The ID Divide

<Monty Solomon <monty@roscom.com>>

Sun, 8 Jun 2008 12:24:21 -0400

Addressing the Challenges of Identification and Authentication in American Society

By Peter Swire, Cassandra Q. Butts, Center for American Progress, 2 Jun 2008

How individuals identify themselves in our country grows more complex by the year. Just last month, 12 nuns were turned away from voting booths during the Indiana presidential primary because they lacked state identification (none of them drives), a stark reminder that the recent Supreme Court ruling that upheld Indiana's voter ID law poses lasting consequences to our democracy. And two years ago last month the personal identification data of 26.5 million veterans were lost from a government laptop, the latest in a series of data breaches that threaten the integrity of everyone's identification.

Those 12 nuns are among 20 million other voting age citizens without driver's licenses, and they join those 26.5 million veterans and many millions of other Americans who suddenly find themselves on the wrong side of what we call the ID Divide-Americans who lack official identification, suffer from identity theft, are improperly placed on watch lists, or otherwise face burdens when asked for identification. The problems of these uncredentialed people are largely invisible to credentialed Americans, many of whom have a wallet full of proofs of identity. Yet those on the wrong side of the ID Divide are finding themselves squeezed out of many parts of daily life, including finding a job, opening a bank account, flying on an airplane, and even exercising the right to vote. ...

http://www.americanprogress.org/issues/2008/06/id_divide.html

Full report (pdf)

http://www.americanprogress.org/issues/2008/06/pdf/id_divide.pdf

Identification and Authentication Resources page

http://www.americanprogress.org/issues/2008/06/id_resources.html

ISP Secretly Added Spy Code To Web Sessions: Ryan Singel

<Monty Solomon <monty@roscom.com>>

Fri, 6 Jun 2008 23:13:42 -0400

Ryan Singel, *WiReD* blog, 5 Jun 2008

Leaked Report: ISP Secretly Added Spy Code To Web Sessions, Crashing Browsers

An internal British Telecom report on a secret trial of an ISP eavesdropping and advertising technology found that the system crashed some unsuspecting users' browsers, and a small percentage of the 18,000 broadband customers under surveillance believed they'd been infected with adware.

The January 2007 report (.pdf) -- published Thursday by the whistle blowing site Wikileaks -- demonstrates the hazards broadband customers face when an ISP tampers with raw Internet traffic for its own profit. The leak comes just weeks after U.S. broadband provider Charter Communications told users it would be testing a technology similar to what's described in the BT document.

The report documents BT's partnership with U.K. ad company Phorm, which specializes in building profiles of ISP customers, then serving targeted ads on webpages the user visits.

From late September to early October 2006, British Telecom secretly partnered with Phorm to let the company monitor and track 18,000 of the BT's customers. Phorm installed boxes on BT's network that redirected web requests through their proxy server.

Those boxes inserted JavaScript code into every web page downloaded by the users. That script then reported back to Phorm the contents of the web page, which Phorm used to create ad profiles of a user. Additionally, Phorm purchased advertising space on prominent web sites, showing a default ad for a charity. But when a user who had previously looked at car sites visited one of those pages, he instead got an advertisement for car insurance.

The users were not informed they were being made guinea pigs for a new revenue system for BT and had no way to opt out of the system, according to the report. The JavaScript caused flickering problems for some users as the script reported back information about the content of the web page to a Phorm server. The script also crashed browsers that loaded a website that relied excessively on anchor tags. Additionally, the rogue JavaScript showed up unexpectedly in user's posts to some web forums. ...

<http://blog.wired.com/27bstroke6/2008/06/isp-spying-made.html>

Advice from HM Revenue & Customs on NI number fraud

<MellorPeter@aol.com>

Sat, 7 Jun 2008 10:26:09 EDT

The following is a link to document NIM39140 - National Insurance Numbers (NINOs): Format and Security: What to do if you suspect or discover fraud. (For non-UK readers, the NI number is the UK equivalent of the US Social Security number.)

I am sure that we all appreciate this sound advice from HMRC! :-)

<http://www.hmrc.gov.uk/manuals/nimmanual/NIM39140.htm>

Stanford employees' data on stolen laptop

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

Sun, 8 Jun 2008 10:03:37 PDT

Stanford University has notified tens of thousands of past and present employees that their personal information was on a university laptop that was stolen for people hired before 28 Sep 2007 -- possibly as many as 72,000. [Someday encrypting such data sets will become the default. PGN]

✶ Sometimes the computer is right...

<David Hollman <dah8@cornell.edu>>

Fri, 6 Jun 2008 00:57:29 +0100

Here's a case where social engineering defeated an apparently correctly working automated security system and allowed a burglary:

"An experienced jewelry thief may have hoodwinked the University of British Columbia's campus security by telling them to ignore security alarms on the night of last month's multi-million dollar heist at the Museum of Anthropology...

Four hours before the break-in on May 23, two or three key surveillance cameras at the Museum of Anthropology mysteriously went off-line.

Around the same time, a caller claiming to be from the alarm company phoned campus security, telling them there was a problem with the system and to ignore any alarms that might go off.

Campus security fell for the ruse and ignored an automated computer alert sent to them, police sources told CBC News."

Full article:

<http://www.cbc.ca/arts/story/2008/06/04/bc-ubc-security-ruse.html>

✶ "She'll never fail to stop at a railroad crossing ever again"

<msb@vex.net (Mark Brader)>

Wed, 4 Jun 2008 14:39:11 -0400 (EDT)

Posted by Jeff Rosen, 3 Jun 2008, <http://www.subchat.com/read.asp?Id=627920>

Correction: Due to incorrect information received from the Clerk of Courts Office, Diane K Merchant was incorrectly listed as being fined for prostitution in Wednesday's paper. The charge should have been failure to stop at a railroad crossing. The Public Opinion apologies for the error.

I don't know what happened here, but it's got to involve a computer, hasn't it?

[Well, it could have been a typo in the officer entering the description code. Or the officer could have been on the wrong track himself. PGN]

✂ Experts Revive Debate Over Cellphones and Cancer

<Monty Solomon <monty@roscom.com>>

Wed, 4 Jun 2008 09:03:17 -0400

Experts Revive Debate Over Cellphones and Cancer;
What do brain surgeons know about cellphone safety that the rest of us don't?
Tara Parker-Pope, *The New York Times*, 3 June 2008

Last week, three prominent neurosurgeons told the CNN interviewer Larry King that they did not hold cellphones next to their ears. "I think the safe practice," said Dr. Keith Black, a surgeon at Cedars-Sinai Medical Center in Los Angeles, "is to use an earpiece so you keep the microwave antenna away from your brain."

Dr. Vini Khurana, an associate professor of neurosurgery at the Australian National University who is an outspoken critic of cellphones, said: "I use it on the speaker-phone mode. I do not hold it to my ear." And CNN's chief medical correspondent, Dr. Sanjay Gupta, a neurosurgeon at Emory University Hospital, said that like Dr. Black he used an earpiece.

Along with Senator Edward M. Kennedy's recent diagnosis of a glioma, a type of tumor that critics have long associated with cellphone use, the doctors' remarks have helped reignite a long-simmering debate about cellphones and cancer. ...

<http://www.nytimes.com/2008/06/03/health/03well.html?partner=rssuserland&emc=rss&pagewanted=all>

✂ Re: Risks in Instant Runoff Voting

<Richard Gadsden <richard@gadsden.name>>

Wed, 4 Jun 2008 11:33:19 +0100

Peter G. Neumann* ([RISKS-25.18](#)) has missed the point of Arrow's Theorem by expressing it as identifying a problem with ranked preference systems. Arrow presumes that voters have a ranking of candidates; indeed the underlying assumption of Arrow is that voters' preference as between candidates is ordinal, not cardinal.

[* Not really. The discussion of Arrow's Theorem should actually have been more clearly attributed to the review article by Peter Baker. PGN]

Arrow's proof - that no election system can be simultaneously monotonic, deterministic, universal, unrestricted in domain and independent of irrelevant alternatives without being a dictatorship - applies not only to

ranked preference systems, but to all elections without exception. Only by rejecting the assumption of ordinality of preference, or by rejecting one of criteria, can any voting system be established. Most real election systems - including simple plurality, instant runoff and conventional runoff - fail on the criterion of independence of irrelevant alternatives (IIA); that is, a (losing) candidate or candidates can be introduced into an election or removed from an election and that will change the winner.

In many real-world elections, there is a "Condorcet" winner, ie someone who is preferred by a majority of the electorate to every other candidate (it may be a different majority in each case). If there is such a winner, then electing them fulfills Arrow's theorem. The problem is that in some elections, preferences are circular (ie $A > B$, $B > C$ and $C > A$, where $>$ represents 'is preferred to' rather than the usual 'is greater than'). Where this occurs, no system can fulfill Arrow's criteria - either the system will elect someone who would lose in a simple majority two candidate election (which fails Arrow's dictatorship criterion) or IIA will be breached, as any proposed winner can be defeated by the withdrawal of one of his opponents.

A key corollary of Arrow's theorem is that voters always have an incentive to be insincere in how they cast their votes. For example, in the 2000 US Presidential election, voters whose true preference was $Nader > Gore > Bush$ had a strong incentive to insincerely vote for Gore. Similar arguments can be applied to all electoral systems - even ones that elect a Condorcet winner, as they must have a (by definition manipulable) tie-breaker when there are circular preferences, and voters could vote insincerely to create a circularity and then manipulate the tie-breaker.

Re: Fire at The Planet takes down thousands of websites ([R 25 18](#))

*"Paul Czyzewski" <tallpaul@gmail.com>
Sat, 7 Jun 2008 20:19:10 -0700*

< [Power was restored on 2 Jun. PGN]

Actually, things didn't go that smoothly and, in fact, it appears that some users (those whose hard drives were damaged by the initial power failure) are **still** having problems.

The Planet forum (<http://forums.theplanet.com/index.php?showtopic=90185>) contains about 80 messages from the Planet, sent over the past week, on the status of their outage. It includes such highlights of the sort "now all the remaining servers are up on generators". "oops, the generator tripped its circuit breakers, so those 3000 servers are down again." "We fixed the generator." "Oops, the fix to the generator didn't work and" you get the idea.

I have no reason to doubt the competence of the Planet staff; it's not an easy problem to recover from.

Re: Whose Rules Does Your Media Center Play By? ([RISKS-25.18](#))

<Steve Wildstrom <steve_wildstrom@wdc.exchange.businessweek.com>>
Wed, 4 Jun 2008 09:07:51 -0400

Bashing Microsoft is fun-I've done it often enough myself-but in this case, EFF is barking up the wrong tree. Assuming, arguendo, that this wasn't just a dumb mistake, the party at fault is NBC. As the Microsoft spokesperson said, the Media Center code merely implements what was, at the time the code was written, an FCC requirement. The later court rejection of the broadcast flag rules didn't require changing the code, it prohibited broadcasters from implementing the flag. NBC broadcast a program with the flag set, which it should not have done, and the Media Center responded exactly the way it was supposed to, and, for the record, exactly the way Microsoft has always said it would.

Steve Wildstrom, BusinessWeek, 1200 G St NW, Suite 1100, Washington, DC 20005
Technology & You <<http://www.businessweek.com/technology/wildstrom.htm>>

Re: Beware of Error Messages At Bank Sites (Sherwood, [R 25 18](#))

<Paul Czyzewski <tallpaul@gmail.com>>
Sat, 7 Jun 2008 20:26:21 -0700

This scam sounded vaguely familiar, and I found this article, The Failure of Two-Factor Authentication, which was written by Bruce "Nostradamus" Schneier three years ago.

http://www.schneier.com/blog/archives/2005/03/the_failure_of.html

Besides the bank scam, Bruce discusses the inherent flaws in two-factor authentication, generally.

Re: An iTunes ... problem Apple will never fix (McDonald, [R-25.18](#))

<Henry Baker <hbaker1@pipeline.com>>
Wed, 04 Jun 2008 11:43:02 -0700

Alistair, This iTunes file retention bug happens to me all the time. When audio podcasts are deleted in iTunes, the underlying file is deleted. However, when video podcasts are deleted in iTunes, the underlying file isn't deleted -- there's no error message or anything. I've gotten to playing video podcasts directly from the underlying file system & deleting the files behind iTunes's back, just to make sure that the file really gets deleted. Since video files are typically much larger than audio files, the inadvertent retention of video files can quickly fill up your disk.

I haven't tried this on Mac iTunes, but I suspect that the same thing happens there, so I don't think this is an OS-specific bug.

I've given up reporting bugs to large corporations, because they don't even bother to acknowledge the email. They're too busy putting in additional misfeatures to have time to fix the ones they already have.

Re: An iTunes ... problem Apple will never fix (McDonald, [R-25.18](#))

<Max Power <dist23@juno.com>>

Wed, 4 Jun 2008 19:06:37 -0700

I ASSURE YOU THAT THE iTunes 'disk usage' bug IS REAL.

NOTE

- * iTunes (across all OSes it runs on) offers [or has access to] a built in update program [offers: Win; access: OSX]
- * Most people use that update program most of the time. Most people have the current version of iTunes
- * Apple has no obvious way to submit bugs for the software it writes. There may be ways, but I don't know what they are.
- * I am a telecommunications consultant: if I can't find a way to submit iTunes bugs to Apple, it is probable no one can.
- * UNLESS there is an outstanding telecommunications issue that makes updating Apple software more difficult or impossible [like the user living on Pitcairn, with a 56kbs link] it would reason that 90% of iTunes users are up to date.
- * It is impossible [or not highly likely] for this disk usage problem to affect older versions of iTunes.
- * I don't know where this bug originated in the iTunes version tree.

Known or Suspected 'problem areas'

Operating systems affected: ALL

(Windows family 100%, OSX assumed 100% pending proof)

TCP / IP version issues:

NONE that I know of, this is a File System issue (?) not an IP issue

User Interfaces affected: ALL CURRENT

iTunes Versions affected [addendum]

- * It is probable that all versions since the introduction of Podcasts and Vodcasts are affected by this FS or UI problem.
- * I don't know where to find an adequately detailed Apple iTunes version tree, iTunes is not Winamp.
- * This lack of traceability makes it extremely difficult to track down where this disk space issue started, much less submit a bug report.

Will Apple ever fix the problem?

Since the transmission of my original "Comp.Risks" submission I have not received a single e-mail or postal letter from Apple [asking me for clarifications of the iTunes disk usage problem]. My suspecting that Apple may never fix this is based on a total lack of contact from Apple.

It would be nice if Apple would toss one of their mini PCs my way for my

BOINC distributed computing project [for uncovering such a fundamental software design flaw] ... but Apple is an American corporation so I don't see this ever happening. As corrupt as Microsoft is [as a corporation] and as vast as its' labyrinthine bureaucracy is ... Microsoft is more responsive to bug reports.

Where is the program problem finding itself? Is this a User Interface (UI) bug and not a File System (FS) usage tracking bug? I don't know. I believe it is clearly a UI problem, but it may be a side effect of the way that iTunes interacts with the host OS file systems. Further use at my end implies it is a Vodcast problem, at least on my hardware and software platform. Podcasts seem to delete cleanly and their existence seems to be reported correctly, but I have not experimented with 20 gb+ of MP3 podcasts with this software to see if the same phenomena is at work.

MORAL:

No matter what

- * You should not be able to "delete all Vodcasts" (when disk use = 99%) and not have the podcasts continue to reside on your HD eating up space.
- * There should only be mechanisms for moving or deleting podcasts on a PC's file system for programs like iTunes.
- * RSS feed displays (be they Podcasts or Vodcasts) need to have a 1 to 1 correspondence with the files represented on the drive.
- * Programs that use [and manage] a lot of disk space need to be truthful about how the disk space is being used to the user.
- * All high profile programs need to have a clearing house for submitting bugs.

I am still working on figuring out the extent of the bug, but I don't expect it to be fixed before 2009 or 2010.

Max Power, CEO, Power Broadcasting <http://HireMe.geek.nz/>
Adelaide / Wellington / Vancouver / Seattle



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 20

Sunday 15 June 2008

Contents

- [Security hole exposes utilities to Internet attack](#)
[PGN](#)
- [Representative Frank Wolf's computer owned by China](#)
[PGN](#)
- [Hidden Code Costs Poker Players Thousands](#)
[Chuck Weinstock](#)
- [Wikipedia for medical students?](#)
[Steven M. Bellovin](#)
- [Wartime global temperature anomaly kicks the bucket](#)
[Mark Brader](#)
- [Colleges With Federal Contracts Will Have to Use New E-Verify](#)
[PGN](#)
- [Google "safebrowsing" diagnostic page](#)
[Rob Slade](#)
- [ID cards by the back door](#)
[Peter Mellor](#)
- [Spuds and system security](#)
[Rob Slade](#)
- [Clothing firm "Cotton Traders" customer database breached](#)
[Peter Mellor](#)
- [Update on ISP Actions Regarding C-Porn and Usenet](#)
[Lauren Weinstein](#)
- [Re: Risks in Instant Runoff Voting](#)
[Stewart Fist](#)
[Andrew Koenig](#)
- [Re: Stanford employees' data on stolen laptop](#)
[Hal Murray](#)
- [Re: Advice from HM Revenue and Customs](#)
[Edward Rice](#)
- [Re: She'll never fail to stop at a railroad crossing](#)
[Leonard Finegold](#)
- [Re: An iTunes ... problem Apple will never fix](#)
[Andrew M. Langmead](#)
- [Tracking the Trackers: Piatek et al.](#)
[Monty Solomon](#)

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

Security hole exposes utilities to Internet attack

<"Peter G. Neumann" <neumann@csl.sri.com>>
Fri, 13 Jun 2008 16:11:17 PDT

Attackers could gain control of water-treatment plants, natural-gas pipelines and other critical utilities because of a vulnerability in the software that runs some of those facilities. The bug has now been patched, but the vulnerability could have counterparts in other so-called supervisory control and data acquisition (SCADA) systems.

<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/06/11/financial/f015433D06.DTL&type=printable>

Representative Frank Wolf's computer owned by China

<"Peter G. Neumann" <neumann@csl.sri.com>>
Wed, 11 Jun 2008 10:54:09 PDT

[Congress Daily, 11 Jun 1008, courtesy of Marcus H. Sachs]

SPYWARE? SPY WHERE? Rep. Frank Wolf, R-Va., today said the FBI determined four of his government computers have been hacked by someone in China. Wolf, a longtime critic of the Chinese government's record on human rights, said computers in the offices of other lawmakers and at least one House committee have also been hacked and he is calling for hearings to investigate. Wolf said it seemed logical that Senate computers would also be compromised.

[*USA Today* on 13 Jun 2008 warned about leaving any digital devices unattended for even a few minutes while in China for the Olympics.]

Hidden Code Costs Poker Players Thousands

<Chuck Weinstock <weinstock@sei.cmu.edu>>
Mon, 9 Jun 2008 18:04:37 -0400

On May 29, UltimateBet.com, an online poker room, announced that it had discovered "unfair play" on its site. The press release at <http://www.ultimatebet.com/poker-news/2008/may/NioNio-Findings> discusses how they investigated the alleged cheating (a word they don't use) by certain players who worked for the previous ownership of UltimateBet and who exploited "unauthorized software". The paragraph of interest to Risks readers is:

"The fraudulent activity was enabled by unauthorized software code that

allowed the perpetrators to obtain hole card information during live play. The existence of this vulnerability was unknown to Tokwiro until February 2008 and existed prior to UltimateBet's acquisition by Tokwiro in October 2006. Our investigation has confirmed that the code was part of a legacy auditing system that was manipulated by the perpetrators. Gaming Associates, independent auditors hired by the KGC, have confirmed that the software code that provided the unfair advantage has been permanently removed."

The individuals involved targeted the highest limit games and it is my understanding that some players were hit for 6 figures. UltimateBet is or is in the process of repaying those who were cheated.

✂ Wikipedia for medical students?

<"Steven M. Bellovin" <smb@cs.columbia.edu>>
Mon, 9 Jun 2008 22:03:07 -0400

A Washington Post story

(<http://www.washingtonpost.com/wp-dyn/content/article/2008/06/09/AR2008060901043.html?hpid=topnews>)
on new iPhone applications had this:

Modality: An anatomy app for medical students. The app is filled with anatomy drawings and images linked to Google and Wikipedia for more detailed information.

Would you trust a doctor whose knowledge of anatomy came from Wikipedia?

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

[Of course, it depends on who provided the wikinformation -- and who kept it up to date as knowledge changes. PGN]

✂ Wartime global temperature anomaly kicks the bucket

<msb@vex.net (Mark Brader)>
Thu, 12 Jun 2008 01:18:51 -0400 (EDT)

This item in *New Scientist* reports on a letter in Nature by one David Thompson and three colleagues. (Long URL: you may have to join parts.)

http://environment.newscientist.com/article/dn14006-buckets-to-blame-for-wartime-temperature-blip.html?DCMP=ILC-hmts&nsref=news7_head_dn14006

Fee-paying readers can access the Nature letter here:

<http://www.nature.com/nature/journal/v453/n7195/full/nature06982.html>

Thompson's group analyzed the data set of world temperatures commonly used

in climate studies and found an unrecognized flaw in it, which could affect those studies' conclusions. What they realized was that after filtering out effects like El Nino years and volcanic eruptions, the record showed a marked dip of 0.3 degrees Celsius in 1945 -- but **not** if only temperatures taken on land were counted.

Which suggested a measurement error, and they figured out what it was. What happened in 1945 was that as Britain's Royal Navy returned to peacetime duties, they had more time to report sea temperatures! So suddenly there were **more** of their measurements in comparison to those taken by the US Navy.

And why did that matter? Because the seawater that the Americans actually measured was drawn from engine cooling-system intakes, while the British dipped a bucket into the sea. One method reads high, the other low.

Colleges With Federal Contracts Will Have to Use New E-Verify

<"Peter G. Neumann" <neumann@csl.sri.com>>
Fri, 13 Jun 2008 19:12:12 PDT

[Source: The Chronicle of Higher Learning, 13 Jun 2008]
http://chronicle.com/news/index.php?id=4674&utm_source=pm&utm_medium=en

All colleges and universities entering into federal-government contracts will be required to use the Department of Homeland Security's E-Verify system to establish the immigration status of newly hired employees and all employees working on such contracts, under an executive order signed this week by President Bush.

E-Verify is the federal governments automated system for allowing employers to verify job applicants eligibility to work as U.S. citizens, legal permanent residents, or authorized immigrants. When an employer submits an applicants name and personal information for eligibility verification, E-Verify checks that information against Social Security Administration and Homeland Security Department databases.

[See the USACM website for testimony by PGN, Annie Anton, and most recently Gene Spafford (on EEVS, the Employee Eligibility Verification System, precursor of E-Verify). It is evident that the warnings of these testimonies were not heeded.

Google "safebrowsing" diagnostic page

<Rob Slade <rMslade@shaw.ca>>
Sun, 08 Jun 2008 11:23:39 -0800

Google has a set of tools for Webmasters at
<http://www.google.ca/webmasters/tour/tour1.html>

You have to sign up to use them, but you can, seemingly, get at some of the tools individually if you know the URL. One that is making the rounds is a diagnostic page for the safety of a URL, at:

<http://www.google.com/safebrowsing/diagnostic?site=> (Actually, if you just put that in your browser you get a "Bed Request" page: you have to fill in a URL on the end.)

I tried it out on an advertising site that has been used a lot, recently, for referrals/redirections to malware, and it got a clean bill of health.

I've tried it with a site that has been serving a version of Nuwar for at least a week, and confirmed that the site was still serving the malware directly. (This is not a referral situation.) Google gave it a clean bill of health.

I'd say the Google page was unreliable at the very best.

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

ID cards by the back door

*<Peter Mellor <MellorPeter@aol.com>>
Sat, 14 Jun 2008 09:03:55 EDT*

The gist of this report is that the "National Entitlement Card" contains a concealed chip with lots of personal information, and may be part of a scheme by the British Government to introduce identity cards by stealth.

The author, Stuart Hill, who lives in the Shetland Isles, has done his research, and this should not be dismissed as just another paranoid conspiracy theory.

<http://www.idcardsexposed.com/>

-- Excerpt from start of report --

In Shetland a vulnerable section of the community is being used to pilot a scheme that threatens our fundamental freedoms. It is quite clear that the new 'National Entitlement Card' that provides access to free travel for the elderly and disabled, in fact marks the introduction of ID Cards by the back door.

My research shows that:

This is an EU scheme being carried out by the UK government and the Scottish Executive. The government is planning a stealth programme for ID cards, the steps for which are:

- introduction, the current stage where we are offered the bribe of free travel

- full coverage, everybody is required to have one
- full compulsion sounds good in a free country - and finally
- full identity services availability - in other words you can get no access to services without the card.

[...]

Recently I was denied free travel on the bus because I refused to submit my new 'smart' card to the card reader on the bus. Before the machines were fitted it was sufficient to show the card to the driver. This time it was apparently not enough that I could show my card -- it had to go on the machine for data to be recorded. As far as I know, I have not given permission for my personal details to be collected in this way.

-- End of excerpt --

Peter Mellor <MellorPeter@aol.com> +44 (0)20 8459 7669

Spuds and system security

<Rob Slade <rMslade@shaw.ca>>

Fri, 13 Jun 2008 14:50:16 -0800

Recently, there has been a great deal of concern over the rise in prices of common staple food grains. A frequently cited cause for this price jump is international speculation in commodity markets, and the disproportionate aspect this can have on the price of the commodities themselves, quite apart from the usual cycles of supply and demand.

What fewer people may know is that the UN declared 2008 as the international year of the potato. (They did this, of course, some time ago, so the contrast in notions becomes even more intriguing.)

There is some irony in that, but it gets better. (Both from the perspective of irony, and from the point of view of useful analogies for infosec.)

The potato (the "humble" potato, as it is frequently described) is suitable to a great many climatic conditions, and is generally more productive than grain crops (and *much* more productive than meats, etc.) It is also surprisingly nutritious.

(Ah! I hear you cry, what about the Potato Famine? Well, in that case the potato was, oddly, a victim of its own success. We know, or should know, the dangers of the monoculture, which was what led to the famine. [And that topic has relevance to infosec as well, but it has been amply discussed elsewhere.] However, what is less well known is that the introduction of the potato, 250 years prior to the famine, led to a 5-8 fold increase in the population of Ireland over those twenty-five decades, due to an increase in both food source and in nutrition.)

So, what about world food crops, commodities, and skyrocketing prices? If

we convinced people to grow potatoes, wouldn't we just become dependent upon potatoes, and then there would be speculation in potato futures? Well, oddly, it seems not.

Grain, when harvested, is fairly dry, and can easily be dried even more for storage and shipment. And, to pretty much anyone except a pasta maker, wheat flour is wheat flour. You can make any product you want out of basically any flour you can get.

Potatoes are wet. They get used fresh, for the most part. (The technical advances in producing dried mashed potatoes seems to parallel that of artificial intelligence: there is a lot of interest, and a lot of work, but those who have tried the results can tell you that there is work yet to be done.) Also, people who use and eat potatoes tend to have preferences. (And there are a great many varieties of potatoes. Remember that monoculture bit?)

It seems that potatoes are one of the few staple crops that are resistant to commodity markets (however susceptible it may be to the blight).

So, what's the point for infosec? Remember the lessons of security architecture. Build your architecture based on resilient and resistant technologies, not on the most popular. It's not a new lesson: it rests on the foundation of risk management which should be foundational to all security.

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

✶ Clothing firm "Cotton Traders" customer database breached

<MellorPeter@aol.com>

Sat, 14 Jun 2008 10:29:02 EDT

The size of the breach (number of records compromised) has not been confirmed, but is said to be "up to 38,000. Attackers gained access to customers' addresses and (worryingly) data used in "card not present" transactions.

The report states: "Apacs, the trade association for the payment industry, said a specialist police force was investigating the case." There is a rumour (not mentioned in the report) that, although the breach occurred "earlier in the year", Apacs only informed the banks a few weeks ago and they are still dealing with it.

For details, see <http://news.bbc.co.uk/1/hi/technology/7446871.stm>

Peter Mellor <MellorPeter@aol.com> +44 (0)20 8459 7669

Update on ISP Actions Regarding C-Porn and Usenet

<Lauren Weinstein <lauren@vortex.com>>

Tue, 10 Jun 2008 17:02:30 -0700

[From Network Neutrality Squad. PGN]

Update on ISP Actions Regarding C-Porn and Usenet

<http://lauren.vortex.com/archive/000390.html>

Greetings. The related ISPs have been working to clarify aspects of the New York Times story that I discussed earlier today (<http://lauren.vortex.com/archive/000389.html>).

The upshot is interesting. In contrast to the implications of the Times piece, it appears that U.S. ISPs (unlike a newly penned deal in France involving French ISPs) will not for the moment be actively blocking any "class" of Web content, but rather will work to remove c-porn sites from their servers (something most people apparently assumed they'd been doing anyway ...).

So the big to-do from the politicos about this aspect seems to best be filed under grandstanding.

But there is a very disturbing additional element to this story. Time Warner Cable says that they are cutting off subscriber access to all Usenet newsgroups (child porn was found in 88 of the vast number of total newsgroups). Sprint is cutting off 10's of 1000's of alt.* newsgroups (and what a war it was back when those were created long, long ago!) Verizon plans "broad" newsgroup cutoffs.

While Usenet newsgroups are certainly not the draw that they were many years ago, they still have an important role to play in the free exchange of legal information on the Internet today.

Using the presence of illicit materials in some portion of a content stream as an excuse to abolish or decimate the legal content is inexcusable. In fact, that sort of "guilt by association" and "we can get away with this because most people don't know about it" action is the very essence of a particularly insidious form of censorship.

Of course, the ISPs could argue that they're under no legal obligation to carry Usenet newsgroups in any form. This is true. But then, most ISPs aren't under a legal mandate to provide connectivity to any given Web sites, either.

So one might wonder, given these ISPs' eagerness to hoist much or all of the completely legal content of Usenet on the petard of fettering out c-porn, which aspects of the Internet will be next to fall into the line-of-sight of their big red cutoff switch?

Lauren Weinstein lauren@vortex.com +1 818 225-2800 <http://www.pfir.org/lauren>
PFIR <http://www.pfir.org> Network Neutrality Squad - <http://www.nnsquad.org>

PRIVACY Forum - <http://www.vortex.com> Lauren's Blog: <http://lauren.vortex.com>

Re: Risks in Instant Runoff Voting (Gladsen, [RISKS-25.19](#))

<Stewart Fist <stewart_fist@optusnet.com.au>>

Mon, 9 Jun 2008 12:50:29 +1000

Your correspondents on preferential voting systems rightly point out that no preferential or proportional voting system can ever faithfully reproduce the will of the people, because no such perfect measure of group-will exists. At best, an electoral system can only generally reproduce the expressed intentions of the voting public, and the preferential system probably does this best.

While people vote for a candidate, they also vote against other candidates. So Richard Gladsen's statement:

> For example, in the 2000 US Presidential election, voters whose true
> preference was Nader>Gore>Bush had a strong incentive to insincerely vote
> for Gore.

can equally translate to "... had a strong incentive to sincerely vote against Bush". A preferential system would have permitted the Nader voters to sincerely vote for Nader>Gore and against Bush, if that was their intention ... or, indeed, to vote for Nader>Bush and against Gore, if that was equally their intention.

So the claim that "voters always have an incentive to be insincere in how they cast their votes" is not really valid.

Behind this discussion is also the assumption that the only concern when choosing a voting system is that it closely reflects this idealistic expression of group-will. Of equal importance is that the system leads to a stable system of government, and that this stable government does not become entrenched.

The electoral system should tend to err on the side of "overreflecting" the will of the people -- and thereby giving the governing party a reasonable majority so that it is strong and stable enough to make some (possibly unpopular) changes to tax and other laws -- yet allow for quick and clean changes of government when a swing in public attitudes against the governing party occurs.

In other words, it needs to be a "toggle" -- where a small change in public position, should on a regular basis, reflect a larger proportional change in political representation, and possibly a change of government. You often need this to overcome the advantage of incumbency.

Proportional representation systems tend to create unstable governments for this reason.

Lastly, stable political systems appear to depend on the country having two, or possibly three (at most) major parties -- not dozens. This means that the parties will go into an election with clearly established and reasonably-defined policies on display. Alternative systems, like that of Italy, produce a multiplicity of small parties which then must form unstable coalitions through backroom deals in order to govern. So priorities and policies are largely set after the election, and governments can be blackmailed by a small party in the coalition.

Preferential systems tend to encourage voters to select a major party as their favourite, while also allowing them to give support and encouragement to individuals/small parties like Nader in America, and the Green/Democratic parties elsewhere. These individuals can then sometimes challenge the majors for the swinging vote -- and, in effect, create the "toggle" -- which has the effect of "keeping the bastards honest" (the slogan of Australia's small third party).

Stewart Fist, 70 Middle Harbour Rd, LINDFIELD, NSW 2070 Australia
Ph +61 2 9416 7458 stewart_fist@optusnet.com.au

✉ Re: Risks in Instant Runoff Voting (Gladsen, [RISKS-25.19](#))

<"Andrew Koenig" <ark@acm.org>>
Mon, 9 Jun 2008 12:43:39 -0400

Richard Gladsen claims that Arrow's Theorem proves that every election system gives voters a reason to vote insincerely.

I remember reading an article many years ago, probably by Martin Gardner, that claims that under approval voting, there is never a reason to vote insincerely. Approval voting is very simple: Each voter can cast zero or one votes for each candidate; all votes counts equally. The candidate with the largest number of votes wins. Note that voting for every candidate is equivalent to not voting at all, and that approval voting degenerates to traditional voting if there are only two candidates.

It should be clear that approval voting will elect the candidate that the largest number of voters find acceptable (as defined by their willingness to vote for that candidate), and that this candidate might not be the favorite of the largest number of voters. We can argue separately about that property of approval voting. But I think my recollection is correct that under approval voting, there is never any reason to vote insincerely.

✉ Re: Stanford employees' data on stolen laptop ([RISKS-25.18](#))

<Hal Murray <hmurray@megapathdsl.net>>
Sun, 08 Jun 2008 19:15:11 -0700

> [Someday encrypting such data sets will become the default. PGN]

Then we'll just have a different set of RISKS, and Murphy says they will be harder to understand and explain.

Do you think people will use good passwords? Do you think they will write them down?

I'll bet companies would try to wiggle out of notifying victims when a laptop is stolen: Your data is safely encrypted. Why should we worry everybody?

I was going to suggest that sensitive data shouldn't be stored on laptops. I'll bet the alternatives are worse, or at least more complicated to analyze and explain.

Re: Advice from HM Revenue and Customs (Mellor, [RISKS-25.19](#))

<Edward Rice <ehrice@his.com>>

Wed, 11 Jun 2008 21:48:22 -0400

I queried HMRC for further information and received the following explanation of that web page.

At 10:50 AM +0100 6/11/08, Storey, Michael (CustCon Online Services) wrote:

>Thank you for your e-mail. The text on this page has been withheld from
>the general public due to exemptions in the Freedom of Information Act
>2000.

>The manuals used by Her Majesty's Revenue & Customs (HMRC) are written for
>internal instructional purposes and because of that we have to withhold
>certain information when these manuals are published to the website as it's
>not intended for public consumption. These manuals are published in line
>with the Code of Practice on Access to Government Information.

>Michael Storey, HMRC Web Team

Re: She'll never fail to stop at a railroad crossing ([R 25 19](#))

<Leonard Finegold <L@drexel.edu>>

Sun, 8 Jun 2008 16:13:57 -0400

My physician was trying to enter a diagnosis into his computer, during an office visit. The computer insisted on entering Prostitute for me; he was trying to put in Prost ate.

He did an end-run.

PS. I'm no prostitute, although some people think that most faculty members are (intellectually).

Re: An iTunes ... problem Apple will never fix (Power, [RISKS-25.19](#))

<"Andrew M. Langmead" <aml@world.std.com>>

Sun, 8 Jun 2008 15:31:01 -0400

Max Power seems to have overlooked the selection "Provide iTunes Feedback" from the "Help" menu" or his search seemed to have not included anything as obvious as entering "itunes bug report" into a search engine like Google.

I guess the risk here software defects can exist by users failing to tell the software publisher when the software fails to meet their needs, and that users will choose inappropriate avenues to vent their frustration.

[This and related comments were received from many readers.

For example, try <http://bugreport.apple.com/>. PGN]

Tracking the Trackers: Piatek et al.

<Monty Solomon <monty@roscom.com>>

Wed, 11 Jun 2008 00:30:49 -0400

Michael Piatek, Tadayoshi Kohno, Arvind Krishnamurthy
University of Washington, Department of Computer Science & Engineering

Overview

As people increasingly rely on the Internet to deliver downloadable music, movies, and television, content producers are faced with the problem of increasing Internet piracy. To protect their content, copyright holders police the Internet, searching for unauthorized distribution of their work on websites like YouTube or peer-to-peer networks such as BitTorrent. When infringement is (allegedly) discovered, formal complaints are issued to network operators that may result in websites being taken down or home Internet connections being disabled.

Although the implications of being accused of copyright infringement are significant, very little is known about the methods used by enforcement agencies to detect it, particularly in P2P networks. We have conducted the first scientific, experimental study of monitoring and copyright enforcement on P2P networks and have made several discoveries which we find surprising. ...

<http://dmca.cs.washington.edu/>

FAQ

<http://dmca.cs.washington.edu/faq.html>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 21

Sunday 29 June 2008

Contents

- [Federal Agency Grounds Light Jet Used as Air Taxi](#)
[Matthew Wald](#)
- [Spyware bill cloaks a mini-UCITA](#)
[Ed Foster via Monty Solomon](#)
- [Wireless systems called disruptive](#)
[Robert P Schaefer](#)
- [More on election system integrity](#)
[Gene Wirchenko](#)
- [Re: Risks in Instant Runoff Voting](#)
[Scot Drysdale](#)
- [Chrysler announces the rolling WiFi hotspot automobile](#)
[Drew Lentz](#)
- [X-rated SMS case gives employees some privacy guarantees](#)
[John Timmer via Monty Solomon](#)
- [Attorney-client calls from jail recorded](#)
[Joel Garry](#)
- [HTML comments reveal corporate weakness](#)
[jidanni](#)
- [Photos and laptop crypto](#)
[Rob Slade](#)
- [Michael Fiola fired](#)
[Gene Wirchenko](#)
- [REVIEW: "Challenges to Digital Forensic Evidence", Fred Cohen](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

✉ Federal Agency Grounds Light Jet Used as Air Taxi: Matthew Wald

<"Peter G. Neumann" <neumann@csl.sri.com>>
Sun, 15 Jun 2008 21:12:54 PDT

On 5 Jun 2008, both engines of an Eclipse 500 (a light jet popular as an air taxi of small corporate plane) became stuck at full throttle on approach to

landing. The pilots aborted the landing, flew around while looking through the manual, and discovered procedures for failure of one engine control or the other, but not both. "They shut down one engine and then lost control of the other, because of a possible software flaw." They were able to land safely, although blowing out the tires.

"A week later, the Federal Aviation Administration issued an emergency order Thursday grounding the planes of that model until the throttle controls can be inspected."

[Source: Matthew L. Wald, *The New York Times*, 13 Jun 2008; PGN-ed]

✶ Spyware bill cloaks a mini-UCITA

<Monty Solomon <monty@roscom.com>>

Mon, 16 Jun 2008 14:28:51 -0400

By Ed Foster, Section The Gripeglog, Mon Jun 16, 2008

The holy grail for the software industry's political muscle has long been what in UCITA was called "electronic self help" - the right of software publishers to remotely disable their software on the mere suspicion that it hasn't been paid for. UCITA was ultimately stopped, but last Wednesday the Senate Commerce Committee held a hearing on a bill that nominally is supposed to fight spyware but seems intended to make remote disabling legal.

<http://www.gripe2ed.com/scoop/story/2008/6/16/1219/71034>

✶ Wireless systems called disruptive

<"Schaefer, Robert P \{(US SSA)\}" <robert.p.schaefer@baesystems.com>>

Wed, 25 Jun 2008 08:23:40 -0400

I caught this in *The Boston Globe*, 25 Jun 2008, under "Wireless systems are called disruptive", but found a better reference here:

"Wireless systems used by many hospitals to keep track of medical equipment can cause potentially deadly breakdowns in lifesaving devices such as breathing and dialysis machines, researchers reported Tuesday in a study that warned hospitals to conduct safety tests."

<http://www.chicagotribune.com/news/local/chi-ap-med-microchipdangers.0.6525457.print.story>

The research was published in JAMA under the title "Electromagnetic Interference From Radio Frequency Identification Inducing Potentially Hazardous Incidents in Critical Care Medical Equipment".

A quote: "Results In 123 EMI tests (3 per medical device), RFID induced 34 EMI incidents: 22 were classified as hazardous, 2 as significant, and 10 as light."

<http://jama.ama-assn.org/cgi/content/short/299/24/2884>

✂ More on election system integrity

<Gene Wirchenko <genew@ocis.net>>
Wed, 25 Jun 2008 08:51:22 -0700

Yet another story on the vulnerability of voting systems:
Rogue code could seriously skew US presidential election results
<http://www.itbusiness.ca/it/client/en/home/News.asp?id=48929>

✂ Re: Risks in Instant Runoff Voting (Koenig, [RISKS-25.20](#))

<Scot Drysdale <scot@cs.dartmouth.edu>>
Mon, 16 Jun 2008 22:37:02 -0400

I don't know what Martin Gardner said, but if "voting insincerely" means voting something other than your true preference in order to get a desired result, then there certainly can be a reason for voting insincerely under approval voting. Suppose 60% of the voters prefer A but also are happy with B, 20% like only B, and 20% like only C. Then if the 60% vote sincerely they would list A and B, and B (with 80% approval) would be the elected candidate. But if the 60% only vote for A, then A gets elected. Thus voting insincerely (saying that you do not approve B when in fact you do approve B) leads to a better result.

Instant runoff can also lead to unfortunate results. Suppose that there are 11 candidates. A1 through A10 are each preferred by 10% of the voters and hated by the other 90%. B is everybody's strong second choice, liked almost as much as their first choice. In instant runoff B is eliminated in the first round, and the election will eventually elect a candidate that 90% of the voters hate, instead of a candidate that everybody is happy with. Here approval voting works much better, because B will appear on every ballot and will be elected (if voters vote sincerely).

✂ Chrysler announces the rolling WiFi hotspot automobile

<Drew Lentz [drew@drewlentz.com]>
Mon, 23 Jun 2008 6:11 xDT

[From Dave Farber's IP]

Thought you (and the list) might be interested in this. Chrysler's announcement to deploy Wi-Fi in vehicles to me spells opportunity for malicious script kiddies and a "rolling" increase in the 2.4 noise floor.

<http://www.itwire.com/content/view/18956/53/>

[See IP archives for further discussion. PGN]

IP Archives: <http://www.listbox.com/member/archive/247/=now>

X-rated SMS case gives employees some privacy guarantees

<Monty Solomon <monty@roscom.com>>

Fri, 20 Jun 2008 11:46:17 -0400

John Timmer, Arstechnica, 20 Jun 2008

Yesterday, the 9th Circuit Court released a ruling with huge implications for privacy rights. In a case involving personal use of a work-provided messaging service by a police officer, the court held that the employee had a right to expect that the privacy of his messages would be honored, and that any police access to those messages had to meet the standards of a reasonable search. The ruling provides an extensive space for workspace privacy, at least as long as the NSA isn't involved.

The decision arises from Quon vs. Arch Wireless (PDF), which has a rather complicated background. Jeff Quon was a member of the city of Ontario, CA SWAT team. The city provides its officers with access to a wireless text messaging pager provided by Arch Wireless, which came with a monthly character limit. Formally, the announced departmental policy was that the content of the messages sent could be audited at any time. In practice, however, the pagers were handled quite differently. The department never viewed their content, and simply asked users to pay any charges for running over the character limit.

Things proceeded uneventfully until the day when, as the decision phrases it, "Lieutenant Duke grew weary of his role as bill collector." The department decided to determine if the character limit was too low for departmental business, so they requested a copy of all messages on their account from Arch Wireless with the intent of determining whether business or personal use was driving the overage charges. With the contents in hand, they discovered many of Quon's messages were both personal and X-rated. An internal investigation ensued, and Quon and the people he exchanged messages with sued the city, its police department, and Arch Wireless. ...

<http://arstechnica.com/news.ars/post/20080620-x-rated-sms-case-gives-employees-some-privacy-guarantees.html>

Attorney-client calls from jail recorded

<Joel Garry <joel-garry@cox.net>>

Sat, 21 Jun 2008 10:50:38 -0700

A jail telephone system would record all calls, except those to numbers listed in an attorney database. The database was incomplete - most obviously in not containing attorney's direct lines or cellphones.

California law prohibits recording calls from jail between inmates and attorneys (just as doctors and patients, and ministers and penitents). It may be a felony with up to a \$5,000 penalty per call. One attorney found out when the prosecutors gave him a cd with his recorded calls on it. The San Diego County Sheriff's Department says it was a glitch in the telephone system. The extent of the problem is unknowable. Prosecutors had access to the recordings from their PC's. "We thought we had a better database" said Sheriff's Department Legal Advisor Sanford Toyen.

The system has been turned off; investigations and court paper filings are underway. The system is being changed to give a number for attorneys to call to be added to the database.

One risk would be assuming a poorly designed technology driven system will be adequate to protect legally-required privacy. Poor design decisions include assuming perfect data in the database, assuming Sheriff's Department users would be able to assess such risk, and assuming telephone users would both hear and properly understand an aural message that the call is being recorded. Another risk may be added by the change: an opt-out system isn't fast enough unless done properly (read: expensive). Lawyer involvement is left as an exercise for the cynical.

http://www.signonsandiego.com/uniontrib/20080621/news_1n21calls.html
<http://www.garry.to>

#HTML comments reveal corporate weakness

<jidanni@jidanni.org>

Tue, 24 Jun 2008 02:03:01 +0800

We all know of the supposedly invisible parts of PDF documents, but how about HTML comments? Beside the typical

`<!-- headline Comes Here -->`

`<!-- Quick Links Section -->`

`<!-- Main Content Section -->`

here's one from my million dollar retirement account:

`<!-- ~~~~~concreate row that makes ns47 beahve~~~~~-->`

So we see behind the steely corporate facade that if they don't "concreate" that row, then "ns47" won't "beahve", probably bringing the entire house of cards down.

#Photos and laptop crypto

<Rob Slade <rMslade@shaw.ca>>

Sun, 15 Jun 2008 13:21:10 -0800

The lead article/editorial in Bruce Schneier's latest CryptoGram

(<http://www.schneier.com/crypto-gram.html>) points out the foolishness in warning people to beware of terrorists taking pictures. Millions of people take billions of pictures every year for legitimate or innocent reasons, and the major terrorist attacks have not involved terrorists walking around taking photographs of the targets. It doesn't make sense to try and protect yourself by raising an alarm about an activity that is probably (*extremely* probably) not a threat.

Rather ironically, the second piece talks about the fact that your laptop may be searched when you fly to another country, and the advisability of laptop encryption. Leaving aside privacy and legality concerns, Schneier is for encryption.

Now, I don't fly as much as some, but more than many. Since I'm a security researcher, I've got all kinds of materials on my laptop that would probably raise all kinds of flags. I've got files with "virus," "malware," "botnet," and all kinds of other scary terms in the filenames. (I've got a rather extensive virus zoo in one directory.) Nobody at immigration has ever turned a hair at these filenames, since nobody at immigration has ever asked to look at my laptop. (Even the security screeners don't ask me to turn it on as much as they used to, although they do swab it more.)

I'm not arguing that people shouldn't encrypt materials on their laptops: it's probably a good idea for all kinds of reasons. However, unless I'm very fortunate in my travels (and, from my perspective, I tend to have a lot more than my fair share of travel horror stories), the risk of having immigration scan your laptop is not one of them.

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

✂ Michael Fiola fired

<Gene Wirchenko <genew@ocis.net>>
Thu, 19 Jun 2008 08:14:32 -0700

This one is nasty. Mr. Fiola was abruptly fired for having child pornography on his employee-issued laptop, but now, it seems that there was insufficient evidence to show that he downloaded it. His life has been hellish for the last 18 months though:

<http://www.itbusiness.ca/it/client/en/home/News.asp?id=48856>

✂ REVIEW: "Challenges to Digital Forensic Evidence", Fred Cohen

<Rob Slade <rmslade@shaw.ca>>
Mon, 23 Jun 2008 12:19:36 -0800

BKCHTDFE.RVW 20080318

"Challenges to Digital Forensic Evidence", Fred Cohen, 2008,
1-878109-41-3, U\$39.00
%A Fred Cohen
%C 572 Leona Dr, Livermore, CA 94550
%D 2008
%G 1-878109-41-3
%I Fred Cohen and Associates
%O U\$39.00 925-454-0171 all.net
%O <http://www.amazon.com/exec/obidos/ASIN/1878109413/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/1878109413/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/1878109413/robsladesin03-20>
%O Audience s+ Tech 2 Writing 2 (see revfaq.htm for explanation)
%P 122 p.
%T "Challenges to Digital Forensic Evidence"

Fred Cohen knows his stuff when it comes to digital forensics, despite the fun he has with legalities in the frontmatter of this book. Cohen states, in chapter one, he wrote the book because of the mistakes he had seen people make when bringing technical materials into a legal setting. The work is a solid background for a forensic examiner, and covers a number of areas that are missed in most of the current literature on this topic. Forensics is more than simply getting bits out of a given operating filesystem.

Chapter two concentrates on the errors or problems that arise in the process of collecting evidence. Many computer forensics books list the sections that should be included in a written report, but this author provides, in chapter three, practical advice on both wording and approaches, including such aspects as the reporting of errors in previously submitted reports. Chapter four demonstrates difficult situations, some covered in prior chapters and some new, based on actual cases.

Chapter five reiterates and emphasizes a point that Cohen raises frequently throughout the book: as an expert, you are working within, and subject to, an adversarial system and all its attendant limitations, but your primary responsibility is to the truth. Being honest in your work and statements is the basis for all of your testimony. As chapter six points out, it is also the best way to avoid being challenged.

There are many books that talk about forensic tools: this isn't one of them. There are a number of works that address specifics of file systems and storage devices: this isn't one of them. A few texts even address some aspects of the investigative process and management: Cohen addresses some of those issues. However, I have not seen any other guides that will tell you, clearly and plainly, how to avoid the most common failings of technical experts trying to provide evidence in a decidedly non-technical legal system.

copyright Robert M. Slade, 2008 BKCHTDFE.RVW 20080318
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 22

Tuesday 8 July 2008

Contents

- [InciWeb map coordinate errors for California fire](#)
[Henry Baker](#)
- [Oyster and Mifare cracked: NXP sues to silence Oyster researchers](#)
[PGN](#)
- [Free Berlin subway rides](#)
[Debora Weber-Wulff](#)
- [Citibank ATM breach reveals PIN security problems](#)
[Jordan Robertson](#)
- [Web-based SSH key generation with escrow](#)
[Tina Bird](#)
- [ComCast in Concrete?](#)
[Robert P Schaefer](#)
- [State Dept: Celebrity passport files viewed repeatedly - CNN.com](#)
[PGN](#)
- [California's Super-Stupid Anti-Science Cell Phone Law Takes Effect](#)
[Lauren Weinstein](#)
- [Re: HTML comments reveal corporate weakness](#)
[Ivor Hewitt](#)
- [Re: Approval voting and sincerity](#)
[Andrew Koenig](#)
[Dag-Erling Smørgrav](#)
- [REVIEW: "The dotCrime Manifesto", Phillip Hallam-Baker](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

Map coordinate errors for California fire

<Henry Baker <hbaker1@pipeline.com>>
Thu, 03 Jul 2008 09:11:01 -0700

InciWeb is (apparently incorrectly) reporting the location of the "Gap" fire as 34.487 latitude, -119.783 longitude:

<http://165.221.39.44/incident/1384/>

This places the fire almost on Highway 154, and a number of miles away from the description of the fire location as "The Gap Fire started at approximately 5:45p.m. on July 1 in the West Camino Cielo area, 4 miles west of State Highway 154 in Los Padres National Forest".

Google/Keyhole has the more-or-less correct location as 34°30'1.34"N, 119°51'26.50"W (=N34.50036 W119.85736), which places it very near West Camino Cielo, as reported.

<http://bbs.keyhole.com/ubb/download.php?Number=1198058>

I would be willing to bet that this discrepancy is caused by conversion among the plethora of different latitude/longitude formats, some having decimal degrees, some having integral degrees and decimal minutes, and some having integral degrees and minutes, but decimal seconds. Unfortunately, I can't figure out which conversion reproduces this error.

Needless to say, an incorrect location for a major fire can cause significant problems.

✂ Oyster and Mifare cracked: NXP sues to silence Oyster researchers

<"Peter G. Neumann" <neumann@csl.sri.com>>
Tue, 8 Jul 2008 5:56:07 PDT

[Source: *The Register*, 8 Jul 2008; PGN-ed]
http://www.theregister.co.uk/2008/07/08/nxp_sues_oyster_researchers/

Researchers at Nijmegen's Radboud University have evidently cracked and cloned London's Oyster travel card, after previously having had similar success with the Dutch MIFARE travel card (which is supposed to replace paper tickets on all trams, buses, and trains in The Netherlands).
http://www.ru.nl/english/general/radboud_university/vm/security_flaw_in/

The Dutch researchers are planning to publish their scientific paper, Dismantling MIFARE Classic, in October at Esorics, in Spain. The paper extends a preliminary report.
<http://www.cs.virginia.edu/~kn5f/pdf/Mifare.Cryptanalysis.pdf>

The dichotomy between belief in security by obscurity and flawed systems continues.

✂ Free Berlin subway rides

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>
Mon, 07 Jul 2008 20:50:55 +0200

Berlin newspapers report that on 1 Jul 2008 it was not possible to buy a subway ticket during the morning rush hour.

http://www.morgenpost.de/berlin/article650601/BVG_Fahrkartenautomaten_komplett_ausgefallen.html

More than 600 of the 700 ticket machines refused to work after they were updated from a central server overnight. An unnamed Swiss company was updating the database (probably for fare calculation) when the machines began failing. It took until 1 pm for the error to be fixed on all machines.

In the meantime, security people walked around encouraging people to just get on the trains. The ticket checkers (who travel undercover and announce ticket controls just after the doors close) were pulled from the subway and put on bus and tram duty.

The BVG won't say how much income it lost in the incident, but they do state that only a very few people complained about having to ride for free.

[These were probably people with passes who could not take advantage of a free ride. -- dww]

Debora Weber-Wulff, FHTW Berlin, Internationale Medieninformatik, Treskowallee 8, 10313 Berlin +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

✶ Citibank ATM breach reveals PIN security problems

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

Wed, 2 Jul 2008 12:50:09 PDT

Hackers broke into Citibank's network of ATMs inside 7-Eleven stores and stole customers' PIN codes, according to recent court filings that revealed a disturbing security hole in the most sensitive part of a banking record. Hackers are targeting the ATM system's infrastructure, which is increasingly built on Microsoft's Windows operating system and allows machines to be remotely diagnosed and repaired over the Internet. despite industry standards that call for protecting PINs with strong encryption -- which means encoding them to cloak them to outsiders -- some ATM operators apparently aren't properly doing that. The PINs seem to be leaking while in transit between the ATMs and the computers that process the transactions. [Source: Jordan Robertson, Associated Press, 2 Jul 2008; PGN-ed]

Full story here: <http://www.wtop.com/?nid=108&sid=1432201>

✶ Web-based SSH key generation with escrow

<Tina Bird <tbird@precision-guesswork.com>>

Sun, 29 Jun 2008 12:58:02 -0500

<http://sshkeygen.com/>

Risks are left as an exercise to the reader...

[This one requires little explanation by your moderator. PGN]

ComCast in Concrete?

*"Schaefer, Robert P \{US SSA\}" <robert.p.schaefer@baesystems.com>>
Mon, 7 Jul 2008 10:42:27 -0400*

This happened to me over the holiday weekend...

On 3 Jul 2008, approximately 9PM, my son detected that our desk PC (windows 98) was no longer able to access the Internet through the cable modem. I started diagnosing the problem midday July 5. Resetting the cable box and the computer several times did not help, neither did running ipconfig/release ipconfig/renew at the command prompt. The error that ipconfig returned was "DHCP Client refused". I phoned the Comcast 800 number, and after several resets at both ends with no success Comcast revealed that they refused to support the Firefox browser. On that same phone session I then attached a laptop running XP and Explorer to the cable modem and successfully reconnected to the Internet.

I went back to the first computer and the Internet still did not connect. It appears that Comcast not only does not support Firefox but can now detect either Firefox or Win98 (which together form an ambiguity group) and refuse to connect. The Win98 PC was initially also connected to a Lynksys wireless router so I could connect to the Internet from the laptop anywhere in the house. I connected the cable modem directly to the wireless router and disconnected the laptop, I discovered that I could no longer connect to the Internet through the wireless although the laptop saw full signal strength.

To recap: Win98 no, XP yes, direct cable yes, cable plus wireless, no.

I phoned Comcast a second time and learned that Comcast did not support the Lynksys wireless router but they immediately and cheerfully without my prompting provided the 800 number for Lynksys. The call to Lynksys revealed that my wireless router was out of warranty, but for only \$29.95..., I said thank you and hung up. I phoned Comcast a third time and asked which particular wireless router they did support, their answer was "none". Luckily for me, I had an extra wireless router, Belkin, that I had bought when I had to re-install the Lynksys but thought I had lost the installation disk (and couldn't get any help from their website - Of course the Lynksys installation disk turned up after I had bought its replacement.) Anyway, I installed the Belkin and was good to go. Later, using a second desktop with XP, Firefox, and a wireless modem I was also able to connect to the Internet. That experiment adjusts the probability on the ambiguity group (Win98 or Firefox) to point to either Win98 or now the Firefox "version". I only just now in writing this realize that I could also have tried re-reconfiguring the Lynksys again through the laptop, but it had worked before, and the laptop did see full signal strength, so probably something else was going on.

To sum up, the implication is that at the same instant that Comcast chose to

refuse to work with Firefox browsers on Win98 machines they also were (allegedly) in collusion with Lynksys to obsolete a model of wireless router, all scheduled to occur just in time for the July 4th holiday. Two hours of my life as an unpaid system administrator for my home computers I will never get back.

[Subject line retitled by PGN.]

State Dept: Celebrity passport files viewed repeatedly - CNN.com

<"Peter G. Neumann" <neumann@csl.sri.com>>
Fri, 4 Jul 2008 8:22:20 PDT

[Thanks to Gene Spafford]

<http://www.cnn.com/2008/POLITICS/07/03/us.passport.files/index.html>

California's Super-Stupid Anti-Science Cell Phone Law Takes Effect

<Lauren Weinstein <lauren@vortex.com>>
Tue, 1 Jul 2008 13:26:56 -0700 (PDT)

Greetings. Well, today's the day that political expediency and anti-science stupidity combine for the banning of handheld cell phones while driving in California.

I've discussed this topic here several times before, noting that virtually every study shows no reduction in accident rates when talking on a hands-free cell phone vs. handheld units. In fact, there are concerns that people fumbling around to dial and answer hands-free units may actually make matters worse.

Even the Luddite who spent years pushing through this legislation admits that the science and studies are against him, but he's convinced that having both hands on the wheel is safer. Of course, the law doesn't require two hands on the wheel -- which would be fairly difficult for stick drivers like me in any case, eh?

When I was out driving earlier today, I saw one woman swerving while putting on make-up, and a guy weaving all over while apparently wolfing down a burger. Another car almost didn't make a stop while the woman inside appeared to be screaming at her kids in the back seat -- all classic distractions unaffected by the new law. However, I saw several people now driving illegally but safely with handheld cell phones.

There are already laws against distracted driving. The new cell phone law (as applied to adult drivers) is both unnecessary and counterproductive -- the latter by making people erroneously believe that they're safer with

hands-free phones while driving.

This sort of "feel good" law that flies in the face of science, <http://lauren.vortex.com/archive/000271.html>>studies, and logic, is an example of our political system operating as a pandering pomposity of the most inane kind.

<http://lauren.vortex.com/archive/000396.html>

Re: HTML comments reveal corporate weakness (Jidanni, [RISKS-25.21](#))

<Ivor Hewitt <Ivor.Hewitt@MorganStanley.com>>

Mon, 30 Jun 2008 14:24:57 +0100

The "risk" in HTML comments revealing corporate weakness looks simply like an HTML workaround technique for a bug in Netscape Navigator 4.7 (ns47) that probably doesn't display correctly (behave) without having a fake "concreate"(sic) row (i.e. HTML table).

Unlikely to bring "the entire house of cards down", simply a developer documenting why he was required to do something weird in the markup.

[Also noted by several others. PGN]

Re: Approval voting and sincerity (Drysdale, [RISKS-25.21](#))

<"Andrew Koenig" <ark@acm.org>>

Mon, 30 Jun 2008 13:35:30 -0400

If I remember correctly, the article deals with this question, but unfortunately I don't remember all the details.

Approximately, though, the reasoning hinges on the definition of "approval." The article claims that a voter's optimum strategy is to rank-order the candidates, and then vote for all the candidates above a given threshold, where that threshold depends in a way I do not recall on the voter's assessment of how likely each candidate is to be elected.

In other words, if A is my favorite candidate, I am willing to tolerate B, and I never want C to be elected, then I should certainly vote for A and certainly not vote for C. Whether I vote for B depends (again, according to an algorithm that I do not recall) on how likely I think it is that my vote will cause B to be elected instead of A.

If you consider the process of rank-ordering the candidates and then voting for all the candidates beyond a threshold to be insincere, then I guess approval voting could foster insincerity. But I don't consider it that way, and, if I remember correctly, neither did the article.

Re: Approval voting and sincerity (Drysdale, [RISKS-25.21](#))

<Dag-Erling Smørgrav <des@des.no>>
Mon, 30 Jun 2008 03:16:00 +0200

> Thus voting insincerely ... leads to a better result.

Define "better". In the first scenario, 20% of the voters (those who voted for C) are dissatisfied. In the second scenario, 40% of the voters (those who voted for B plus those who voted for C) are dissatisfied.

Dag-Erling Smørgrav - des@des.no

REVIEW: "The dotCrime Manifesto", Phillip Hallam-Baker

<Rob Slade <rmslade@shaw.ca>>
Thu, 03 Jul 2008 11:06:12 -0800

BKDCRMNF.RVW 20080317

"The dotCrime Manifesto", Phillip Hallam-Baker, 2008, 0-321-50358-9,
US\$29.99/C\$32.99

%A Phillip Hallam-Baker dotcrimemanifesto.com hallam@gmail.com

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

%D 2008

%G 978-0-321-50358-9 0-321-50358-9

%I Addison-Wesley Publishing Co.

%O US\$29.99/C\$32.99 416-447-5101 fax: 416-443-0948 800-822-6339

%O <http://www.amazon.com/exec/obidos/ASIN/0321503589/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0321503589/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0321503589/robsladesin03-20>

%O Audience n+ Tech 2 Writing 2 (see revfaq.htm for explanation)

%P 415 p.

%T "The dotCrime Manifesto: How to Stop Internet Crime"

In the preface, the author notes that network and computer crime is a matter of people, not of technology. However, he also notes that changes to the network infrastructure, as well as improvements in accountability, would assist in reducing user risk on the net.

Section one enlarges on the theme that people are more important than machines or protocols. Chapter one looks at the motive for Internet crime (money, just like non-computer crime), and repeats the motifs of the preface. The text goes on to list various categories and examples of network fraud. The content of chapter two is very interesting, but it is hard to find a central thread. Overall it appears to be saying that computer criminals are not the masterminds implied by media portrayals, but that the problem of malfeasance is growing and needs to be seriously addressed. What Hallam-Baker seems to mean by "Learning from Mistakes," in

chapter three, is that security professionals often rely too much on general principles, rather than accepting a functional, if imperfect, solution that reduces the severity of the problem. Chapter four presents the standard (if you'll pardon the expression) discussion of change and the acceptance of new technologies. A process for driving change designed to improve the Internet infrastructure is proposed in chapter five.

Section two examines ways to address some of the major network crime risks. Chapter six notes the problems with many common means of handling spam. SenderID and SPF is promoted in chapter seven (without expanding the acronym to Sender Policy Framework anywhere in the book that I could find). Phishing, and protection against it, is discussed in chapter eight. Chapter nine is supposed to deal with botnets, but concentrates on trojans and firewalls (although I was glad to see a mention of "reverse firewalls," or egress scanning, which is too often neglected).

Section three details the security tools of cryptography and trust. Chapter ten outlines some history and concepts of cryptography. Trust, in chapter eleven, is confined to the need for aspects of public key infrastructure (PKI).

Section four presents thoughts on accountability. Secure transport, in chapter twelve, starts with thoughts on SSL (Secure Sockets Layer), and then moves to more characteristics of certificates and the Extended Verification certificates. (The promotion of Verisign, infrequent and somewhat amusing in the earlier chapters is, by this point in the book, becoming increasingly annoying. The author is also starting to make more subjective assertions, such as boosting the trusted computing platform initiative.) Domain Keys Identified Mail (DKIM) is the major technology promoted in support of secure messaging, in chapter thirteen. Chapter fourteen, about secure identity, has an analysis of a variety of technologies. (The recommendations about technologies are supported even less than before, and the work now starts to sound rather doctrinaire.) It may seem rather odd to talk about secure names as opposed to identities, but Hallam-Baker is dealing with identifiers such as email addresses and domain names in chapter fifteen. Chapter sixteen looks at various considerations in regard to securing networks, mostly in terms of authentication. Random thoughts on operating system, hardware, or application security make up chapter seventeen. The author stresses, in chapter eighteen, that the law, used in conjunction with security technologies, can help in reducing overall threat levels. Chapter nineteen finishes off the text with a proposed outline of action that recaps the major points.

Hallam-Baker uses a dry wit well, and to good effect in the book. The humour supports and reinforces the points being made. So does his extensive and generally reliable knowledge of computer technology and history. In certain areas the author is either less knowledgeable or careless in his wording, and, unfortunately, the effect is to lessen the reader's confidence in his conclusions. This is a pity, since Hallam-Baker is championing a number of positions that would promote much greater safety and security on the Internet. Overall this work is, for the non-specialist, a much-better-than-average introduction to the issue of Internet crime and protection, and is also worth serious consideration by security professionals for the thought-provoking

challenges to standard approaches to the problems examined.

copyright Robert M. Slade, 2008 BKDCRMNF.RVW 2008031
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 23

Friday 18 July 2008

Contents

- [E-mail response to wrong address, intended recipient arrested](#)
[Danny Burstein](#)
- [San Francisco admin hijacks city net](#)
[David Lesher](#)
- [Risks of wrong preprogrammed emergency message system being sent](#)
[C.Y./J.E. Cripps](#)
- [P2P Data Breach affects SCOTUS](#)
[Jay R. Ashworth](#)
- ["Plug and Play" Hospitals](#)
[Terrence Enger](#)
- [Gmail Reveals the Names of All Users](#)
[Gene Wirchenko](#)
- [Google Desktop, Word may expose encrypted data](#)
[Gene Wirchenko](#)
- [UPS "Virus Warning" virtually indistinguishable from phishing attack](#)
[Jonathan Kamens](#)
- [DR/BCM lessons from the Vancouver fire](#)
[Daniel Wesemann in SANS via Brent J. Nordquist](#)
- [Re: Map coordinate errors for California fire](#)
[Henry Baker](#)
[Al Stangenberger](#)
- [California's Super-Stupid Anti-Science Cell Phone Law Takes Effect](#)
[Kurt Thams](#)
- [Handheld mobile safety](#)
[Paul D. Smith](#)
- [The toll for terrorism is too high](#)
[David Lesher](#)
- [Firefox 3's Step Backwards For Self-Signed Certificates](#)
[Lauren Weinstein](#)
- [A not-so-obvious hyperinflation risk](#)
[B. Elijah Griffin](#)
- [Re: Approval voting and sincerity](#)
[Anthony W. Youngman](#)
- [Re: ComCast in Concrete? \(](#)
[Greg Fife](#)

[Paul Wallich](#)

• [US FTC seeks comments on privacy in contactless payments](#)

[Kevin Fu](#)

• [Info on RISKS \(comp.risks\)](#)

✂ E-mail response to wrong address, intended recipient arrested

<danny burstein <dannyb@panix.com>>

Thu, 10 Jul 2008 09:04:04 -0400 (EDT)

(slightly edited/reformatted for clarity)

<http://www.law.com/jsp/nylj/PubArticleNY.jsp?hubtype=TopStories&id=1202422872356>

Mark Hamblett, Mistaken Identity in Civil Rights Lawsuit

Bronx [NYC] resident William Hollowell filed suit in the Southern District yesterday claiming police and prosecutors blundered by wrongfully arresting him for an e-mail he never sent.

Mr. Hollowell was working part time at the Riverdale Country School Library in April 2007, and exchanging e-mails about the return of a library key with his supervisor, Robin Berson, when Ms. Berson inadvertently typed the wrong e-mail address - to a Ben Hollowell.

She received in return an unsigned e-mail saying the recipient had sold the key for "hookers," a "handful" of drugs and a gun. The writer also professed his desire for Ms. Berson and proposed a sexual liaison in the library.

The lawsuit alleges that, on a complaint from Ms. Berson, New York City police, "Despite the obvious lack of evidence against him," arrested William Hollowell and held him for more than 30 hours.

The complaint, charging false arrest and malicious prosecution, states, "Determined to make an arrest, any arrest, defendants bluntly violated Mr. Hollowell's rights by turning a blind eye to the overwhelming evidence of his innocence," and blames prosecutors for waiting for four months to dismiss the case. The Bronx County District Attorney's Office declined comment.

✂ San Francisco admin hijacks city net

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

Tue, 15 Jul 2008 23:39:00 -0400 (EDT)

San Francisco IT worker arrested in hijacking of city network, CNET

<http://news.cnet.com/8301-1009_3-9991769-83.html?part=rss&subj=news&tag=2547-1_3-0-20>

A disgruntled city worker is in jail on \$5 million bail after allegedly

locking other administrators out of the city's wireless network.

The Risk? The same one the Intelligence Community faces daily: the people often are the problem...

[Jim Horning noted "S.F. officials locked out of computer network" in the *San Francisco Chronicle*. PGN]
<<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/14/BAOS11P1M5.DTL>>

✶ Risks of wrong preprogrammed emergency message system being sent

<"C.Y./J.E. Cripps" <cycmn@nyct.net>>
Thu, 10 Jul 2008 23:45:59 -0400 (EDT)

Potential risks in preprogrammed emergency message systems:

About 2,000 State Farm employees spent almost two hours Thursday afternoon in the lower level of the company's corporate headquarters [in Bloomington, Illinois] after a passer-by reported seeing a man with a "long gun" outside the building.

A preprogrammed tornado announcement sent people to the lower level when the company had intended to send out an emergency warning.

Police eventually determined the person actually saw a custodian holding what probably was a pipe.

[Source: Pantagraph.com State Farm, police pleased with response to security threat; see link for full article and some further risks. PGN]
<http://www.pantagraph.com/articles/2008/07/08/news/doc487256756564f585165529.txt>

✶ P2P Data Breach affects SCOTUS

<"Jay R. Ashworth" <jra@baylink.com>>
Wed, 9 Jul 2008 09:57:30 -0400

Mr Justice Stephen Breyer was apparently among the over 2000 people affected by a personal data breach caused when an employee of a financial services firm installed Limewire on a computer he used for work, was careless about how he configured it, and shared some directories containing the data in question.

Brian Krebs' piece in *The Washington Post* [1] missed both of the important points; the one I made above in how I (correctly) characterized what (probably) actually happened -- not glossing over the fact that p2p server software is not inherently black-hat, as the piece encourages the reader to assume -- and the other one, covered by the comment I posted, which I reproduce here:

I'm more than a little bit disappointed that this piece fails to mention the root cause of *why* this breach bothers so many people -- because the last clear chance to avoid it did not happen when the file sharing program was installed.

It happened when AT&T, and the credit card companies, and whosoever, saw fit to treat as *authenticators* the mere knowledge of birthdates and SSNs.

That someone knows my bday, or SSN, *does not prove they're me*, and this problem will not go away until large corporations cease acting as if it does... which is a point privacy activists have been making loudly in public places since at least 1992 that I know of, and likely longer.

If you want to authenticate me, do a better job. And don't make *me* responsible for paying to deal with the consequences of you not being smart enough to do so.

That's my manifesto. Maybe if enough other people say it too, loudly, it will stop. This is why I customarily refuse to give out my SSN.

This is not an idea original to me, of course, and I originally stole it either from RISKS or from Lauren Weinstein's Privacy Forum, to which I've CC:ed this message.

But the risks here are multiple, and subtle (at least to some :-), so I'll enumerate them:

1) Thinking that p2p software is all inherently bad because a) a p2p server producer picked a bad default and a non-savvy user accepted it.

2) Blaming the subsequent breach on p2p software inherently, and painting it as a bad thing -- when indeed several major companies are developing legit p2p distribution networks for various things.

2a) The fact that so many supposedly technology-centric reporters miss the most important points on stories where technology intersects with society and the law -- which is most of them these days, right?

3) Blaming the breach on even the bad guys, when the root cause is an excruciatingly poor process design decision on the part of the good guys, to wit: choosing to use, as absolute proof that an applicant is who they claim to be, the fact that they know a birthdate, SSN, mother's maiden name, or city of birth.

Just as with reusable password security: one of the reasons you use different passwords for different services (or at least, different security classes of service) *is because you can't trust the operator of the service not to leak them*.

Well, this is worse: just like with biometrics, *you can't change the things these companies are asking for*.

And nowadays, you can't even lie about them, since apparently, violating the

terms of service of a *free* website is a felony[2].

Does anyone see any reasonable way out of this conundrum? 'Cause I don't.

[1]

<http://www.washingtonpost.com/wp-dyn/content/article/2008/07/08/AR2008070802997.html>

[2] <http://www.secureworks.com/research/falsepositive.php>

Jay R. Ashworth, Ashworth & Associates, St Petersburg FL USA +1 727 647 1274

<http://baylink.pitas.com>

✂ "Plug and Play" Hospitals

<Terrence Enger <tenger@iseries-guru.com>>

Thu, 10 Jul 2008 11:20:55 -0400

MIT's *Technology Review* has an article "Plug and Play" Hospitals: Medical devices that exchange data could make hospitals safer. Just the title is enough to excite my "oh yeah?" reflex.

<<http://www.technologyreview.com/Biotech/21052/?a=f>>.

The body of the article focuses entirely on the benefits of the new technology. Speaking of the ventilators, which are potentially life-preserving, it says the following without even a hint that there may be a risk:

Goldman says that as a result of his demonstration, standards for ventilators are in the process of being revised so that future versions of the devices will include a pause function and will be subject to network control, moving toward interoperability.

Don't hold your breath. [What about the nurse who takes a nap on the remote controller? And of course the veterinarian in the missing L-wing is "Pug and Pay". PGN]

✂ Gmail Reveals the Names of All Users

<Gene Wirchenko <genew@ocis.net>>

Thu, 17 Jul 2008 08:16:27 -0700

<http://tech.slashdot.org/article.pl?sid=08/07/16/2220232&from=rss>

"Have you ever wanted to know the name of admin@gmail.com? Now you can. Through a bug in Google calendars the names of all registered Gmail accounts are now readily available. All you need to find out the names of any gmail address is a Google calendar account yourself. Depending on your view this ranges from a harmless "feature" to a rather serious privacy violation. According to some reports, spammers are already exploiting this

"feature"/bug to send personalized spam messages."

Google Desktop, Word may expose encrypted data

<Gene Wirchenko <genew@ocis.net>>

Thu, 17 Jul 2008 08:33:28 -0700

Opening paragraphs:

"If you're using encryption software to keep part of your computer's hard drive private, you may have a problem, according to researchers at the University of Washington and British Telecommunications.

They've discovered that popular programs like Word and Google Desktop store data on unencrypted sections of a computer's hard drive -- even when the programs are working with encrypted files."

<http://www.itbusiness.ca/it/client/en/home/News.asp?id=49190>

UPS "Virus Warning" virtually indistinguishable from phishing attack

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

Tue, 15 Jul 2008 09:33:26 -0400

This morning, I received an e-mail message purporting to be from UPS (I have an account at ups.com) and reading in part as follows:

Attention Virus Warning

We have become aware there is a fraudulent e-mail being sent that says it is coming from UPS and leads the reader to believe that a UPS shipment could not be delivered. The reader is advised to open an attachment reportedly containing a waybill for the shipment to be picked up.

(I'm sure we've all seen the spam to which the warning is referring.)

My full name is not mentioned anywhere in the message. The numerous links in the message are all encrypted query strings and point at rm04.net rather than ups.com. The e-mail header contains a bunch of randomized garbage (for example, the envelope address looks like this: v-dj_dklajdn_ndk_jccfkddpdkkkkhhbk_@bounce1.rm05.net), and ups.com doesn't appear anywhere in it.

I'm savvy enough to know that this is /probably/ a legitimate e-mail message from UPS, but a savvy attacker could craft a message that looks exactly like this one, so I'm also savvy enough to know not to be foolish enough to click on any of the links.

On the other hand, checking out the links with lwp-request (a Perl command-line HTTP client) is safe enough. I checked the "Privacy Policy" link, and it redirects to <http://www.ups.com/content/us/en/privacy.html>, so at least one of the encrypted links in the message is legitimate.

In this day and age, it is amazing to see a corporation as large as UPS failing to use the two easiest and most well-known methods of differentiating legitimate e-mail from scams -- put the customer's name in the e-mail, and make sure that all the links point directly at your site.

Are there any RISKS readers with connections inside UPS to whose attention they might bring this matter?

✂ DR/BCM lessons from the Vancouver fire (Daniel Wesemann in SANS)

*<"Brent J. Nordquist" <brent@nordist.net>>
Tue, 15 Jul 2008 08:13:44 -0500*

[quoting from <http://isc.sans.org/diary.html?storyid=4729>:]

DR/BCM lessons from the Vancouver fire
Published: 2008-07-14 by Daniel Wesemann (Version: 1)

An fire in an underground power distribution room today knocked a good portion of Vancouver's inner city power grid offline. Several news media like the Vancouver Sun are carrying the story by now.

As bad as this event is on its own, the e-mail provider Hushmail reports on its web page some additional interesting details. What happened, apparently, was that Vancouver's "Harbour Centre" web hosting location brought their emergency generator successfully online when the power dropped. But as soon as the fire department started drawing massive amounts of water in their attempt to contain the fire, the water pressure in the mains was reduced to a level where the (water cooled) emergency generator couldn't operate any more. Poof. Darkness.

Now, let me guess how many BCM/DR plans out there didn't think of that one... Time to update!

✂ Re: Map coordinate errors for California fire (Baker, [RISKS-25.22](#))

*<Henry Baker <hbaker1@pipeline.com>>
Wed, 09 Jul 2008 00:33:24 -0700*

After additional research, this particular error may not be a conversion error at all, but a more classical error. Apparently, the "Gap" fire was originally reported to have started at the "Gap", which does indeed reside

at the original coordinates close to Highway 154. However, this original report was in error, so the naming of the "Gap Fire" after the "Gap" was actually a misnomer. Unfortunately, once the fire had been named the "Gap Fire", it would have been even more confusing to change its name, so the name has stuck, even though (so far) the fire hasn't come near the actual "Gap".

This naming error is entirely analogous to the naming of mathematical theorems, very few of which are named after their actual/original discoverers.

✂ Re: Map coordinate errors for California fire (Baker, [RISKS-25.22](#))

*<Al Stangenberger <forags@nature.berkeley.edu>>
Mon, 14 Jul 2008 17:45:24 -0700*

Fortunately, InciWeb is not part of the command and control system for fighting fires, but is an informational database which attempts to supply information on incidents nationwide. Hence the consequences of an error in location of a fire are not catastrophic.

However, InciWeb has been plagued by instability (possibly server overload) during the California fire emergency of the past couple of weeks.

As I write this, the Plumas National Forest has set up a Google group to release information on the Canyon Complex of fires in a timely fashion.

From the PNF homepage: "Due to the unstable nature of InciWeb, updated information about the Canyon Complex can temporarily be found here [URL for the Google group]".

Al Stangenberger, Univ. of California at Berkeley, Center for Forestry
145 Mulford Hall # 3114 1-510-642-4424 Berkeley, CA 94720-3114

✂ California's Super-Stupid Anti-Science Cell Phone Law Takes Effect

*<Kurt Thams <thams@thams.com>>
Tue, 08 Jul 2008 12:08:27 -0700*

On day 3 of the new law, we were speculating whether forcing people to use headsets would have the effect of encouraging people to talk longer, increasing overall risk.

During our discussion, a friend called to say she'd be late. While fumbling for her headset she had hit a curb and blown a tire.

✂ The toll for terrorism is too high

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

Thu, 17 Jul 2008 11:07:11 -0400 (EDT)

The *Los Angeles Times* is reporting that the city is using \$16,000,000 of "anti-terrorism" money to install faregates on their rail lines.

Both Los Angeles Mayor Antonio Villaraigosa and state Homeland Security Advisor Matthew Bettenhausen said the turnstiles will enhance security at the rail lines, as well as stop fare jumpers, although a transportation security expert said the gates by themselves will have only a nominal effect on stopping potential terrorist attacks.

Of course, someone, in this case Don Surber of the Charlston Daily Mail, HAD to mention the "Gov. William J. Le Petomane Thruway" <http://blogs.dailymail.com/donsurber/2008/07/16/turnstiles/> approach. Why am I reminded of "Terrorists Can't Type" yet again?

RISK 1: Throw enough money into the air, and it's amazing how many problems shall appear that need it... for some value of "need"...

RISK 2: With enough RISK 1's, and the fighting over the spoils that results; real honest-to-gosh threats can be, well, lost in the dust.

Firefox 3's Step Backwards For Self-Signed Certificates

<Lauren Weinstein <lauren@vortex.com>>

Tue, 8 Jul 2008 12:25:28 PDT

Firefox 3's Step Backwards For Self-Signed Certificates

<http://lauren.vortex.com/archive/000402.html>

Greetings. If you've switched over to Firefox 3 as your Web browser already -- and in general it's a fine upgrade -- you may at some point discover that rather than encourage (or at least not overly discourage) the use of self-signed security certificates, Firefox 3 makes it *less* likely that anyone other than an expert user will ever accept a self-signed certificate. This is particularly of concern to me since I've urged an expansion of self-signed certs deployment as a stopgap measure toward pervasive encryption (<http://lauren.vortex.com/archive/000339.html>).

Compared with Firefox 2, version 3 throws up so many barriers and scary-sounding warnings to click through to accept such certs, that it would be completely understandable if most persons immediately aborted.

What's going on is that Firefox is now putting so much emphasis on identity confirmation that it's making it even harder for people to use the basic encryption functionality of the browser, which works just fine with self-signed certificates (which admittedly are not good carriers for identity credentials).

But in many situations, we're not concerned about identity in particular, we just want to get the basic https: crypto stream up and running.

I am fully aware of the associated identity considerations, and I know that basic signed certificates that will work in Firefox and some other browsers (but last I heard not in Internet Explorer at this time) can be obtained for free. If browser acceptance of free signed certs broadens out (and especially if wildcard certificates also become freely available) the need for self-signed certificates could significantly diminish.

But for now, Firefox 3 is going overboard with its complicated and alarming warnings, which if nothing else could include improved explanatory text, so that users would be able to better judge whether or not they should accept any particular self-signed certificate. The current wording is unreasonably judgmental given the range of perfectly legitimate situations where self-signed certificates might be used.

I'm not saying to give self-signed certs the same invisible, automatic acceptance as signed certificates, but Firefox 3 has simply gone too far toward making self-signed certs unusable -- from a practical standpoint -- in many situations where they otherwise would be completely adequate and suitable.

Lauren Weinstein +1(818)225-2800 <http://www.pfir.org/lauren>

Co-Founder, PFIR and NNSquad (Network Neutrality Squad,
<http://www.nnsquad.org>) PRIVACY Forum - <http://www.vortex.com> Lauren's Blog:
<http://lauren.vortex.com>

✶ A not-so-obvious hyperinflation risk

*<eli@panix.com (B. Elijah Griffin)>
Wed, 16 Jul 2008 17:49:57 -0400 (EDT)*

The Zimbabwe government is facing a money printing crisis: the government has been able to maintain power by printing more and more money to pay the security forces. Now there is a threat to the paper supply needed to print more and more money. No computer risk there, but the last paragraph has a kicker. Besides needing paper to print more money, they use computer software to design the ever larger denominations required to keep pace with the hyperinflation, and there is a risk: "that its software license for the European banknote design technology that it uses could be withdrawn because of new sanctions threatened against the Mugabe government."

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/15/MNR011OT0Q.DTL>

✶ Re: Approval voting and sincerity (Drysdale, [RISKS-25.21](#))

*<"Anthony W. Youngman" <wol@thewolery.demon.co.uk>>
Tue, 8 Jul 2008 20:19:51 +0100*

The best proportional system I've come across requires ranking but doesn't seem to have been covered here so far.

The voter lists all the candidates they wish to in order of preference. If you don't list the candidate, they don't count as far as your vote goes.

When counting the votes, it's treated as a series of two-horse races - for each pair of candidates you count how many people list A above B, and B above A. Unless you get a very weird result (i.e., it's statistically very unlikely), one candidate will win all his individual contests. That person should be elected.

Failing that, someone will almost certainly lose all his contests and should be eliminated. When they're removed from consideration the win-lose cycle can be repeated until you're left with a winner.

(Effectively, you're voting FOR the people you DO want, AGAINST the people you DON'T want, and ABSTAINING for people you DON'T CARE about.)

Re: ComCast in Concrete? (Schaefer, [RISKS-25.22](#))

*<Greg Fife <greg@frozenfog.com>>
Wed, 09 Jul 2008 07:15:01 -0400*

I ran across this problem with ComCast in Harrisonburg, VA about a year ago. The Linksys router's "MAC Address Clone" feature was sufficient to fix the problem.

The ethernet adapter in a PC and the ethernet "WAN Port" on a router both have a unique six byte identification known as a MAC (Medium Access Control) address. The first three bytes identify the manufacturer (i.e. Linksys), and the other three bytes identify the specific device. Default values are assigned by the manufacturer and programmed into the hardware. A "MAC Address Clone" merely allows you to change the factory assigned external MAC address on a router.

Basically, ComCast's DHCP server just takes each distinct MAC address and assigns an Internet Protocol (IP address). From the pathological behavior that we've seen, I assume that ComCast programs their DHCP server to reject equipment made by Linksys, Belkin, DLink, and so on.

In most consumer routers that I've worked with, the MAC Address Clone is somewhere in the advanced configuration pages of the web configuration system. It will probably default to clone the MAC address of your PC's ethernet adapter, but if not, you can get your PC's mac address from "IPCONFIG /ALL" in a Windows XP command window or the WINIPCFG program in Windows 98.

If this doesn't work, I would turn off remote management, "Universal Plug and Play," and anything else that might allow the cable company to interact

with your router over the network and recognize its specific behavior.

Greg Fife <greg@frozenfog.com> 1-540-447-4038

Re: ComCast in Concrete? (Schaefer, [RISKS-25.22](#))

<Paul Wallich <pw@panix.com>>

Tue, 08 Jul 2008 16:47:49 -0400

> To sum up, the implication is that at the same instant that ComCast chose to
> refuse to work with Firefox browsers on Win98 machines they also were
> (allegedly) in collusion with Lynksys to obsolete a model of wireless
> router, all scheduled to occur just in time for the July 4th holiday. ...

This sounds fishy at best (albeit it's unclear where the fishiness is). At the point where you're doing DHCP negotiation, it's impossible for the ISP to know what browser you're using. It may be a little easier to know which router or other machine is attached to the cable modem, but the motivation for keeping a list of allowed and disallowed routers (especially given the possibilities for spoofing) seems unclear to me. What I do know is that customer service representatives are typically graded on their ability to get a customer off the line quickly, and if telling them "We don't support X" will do it faster than "One of our internal routers just went belly-up" then that's likely what they'll do.

On the other side of the argument, ComCast is pretty much known for doing thorough inspection, aka wiretapping, of the packets its customers send out, and for sending packets that misrepresent the state of machines with which their customer is communicating. So it seems they would be perfectly capable of bollixing someone's connection in this way, with the only question being where the profit is.

US FTC seeks comments on privacy in contactless payments

<Kevin Fu <kevinfu@cs.umass.edu>>

Wed, 9 Jul 2008 18:46:30 -0400

The US Federal Trade Commission issued a request for comments on issues such as security and privacy of contactless payments last month, but the FTC has extended the deadline to submit comments. If you have any comments for the FTC on privacy for contactless payments, do submit ASAP. Here are the comments received thus far.

<http://www.ftc.gov/bcp/workshops/payonthego/index.shtml#comments>

<http://www.ftc.gov/os/comments/payonthego/index.shtm>

You may submit either by e-mail or the Web form.

Kevin Fu, Assistant Professor, Computer Science Department, Univ. of

Massachusetts Amherst 413-545-4006 <http://www.cs.umass.edu/~kevinfu/>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 24

Wednesday 23 July 2008

Contents

- [Washington Metro farecard fraud](#)
[David Leshner](#)
- [The \\$100,000 Keying Error](#)
[Patrick O'Beirne](#)
- [What happened to handcuffing the briefcase to James Bond's wrist?](#)
[Randall Webmail](#)
- [Taking a grab at what's the real system error](#)
[Jared](#)
- [What's in a name?](#)
[Peter Houppermans](#)
- [Yet more GPS risks: Angry Mob Stones Lost Tourist](#)
[Steven J Klein](#)
- [Shocking idea for air passenger security](#)
[Robin Stevens](#)
- [Re: Oyster card hack to be published](#)
[Amos Shapir](#)
- [Re: San Francisco admin hijacks city net: Paul Venezia](#)
[David Leshner](#)
- [Re: ComCast in Concrete? MAC addresses](#)
[R A Lichtensteiger](#)
- [Re: P2P Data Breach affects SCOTUS](#)
[Pete Klammer](#)
[Jay R. Ashworth](#)
- [Re: Approval voting and sincerity](#)
[Geoffrey Brent](#)
[Richard Gadsden](#)
- [NC State Voter site exposes voter addresses](#)
[John O Long](#)
- [Info on RISKS \(comp.risks\)](#)

Washington Metro farecard fraud

<"David Leshner" <wb8fz@panix.com>>
Sun, 20 Jul 2008 01:25:01 -0400 (EDT)

The Washington Post reports six arrests in a Metro Farecard fraud scheme.

<<http://www.washingtonpost.com/wp-dyn/content/article/2008/07/18/AR2008071801912.html>>

Allegedly the accused would buy a paper farecard; split the 0.25" wide magstrip into 4 ribbons and glue each atop a blank card.

Then they'd trade in the card by adding some small cash value, getting a new card in return.

Metro's first response was to lower the allowable trade-in value from \$30 to \$4.

It's not clear if a Metro employee noticed the altered cards in the discard bin inside of a ticket vending machine; or they were tipped off by other system safeguards, such as. A duplicate-card serial-number detector.

Comment: I recall a similar BART fraud of about 2 decades ago, which used a steam iron and knowledge of Curie points.

I wonder if Metro will try to use this to mandate moving to their traceable stored value "Smartrip" cards...

What happened to handcuffing the briefcase to James Bond's wrist?

<Randall Webmail [rvh40@insightbb.com]>

Sun, 20 Jul 2008 7:40 PM

[From Dave Farber's IP distribution.]

On 20 Jul 2008, the Ministry of Defence confirmed another laptop with "sensitive information" has been stolen while one of their officials checked out of a hotel. An MoD spokesman said the theft from the Britannia Adelphi hotel in Liverpool city centre on 17 Jul 2008 brought the total of laptops stolen to 659. On 18 Jul 2008 the MoD admitted that 658 of its laptops had been stolen over the past four years - nearly double the figure previously claimed. The department also said 26 portable memory sticks containing classified information had been either stolen or misplaced since January 2008. [Another MoD laptop stolen, *The Guardian*, 20 Jul 2008; PGN-ed]

<<http://www.guardian.co.uk/uk/2008/jul/20/military.ukcrime>>

IP Archives: <https://www.listbox.com/member/archive/247/=now>

The \$100,000 Keying Error

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

Wed, 23 Jul 2008 11:45:55 +0100

When testing your systems, you do check for length as well as checksum errors, don't you?

http://www.computer.org/portal/site/computer/menuitem.5d61c1d591162e4b0ef1bd108bcd45f3/index.jsp?&pName=computer_level1_article&TheCat=1015&path=computer/homepage/0408&file=profession.xml&xsl=article.xsl&

An ordinary bank customer, Grete Fossbakk, used Internet banking to transfer a large amount to her daughter. She keyed one digit too many into the account number field, however, inadvertently sending the money to an unknown person. This individual managed to gamble away much of the sum before police confiscated the remainder.

<http://kursinfo.himolde.no/in-kurs/inf111/pensum/bank.pdf>

Patrick O'Beirne, Systems Modelling Ltd. <http://www.sysmod.com/>
(+353)(0) 5394 22294

✂ Taking a grab at what's the real system error

<jared <jared@netspace.net.au>>
Sat, 19 Jul 2008 09:33:28 -0600

The Capital Letters feature of the Saturday Guardian discusses a risk of on-line banking - what you see is not what you have.

<http://www.guardian.co.uk/money/2008/jul/19/consumeraffairs>

Q: I have a number of savings accounts with Bradford & Bingley which I access online. The total value is around 100,000 pounds. But often the on-screen version does not tally with the balance over the phone. Even worse, sometimes one of my accounts shows a negative figure, even though savings accounts cannot go below zero. The call centre says there must be a system error -- this appears every month.

A: At first B&B said it was impossible to be in the red on a savings account -- yours showed minus 1,100 pounds. But once you sent in your screen grab, clarity emerged.

You have, among others, an eSavings account where daily "updates" take place between the "core" system and the "Internet platform". To ensure the systems are fully aligned, B&B runs numerous "exchanges" of information.

So there can be times when the "processed balance" does not coincide with your available balance. Had you looked even a few minutes later, the minus figure would have gone. You have not lost by this.

B&B says it has not encountered this elsewhere and will have its systems people work on your account. It will apologise and send 50 pounds as a goodwill gesture.

[Sounds like you need some *original* B&B: Benedictine and Brandy. PGN]

#What's in a name?

*<Peter Houppermans <peter@houppermans.com>>
Sat, 19 Jul 2008 10:26:25 +0200*

Well, I found sequencing to be a problem too.

It is traditional to have more than one first name where I come from, so I have 3. One of them is the name by which I'm called, "Peter". The twist is that it is not the FIRST name of the three.

In my country of origin this is not a problem, it's accepted practice and calling names are stored separately from forenames (also because the formal names are often written in a more archaic form). But cross the borders and problems start, sometimes to the point of causing danger.

In the UK, for instance, it's a bit pot luck. When I moved to another place I had quite some trouble convincing a GP administrator to then enter my calling name first, but that "wasn't as in my passport" - the fact that business cards, credit cards and even the data from the former GP were labeled "Peter" had no impact. Only when I presented her with a letter to sign for acceptance of liability was it suddenly possible - the RISK was that an accident could put me in hospital in a state unable to explain they should look for my data under another name.

I moved again (this time to another country), and the circus has restarted. On entry, some official omitted the flag that marks the name by which I am called (in the new county they appear to have at least a way of marking the name - if it wasn't for the fact that my passport does NOT have such a mark - I think it's an omission in the EU passport standards). The knock-on effect is that I have to undo insurances, car registration and personal ID all in the wrong name. It's a long process..

Over the years I even had an official suggesting I should change my name or at least the sequence. So the idea is that I change my name to suit what is a clear lack of flexibility in official systems. Alas, I'm just on the wrong side of stubborn to rename myself to 12889-999-111, the logical end of that route.

Besides, I do derive some professional amusement from breaking systems :-).

#Yet more GPS risks: Angry Mob Stones Lost Tourist

*<Steven J Klein <steveklein@mac.com>>
Tue, 08 Jul 2008 11:18:56 -0400*

RISKS has run numerous reports of the trouble people get into by blindly following the instructions of their GPS navigation devices.

The Jewy News website just published the stories of two people who, following instructions from their GPS units, drove into dangerous neighborhoods and were attacked by mobs. Excerpt:

An American tourist was lightly injured by rocks hurled at him when he accidentally drove into the Qalandiyah refugee camp, west of Ramallah, Wednesday afternoon. Army sources said Wednesday that since the beginning of this year there have been several dozen cases of Israeli civilians mistakenly entering Area A, because of GPS navigational errors, and despite clear signs at the entrance to Palestinian towns warning Israelis not to enter.

<http://jewynews.com/2008/07/08/angry-arab-mob-stones-lost-american-tourist/>

Steven J Klein Your Mac Expert Phone: (248) YOUR-MAC or (248) 968-7622

✶ Shocking idea for air passenger security

<Robin Stevens <rejs@cynic.org.uk>>

Wed, 23 Jul 2008 18:45:38 +0100

In order to enhance the security of air travel and to help manage illegal immigration, the Department of Homeland Security has solicited a proposal from a Canadian security company to develop a passenger stun bracelet.

"By further equipping the bracelet with EMD technology, the bracelets will allow crew members, using radio frequency transmitters, to quickly and effectively subdue hijackers"

<http://www.informationweek.com/news/security/intrusion_prevention/showArticle.jhtml?articleID=208803214>

Now, what could *possibly* go wrong with this idea?

Robin Stevens <rejs@cynic.org.uk> <http://www.cynic.org.uk/>

✶ Re: Oyster card hack to be published ([RISKS-25.22](#))

<Amos Shapir <amos083@hotmail.com>>

Tue, 22 Jul 2008 17:40:58 +0300

"Details of how to copy the Oyster cards used on London's transport network can be published, a Dutch judge has ruled."

Full story at:

<http://news.bbc.co.uk/2/hi/technology/7516869.stm>

IMHO the most important sentence in the judge's ruling is : ""Damage to NXP is not the result of the publication of the article but of the production and sale of a chip that appears to have shortcomings." IOW (unlike what seems to be the law in the USA), if the King is naked it's his fault, not

the little boy's.

Re: San Francisco admin hijacks city net: Paul Venezia (RISKS-25.23)

<David Lesher <wb8foz@8es.com>>

Sat, 19 Jul 2008 23:49:23 -0400

[Source: Paul Venezia, *InfoWorld*, 19 Jul 2008]

<http://www.pcworld.com/businesscenter/article/148669-1/the_story_behind_san_franciscos_rogue_network_admin.html>

On 13 Jul 2008, Terry Childs, a network administrator employed by the City of San Francisco, was arrested and taken into custody, charged with four counts of computer tampering. He remains in jail, held on US\$5 million bail. News reports have depicted a rogue admin taking a network hostage for reasons unknown, but new information from a source close to the situation presents a different picture.

In posts to my blog <<http://weblog.infoworld.com/venezia/>>, I postulated about what might have occurred. Based on the small amount of public information, I guessed that the situation revolved around the network itself, not the data or the servers. A quote from a city official that Cisco was getting involved seemed to back that up, so I assumed that Childs must have locked down the routers and switches that form the FiberWAN network, and nobody but Childs knew the logins. If this were true, then regaining control over those network components would cause some service disruption, but would hardly constitute the "millions of dollars in damages" that city representatives feared, according to news reports.

Apparently, I wasn't far off the mark. In response to one of my blog posts, a source with direct knowledge of the City of San Francisco's IT infrastructure and of Childs himself offered to tell me everything he knew about the situation, under condition that he remain anonymous. I agreed, and within an hour, a long e-mail arrived in my in box, painting a very detailed picture of the events. Based on this information, the case of Terry Childs appears to be much more -- and much less -- than previously reported.

It seems that Terry Childs is a very intelligent man. According to my source, Childs holds a Cisco Certified Internetwork Expert certification, the highest level of certification offered by Cisco. He has worked in the city's IT department for five years, and during that time has become simply indispensable.

Although Childs was not the head architect for the city's FiberWAN network, he is the one, and only one, that built the network, and was tasked with handling most of the implementation, including the acquisition, configuration, and installation of all the routers and switches that comprise the network. According to my source's e-mail, his purview extended only to the network and had nothing to do with servers, databases, or applications:

"Terry's area of responsibility was purely network. As far as I know (which admittedly is not very far), he did not work on servers, except maybe VoIP servers, AAA servers, and similar things directly related to the administration of the network. My suspicion is that you are right about how he was "monitoring e-mail"; it was probably via a sniffer, IPS, or possibly a spam-filtering/antivirus appliance. But that's just conjecture on my part."

Re: ComCast in Concrete? MAC addresses (Fife, [RISKS-25.23](#))

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

Sat, 19 Jul 2008 11:18:38 -0400

> The ethernet adapter in a PC and the ethernet "WAN Port" on a router both
> have a unique six-byte identification known as a MAC (Medium Access Control)
> address. The first three bytes identify the manufacturer (i.e., Linksys),
> and the other three bytes identify the specific device. Default values are
> assigned by the manufacturer and programmed into the hardware.

Forgive the pedantry ...

The last three octets of a MAC aren't a "default" -- they are uniquely assigned to one device within all the ethernet interfaces that manufacturer builds [1] and the entire six octet address is globally unique because the value in the upper three octets are assigned to a single vendor by the IEEE. This is one of the fundamental points in the ethernet spec.

> If this doesn't work, I would turn off remote management, "Universal Plug
> and Play," and anything else that might allow the cable company to interact
> with your router over the network and recognize its specific behavior.

This is useful advice in that one should never expose to network access any functionality that isn't required.

UPnP is used particularly by games that need to open inbound connections on a device that filters traffic (usually a residential router device like a Linksys router performing network address translation [NAT]); the application needs to be able to receive incoming packets from a remote host for purposes of network gameplay.

In the case of the Linksys routers, the last time I looked at the source code (which Linksys makes available because the "firmware" in the device is linux) the routers didn't accept UPnP packets from the outside [WAN] interface.

[1] Or, more likely, purchases from a silicon vendor who builds ethernet chipsets!

Re: P2P Data Breach affects SCOTUS (Ashworth, [RISKS-25.23](#))

<Pete Klammer <netronics-pe@comcast.net>>

Sat, 19 Jul 2008 14:02:49 -0600

Many financial websites now allow you to choose your own security question(s), either from a multiple-choice list, or even an original one of your own choosing.

While considering the dossier that could be constructed from accumulating them (each one knows only my eye color, or only my birthplace, but together, my whole identity may be assembled); it dawned on me recently that I do not have to answer these questions truthfully -- only consistently. That is, if I set up with my eye color purple, and later remember and answer that question with purple, I can have my password resent, etc.

So now I answer all those security questions (even mother's maiden name) dishonestly, but with answers that I will not be able to forget.

In fact, it might behoove the webpage security designers to change the security questions to promote such behavior: "If Abcorp needs to confirm your identity, how would you answer the question, 'What color are your eyes?'"

Peter F. Klammer, P.E. / NETRONICS Professional Engineering, Inc.
3200 Routt Street / Wheat Ridge, Colorado 80033-5452 1-303-915-2673

Re: P2P Data Breach affects SCOTUS (Klammer, [RISKS 25.24](#))

<"Jay R. Ashworth" <jra@baylink.com>>

Mon, 21 Jul 2008 15:03:02 -0400

In light of the recent MySpace case, where prosecutors with nothing else to hang a case on are trying to convict that mother of *lying on her profile*, perhaps you *shouldn't* lie in the answers to those questions... but of course that just makes it worse. 1/2 :-)

You make a good point though, which was inherent in the observations I made, but subtle enough that I missed it: since you can't trust the site operators with passwords, there's no reason you believe that you can trust them with any other data either.

People would be inclined to say "but it's not reasonable to believe that large corporate sites would be involved in this sort of collusion!".

But we wouldn't have expected either of these things either:

http://rawstory.com/news/2008/Wiretap_immunity_bill_gets_closer_to_0709.html

http://rawstory.com/news/2008/Cybersecurity_expert_raises_allegations_of_2004_0717.html

and yet they appear to have happened.

Some sites do, in fact, ask the applicant to supply both the question and the answer, which seems perfectly reasonable: at least, it permits security-thoughtful applicants to protect themselves from this sort of thing.

All of this is also akin to the Middle Initial Gambit: tracking junkmail (usually of the paper variety) by putting a different middle initial in your name for each primary source, something which will usually pass in-band through the filters of the mailers in the middle. This sort of service is handled by disposable email addresses in this day and age, of course.

Jay R. Ashworth, Ashworth & Associates, St Petersburg FL USA +1 727 647 1274
<http://baylink.pitas.com> <jra@baylink.com>

Re: Approval voting and sincerity (Re: Youngman, [RISKS-24.23](#))

<Geoffrey Brent <gpbrent@optusnet.com.au>>
Sat, 19 Jul 2008 11:50:00 +1000

"Unless you get a very weird result (i.e., it's statistically very unlikely), one candidate will win all his individual contests. That person should be elected. Failing that, someone will almost certainly lose all his contests and should be eliminated. When they're removed from consideration the win-lose cycle can be repeated until you're left with a winner."

It won't do that. If you don't *immediately* have a candidate who has won all his individual contests (call that a 'universal winner'), then iteratively eliminating 'universal losers' will never produce a universal winner.

If nobody wins all their individual contests, then each candidate loses to somebody else. Suppose you can indeed find a 'universal loser' candidate Z. By definition, Z is *not* the guy that anybody else loses to, so if you remove him from the pool each of the remaining candidates still lose to one of the other remaining candidates. Removing Z might produce a new universal loser amongst the remaining candidates, but it will never produce a universal winner (and since you only have a finite number of candidates, eventually you'll hit the point where you run out of universal losers too).

To see how something like this might come about, consider a three-cornered election in which approximately one-third of voters are primarily concerned about foreign policy, one-third about healthcare, and one-third about taxation. If you randomly order the candidates' credibility on each of these three issues, you have a 1/18 chance of getting a deadlock where people are voting e.g. A-B-C, B-C-A, and C-A-B. Obviously real-life politics isn't that clear-cut, and the chances of a deadlock may be somewhat lower... but they could also be higher, especially when people modify their campaigning strategies to take advantage of the new system, and even a small rate of unresolved elections has the potential to cause a lot of trouble.

You can of course set up some sort of tie-breaker for such situations - e.g. use some other form of preferential counting among the remaining candidates - but this will inevitably run into one of the other clauses of Arrow's Theorem.

✉ Re: Approval voting and sincerity (Re: Youngman, [RISKS-24.23](#))

<"Richard Gadsden" <richard@gadsden.name>>

Tue, 22 Jul 2008 12:31:01 +0100

Not wishing to get into this debate in too much detail - this isn't infosec, and really shouldn't be on RISKS - but this is a Condorcet system, which has well-known vulnerabilities; voters who are confident that their first-choice will win the tiebreaker can deliberately induce a top cycle to block a sincere Condorcet winner where that winner is a centre-compromise candidate.

[Several of the words in the above paragraph are terms of art, notably "Condorcet", "sincere", "centre-compromise", "top cycle", "vulnerability"]

Rather than doing a worked example, my suggestion of the RISK here is that voting theory is a very specialised area of knowledge, and that non-experts should no more expect to be able to invent a voting algorithm than an encryption algorithm. RISKS doesn't normally discuss design details of encryption algorithms, and I would suggest that we should cease trying to discuss voting algorithms.

Suffice it to say that there are many different properties of voting algorithms, and different systems are optimised for different properties. One property that many would like to optimise for is that voters should not need information about other voters' likely ballots to determine how to cast their vote most effectively. What is meant (in the field of voting theory) by a 'sincere vote' is the vote that voter would cast given no information about other voters, just information about the candidates. Gibbard-Satterthwaite and Duggan-Schwartz and the extensions of their theorems to many non-preferential systems (approval, disapproval and scoring systems included) prove that this property is unachievable in theory.

For those wishing to try their own thought experiments, usual insincere votes are

- 1) Voting more strongly against a candidate you regard as middling in order to help your first choice.
- 2) Voting more strongly for a candidate you regard as middling to damage a candidate you are opposed to, often abandoning your first choice to do so.
- 3) Voting for a candidate you really hate in order to put them above someone you merely dislike, where the one you dislike has a chance of winning and the one you hate does not.

✂ NC State Voter site exposes voter addresses

<John O Long <j1long@mindspring.com>>

Tue, 22 Jul 2008 09:57:49 -0400 (GMT-04:00)

The North Carolina Board of Elections has made it possible to learn quite a bit about any registered voter in the state.

Go to their site at <http://www.sboe.state.nc.us/Default.aspx?s=0> and click on My Election Information. Select Show Me My Voter Information and enter your name and county. You are then presented with all of the people who match your first and last name in your county. You can select any of them and find out:

- their address
- what party they are registered with
- which elections and primaries they voted in
- voter registration number

I think a lot of people wouldn't want their address exposed in this way. I know I wasn't too happy to see this.

However, it also makes it easier for voter fraud to take place. If I find someone in my county who doesn't vote very often, I can show up at their polling place and vote for them. If necessary, I can provide their voter registration number. However, I don't need to provide a photo ID.

[Most of this information is publicly available. However, systematically data mining it to identify folks who were not voting could indeed lead to organized fraud. For example, I recall a former North Carolina resident telling me that when he returned to NC after many years of voting as a resident of California, he went to register again in NC. He was informed that not only was he *still* registered -- he was recorded as having voted in every election (while he was voting in California)! PGN]



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 25

Sunday 3 August 2008

Contents

- ["Software bug" downs AA baggage handling at JFK](#)
[PGN](#)
 - [Intermittent network card causes air traffic control problems](#)
[Steven M. Bellovin](#)
 - [Crypto box failure causes MTA credit card processing failure](#)
[Steven M. Bellovin](#)
 - [200,000 medical records sent to wrong patients, some with SSNs](#)
[George Mannes](#)
 - [DNA Database Searches](#)
[jared](#)
 - [Another GPS error story](#)
[Gene Spafford](#)
 - [Electronic voting: Indications of Sanity?](#)
[Geoff Newbury](#)
 - [Risks of Inflation: new Zimbabwe bank notes](#)
[Jim Reisert](#)
 - [Bruce Schneier: Inside the Twisted Mind of the Security Professional](#)
[jidanni](#)
 - [Details of DNS Flaw Leaked](#)
[Kim Zetter via Monty Solomon](#)
 - [Apple Fails to Patch Critical Exploited DNS Flaw](#)
[Rich Mogull via Monty Solomon](#)
 - [Fascinating phishing attack: valid links, dangerous toll-free number](#)
[Jonathan Kamens](#)
 - [Re: San Francisco FiberWAN and Terry Childs](#)
[Jeff Williams](#)
 - [Re: ComCast in Concrete? MAC addresses](#)
[Tanner Andrews](#)
 - [REVIEW: "Internet Denial of Service", Jelena Mirkovic et al.](#)
[Rob Slade](#)
 - [REVIEW: "AVIEN Malware Defense Guide for the Enterprise", David Harley et al.](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

"Software bug" downs AA baggage handling at JFK

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

Wed, 30 Jul 2008 14:45:16 PDT

[TNX to Lauren Weinstein for spotting this one. PGN]

American Airlines had a baggage problem at JFK that caused many bags to miss their intended flights, despite that fact that 35 flights were delayed up to an hour and one-half. Beginning at 4:45am, the software controlling the baggage sorting operations malfunctioned, and bags had to be sorted by hand.

<http://travel.latimes.com/daily-deal-blog/index.php/baggage-snafu-hits-a-2395/>

Intermittent network card causes air traffic control problems

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Sun, 27 Jul 2008 10:42:26 -0400

According to <http://www.techcentral.ie/article.aspx?id=12346> an intermittent failure in a network card caused problems for the air traffic control system in Ireland. Apparently, the fact that the failure was intermittent was enough to confuse the fail-over mechanisms. The trouble lasted for about six weeks before it was diagnosed. "Thales ATM stated that in ten similar Air Traffic Control Centres worldwide with over 500,000 flight hours (50 years), this is the first time an incident of this type has been reported."

--Steve Bellovin, <http://www.cs.columbia.edu/~smb>

Crypto box failure causes MTA credit card processing failure

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Thu, 31 Jul 2008 17:08:26 -0400

Many people buy MetroCards -- mag stripe swipe cards for riding New York City subways and buses -- using credit cards. For a few days, though, this wasn't working well during rush hour; credit card transactions were being rejected. They finally figured it out: one of the crypto units to protect credit card numbers in transit had failed. There was another unit, but it couldn't handle peak loads by itself, so transactions timed out and hence failed.

<http://cityroom.blogs.nytimes.com/2008/07/31/mta-blames-encryption-for-metrocard-problems/>

There are a few lessons here. One, of course, is that headline writers shouldn't be trusted to get technical details right. Saying "M.T.A. Blames Encryption for MetroCard Problems" is just wrong -- the MTA didn't blame encryption, they blamed the failure of a particular unit.

More substantively, there were two serious problems with the technical design of the system. First, there was insufficient redundancy; failure of a single unit left the system unable to handle the load. Second, there was no notification to the administrators of the failure of the unit. Once they figured it out, they were able to cope -- they had a spare available -- but they didn't know that there was a failure.

--Steve Bellovin, <http://www.cs.columbia.edu/~smb>

#200,000 medical records sent to wrong patients, some with SSNs

<"George Mannes" <gmannes@gmail.com>>

Tue, 29 Jul 2008 11:29:39 -0400

[Source: Andy Miller, *The Atlanta Journal-Constitution*, 29 Jul 2008; PGN-ed]

A change in a computer system was "not properly tested";

Private medical data exposed;

Insurance benefit letters sent to wrong addresses by Blue Cross and

Blue Shield reveal claim histories, open door to ID theft.

http://www.ajc.com/news/content/news/stories/2008/07/29/bluecross.html?cxntnid=amn072908e&cxntlid=homepage_tab_newstab

BC&BS sent an estimated 202,000 benefits information letters containing personal and health information -- identities, ID numbers, and service details -- to the wrong addresses last week. Some letters also contained SSNs. This situation seems to be in violation of HIPPA (the U.S. Health Insurance Portability and Accountability Act of 1996).

#DNA Database Searches

<jared <jared@netspace.net.au>>

Thu, 24 Jul 2008 20:49:55 -0600

An article "How reliable is DNA in identifying suspects?" recently appeared.

<http://www.latimes.com/news/local/la-me-dna20-2008jul20,0,1506170,full.story>.

The lead is:

A discovery leads to questions about whether the odds of people sharing genetic profiles are sometimes higher than portrayed. Calling the finding meaningless, the FBI has sought to block such inquiry.

The article illustrates two computer risks. The first is that data is not free.

Each jurisdiction operates its own DNA database but relies on American federal CODIS (Combined DNA Index System) to search across multiple databases. Defense lawyers are interested in determining group statistics. DNA comparisons are apparently made based on how many of 13 loci

are similar. They want to know, for example, how many people in the database match in 9, 10, 11, 12 or even 13 loci. (Reportedly some prosecutors cite less than 13 loci matching as a 'DNA evidence'.)

- > FBI officials argue that, under their interpretation of federal
- > law, use of CODIS is limited to criminal justice agencies. In their
- > view, defense attorneys are allowed access to information about
- > their specific cases, not the databases in general.

A court order was made for a search of one state's database. The article reports an FBI employee said that the search could lead to the database being disconnected from CODIS. There was a warning that the search could corrupt the state database. In the end neither event occurred.

The second risk is an overloading of the database's intent. The tricky bit of the search results is that closely related people may match very well but the database, as one might expect, doesn't have this information.

As a note, the article illuminates many of the usual statistical risks.

Another GPS error story

<Gene Spafford <spaf@cerias.purdue.edu>>
Sat, 26 Jul 2008 18:41:07 -0400

Sat-nav driver's 1600-mile error: A DOZY trucker driving from Turkey to Coral Road in Gibraltar ended up at Skegness. Gibraltar is considered part of the UK by the Sat-Nav systems.

<http://www.thesun.co.uk/sol/homepage/news/weird/article1447400.ece>

Electronic voting: Indications of Sanity?

<"R. G. [Geoff] Newbury" <newbury@mandamus.org>>
Thu, 31 Jul 2008 12:59:01 -0400

Indications of Sanity? A politician likes *paper* ballots..

http://www.theregister.co.uk/2008/07/30/debra_bowen_usenix_keynote/

[YES. California Secretary of State Debra Bowen was the keynote speaker at Usenix Security on 30 Jul 2008 in San Jose. She really wowed the audience with her candor, clarity, and relevance. We owe her our enormous gratitude for spearheading the Summer 2007 Top To Bottom Review of voting machines (with reports on software analyses, documentation, penetration testing, and accessibility), for following up on it, and generally for being one of the nation's first high government officials to really grasp the significance of the risks that we have been discussing here for so many years relating to elections -- indeed, since [RISKS-1.01](#). Her efforts are now beginning to be emulated in Ohio and other states. PGN]

✂ Risks of Inflation: new Zimbabwe bank notes

<Jim Reisert AD1C <jjreisert@alum.mit.edu>>
Thu, 24 Jul 2008 17:01:15 -0700 (PDT)

http://www.huffingtonpost.com/2008/07/24/zimbabwes-money-worth-mor_n_114838.html

"One major commercial bank said its automated teller machines are not configured to dispense multi-zero withdrawals and freeze in what it called a "data overflow error." Software writers are busy writing programs to try to overcome the problem."

Jim Reisert <jjreisert@alum.mit.edu>, <http://www.ad1c.us>

✂ Bruce Schneier: Inside the Twisted Mind of the Security Professional

<jidanni@jidanni.org>
Fri, 25 Jul 2008 20:20:20 +0800

[Bruce Schneier's WiReD.com article cited below by jidanni outlines the Security Mindset espoused by Tadayoshi Kohno in an undergraduate course on computer security at the University of Washington. It's worth reading. Security need not be in the eyes of the beholder. It should be in the eyes and ears and fingers and mind of the attackers. PGN]

http://www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters_0320

✂ Details of DNS Flaw Leaked

<Monty Solomon <monty@roscom.com>>
Sun, 27 Jul 2008 11:33:10 -0400

Kim Zetter's WiReD.com blog, Details of DNS Flaw Leaked; Exploit Expected by End of Today, 22 Jul 2008

<http://blog.wired.com/27bstroke6/2008/07/details-of-dns.html>

Despite Dan Kaminsky's efforts to keep a lid on the details of the critical DNS vulnerability he found, someone at the security firm Matasano leaked the information on its blog yesterday, then quickly pulled the post down. But not before others had grabbed the information and reposted it elsewhere, leading Kaminsky to post an urgent 0-day message on his blog reading, "Patch. Today. Now. Yes, stay late."

Hackers are furiously working on an exploit to attack the vulnerability. HD Moore, creator of the Metasploit tool, says one should be available by the

end of the day.

Earlier this month, Kaminsky, a penetration tester with IOActive, went public with information about a serious and fundamental security vulnerability in the Domain Name System that would allow attackers to easily impersonate any website -- banking sites, Google, Gmail and other web mail websites -- to attack unsuspecting users.

Kaminsky announced the vulnerability after working quietly for months with a number of vendors that make DNS software to create a fix for the flaw and patch their software. On July 8, Kaminsky held a press conference announcing a massive multivendor patch among those vendors, and urged everyone who owns a DNS server to update their software.

But Kaminsky broke one of the fundamental rules of disclosure in announcing the bug. He failed to provide details about the flaw so system administrators could understand what it was and determine if it was serious enough to warrant an upgrade to their systems.

Kaminsky promised to reveal those details next month in a presentation he plans to give at the Black Hat security conference in Las Vegas. But he said he wanted to give administrators a 30-day head start to get their systems patched before he provided details that could allow hackers to create an exploit to attack the systems.

Kaminsky asked researchers not to speculate about the bug details in the meantime and to trust that it was a serious issue. Some did as he asked. But many security researchers took his coyness as a challenge to uncover the details Kaminsky was holding back. ...

Apple Fails to Patch Critical Exploited DNS Flaw

*<Monty Solomon <monty@roscom.com>>
Sun, 27 Jul 2008 11:25:51 -0400*

Rich Mogull, TidBITS, 24 Jul 2008, <http://db.tidbits.com/article/9706>

On 08 Jul 2008, a massive security patch was released by dozens of vendors for a major vulnerability in DNS [1] (Domain Name Service), discovered by security researcher Dan Kaminsky. DNS [2] is one of the fundamental underpinnings of the Internet; translating domain names (like tidbits.com) into IP addresses (like 192.168.0.12). Because DNS is so core to the functioning of the Internet, this vulnerability is perhaps the most significant security problem to face the Internet in the last decade.

All users who connect to Mac OS X servers for DNS lookups are at risk: Apple has not yet provided a patch, unlike dozens of other companies that make or distribute operating systems or DNS server software.

Apple was clearly distracted by the largest set of launches in its history: the iPhone 3G, the iPhone 2.0 software, the .Mac-to-MobileMe transition, and

the App Store. Nonetheless, their customers are now in danger and Apple needs to respond immediately.

All companies that provide DNS service to their customers should have already updated their DNS servers. Many have not. You can determine whether your ISP is at risk by visiting Kaminsky's site and clicking Check My DNS [3]. If the site says your DNS is at risk of being poisoned, contact your ISP or your company's IT department immediately. ...

✂ Fascinating phishing attack: valid links, dangerous toll-free number

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

Wed, 30 Jul 2008 15:20:05 -0400

A phishing message in my spam folder caught my eye today, so I decided to take a closer look at it.

It claimed to be from CapitalOne. It had a legitimate sender address, a legitimate Subject line ("Please Call Us Regarding Recent Restrictions"), and convincing-looking content that was mostly lifted straight from a real CapitalOne email message. Most importantly, all of the links in the message were legitimate links pointing at capitalone.com URLs.

The only text in the message that was not boilerplate was this:

```
>Please Call Us Regarding Recent Resctriction [sic]
>
>This is not a promotional e-mail. Please call us
>immediately at (866) 496-5027 regarding recent activity on
>your Capital One Card. We're available 24/7 to take your
>call.
>
>Please disregard this e-mail if you've already call us
>since the date this e-mail was sent.
>
>We appreciate your prompt attention to this matter.
>
>Thank you
>Capital One Card Fraud Prevention Security Department
```

Here's what makes this phishing message different from others I've seen: the "hook" is the phone number, not the links in the email body.

Here's what you hear, recited in a female, synthesized voice, when you call the number shown above:

```
>Welcome to the the card activation center. Please remember
>that we will never ask for your personal information such
>as your social security number, passwords, card numbers,
>etc. via email. Please enter your card number followed by
>the pound key.
```

>
>[doesn't matter what you enter here]
>
>Please enter your personal identification number associated
>with this card followed by the pound key.
>
>Please enter your four-digit expiration number [sic]
>(months year) followed by the pound key.
>
>Please hold while your card is activated.
>
>The card number, personal identification number or
>expiration date doesn't match with our records.
>
>[starts over]

Obviously, whoever set up this toll-free number is collecting card numbers, expiration dates and PINs, which they will then either sell or use to obtain cash advances from ATMs.

I wish there were somewhere I could report this scam to get the toll-free number taken down, but I honestly have no idea who would be interested in doing something about this and able to act quickly.

Re: San Francisco FiberWAN and Terry Childs ([RISKS-25.23,24](#))

*<Jeff Williams <jeffw@lmi.net>>
Wed, 23 Jul 2008 15:36:59 -0700*

San Francisco is a tech powerhouse -- the local daily paper is not. This has led to a lack of good information about one of the most interesting tech stories of the year: the showdown between a contractor and city administrators over proper handling of network security.

Some of you may have already seen this (via Slashdot):
http://www.infoworld.com/article/08/07/18/30FE-sf-network-lockout_1.html

It's an article based on a confidential 3rd party who had a ringside seat.

The risk? Some tech jobs seem to carry the risk that they can ruin your life (I don't mean figuratively). Large corporations and governments wield an enormous power to punish and seemingly no power to understand the nuance and complexity of technical risk. Under this situation being a jerk could be a felony at some job sites. We can stand in judgment of when it makes sense to let go of a fight with your manager, but how many of us would stand up to what we see as a terrible wrong in a way that could ruin us professionally?

That a politically ambitious DA has made this a publicity grabbing event seems to open a serious can-of-worms for ordinary technical workers. The San Francisco DA is inadvertently creating the blueprint for handling nasty

tech employee disputes. Today she has the sheriff saying that Childs set the system up for "meltdown" at the next routine maintenance. The inside story seems to be that he didn't want to store the router configs into flash at the remote sites. When pressed the sheriff acknowledges that the system is up. This might not be the best way to run a shop, but is it a actual crime to not write configs to flash? Does the DA even know what flash is? (Maybe she knows but has decided to make an example of what happens when you stand up to your manager.)

It seems arbitration would have helped here. Would a system of neutral party dispute resolution go a long way to reducing system cost and preserving careers in the tech field without introducing drastic measures such as full-blown unionization? Like other professionals, maybe tech workers should carry general liability insurance where the carrier offers arbitration as a front-line defense against arrest and/ or lawsuit. (And funds to defend yourself if something goes wrong.)

Re: ComCast in Concrete? MAC addresses

*<tanner andrews <tanner@payer.org>>
Thu, 24 Jul 2008 09:48:13 -0400 (EDT)*

> [MAC addresses are unchangeable once set at factory]

Not so. The default is hard to change, because it is set in the part, but for operation you can change it as you will.

For instance, though my network boards on my firewalls will occasionally get zapped by lightening, the ISP does not know that. The ISP believes that my MAC addresses are some that I made up years ago and continue to use.

Thus, when I get zapped and put in a new board, the ISP re-assigns the same IP address I had before. If I do not do this, they will pick a new address.

Not all operating systems support easy changing of the MAC address, so your mileage may vary.

[Several other messages on this topic, but we are drifting in relevance.
PGN]

REVIEW: "Internet Denial of Service", Jelena Mirkovic et al.

*<Rob Slade <rmslade@shaw.ca>>
Thu, 31 Jul 2008 12:03:22 -0800*

BKNTRDOS.RVW 20080420

"Internet Denial of Service", Jelena Mirkovic et al, 2005,

0-13-147573-8, U\$39.99/C\$57.99

%A Jelena Mirkovic

%A Sven Dietrich

%A David Dittrich dittrich@u.washington.edu

%A Peter Reiher

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

%D 2005

%G 0-13-147573-8

%I Prentice Hall

%O U\$39.99/C\$57.99 800-576-3800 416-293-3621 201-236-7139

%O <http://www.amazon.com/exec/obidos/ASIN/0131475738/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0131475738/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0131475738/robsladesin03-20>

%O Audience i+ Tech 2 Writing 2 (see revfaq.htm for explanation)

%P 372 p.

%T "Internet Denial of Service: Attack and Defense Mechanisms"

Chapter one is an introduction to the book itself, rather than the topic, asserting that the work is intended for an audience of system administrators, corporate managers, and those dealing with public policy. The topic is defined in chapter two, which notes that denial of service (DoS) is not like other security risks where intrusion or use (or misuse) of resources is the aim, but prevention of the legitimate use of a system. Much of the material concentrates on distributed denial of service (DDoS), and the text mentions the inherent risk of DoS where a service is being provided. The structure and logical flow of the content is not always obvious, but the information is reasonably clear and readable. The history of DoS attacks, starting with the early, simple assaults intended to gain status and notoriety and progressing through to the recent complex and financially motivated offensives, is covered in chapter three. There is discussion of the fact that the structure of the Internet works against many protective measures and hinders efforts to collect digital forensic evidence. Chapter four examines the process, technology, and tools of DDoS attacks.

Defence is contemplated in chapter five, along with the intrinsic difficulty presented by the need for availability, the possibility of attacking either the computer-based service or the network-based communications, and a poor authentication and tracking infrastructure. The deliberation does note that defence can be attempted in many layers, from secure application development to overt reaction. A detailed analysis of some defensive approaches is provided in chapter six, which assessment is also valuable in terms of business continuity planning. Chapter seven has a listing and review of various research projects on defence. Legal issues are catalogued in chapter eight: most of the content is general, but there is a fair amount that is specific to the United States. Chapter nine summarizes major points, and speculates on future trends.

This is a thorough overview of a topic that is covered poorly, if at all, in most of the security literature. Availability has come very late to add depth to the C-I-A (Confidentiality, Integrity, Availability) triad, and therefore DoS attacks are still misunderstood as mere nuisance. The problem is growing, and this material should be of greater interest to those charged

with protecting both corporate assets and the public infrastructure.

copyright Robert M. Slade, 2008 BKNTRDOS.RVW 20080420
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
victoria.tc.ca/techrev/rms.htm blogs.securiteam.com/index.php/archives/author/p1/

REVIEW: "AVIEN Malware Defense Guide for the Enterprise", David

<Rob Slade <rmslade@shaw.ca>>
Thu, 24 Jul 2008 11:10:25 -0800

Harley et al.

BKAVNMDG.RVW 20080420

"AVIEN Malware Defense Guide for the Enterprise", David Harley et al,
2007, 978-1-59749-164-8, U\$59.95

%A David Harley David.A.Harley@gmail.com

%A Ken Bechtel

%A Michael Blanchard

%A Henk K. Diemer

%A Andrew Lee

%A Igor Muttik

%A Bojan Zdrnja

%C 800 Hingham Street, Rockland, MA 02370

%D 2007

%G 1-59749-164-0 978-1-59749-164-8

%I Syngress Media, Inc.

%O U\$59.95 781-681-5151 fax: 781-681-3585 www.syngress.com

%O <http://www.amazon.com/exec/obidos/ASIN/1597491640/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/1597491640/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/1597491640/robsladesin03-20>

%O Audience i+ Tech 2 Writing 2 (see revfaq.htm for explanation)

%P 540 p.

%T "AVIEN Malware Defense Guide for the Enterprise"

The preface and introduction stress that this work is a collaborative effort, combining the views of a number of AVIEN (Anti-Virus Information Exchange Network) and AVIEWS (Anti-Virus Information and Early Warning System) members, trying to avoid the blind spots that result from perspectives limited to one individual or company.

Chapter one outlines the history of AVIEN, noting the tensions between the (rather small) community that has concentrated on research about malware and protection against the various threats and the general user population. (The general user population includes, for various reasons, many of the producers and vendors of antivirus products.) It is noted (although not stressed) that AVIEN concentrates on protection of medium to large companies, and this point is important in regard to protective approaches.

A brief, historically-oriented, look at malware and related issues, in chapter two, tries to eliminate common confusion and sets a groundwork for further discussion. The Web is now a major source of security

vulnerabilities, but the malware literature has seldom considered the problem as a specific category, so chapter three's excellent overview of the related technologies and exploits is particularly welcome. Botnets are a major threat (or threats: they are used in a variety of ways), and there is a good examination of the major associated concepts in chapter four. Unfortunately, the material is somewhat loosely structured and may be confusing to some readers, and occasionally emphasizes specific (and sometimes dated) technologies rather than the basic ideas. Chapter five examines the often-asked question of who writes malware, bringing up a good deal of interesting material. The text itself may be of scant use to system administrators, although the points made in the summary do indicate trends of concern.

Chapter six turns to protective measures, covering not just the usual antiviral technologies, but advising on layered defence, with the attendant required planning and management. Outsourcing, of security functions in general, and antiviral protection in particular, is reviewed in chapter seven, with attention paid to both the dangers and the conditions, agreements, and other factors that might provide success. Chapter eight's look at security awareness training and user education seems to be intended to promote the idea, but is weaker in providing solutions than other areas of the book, concentrating primarily on the difficulties and failures.

A variety of tools that might be used in malware analysis, ranging from system information utilities through debuggers to online virus detectors, are listed in chapter nine. Chapter ten considers aspects of evaluating antiviral products, and makes a good, general guide.

Chapter eleven notes that the AVIEN organization is changing, and feels like a promotional item to get the reader to become involved, but the lack of detail of what the institution might become does not seem calculated to appeal to busy administrators.

The book contains a tremendous wealth of information and references to specific resources and studies. This is not surprising, given the background of the authors, and would, alone, make the text worthwhile. Overall this work provides a solid overview and compendium of advice on the current malware situation, and should be a required starting point for anyone protecting corporate assets in the current, highly threatening, environment.

copyright Robert M. Slade, 2008 BKAVNMDG.RVW 20080420
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 26

Wednesday 6 August 2008

Contents

- ['Fakeproof' microchipped British e-passport is cloned in minutes](#)
[Martyn Thomas](#)
- [On Metro Fraud and NXP](#)
[David Lesher](#)
- [11 charged in largest ID theft in U.S. history](#)
[Paul Saffo](#)
- [Theft perils 150,000 on Busch laptop](#)
[PGN](#)
- [Verified Identity Pass: CLEAR Suspended Following Laptop Theft](#)
[PGN](#)
- [Unsuspected travelers' laptops may be detained at border](#)
[Ellen Nakashima via Monty Solomon](#)
- [Neglecting to logout from Skype means sharing your Instant Messages](#)
[Michael Weiner](#)
- [Another small interface risk](#)
[Peter Zilahy Ingerman](#)
- [E-Z Pass Maryland training customers to visit random sites?](#)
[Mike Porter](#)
- [Prescription Data Used To Assess Consumers](#)
[Ellen Nakashima via Monty Solomon](#)
- [Re: What's in a name?](#)
[Dag-Erling Smørgrav](#)
- [Re: UPS ... indistinguishable from phishing](#)
[G.M.Sigut](#)
- [Re: Fascinating phishing attack: valid links, dangerous ... number](#)
[Al Macintyre](#)
- [Re: Apple Fails to Patch Critical Exploited DNS Flaw](#)
[Robin Stevens](#)
- [Re: Another GPS error story](#)
[J.R. Stockton](#)
- [Survey: Perception of security in online environments](#)
[Gene Spafford](#)
- [REVIEW: "The Innocent Man", John Grisham](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

'Fakeproof' microchipped British e-passport is cloned in minutes

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

Wed, 06 Aug 2008 09:21:06 +0100

<http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece>

Martyn Thomas CBE FREng <http://www.thomas-associates.co.uk>

On Metro Fraud and NXP

<wb8foz@panix.com (David Leshner)>

Thu, 24 Jul 2008 12:17:57 -0400 (EDT)

I wondered whether the recent mag-stripe card fraud arrests ([RISKS-25.24](#)) would prompt WMATA [DC Metro] to intensify their campaigns to encourage/coerce riders into their new stored value smartcards, over the existing anonymous magstripe/paper ones.

That same day, multiple sources report a Dutch judge ruled that research by Prof Bart Jacobs (see [RISKS-25.17](#)) and colleagues from Radboud University, Nijmegen in March 2008 can be published. This work exposed significant flaws in NXP's smartcards, used in London's "Oyster" transport system ([RISKS-25.22](#) and 24), transit systems in many other cities, and for access to many Dutch government buildings.

The vendor, NXP sought a permanent injunction against releasing the work.

The court ruled: "Damage to NXP is not the result of the publication of the article but of the production and sale of a chip that appears to have shortcomings."

<http://technology.timesonline.co.uk/tol/news/tech_and_web/article4373717.ece>

<<http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7516869.stm>>

11 charged in largest ID theft in U.S. history

<Paul Saffo <paul@saffo.com>>

Tue, 5 Aug 2008 22:21:08 -0700

[Another compelling reminder to go to the ATM and -- USE CASH! -p]

More than 40 million debit and credit card account numbers were stolen from major retailers. Fraud is estimated in the tens of millions of dollars.

[Source: Joseph Menn and Andrea Chang, 11 charged in largest ID theft in U.S. history, *Los Angeles Times*, 5 Aug 2008; PGN-ed]

<http://www.latimes.com/business/la-fi-hack6-2008aug06,0,6262500.story>

Federal authorities said Tuesday that they had cracked the largest case of identity theft in U.S. history, charging 11 people in the theft of more than 40 million credit and debit card account numbers from computer systems at such major retailers as TJ Maxx and Barnes & Noble. The three-year investigation by federal agencies and overseas allies brought home the global nature of the Internet's underground economy as agents tracked leads from China to Ukraine and picked up suspects in Turkey and Germany as well as the U.S.

To the chagrin of the U.S. Secret Service, which handles many electronic fraud investigations, the trail led back to one of its own informants, Albert Gonzalez. Justice Department officials said Gonzalez served as the ringleader and double-crossed the agency by tipping off his cohorts. Prosecutors said Gonzalez could face a life term in prison.

✶ Theft perils 150,000 on Busch laptop

*<"Peter G. Neumann" <neumann@csl.sri.com>>
Tue, 5 Aug 2008 14:16:13 PDT*

About 150,000 people in six states have been affected by the theft in June 2008 of laptops that contained personal information on current and former Anheuser-Busch employees. [Source: a short item in the *San Francisco Chronicle*, 5 Aug 2008, p. D2; PGN-ed]

✶ Verified Identity Pass: CLEAR Suspended Following Laptop Theft

*<"Peter G. Neumann" <neumann@csl.sri.com>>
Tue, 5 Aug 2008 10:36:43 PDT*

[Thanks to Richard M. Smith]

Verified Identity Pass, which operates under the brand name CLEAR, was suspended by the Transportation Security Administration Monday after a laptop containing personal information for 33,000 people signing up for their registered traveler program was stolen from San Francisco International Airport.

The company is in the process of notifying the people, who were signing up for an expedited airport check-in service, that their personal information may have been stolen.

Officials said a laptop containing the data was stolen from a locked office at the airport. The information on the laptop was not encrypted. There was no credit card data or any social security numbers stored on the laptop, but there were names, addresses and other personal data.

Verified Identity Pass will not be able to enroll new customers into the registered traveler program until the TSA verifies that the company is compliant with security procedures.

<http://abclocal.go.com/kgo/story?section=news/local&id=6306342>

[CLEAR-ed out for now, but don't forget TSA Loses Hard Drive With Personal Info on about 100,000 employees, [RISKS-24.66](#), 8 May 2007.

<http://catless.ncl.ac.uk/Risks/24.66.html#subj8>

PGN]

Unsuspected travelers' laptops may be detained at border

<Monty Solomon <monty@roscom.com>>

Mon, 4 Aug 2008 20:05:30 -0400

Ellen Nakashima, Travelers' Laptops May Be Detained At Border; No Suspicion Required Under DHS Policies, *The Washington Post*, 1 Aug 2008, A01

Federal agents may take a traveler's laptop computer or other electronic device to an off-site location for an unspecified period of time without any suspicion of wrongdoing, as part of border search policies the Department of Homeland Security recently disclosed.

Also, officials may share copies of the laptop's contents with other agencies and private entities for language translation, data decryption or other reasons, according to the policies, dated July 16 and issued by two DHS agencies, U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement. ...

<http://www.washingtonpost.com/wp-dyn/content/article/2008/08/01/AR2008080103030.html>

Neglecting to logout from Skype means sharing your Instant Messages

<"Michael Weiner" <michael_weiner@gmx.net>>

Tue, 05 Aug 2008 20:32:32 +0200

Six months ago, I briefly used Skype on a friend's laptop. Yesterday, that very friend -- who is not very computer-savvy -- told another friend of mine that she had found a way to read other people's Skype messages. The other friend looked into the matter -- turns out that I had remained logged in on her laptop for the past six months and that she had read every single of my instant messages during that time. Obviously, I had not noticed that the "Automatically log this user on" box was ticked when I logged on and had forgotten to log out.

The RISKS are obvious. So are possible fixes: The "Automatically log this user on every time Skype starts" box should never be active by default and a confirmation should be requested. Also, Skype should make users aware if they are simultaneously logged into the same account from different

machines. The only way out at the moment is to change the Skype password frequently as this will terminate all sessions you may have forgotten to log out from yourself.

According to several messages on the Skype Community forum, Skype considers the ability to remain logged in to the same account on several machines a "feature" and sees no need to fix anything.

✂ Another small interface risk

*<"Peter Zilahy Ingerman, PhD" <pzi@ingerman.org>>
Thu, 24 Jul 2008 17:07:00 -0400*

Granite Commerce (www.granitewebdesign.com) sells a packaged e-commerce product. I discovered, when setting up an account with a store that uses this software, one of the "security questions" offered is "What city were you born in?". Not, on face, unreasonable.

However ... they only want a one-word answer (and don't say that!), so that any city requiring an embedded space (e.g. "New York City") is rejected as being invalid.

[PGN asked PZI:

Are there any length constraints?

Are there checks for your designated birth city being legitimate?

Otherwise, I suppose you could write Newyorkcity.]

Actually, I verified with the company that purchased the use of the software ... and it is, exactly, that the software "requires" a single word, with no other checks!

[Wow! Spaced-out software. PGN]

✂ E-Z Pass Maryland training customers to visit random sites?

*<Mike Porter <mike@udel.edu>>
Thu, 24 Jul 2008 10:41:19 -0400 (EDT)*

... and type in a PIN?

My EZ-Pass Maryland statements come to me as follows. The From: field does not even make an attempt to represent EZ-Pass Maryland, and the headers do not either. I spoke with the EZ-Pass Maryland help desk and they suggested the message was likely a phishing message.

However, phone calls to the sender led to an IT person who claimed they did in fact handle statements for EZ-Pass Maryland. Eventually, I did type in my PIN and a valid statement was produced.

Email to EZ-Pass Maryland asking for further clarification has been ignored. I still do not know for sure if this message is valid, but the PIN I use for this site is unique. I also receive these each month and do not receive anything else from EZ-Pass Maryland.

----- Forwarded message -----

Return-Path: <ezbounce@isecurus.com>

Received: from md1.nss.udel.edu (md1.nss.udel.edu [128.175.1.11]) ...

Received: from isecurus.com ([198.190.195.76])

Date: Wed, 16 Jul 2008 12:44:25 -0400

From: E-ZPass Customer Service<ezpass@isecurus.com>

To: <me>

Subject: E-ZPass Statement

Reply-To: ezpass@isecurus.com

...

Your statement will be available for 30 days from the date of this e-mail. If you will need to access your statement beyond the 30 day period or wish to save your statement, please access the link below. ...

https://ezpassstatements.gdocs.com/EZPassMtg/EZPass.cfm?p_no=#####

Prescription Data Used To Assess Consumers (Ellen Nakashima)

<Monty Solomon <monty@roscom.com>>

Mon, 4 Aug 2008 18:56:39 -0400

Records Aid Insurers but Prompt Privacy Concerns

[Source: Ellen Nakashima, *The Washington Post*, 4 Aug 2008; A01; PGN-ed]

Health and life insurance companies have access to a powerful new tool for evaluating whether to cover individual consumers: a health "credit report" drawn from databases containing prescription drug records on more than 200 million Americans. Collecting and analyzing personal health information in commercial databases is a fledgling industry, but one poised to take off as the nation enters the age of electronic medical records. While lawmakers debate how best to oversee the shift to computerized records, some insurers have already begun testing systems that tap into not only prescription drug information, but also data about patients held by clinical and pathological laboratories.

<http://www.washingtonpost.com/wp-dyn/content/article/2008/08/03/AR2008080302077.html>

Re: What's in a name? (Houppermans, [RISKS-25.24](#))

<"Dag-Erling Smørgrav" <des@des.no>>

Fri, 25 Jul 2008 14:33:25 +0200

Peter Houppermans <peter@houppermans.com> writes:

> [...] Over the years I even had an official suggesting I should change

> my name or at least the sequence. So the idea is that I change my
> name to suit what is a clear lack of flexibility in official systems.

There was a news report a few years ago of a Norwegian company that decided to drag its blue-collar employees kicking and screaming into the 21st century by giving them all free Internet access and email accounts. The IT department arrived at a strict email account naming policy, following the usual firstname.surname@example.com pattern.

You can see it coming a mile away: the company happened to have two employees with the exact same name. The IT department refused to make an exception, citing technical limitations. Their proposed solution was that one of the pair should have his name legally changed to accommodate their policy.

You can't make this up, folks.

Dag-Erling Små, rgrav - des@des.no

✂ Re: UPS ... indistinguishable from phishing (Kamens, [RISKS-25.23](#))

<"G.M.Sigut" <sigut@id.ethz.ch>>

Tue, 29 Jul 2008 10:30:59 +0200

> In this day and age, it is amazing to see a corporation as large as UPS
> failing to use the two easiest and most well-known methods of
> differentiating legitimate e-mail from scams -- put the customer's name in
> the e-mail, and make sure that all the links point directly at your site.

In this day and age you can see the most amazing array of entities, which you would expect to behave professionally, using subcontractors, so that various links or mail addresses have names different from what you would expect. It is part of the same mindset, which forces you to leave JavaScript enabled, if you want to be able to use your browser for more than the very few responsible web sites.

George M. Sigut, ETH Zurich, Informatikdienste, CH-8092 Zurich Swiss Federal Inst. of Technology Zurich, IT Services, System Services +41 44 632 5763

✂ Re: Fascinating phishing attack: valid links, dangerous ... number

<Al Macintyre <macwheel99@wowway.com>>

Mon, 04 Aug 2008 11:22:06 -0500

If you were a member of KNUJON (no junk backwards) and had passed this on to them, they would likely have passed the info onto US Secret Service, or equivalent organization if some other nation involved, because they protect the nation's currency.

Knujon wants your spam, to use in the fight against those that generate it, and provide the criminal infrastructure, such as crooked web sites, and phone#s for crooks. They have put approx 60,000 cyber criminals out of business since March 2005. I suggest you familiarize yourself with KNUJON services in fighting cyber crime. <http://www.knujon.com/>

Re: Apple Fails to Patch Critical Exploited DNS Flaw (RISKS-25.25)

<Robin Stevens <rejs@cynic.org.uk>>

Tue, 5 Aug 2008 18:49:27 +0100

I too was unimpressed by Apple's slow response to Kaminsky's DNS flaw (which appears to be inadequate - see <<http://db.tidbits.com/article/9721>>). Unfortunately it's far from the only flaw they've been slow to correct.

Their latest version of the operating system (OS X 10.5) still ships with a root hints file dating from 2002. This hints file is that used to "bootstrap" the whole process of DNS resolution, by listing the IP addresses of the thirteen top-level servers. Unfortunately, since 2002, two of the IP addresses have changed. This isn't generally a problem; if the first address tried fails to respond, then a nameserver will simply try another.

But what if, instead of getting no response from an obsolete root server address, a malicious response is received from a third party? This isn't purely scare-mongering. Hijacking of an old address has already been seen, e.g.:

<http://www.renesys.com/blog/2008/05/identity_theft_hits_the_root_n_1.shtml>

following the most recent address change. There's no reason to suspect any malicious intent in this case, but it could have happened.

I reported to Apple in early 2006 that their root hints file was out of date. They responded, telling me they were already aware of this. OS X 10.5 shipped last year, with the same outdated hints file. It's **still** unfixed - why?

Robin Stevens <rejs@cynic.org.uk> <http://www.cynic.org.uk/>

Re: Another GPS error story (Spafford, RISKS-25.25)

<Dr J R Stockton <jrs@merlyn.demon.co.uk>>

Mon, 4 Aug 2008 17:33:53 +0100

>Sat-nav driver's 1600-mile error: A DOZY trucker driving from Turkey to
>Coral Road in Gibraltar ended up at Skegness. Gibraltar is considered part
>of the UK by the Sat-Nav systems.

That omits an important point -- the driver was in fact directed to **Gibraltar Point**, which is on the outskirts of Skegness in Lincolnshire (see Wikipedia, etc.).

Iberian Gibraltar is British, but is not part of the UK.

[Also noted by Tony Ford. PGN]

✂ Survey: Perception of security in online environments

<Gene Spafford <spaf@cerias.purdue.edu>>

Sun, 3 Aug 2008 20:12:52 -0400

Please participate, and please pass the invitation along to others...

From: Johannes Strobel [mailto:johannes.strobel@gmail.com]

Survey: Security Incidents and perception of security in online environments

Invitation to Participate in Survey

As a team consisting of members of the Center for Education and Research in Information and Security (CERIAS) and Educational Technology at Purdue University, we are conducting a study investigating information security incidents and perception of security in online environments (games and virtual worlds), especially when it comes to educational institutions.

We developed a survey and invite you to participate.

Your identity will be kept confidential and not published or disclosed. Your participation will be strictly voluntary and you will be free to withdraw from participation at any time. It is entirely up to you, if you want to be contacted for some follow up questions. In all likelihood, unless you write extensive responses to the open-ended questions (which we would encourage), the survey should take about 15 minutes. It will be online until late August.

The url for the survey is:

http://www.surveymonkey.com/s.aspx?sm=3D_2fKEhOBQUA5MxHCc7g7F_2fPA_3d_3d

If you have any questions please email us.

Thank you in advance.

Johannes Strobel & Fariborz Farahmand

✂ REVIEW: "The Innocent Man", John Grisham

<Rob Slade <rmslade@shaw.ca>>

Mon, 28 Jul 2008 14:33:17 -0800

BKINCTMN.RVW 20080715

"The Innocent Man", John Grisham, 2006, 0-385-51723-8, U\$28.95/C\$35.95
%A John Grisham www.jgrisham.com
%C 666 Fifth Ave., New York, NY 10103
%D 2006
%G 0-385-51723-8
%I Bantam Books/Doubleday/Dell
%O U\$28.95/C\$35.95 800-323-9872 www.bdd.com www.doubleday.com
%O <http://www.amazon.com/exec/obidos/ASIN/0385517238/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0385517238/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/0385517238/robsladesin03-20>
%O Audience n+ Tech 2 Writing 3 (see revfaq.htm for explanation)
%P 360 p.
%T "The Innocent Man: murder and injustice in a small town"

In seminars dealing with forensics and investigation, I stress to my students that it is important to be scrupulous, unprejudiced, and honest in your investigation. This is not only to give the suspect a "fair chance," but also because when you become fixated on proving the guilt of an individual, you may fail to determine the identity of the person who actually committed the crime.

"The Innocent Man" is the story of the improper conviction of Ron Williamson for murder, as well as the interrelated stories of other improper convictions around the same time and place.

John Grisham's popular novels have demonstrated his ability to write. They have also established his knowledge of the law and competence in research. This, the author's first non-fiction text, puts that expertise to good work. The ground is covered thoroughly, noting limitations on the part of all involved. Grisham is, in fact, very careful to be fair, and avoids imputations of motive (which is rather at odds with the descriptions of motivation he must make in his fictional works). United States case law in regard to investigations, confessions, and aspects of forensic evidence and presentation is introduced carefully at every point.

There are, of course, a great many books written about specific crimes and their outcomes. A number have been written about wrongful convictions. However, "The Innocent Man" is particularly relevant to those interested in the management of investigations, especially where forensic, rather than direct, evidence plays a major part in the case. In one sense, it is an excellent primer on how not to conduct an investigation.

The justice system is created and staffed by people, and people make mistakes. This is why structures have been created to catch possible errors. The adversarial system itself, and various appeals processes, is intended to act as audits, checks, and balances for the system. It is, therefore, critical to note one other disturbing point that arises from the events in the book. There are numerous layers of appeals, but a consistency of personnel and direction between the various offices. As any student of internal controls knows, weak separation of duties creates the possibility of all kinds of problems.

This book is entertaining, readable, distressing, and important.

copyright Robert M. Slade, 2008 BKINCTMN.RVW 20080715
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
victoria.tc.ca/techrev/rms.htm blogs.securiteam.com/index.php/archives/author/p1/



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 27

Friday 8 August 2008

Contents

- [Strange Yahoo! vote count](#)
[PGN](#)
- [Trust TSA? Maybe... Trust Akamai...?](#)
[David Leshner](#)
- ["How reliable is DNA in identifying suspects?"](#)
[Robert P Schaefer](#)
- [GPS causes nightmare vacation](#)
[PGN](#)
- [Re: Another small interface risk](#)
[Thomas Wicklund](#)
- [Re: Unsuspected travelers' laptops may be detained at border](#)
[Thomas Hamann](#)
- [Re: Neglecting to logout from Skype](#)
[Dimitri Maziuk](#)
- [Pizza delivery and postal addresses](#)
[Mark Brader](#)
- [Info on RISKS \(comp.risks\)](#)

✉ Strange Yahoo! vote count

<"Peter G. Neumann" <neumann@csl.sri.com>>
Thu, 7 Aug 2008 13:52:46 PDT

The original statement from the Yahoo! Annual Meeting suggested strong support for the Yahoo! board. However, reportedly exactly 200 million votes seemed to have vanished from some of the expected totals. Subsequently, the final numbers showed some large discrepancies -- an EXACTLY 100 million vote change for two of the directors, and an EXACTLY 200 million vote change for three of the directors. That is, half of that number of votes were misallocated -- first FOR, then AGAINST for those candidates. (Four others were unchanged.) The anomalies were apparently blamed on "truncation errors", which seems very curious. Once again, who knows what really happened?

Sources:

<http://breakoutperformance.blogspot.com/2008/08/missing-200-million-yahoo-shares-from.html>

<http://www.techcrunch.com/2008/08/06/yahoo-vote-recount-shows-how-close-yang-and-bostock-were-to-being-ousted-from-the-board/>

#Trust TSA? Maybe... Trust Akamai...?

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

Fri, 8 Aug 2008 16:13:03 -0400 (EDT)

\$ <https://www.tsa.gov>

www.tsa.gov uses an invalid security certificate.
The certificate is only valid for a248.e.akamai.net

Is it any wonder we can't teach people about phishing when.....

#"How reliable is DNA in identifying suspects?"

<"Schaefer, Robert P \ (US SSA)" <robert.p.schaefer@baesystems.com>>

Thu, 7 Aug 2008 07:45:54 -0400

The risks of database searches:

http://www.latimes.com/news/local/la-me-dna20-2008jul20_0,1506170,full.s

tory

"State crime lab analyst Kathryn Troyer was running tests on Arizona's DNA database when she stumbled across two felons with remarkably similar genetic profiles."

#GPS causes nightmare vacation

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

Thu, 7 Aug 2008 9:51:44 PDT

Convoy Rescued After GPS Led to Utah Cliff; GPS Device Was a 'Nightmare' and 'A Vacation from Hell', Associated Press item, 7 Aug 2008

Trying to go from Bryce Canyon to the Grand Canyon by lesser traveled roads, a convoy of tourists (16 adults and 10 children) attempted to use a GPS device, which led them with various wrong turns onto inappropriate dirt roads to the edge of a sheer cliff deep inside the Grand Staircase-Escalante National Monument. One vehicle got stuck in soft sand, two others ran low on fuel.

<http://abcnews.go.com/Travel/Weather/wireStory?id=5522295>

[TNX to Lauren Weinstein for spotting this one.]

Re: Another small interface risk ([RISKS-25.26](#))

<Thomas Wicklund <wicklund@eskimo.com>>

Thu, 7 Aug 2008 09:46:16 -0700 (PDT)

Security questions such as birth city have always seemed to be very difficult. I found one site which had a security question (mother's maiden name I think) but required that the field be at least 8 characters. Something of a problem.

Worse are the sites where the only questions are "what is your favorite xyz". I find my favorite "xyz" can vary from day to day and the only solution is to write the answers down someplace. I had to call to get access to my new health insurance's web site because I had that insurance 5 years ago, was still registered, and didn't have any idea what I used for an answer to one of their "favorite" questions.

Comparing these answers seems a programmer's nightmare. It can't be case sensitive. Spaces have to be normalized. Did I type "Kansas City" or "Kansas City, MO" as my answer? What if I leave off the comma?

Re: Unsuspected travelers' laptops may be detained at border ([R-25.16](#))

<Thomas Hamann <T.D.Hamann@umail.LeidenUniv.nl>>

Fri, 8 Aug 2008 12:12:56 +0200

This policy seems like a major risk to the US economy should it ever be seriously enforced. It seems to basically provide a legal means for massive industrial and scientific espionage. I know the article mentions that "reasonable measures must be taken to protect business information and attorney-client privileged material", but the US government's track record on the enforcements of such measures is spotty, to say the least (also note that '(unpublished) scientific information' isn't specifically listed...).

>They also cover "all papers and other written documentation," including books, >pamphlets and "written materials commonly referred to as 'pocket trash' >or 'pocket litter.' "

This rings all alarm bells (also, the words 'police state' come to mind). I think that anyone who is considering traveling to the US should think twice before doing so. I wonder what would happen to anyone who has the 'wrong' combination of digital data and paperwork on him...

Re: Neglecting to logout from Skype ([RISKS-25.26](#))

<Dimitri Maziuk <dmaziuk@bmr.b.wisc.edu>>

Thu, 07 Aug 2008 09:43:13 -0500

> Date: Tue, 05 Aug 2008 20:32:32 +0200

> From: "Michael Weiner" <michael_weiner@gmx.net>

> Subject: Neglecting to logout from Skype means sharing your Instant Messages

> ... According to several messages on the Skype Community forum, Skype

> considers the ability to remain logged in to the same account on several

> machines a "feature" and sees no need to fix anything.

There are legitimate reasons for logging on to more than one office computer (that is why I never used Gnome: the early versions wouldn't let one do so) and there are legitimate reasons for having your messages arrive at more than one computer. I'd side with Skype on this and blame you: what you did is effectively give your friend your password. Auto-login is a bad default in this case, however, it's a convenient one and in the case of one computer - one user it's not unreasonable.

The risk is believing that software will magically know where you want to go today and will take you there when you click on start button. In reality default out of the box configuration may (or may not) work for what developers imagine their average user to be, but it probably won't work right for you -- in real life "one size fits all" doesn't fit anyone in particular.

✂ Pizza delivery and postal addresses

<msb@vex.nte (Mark Brader)>

Thu, 7 Aug 2008 17:14:46 -0400 (EDT)

[Posted by David Cantrell <david@cantrell.org.uk> in uk.transport.london]

The building I live in has three flats in it, numbered 1, 2 and 3. Flats 2 and 3 share a common front door and hallway, having their own doors off that. As far as normal people are concerned, that's three flats and three addresses. Post for flats 2 and 3 is delivered through a single letterbox. Consequently, as far as the post office is concerned, there are only *two* addresses, one for flat 1, and one for the shared letterbox of flats 2 and 3.

This is quite irritating, especially when stupid programmers working for stupid companies insist that I tell them my address by typing in my postcode and then selecting one of the addresses that the post office think exist. Normally it doesn't matter, of course, but it does matter when I'm trying to do something like order a pizza late at night and want the delivery boy to ring *my* doorbell and not have to guess at random between mine and my upstairs neighbour's.

[Note added by David Cantrell when giving permission to forward to Risks]

It's worth noting, however, that **most** companies who use the PAF do allow the user to type it in themselves if their address isn't in the list. It's some time since I last read the PAF docs, but I **think** they recommend doing that, because of, eg, people living in brand new developments which haven't yet filtered through to your local copy of the database, which might only get updated once a quarter or once a year.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 28

Tuesday 12 August 2008

Contents

- [Internet attacks against Georgian web sites](#)
[Gadi Evron](#)
[Gadi Evron](#)
- [Russia/Georgia: Tanks, Bombers, Keyboards](#)
[Edward Rice](#)
- [Patch for Web Security Hole Has Some Leaks of Its Own](#)
[John Markoff](#) via PGN
- [MIT Students Gagged by Federal Court Judge](#)
[EFF](#) via [David Farber](#)
- [CloudAV](#)
[Rob Slade](#)
- [Two on-line travel booking risks](#)
[Chris Drewe](#)
- ['Fakeproof' microchipped British e-passport ...](#)
[Lars Poulsen](#)
- [Re: Unsuspected travelers' laptops may be detained ...](#)
[Steven M. Bellovin](#)
[R. G. Newbury](#)
- [Re: GPS causes nightmare vacation](#)
[Fernando Pereira](#)
- [Re: How reliable is DNA ...?](#)
[Michael Black](#)
[Steve Schafer](#)
- [Re: Neglecting to logout from Skype ...](#)
[Al Macintyre](#)
- [Info on RISKS \(comp.risks\)](#)

✉ Internet attacks against Georgian web sites

<Gadi Evron <ge@linuxbox.org>>
Mon, 11 Aug 2008 01:37:59 -0500 (CDT)

In recent days, news and government Web sites in Georgia suffered DDoS

attacks. While these attacks seem to affect the Georgian Internet, it is still there.

Facts:

1. There are botnet attacks against .ge websites.
2. These attacks affect the .ge Internet infrastructure, but it's reachable.
3. It doesn't seem Internet infrastructure is directly attacked.
4. Every other political tension in the past 10 years, from a comic of the

Prophet Muhammad to the war in Iraq, were followed by online supporters attacking targets which seem affiliated with the opposing side, and vice-versa.

Up to the Estonian war, such attacks would be called "hacker enthusiast attacks" or "cyber terrorism" (of the weak sort). Nowadays any attack with a political nature seems to get the "information warfare" tag. When 300 Lithuanian web sites were defaced last month, "cyber war" was the buzzword.

Running security for the Israeli government Internet operation and later the Israeli government CERT such attacks were routine, and just by speaking on them in the local news outlets I started bigger so-called "wars" when enthusiasts responded in the story comments and then attacks the "other side".

Not every fighting is warfare. While Georgia is obviously under a DDoS attacks and it is political in nature, it doesn't so far seem different than any other online after-math by fans. Political tensions are always followed by online attacks by sympathizers.

Could this somehow be indirect Russian action? Yes, but considering Russia is past playing nice and uses real bombs, they could have attacked more strategic targets or eliminated the infrastructure kinetically.

Coulda, shoulda -- the nature of what's going on isn't clear, but until we are certain anything state-sponsored is happening on the Internet it is my official opinion this is not warfare, but just some unaffiliated attacks by Russian hackers and/or some rioting by enthusiastic Russian supporters.

It is too early to say for sure what this is and who is behind it.

The RBN blog (following the Russian Business Network) is of a different opinion:

<http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html>

and:

<http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare-2-sat-16-00.html>

Also, Renesys has been following the situation and provides with some data:

http://www.renesys.com/blog/2008/08/georgia_clings_to_the_net.shtml

(Thanks to Paul Ferguson for the URLs)

DDoS attacks harm the Internet itself rather than just this or that web site, so soon this may require some of us in the Internet security

operations community getting involved in mitigating the attacks, if they don't just drop on their own.

Gadi Evron.

["You don't need your firewalls! Gadi is Israel's firewall."

-- Itzik (Isaac) Cohen, "Computers czar", Senior Deputy to the Accountant General, Israel's Ministry of Finance, at the government's CIO conference, 2005.

(after two very funny self-deprecation quotes, time to even things up!)]

<http://www.linkedin.com/in/gadievron>

[There were a lot of lessons that should have been learned from the Estonian DDoS attacks that still remain to be learned. PGN]

Internet attacks against Georgian web sites

<Gadi Evron <ge@linuxbox.org>>

Tue, 12 Aug 2008 16:06:59 -0500 (CDT)

This is an update of my previous post on the subject.

To be honest here, no one truly knows what's going on in Georgia's Internet except for what can be glimpsed from outside, and what has been written by the Georgians on their blog

(<http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html>

outside their country). They are probably a bit busy avoiding kinetic bombing.

As mentioned in the previous post, Renesys has been following the Georgian links, which seem to be there, but occasionally drop due to possibly power failures. Renesys URL here:

http://www.renesys.com/blog/2008/08/georgia_clings_to_the_net.shtml

Shadowserver and others have been following the botnets attacking the Georgians web sites, and that is confirmed as happening. Shadowserver was quoted, here:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9112399&intsrc=hm_list

According to Dancho Danchev, there have also been some defacements, which he describes here, along with other conclusions I don't necessarily agree with: <http://blogs.zdnet.com/security/?p=1670>

So--it is clear their web sites are under attack, and that Internet visibility-wise, the impact is real for the Georgians. And yet, it is simply too early and there is not enough information to call this an Internet war. It is too early to establish motive or who the perpetrator is, however much we may want to point fingers.

Following every and any political or ethnic tension, world-wide, an online

aftermath comes, in the form of attacks, defacements, and enthusiast hackers swearing at the other side (which soon does the same, back).

While Georgia's suffering is real, such attacks are nothing but routine here in Israel. When I ran the defense for the Israeli government Internet operation and then the Israeli government CERT, such attacks would occur daily. Hackers on the other side would band together, talk, coordinate a date, exchange tools, and attack.

While I apologize for the analogy, post-9/11 Israelis were shocked. We were sympathizing and crying for the victims. What we did not understand was why people were still shocked ten minutes past, as this was a normal every-day life happening for us over here. The same applies for cyber-space, the Internet--we are used to this.

The difference in this attack was that the Georgian authorities, like numerous others around the world still aren't, were not prepared to face and fend against such an attack.

In my article "Fighting Botnets and Online Mobs" for the Georgetown Journal of International Affairs covering the Internet war in Estonia, I state how our opponents will no longer be just countries, or even organizations as Martin van Creveld once predicted ahead of his time, but that on the Internet playing field any individual or loosely affiliated group can be a player, affecting countries and yes, corporations as well.

My article can be found here:

<http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf>

The best article describing the events so far is by John Markoff at *The New York Times*.

<http://www.nytimes.com/2008/08/13/technology/13cyber.html?em>

Gadi Evron.

***Russia/Georgia: Tanks, Bombers, Keyboards**

<Edward Rice <ehrice@his.com>>

Sat, 9 Aug 2008 03:40:47 -0400

The New York Times reports that in the "hot war" currently going on between Russia and Georgia, cyberwarfare appears to have broken out as well:

> Neither side showed any indication of backing down. Prime Minister
> Vladimir V. Putin of Russia declared that "war has started," and President
> Mikheil Saakashvili of Georgia accused Russia of a "well-planned invasion"
> and mobilized Georgia's military reserves. There were signs as well of a
> cyberwarfare campaign, as Georgian government Web sites were crashing
> intermittently during the day.

<<http://www.nytimes.com/2008/08/09/world/europe/09georgia.html>>

✂ Patch for Web Security Hole Has Some Leaks of Its Own

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

Tue, 12 Aug 2008 14:30:37 PDT

Evgeniy Polyakov has demonstrated that the emergency patch to the Domain Name System for the vulnerability noted by Dan Kaminsky ([RISKS-25.25](#)) is itself flawed and relatively easily exploited. [Source: John Markoff, *The New York Times*, 9 Aug 2008, B1 (National Edition); PGN-ed]

✂ [IP] MIT Students Gagged by Federal Court Judge

<David Farber <dave@farber.net>>

Sat, 9 Aug 2008 17:21:27 -0400

Bad decision by the Judge djf

[Boston's Charlie Card vulnerability. Note that the student's paper explicitly does not reveal the key details of the vulnerability. Another example of shooting the messenger rather than getting to the root of the problems. PGN]

Begin forwarded message:

From: EFF Press <press@eff.org>
Date: August 9, 2008 5:14:30 PM EDT
To: presslist@eff.org
Subject: [E-B] EFF: MIT Students Gagged by Federal Court Judge
Reply-To: press@eff.org

Electronic Frontier Foundation Media Release

For Immediate Release: Saturday, August 09, 2008

Contact:

Jennifer Stisa Granick
Civil Liberties Director
Electronic Frontier Foundation
jennifer@eff.org
+1 415 271-4879

Marcia Hofmann
Staff Attorney
Electronic Frontier Foundation
marcia@eff.org
+1 415 436-9333 x116

Rebecca Jeschke

Media Coordinator
Electronic Frontier Foundation
press@eff.org
+1 415 436-9333 x125

MIT Students Gagged by Federal Court Judge

EFF Backs Researchers Forced to Cancel Presentation on Transit Fare Payment System

Las Vegas - Three students at the Massachusetts Institute of Technology (MIT) were ordered this morning by a federal court judge to cancel their scheduled presentation about vulnerabilities in Boston's transit fare payment system, violating their First Amendment right to discuss their important research.

The Electronic Frontier Foundation (EFF) represents Zack Anderson, RJ Ryan and Alessandro Chiesa, who were set to present their findings Sunday at DEFCON, a security conference held in Las Vegas. However, the Massachusetts Bay Transit Authority (MBTA) sued the students and MIT in United States District Court in Massachusetts on Friday, claiming that the students violated the Computer Fraud and Abuse Act (CFAA) by delivering information to conference attendees that could be used to defraud the MBTA of transit fares. This morning District Judge Douglas P. Woodlock, meeting in a special Saturday session, ordered the trio not to disclose for ten days any information that could be used by others to get free subway rides.

"We wanted to share our academic work with the security community and had planned to withhold a key detail of our results so that a malicious attacker could not use our research for fraudulent purposes," said Anderson. "We're disappointed that the court is preventing us from presenting our findings even with this safeguard."

Vulnerabilities in magnetic stripe and RFID card payment systems implemented by many urban transit systems are generally known. The student research applied this information to the specific case of Boston's Charlie Card and Charlie Ticket, and the project earned an A from renowned computer scientist and MIT professor Dr. Ron Rivest.

The court relied on a federal law aimed at computer intrusions in issuing its order, holding that even discussing the flaws at a public conference constituted a "transmission" of a computer program that could harm the fare collection system.

"The court's order is an illegal prior restraint on legitimate academic research in violation of the First Amendment," said EFF Civil Liberties Director Jennifer Granick. "The court has adopted an interpretation of the statute that is blatantly unconstitutional, equating discussion in a public forum with computer intrusion. Security and the public interest benefit immensely from the free flow of ideas and information on vulnerabilities. More importantly, squelching research and scientific discussion won't stop the attackers. It will just stop the public from knowing that these systems are vulnerable and from pressuring the companies that develop and implement them to fix security holes."

This case is part of EFF's Coders' Rights Project, launched just this week to protect programmers and developers from legal threats hampering their cutting-edge research. EFF will seek relief for the researchers in the courts.

For the full temporary restraining order:

<http://www.eff.org/files/filenode/MIT%20students%20TRO.pdf>

For more on the Coders' Rights Project:

<http://www.eff.org/issues/coders>

For this release:

<http://www.eff.org/press/archives/2008/08/09>

About EFF

The Electronic Frontier Foundation is the leading civil liberties organization working to protect rights in the digital world. Founded in 1990, EFF actively encourages and challenges industry and government to support free expression and privacy online. EFF is a member-supported organization and maintains one of the most linked-to websites in the world at <http://www.eff.org/>

#CloudAV

<Rob Slade <rMslade@shaw.ca>>

Mon, 11 Aug 2008 11:27:22 -0800

A few media sources seem to be picking up a press release from the University of Michigan.

<http://www.ns.umich.edu/htdocs/releases/story.php?id=6666>

This reports on "CloudAV," a project and series of papers about having antivirus detection run "in the cloud" rather than on the PC.

<http://www.eecs.umich.edu/fjgroup/cloudav/>

As usual, there seems to be some misunderstanding about what is going on here. CloudAV is not really a new approach, it is simply the use of multiple scanners, which the AV research community has advocated for years. It's like having a bunch of scanners installed on your desktop, or a system like Virustotal, with the exception that the scanners run on different computers so you get a bit of performance advantage (absent the bandwidth lag/drain for submitting files to multiple systems).

rslade@vcn.bc.ca rslade@computercrime.org victoria.tc.ca/techrev/rms.htm
blogs.securiteam.com/index.php/archives/author/p1/

#Two on-line travel booking risks

<"Chris Drewe" <e767pmk@yahoo.co.uk>>
Sun, 10 Aug 2008 18:18:12 +0100

Here are two items from the readers' queries feature in the travel section of the weekend newspaper recently (don't know if they're in the on-line version, but it's <http://www.telegraph.co.uk/travelexperts> , Aug 2 & 9):

* A reader wrote about booking 3 air tickets on-line for himself and two other people via the airline's web site, and ended up with three tickets with his own name on them, which cost a small fortune to correct. This was suggested as being due to the `autofill' function of his web browser (it didn't say which one), and also returning to a previous stage of the booking process with the browser back arrow rather than the `Back' link on the web page. The airline was quoted as saying that it can't disable or detect this as an error (unlike, say, an empty name field), so it's the customers' responsibility to check when entering data.

* In the UK, passports last for 10 years, but they can be renewed slightly before they expire, with the unused period transferred to the new one (thus allowing you to renew your passport in good time without losing part of its validity period), hence it's possible to have a passport with an expiry date just over 10 years in the future. A reader comments that the US Electronic System for Travel Authorisation application site at <https://esta.cbp.dhs.gov> didn't accept his passport because it was valid for more than 10 years. Response was that the Department for Homeland Security claims to have fixed this, but as the on-line permit is compulsory from next year, it may be something to be aware of.

#'Fakeproof' microchipped British e-passport ... (Thomas, [RISKS-25.26](#))

<Lars Poulsen <lars@beagle-ears.com>>
Sun, 10 Aug 2008 06:49:01 -0700

I have been watching with increasing puzzlement the security theater about "electronic passports", and I still cannot figure out what it is that the system is supposed to accomplish. It seems to me that it is going backwards.

Indeed, the world has changed since the traditional passport system was established. The traditional passport relies on "secure paper" technology: Textile paper with watermarks was considered to be too difficult to fake. Modern printers can create something that looks close enough to fool a quick look.

It seems to me that the response to this would be to take advantage of Internet technology: One should no longer trust the passport, but use only the embedded barcode or OCR digit string to furnish a record identifier and then pull the passport information from the issuing agency's database. Then a forged paper passport would be worthless at border crossings.

Instead, we have replaced the reliance on "secure paper" with a reliance on "secure silicon", even though it should be obvious to anyone that a writable memory chip can be reprogrammed in the field ... indeed the standard method of deployment of the genuine instrument relies on this property. Any digital signing on the chip to ensure that it has not been altered requires a functioning network link to the issuer's database. And with that link, the chip is unnecessary.

I know that I am not so smart that I have figured out something that all the experts have overlooked, so I must be missing something critical. What have I overlooked?

Lars Poulsen, Afar Communications Inc

Re: Unsuspected travelers' laptops may be detained ... (RISKS-25.16)

<"Steven M. Bellovin" <smb@cs.columbia.edu>>
Mon, 11 Aug 2008 15:59:44 -0400

It's worth noting -- repeating, actually -- that border searches of laptops are not restricted to the US. See, for example, <http://news.bbc.co.uk/1/hi/sci/tech/150465.stm> which reports on British policy. Also note the date: 1998. I have a different question: which developed economies have explicit policies saying that they will not search (the information on) laptops?

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

Re: Unsuspected travelers' laptops may be detained... (RISKS-25.16)

<"R. G. Newbury" <newbury@mandamus.org>>
Sat, 09 Aug 2008 21:05:58 -0400

The worst features of this are that IF you have done the smart thing and used strong encryption to protect your data, the Customs agent will be MORE likely to take away your entire laptop for examination... and he will take your entire laptop, not just the hard drive out of it.

In effect, you have no Fourth or Fifth Amendment rights when crossing the border into the US. Must scare the living bejusus out of most corporate counsel and CIO guys.

As for me, the next time I cross the border with my laptop, it will have an entirely brand spanking new Fedora install on the laptop's original (small) hard drive with not one single piece of important data.

Re: GPS causes nightmare vacation

<Fernando Pereira <pereira@cis.upenn.edu>>
Fri, 8 Aug 2008 20:39:11 -0700

GPS caused nothing there, no computer risks involved. The risk is for people travel in wild places with no clue about what they are about to experience. They blamed the GPS because they had to find an excuse for their ignorance and stupidity. They were lucky that they got away with just embarrassment, others with a similar attitude have paid with their life.

Re: How reliable is DNA ...? (Schaefer, [RISKS-25.27](#))

<"Michael Black" <mdblack98@yahoo.com>>
Sat, 9 Aug 2008 08:40:24 -0500

I've long been a critic of DNA matches -- seems it's always being presented as an almost "sure thing". I always said that when the database got large enough they'd start having problems.

Well, a recent article has caused me to analyze the probabilities. It's quite eye-opening when you understand how it really works.

You always hear of one-in-million or billion chances but it would seem, by simple analysis, that this is not true, and would certainly explain why the FBI is fighting against people being able to do studies such as are quoted in this article. But you really don't need to do any studies. That statistics are pretty simple.

For those of you who are computer-wise, DNA matching is apparently a binary coded system. "9 loci" matches are frequently used to find matches. I don't know where the numbers come from that I hear in the court cases...but this is how it quite apparently works. As the article below pointed out -- they found 122 matches in the Arizona database of 65,000 where there was a 9-loci or more match. This very closely matches the following table that I calculated based on simple binary probabilities showing # of loci, cumulative probability, and resulting number of average matches expected at each loci match level:

1	0,5	32500
2	0,25	8125
3	0,125	4063
4	0,0625	2031
5	0,03125	1016
6	0,015625	508
7	0,007813	254
8	0,003906	127
9	0,001953	63
10	0,000977	32
11	0,000488	16
12	0,000244	8

9 loci or better" numbers gives you 63 likely matches -- The 122 in the study may well be due to the lack of independence -- e.g.. relatives and the distribution of the actual DNA samples (which one would have to do a study to find out).

Given the current U.S. population of 305 million then, how many matches would there be in the U.S.? At 9 loci or more you would expect 595,703 matches. Proof beyond doubt? Hardly. At 12 loci it would be 74,463 and at 13 loci 37,231.

This is why DNA evidence alone is NOT a sure thing and should never be used as the sole evidence in a case. So the next question would be -- if I already have a suspect and his DNA matches -- how good is that? That question is simply, "what are the odds that a specific DNA sample will match somebody else in the database?" For the U.S. population that turns out to be 1-in-546 or a 99.82% match at 9 loci and 1-in-8192 at 12 loci or a 99.99% match. As a juror I don't think I would see much difference between 99.82% and 99.9988%. And stating it as 1-in-8192 puts a whole different spin on 99.99%.

DNA can be used to EXCLUDE beyond any doubt. But it cannot be used to INCLUDE beyond any doubt. Question being what is "reasonable doubt" statistically? As a defense lawyer you might be able to say "in this city of 65,000 alone there are approximately 122 people with the same DNA profile as my client" -- that would be the 9-loci case -- or "8 people" at 12 loci. That sounds like reasonable doubt to me and would make me completely discount the DNA evidence. Without other supporting evidence I would never convict somebody on DNA alone.

Re: How reliable is DNA ...? (Schaefer, [RISKS-25.27](#))

<Steve Schafer <steve@fenestra.com>>

Sat, 09 Aug 2008 08:39:05 -0400

The controversy arises here because this situation is analogous to the well known Birthday Problem (sometimes called the Birthday Paradox), which is the difference between the following two questions:

Q1: How many people do I have to invite to a party before the probability that two of the guests have the same birthday exceeds 99%?

A1: 57.

Q2: How many people do I have to invite to a party before the probability that one of the guests has the same birthday as me exceeds 99%?

A2: 1679.

Another way to look at it: If I invite 57 people to my party, there is a 99% chance that two guests will have the same birthday, but a less than 15%

chance that one of the guests will have the same birthday as me.

* From the description in the news stories, Troyer was asking question 1.
During criminal investigations, investigators ask question 2.

✈ Re: Neglecting to logout from Skype ... ([RISKS-25.27](#))

<Al Macintyre <macwheel99@wowway.com>>
Sat, 09 Aug 2008 16:25:43 -0500

In our travels, work, school, home, we may have need of multiple different locations from which to access various Internet services, but probably not simultaneously.

Those different PCs can often have different default settings and configurations.

I recently was working in part of the flooded Midwest, where many business sites without phones, fax, Internet service etc. so I was using computer at motel to catch up on e-mail etc. The computer in hotel lobby was shared by 200 hotel room guests, on first come first served basis.

Important to log out each day, maybe change password daily, because unknown what gets saved on that PC cache. I found where one guest had created a folder with particulars about managing their bank accounts, still logged on. Every guest could access every other guest stuff because it was one password for all of us. I figure this kind of infrastructure is magnet for spyware.

For decades in offices where people share some network of data bases, it has been productive to concurrently open multiple sessions ... some updating or entering data, others inquiring into various aspects of the data entry, more related to coping with interruptions. It is nice that at an instant's need, yet another session can be opened to look at the data a different way or to pursue a different interest. But at end of day, time to go home, it is also easy to forget about a session opened hours ago & interrupted by interruptions forgot it was open. This could be at one workstation with 8 sessions open, or multiple work stations, as some persons patrolled a building, dealing with situations, signing onto the most convenient location.

I railed without success at the network configurators to add an icon showing number of sessions you are currently signed on at, a number you want to wind down to zero when you done for the day.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 29

Tuesday 19 August 2008

Contents

- [Olympics Windows crash](#)
[PGN](#)
- [Translate of device mech auto-reproduce](#)
[Rob Slade](#)
- [Electronic voting and antivirus software](#)
[jared](#)
- [Officials Say Flaws at Polls Will Remain in November](#)
[Ian Urbina via PGN](#)
- [Glitch let hundreds get free transit rail tickets](#)
[William Neuman via PGN](#)
- [Big trouble with Germany's New Unified Tax Identification Codes](#)
[Ralf Fritsch](#)
- [Online Consumers at Risk and the Role of State Attorneys General](#)
[CAP/CDT item via Monty Solomon](#)
- [11 charged with massive ID theft](#)
[Monty Solomon](#)
- [Re: Firefox 3's Step Backwards For Self-Signed Certificates](#)
[Michael Barrett](#)
- [Re: 'Fakeproof' microchipped British e-passport](#)
[Hamish Marson](#)
- [Billion dollar IT failure at Census Bureau](#)
[Michael Lewchuk](#)
- [Attempt to muzzle MIT subway research backfires](#)
[B.K. DeLong](#)
- [My date and place of birth are public](#)
[jidanni](#)
- [Re: How reliable is DNA ...?](#)
[Geoff Kuenning](#)
[Rob Searle](#)
[Brian Hayes](#)
[Bob Buxton](#)
- [Info on RISKS \(comp.risks\)](#)

✉ **Olympics Windows crash**

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

Tue, 12 Aug 2008 16:26:50 PDT

This is rather amusing, but not particularly surprising: A Windows XP/Vista-style Blue Screen of Death projected onto an overhead display at the opening ceremonies to the 2008 Olympics in Beijing, courtesy of River Cool Forums.

<http://macenstein.com/default/archives/1562>

✂ Translate of device mech auto-reproduce

<Rob Slade <rMslade@shaw.ca>>

Sun, 17 Aug 2008 14:35:23 -0800

Given the number of times RISKS has noted problems with automatic correction and translation systems, I thought you'd find this cute:

<http://adweek.blogs.com/adfreak/2008/07/then-well-grab.html>

[The sign says something in Chinese that would correctly translate to "... Restaurant". The supposed translation that appears on the sign says "Translate server error." The humorous caption on the photo is "Then we'll grab a bite at 404 Not Found." PGN-ed]

rslade@vcn.bc.ca slade@victoria.tc.ca victoria.tc.ca/techrev/rms.htm
rslade@computercrime.org blogs.securiteam.com/index.php/archives/author/p1/

✂ Electronic voting and antivirus software

<jared <jared@netspace.net.au>>

Sat, 16 Aug 2008 14:21:25 -0600

From an Ohio (USA) Secretary of State press release
www.sos.state.oh.us/PressReleases/2008%20Press%20Releases/2008-0806.aspx

"These malfunctions resulted in dropped votes when memory cards were uploaded to the server. "

"The office is also continuing to test Premier's undocumented contention that the sharing violation is because of virus protection software that had been certified by the Board of Voting Machine Examiners as part of the Premier system at the time it was introduced in Ohio."

The xkcd web comic has a summary: <http://xkcd.com/463/>

[I find the contention that failures of a voting machine could be attributed to interactions with anti-virus software to be really

outrageous. Premier (formerly Diebold) has developed an inherently untrustworthy application on top of an inadequately trustworthy and relatively huge operating system that anyone with access could compromise the application software or merely accidentally disrupt elections. Blaming the anti-virus software (which exists primarily because of the weaknesses of the operating system) seems totally fatuous. There should be no need for anti-virus software in a well-designed voting system. PGN]

✂ Officials Say Flaws at Polls Will Remain in November

<"Peter G. Neumann" <neumann@csl.sri.com>>
Mon, 18 Aug 2008 17:30:42 PDT

Election Assistance Commission officials say they will not be able to certify that flawed machines are actually repaired in time for the November election -- because of the backlog at testing labs. [Source: Ian Urbina, *The New York Times*, 16 Aug 2008; PGNed]

✂ Glitch let hundreds get free transit rail tickets

<"Peter G. Neumann" <neumann@csl.sri.com>>
Mon, 18 Aug 2008 17:27:51 PDT

Apparently due to a programming error, ticket vending machines on the Long Island Railroad and Metro-North Railroad have been giving out free tickets whenever debit cards with inadequate balances were used, since 2001. The problem was discovered only recently, when an audit by the LIRR showed 990 such transactions. Although many people have gotten free travel without even realizing it, three people have been charged with acquiring about \$800,000 worth of tickets -- which they then sold. [Source: William Neuman, *The New York Times* 13 Aug 2008; PGN-ed]

[I read the article over breakfast. George Mannes noted it online.
<http://www.nytimes.com/2008/08/13/nyregion/13scam.html?ref=nyregion>
PGN]

✂ Big trouble with Germany's New Unified Tax Identification Codes

<"Fritzsche, Ralf" <Ralf.Fritzsche@baw.de>>
Thu, 14 Aug 2008 11:28:41 +0200

As a reader of comp.risks digest for at least 13 years I could now for the first time contribute a nice story, happened in my home town Stade, Lower Saxony, 35 miles west from Hamburg.

Since the beginning of August 2008, the "Bundeszentralamt für Steuern"

(Federal Central Tax Office) sends out letters to all 82 millions inhabitants of Germany, from newborns to old men, with information regarding their new Tax Identification Code, a mathematically spoken, eleven-digit hash value dereferencing information like title, surname, given names, birth name, sex, address, birthday, place of birth, country of birth.

Whereas in other places there were no or only minor problems, in Stade near 100% of the information for the roundabout 46000 inhabitants contained errors with birth name, and country of birth. E.g. in my own family (14 year old boy, 11 year old girl, my wife, and me, all native german-born Germans) three of us have as country of birth "Kazakhstan", my daughter has "Italy", and all but my wife have false, entirely fictitious birth names. The registration office of Stade is overwhelmed with complaints, and no one has until now found out, where the errors do come from. As a Stade official said, the raw data of the registration office are correct, and the transport of the data to the Federal Central Tax Office was not done via Internet, but there was sent a CD containing the data (See (1)). Until now, nobody from the Federal Central Tax Office phoned back to enlighten the situation. They said, that a 1000 of errors in 80 Millions of data is not bad, either, and blamed Stade for the error. Against this speaks the fact, that Bremerhaven, and two other towns in Lower Saxony, suffered from the same problem. And furthermore, a quick consistency check of the New Tax ID numbers with tax consultant standard transmission protocol software showed, that 70% of the IDs failed the consistency check (see also (1)).

Until now it is unknown, who or what was responsible for the mess-up. The story made up to the tabloids (see (2)). The town of Stade recommends the inhabitants to do nothing and wait until the situation has cleared up. (see (3)).

Appendix: Cited website information, unfortunately in German :-)

(1)

<http://www.heise.de/newsticker/Kommunen-melden-grobe-Fehler-bei-Ausgabe-der-neuen-Steuernummer--/meldung/114161>

(2)

<http://www.bild.de/BILD/hamburg/aktuell/2008/08/12/steuerdaten-chaos/behoerde-verschickt-bescheide-mit-falschen-namen.html>

(3)

<http://www.kreis-stade.de/default.cfm?DID=1207942>

Dr. Ralf Fritsch, Bundesanstalt fuer Wasserbau Federal Waterways
Engineering and Research Dienststelle Kueste Tel. +49-40-81908-324

[Added by RF 19 Aug 2008:]

The latest news, to be found (auf deutsch) under

<http://www.stadt-stade.info/default.cfm?did=1207884>

"... Fest steht bisher nur, dass offenbar bei der Datenübermittlung vorhandene Leerfelder im Datensatz durch die EDV falsch interpretiert worden sind. Die technischen Gründe hierfür sind derzeit noch nicht geklärt."

That is, "It seems definite, that obviously white spaces in the original data were misinterpreted during data transfer. Technical reasons remain until now unknown."

✂ Online Consumers at Risk and the Role of State Attorneys General

<Monty Solomon <monty@roscom.com>>

Thu, 14 Aug 2008 23:03:10 -0400

Study: State AGs Fail to Adequately Protect Online Consumers

State attorneys general received thousands of complaints about online fraud and abuse in 2006 and 2007. Yet, with the exception of several notable standouts, few states brought significant cases in response to those complaints, according to a report released today from the Center for American Progress and the Center for Democracy and Technology. The study finds online fraud and abuse aren't given a high priority by most attorneys general. The report recommends several steps state attorneys general can take to protect online consumers, such as: assess the applicability and adequacy of state laws; develop computer forensic capabilities; train investigators and prosecutors to identify Internet fraud; and devote greater resources to enforcement efforts.

Online Consumers at Risk and the Role of State Attorneys General
By Reece Rushing, Ari Schwartz, Alissa Cooper | August 12, 2008
Center for American Progress, Center for Democracy and Technology

http://www.americanprogress.org/issues/2008/08/online_consumers_report.html

http://www.americanprogress.org/issues/2008/07/pdf/consumer_protection.pdf

<http://cdt.org/press/20080812press.php>

http://www.cdt.org/privacy/20080812_ag_consumer_risk.pdf

✂ 11 charged with massive ID theft (Re: [RISKS-25.26](#))

<Monty Solomon <monty@roscom.com>>

Thu, 14 Aug 2008 20:27:27 -0400

A ring of people spread across the globe hacked into nine major US companies and stole and sold more than 41 million credit and debit card numbers from 2003 to 2008, costing the companies and individuals hundreds of millions of dollars, federal law enforcement officials said yesterday. "So far as we know, this is the single largest and most complex identity theft case ever charged in this country," US Attorney General Michael Mukasey said at a news conference at the John Joseph Moakley US Courthouse in Boston.

A grand jury indictment released yesterday charged that Albert "Segvec" Gonzalez of Miami and his 10 conspirators (one from Estonia, three from Ukraine, two from China, one from Belarus, and one of unknown origin) cruised around with a laptop computer and tapped into accessible wireless

networks, allegedly concealed the data in encrypted computer servers they controlled. They then hacked into the networks of TJX, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Dave & Buster's, Sports Authority, Forever 21, and DSW. After gaining access to the systems, they installed programs that captured card numbers, passwords, and account information, officials said. [Source: David Abel and Jenn Abelson, *The Boston Globe*, 6 Aug 2008; PGN-ed]

http://www.boston.com/business/articles/2008/08/06/11_charged_with_massive_id_theft/

Re: Firefox 3's Step Backwards For Self-Signed Certificates (R 25 23)

"Barrett, Michael" <mbarrett@paypal.com>>

Wed, 13 Aug 2008 06:14:44 -0700

I read a rather worrying criticism of Firefox 3.0 on RISKS the other day, which made me realize that perhaps there isn't a common agreement amongst the infosec industry about the threatscape and how we should prioritize our response to them. Specifically, the complaint against Firefox 3.0 is that the user experience has been deliberately crafted to make it hard to accept self-signed certificates. The argument is that there are times when simply establishing an encrypted tunnel (i.e. an SSL session) is all that's needed.

I certainly wouldn't argue that encryption is unnecessary, just that the threat has changed. While our old "friend" Mallory isn't particularly busy these days, it's pretty clear that he'd be having a field day if he could easily penetrate communications across the Internet. The attacker however is no longer limited to passive eavesdropping. Modern attacks use active DNS spoofing, active MITM attacks and the like, on public networks. The main threats these days are against the weakest link in the chain - the end user. That's why phishing is such a popular method of e-crime - it's simple and it works. It relies completely on the gullibility of users in clicking on links in e-mails apparently from organizations with whom they have a relationship.

However, it's equally clear that almost everyone who wants to communicate securely using a browser can afford an SSL certificate from CAs such as GoDaddy, Thawte, etc. The cost of single certificates from these sources can only be described as nominal.

My company is a major target of phishing, and as such we've spent quite a bit of time researching what anti-phishing approaches work. We published a whitepaper on this topic (which can be found on the company blog at www.thepaypalblog.com), which explains this in detail. However, a couple of relevant conclusions are that: 1) the vast majority of users simply want to be protected, 2) there's no single "silver bullet", and 3) that what we describe as "safer browsers" such as IE 7, and Firefox 3.0 are a significant part of the solution based on their improvements in user visible security indicators and secure-by-default behaviors.

I conflated two or three separate ideas in that last sentence, and I should

explain them. The general logic is that most users should never be presented with a security dialog that gives them a choice - if they are, there's typically at least a 50:50 chance that the wrong decision will be made. Instead, the browser should make the decision for them. However, in the case of self-signed certificates it's almost impossible to see how any technology can disambiguate between legitimate uses and criminal ones.

When viewed through this lens, the changes to the Firefox user experience for self-signed certificates makes perfect sense. It's not that self-signed certificates are impossible to use - but for most users, the experience will be such that they won't accept them. In the unsafe world in which we live, that will be the right choice. For organizations which wish to use self-signed certs internally, it is still technically possible - but it will require either explicit user training, or deployment of pre-installed certificates on PCs.

I should also add that the major security features which have been added into the most recent browser versions (and which we believe are necessary in order to be considered 'safer') are exactly those which impact this area. That is: support for Extended Validation certificates, which make it clear to end users whose web site they're on; and support for spoof-site black lists, so that users can't easily reach spoof-sites.

While I'm personally a great supporter of RISKS, I think it's important that the Infosec industry speaks with good consensus about risks. In this case, I believe that the criticism of Firefox 3.0 was simply misguided and ill-informed. This is not helpful.

This post is also at: <http://www.thesecuritypractice.com/>

Re: 'Fakeproof' microchipped British e-passport (Poulsen, [R-25.28](#))

*<Hamish Marson <hamish@travellingkiwi.com>>
Wed, 13 Aug 2008 12:07:10 +0100*

> I know that I am not so smart that I have figured out something that all the
> experts have overlooked, so I must be missing something critical. What have
> I overlooked?

Lets see... After a quick think you've missed...

1. Authentication... How does the issuing agency authenticate the border agent requesting the information? Passwords? Secure Certs? One time tokens? Each have their own down sides...

2. Assuming someone solves the problem of how to get all the border agencies to agree on a method of authentication, how do you keep it secure? Passwords get written down... The issuing agency has no control over the remote access devices so can't guarantee the security of any client certs...

3. Comms... Long time readers will be well aware of the risks of depending

on long comms links to be up at inopportune times.

4. How much info would be required? I think this would bring in various privacy laws... Witness the debacle between the EU and the U.S. over passenger data...

5. What's to stop a border agency from just browsing someone else's database by just brute forcing all those passport ID's? Again, what faith can we have that the ID's used won't be easily guessable...

And a myriad of others... Basically they boil down to Connectivity, Authentication of border agents and privacy... Count me out.

✶ Billion dollar IT failure at Census Bureau (Re: [RISKS-25.12,13](#))

<"Michael Lewchuk" <michael.lewchuk@matrikon.com>>
Wed, 13 Aug 2008 10:03:50 -0600

I do have a few comments about this one:

* The handhelds should be simple and cheap. They should be able to download their information to a computer via a common interface (e.g. wireless). How long they survive is dependent upon use and care. If using 10 year old computers seems strange to you, I know of many production plants that are still using 30 year old hardware. The key factor is whether it does what needs doing. If a device is damaged, it may be replaced with a new device (that is, in 12 years the Census Bureau may have another one designed, presumably for a lot less, and enough replacements built to last another 3 censuses).

* I fail to see how anyone could spend \$11B on such things. I mean, that's, what, \$300 per capita? Engineering a small device should be in the single digit millions of dollars, shouldn't it (anyone know how much the Blackberry cost to design)? The device should use standard tech and interface easily with PCs. It should be cheap. Let's say \$100 each for 1 million census workers =3D \$100M. Where do they get \$11B from?!

* If there is significant waste and mismanagement, perhaps someone should consider decapitating the Census Bureau: a simple revocation of all posts pending review.

* One thing I would note is that there should be a law requiring executives of public companies and their subsidiaries to be bondable. That is, in order to work as an executive for a company that is publicly held, or one in which the majority of the ownership is public, you must be trustable.

* Ever notice how managers spend so much time trying to find ways to measure and improve output while there really is no solid criteria by which management itself can be measured? That is, why is executive X paid \$8M/yr rather than \$5M/yr or \$2M/yr? Is said executive really more effective than having the business managed by a potted plant? If so, by how much? Note:

end profit and/or share price, by which a lot of managers are measured, is too dependent upon market fluctuations and simple year-to-year sales. I'm sure that if we replaced the executive of any conglomerate by potted plants that the company would still continue to run for decades due to sheer inertia.

Michael J. Lewchuk, Software Engineer (M.Sc., M.Eng. P.Eng.(Alberta Canada))
MatrikonOPC Technical Lead, Software Development 1-780-448-1010 x.4512

✂ Attempt to muzzle MIT subway research backfires (Re: [RISKS-25.28](#))

<"B.K. DeLong" <bkdelong@pobox.com>>

August 12, 2008 5:41:50 PM EDT

[From Dave Farber's IP distribution.]

Year after year, I am incredibly surprised at the amount and types of companies and organizations that have a knee-jerk reaction to a vulnerability or security hole being presented at either the Black Hat or DEFCON security events. Do PR professionals, crisis response managers, or corporate image specialists do their homework? Why isn't there an industry case study that says the fastest way to HELP a vulnerability in your software or product get absolute full and fast disclosure before you have time to fix it, is to try and stop it being discussed at one of these two events?

In the MBTA's case, they hit the absolute pinnacle by filing a lawsuit in Federal court setting off a trigger to both the cadre of journalists, security researchers, civil libertarian activists, and hackers to begin doing everything in their power to make sure the story gets heard and (in some of their minds), the vulnerability gets exposed.

The Public Relations Society of America should send out a brief every year in mid-July to remind them of the forthcoming security conferences and how extremely public attempts to quash research that may appear to be harmful to an organization's image will backfire horribly. In some cases, even quiet attempts to stop it could be detrimental as well.

It should serve to all companies and organizations across the country (and world) that maybe in the long run cooperation with these researchers very early on (or at least as soon as the talks are announced every year) is the best way to ensure proper lead time to put together patches while allowing for full disclosure of the vulnerabilities that may effect a product's userbase.

Why does no one seem to be getting the hint until after it happens to them?

✂ My date and place of birth are public

<jidanni@jidanni.org>

Thu, 14 Aug 2008 04:01:44 +0800

Like everybody else, I was determined to keep my date and place of birth a secret to prevent identity theft -- until one day I discovered someone had written a Wikipedia entry on me, <http://zh.wikipedia.org/wiki/%E7%A9%8D%E4%B8%B9%E5%B0%BC> Mom will be proud! -- but only if I untwisted one fact first.

Everything on Wikipedia is a battle, for me at least. To establish that I was BORN in Philadelphia, but GREW UP in Chicago, just saying "I was there, I ought to know", is not enough. They need reliable references. Something they can quote. I.e., it all spelled out on my personal website, which I then did.

And of course all proper famous people have a date of birth listed (which I dare not cheat on as you never know what database they'll be using at Heaven's Gate on Judgment Day :-)

By the way, one's Taiwan temporary Tax ID is date of birth + first two letters of surname: 19601216JA. Good thing I don't have a twin.

So I'm now "living in a glass house". Well, plastic:

<http://jidanni.org/me/home/images/>

✉ Re: How reliable is DNA ...? (Schaefer, [RISKS-25.27](#))

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

Wed, 13 Aug 2008 01:50:09 -0700

Actually, there's a third question that can be asked: if you randomly choose a particular person at your party, what is the probability that that person shares your birthday? Obviously, it's one in 365.25, or about 0.3%, and the probability is independent of the number of people at the party.

The problem is that during criminal investigations, investigators can ask either question 2 or question 3, but evidence presented to the jury quite consistently gives the probabilities from question 3, and in a number of cases judges have prevented defense attorneys from pointing out that the wrong calculation has been used.

(Question 3 gets asked when the police have identified a suspect through other means, and the DNA match is used to confirm or reject the hypothesis. Question 2 gets asked when there is no suspect, and a statewide DNA database is searched. If you have a big enough database--and some states do--you're almost guaranteed to get a hit.)

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

✂ Re: How reliable is DNA ...? Schafer [RISKS 25.28](#)

<rob_searle <robert.searle@tait.co.nz>>

Thu, 14 Aug 2008 11:09:31 +1200

I mostly agree with this interpretation but the asterisk note at the end is more a hope a truth. In a number of investigations an entire community is asked to provide DNA "to exclude them" and there is also a lot of "nothing to hide, nothing to fear" innuendo. The DNA evidence in such cases is tainted with the birthday paradox, family relationships (and in many communities secret relationships).

An alternative view, from Medical research, is that a multi-variate study needs to adjust its correlation significance threshold downward to take account of the number of variables. For example, the significance of finding a correlation between behaviour A and disease D in a study of the available evidence is much stronger than that of finding a correlation between one of A, B, C, and one of the diseases D, E, F.

✂ Re: How reliable is DNA ...? (Michael Black, Steve Schafer)

<Brian Hayes <brian@bit-player.org>>

Wed, 13 Aug 2008 23:20:28 -0400

Michael Black's analysis of DNA forensics likens a genetic fingerprint to a binary numeral of nine to thirteen digits. In effect, Black assumes that each genetic locus has just two possible forms, or alleles, which occur with equal probability. In fact, the markers commonly used in DNA forensics have dozens of alleles. Thus the number of possible 13-locus matches is not 2^{13} but N^{13} where N has a value somewhere in the neighborhood of 10 or 15 or even 25. The number is reduced somewhat (and the calculation is made more complicated) by the fact that not all the alleles are equally likely, but the number of variants is well above 8,192.

There's a good explanation of all this in a 1992 report from the National Research Council, The Evaluation of Forensic DNA Evidence (see especially pp. 14-15). The report is available on Google Books at

<http://books.google.com/books?id=SnHYMZxAKQEC>

There's plenty of reason to be skeptical of overwrought claims that DNA never lies, but the numerical counter-evidence isn't quite as stark as Black suggests.

✂ Re: How reliable is DNA ...? (Schaefer, [RISKS-25.28](#))

<Bob Buxton <bob_buxton@uk.ibm.com>>

Thu, 14 Aug 2008 12:19:41 +0100

Steve's analogy to the Birthday Problem/Paradox can be extended further in considering the DNA question.

The birthday problem probabilities contain a number of assumptions:

- We know the number of days in the year
- Births are evenly distributed across the year
- Party invites are random

If we find at my party there are lots of people with a common birthday or more than two with my birthday we have to ask whether:

- This is perfectly normal and likely event based on the probabilities
- It is a rare, but still normal 'fluke'
- The interpretation of the probabilities was incorrect.
- The calculation of the probabilities was incorrect
- There is a flaw in the underlying assumptions.

I am neither a genetics or statistical expert but it seems that Troyer found a result that didn't match the expected results for the first part of the birthday problem. You can't tell much from a single sample but if you get similar results from multiple samples you have a better basis for questioning the underlying assumptions and by modifying them provide a far better estimate of the true probability of an actual genetic match from a profile. With DNA I am not even sure we are confident with knowing the number of day in a year

It seems to me that the FBI in their attempts to prevent lawyers using/misusing statistical data to induce confusion in mathematically naive juries by casting doubt on Troyer's work and blocking attempts to conduct further analysis are actually preventing legitimate research which could ultimately provide a proper basis for the uniqueness statistics.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 30

Thursday 28 August 2008

Contents

- [Bruce Schneier on Airport Photo ID Checks](#)
[PGN](#)
- [Flight-plan FAAilure](#)
[PGN](#)
- [Aug 26 FAA flight plan fiasco](#)
[Ken Knowlton](#)
- [Commuter Flights Grounded Thanks To Bumbling TSA Inspector](#)
[PGN](#)
- [Computer viruses make it to orbit](#)
[Gabe Goldberg](#)
- [Ohio Voting Machines Contained Programming Error That Dropped Votes](#)
[PGN](#)
- [States throw out costly electronic voting machines](#)
[vim](#)
- [Risks of going on Internet record](#)
[Spamcop](#)
- [And here we go off the rails: "spam hunter"](#)
[Identity withheld by request](#)
- [Educational "testing firm" flunks Internet Security 101](#)
[Danny Burstein](#)
- [A cellphone bill roams to the stratosphere](#)
[Gabe Goldberg](#)
- [Weird Clock Issue](#)
[Steven J. Greenwald](#)
- [Risks of omitting off-site backups?](#)
[C.Y./J.E. Cripps](#)
- [Telephone banking password /in/security](#)
[Tim Bradshaw](#)
- [Boston judge tosses MIT students' gag order](#)
[Richard Forno](#)
- [Re: DNA Database Searches](#)
[Hal Murray](#)
[Ken Knowlton](#)
- [Re: Couple of On-Line Travel Booking Risks](#)
[Chris Drewe](#)

- [Re: Germany's New Unified Tax Identification Codes](#)
Ralf Fritzsch
 - [Re: P2P Data Breach affects SCOTUS](#)
Hal Murray
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Bruce Schneier on Airport Photo ID Checks

<"Peter G. Neumann" <neumann@csl.sri.com>>
Thu, 28 Aug 2008 10:00:09 PDT

Opinion

The TSA's useless photo ID rules
No-fly lists and photo IDs are supposed to help protect the flying public from terrorists. Except that they don't work.

By Bruce Schneier

August 28, 2008

<http://www.latimes.com/news/opinion/la-oe-schneier28-2008aug28,0,3099808.story>

The TSA is tightening its photo ID rules at airport security. Previously, people with expired IDs or who claimed to have lost their IDs were subjected to secondary screening. Then the Transportation Security Administration realized that meant someone on the government's no-fly list -- the list that is supposed to keep our planes safe from terrorists -- could just fly with no ID.

Now, people without ID must also answer personal questions from their credit history to ascertain their identity. The TSA will keep records of who those ID-less people are, too, in case they're trying to probe the system.

This may seem like an improvement, except that the photo ID requirement is a joke. Anyone on the no-fly list can easily fly whenever he wants. Even worse, the whole concept of matching passenger names against a list of bad guys has negligible security value.

How to fly, even if you are on the no-fly list: Buy a ticket in some innocent person's name. At home, before your flight, check in online and print out your boarding pass. Then, save that web page as a PDF and use Adobe Acrobat to change the name on the boarding pass to your own. Print it again. At the airport, use the fake boarding pass and your valid ID to get through security. At the gate, use the real boarding pass in the fake name to board your flight.

The problem is that it is unverified passenger names that get checked against the no-fly list. At security checkpoints, the TSA just matches IDs to whatever is printed on the boarding passes. The airline checks boarding passes against tickets when people board the plane. But because no one checks ticketed names against IDs, the security breaks down.

This vulnerability isn't new. It isn't even subtle. I first wrote about it in 2006. I asked Kip Hawley, who runs the TSA, about it in 2007. Today, any terrorist smart enough to Google "print your own boarding pass" can bypass the no-fly list.

This gaping security hole would bother me more if the very idea of a no-fly list weren't so ineffective. The system is based on the faulty notion that the feds have this master list of terrorists, and all we have to do is keep the people on the list off the planes.

That's just not true. The no-fly list -- a list of people so dangerous they are not allowed to fly yet so innocent we can't arrest them -- and the less dangerous "watch list" contain a combined 1 million names representing the identities and aliases of an estimated 400,000 people. There aren't that many terrorists out there; if there were, we would be feeling their effects.

Almost all of the people stopped by the no-fly list are false positives. It catches innocents such as Ted Kennedy, whose name is similar to someone's on the list, and Islam Yusuf (formerly Cat Stevens), who was on the list but no one knew why.

The no-fly list is a Kafkaesque nightmare for the thousands of innocent Americans who are harassed and detained every time they fly. Put on the list by unidentified government officials, they can't get off. They can't challenge the TSA about their status or prove their innocence. (The U.S. 9th Circuit Court of Appeals decided this month that no-fly passengers can sue the FBI, but that strategy hasn't been tried yet.)

But even if these lists were complete and accurate, they wouldn't work. Timothy McVeigh, the Unabomber, the D.C. snipers, the London subway bombers and most of the 9/11 terrorists weren't on any list before they committed their terrorist acts. And if a terrorist wants to know if he's on a list, the TSA has approved a convenient, \$100 service that allows him to figure it out: the Clear program, which issues IDs to "trusted travelers" to speed them through security lines. Just apply for a Clear card; if you get one, you're not on the list.

In the end, the photo ID requirement is based on the myth that we can somehow correlate identity with intent. We can't. And instead of wasting money trying, we would be far safer as a nation if we invested in intelligence, investigation and emergency response -- security measures that aren't based on a guess about a terrorist target or tactic.

That's the TSA: Not doing the right things. Not even doing right the things it does.

✈ Flight-plan FAAilure

*<"Peter G. Neumann" <neumann@csl.sri.com>>
Tue, 26 Aug 2008 19:11:09 PDT*

On 26 Aug 2008, the Atlanta Federal Aviation Administration facility had difficulties processing data, which meant that all of its flight-plan information had to be processed by the Salt Lake City facility -- which became overloaded. As a result, airports experienced hours of flight delays on Tuesday afternoon and into the evening. A similar event occurred on 8 Jun 2007. [Source: CNN.com item, 26 Aug 2008; PGN-ed]

<http://www.cnn.com/2008/TRAVEL/08/26/faa.computer.failure/index.html>

✂ Aug 26 flight plan fiasco

<KCKnowlton@aol.com>

Wed, 27 Aug 2008 12:14:36 EDT

Apropos of the Aug 26 flight plan disaster, FAA spokeswoman Diane Spitaliere said that the investigation into what caused the problem is still ongoing, and she did not know when it would be completed. "It usually takes a while to be quite honest," she said. (AP, 8/26/08)

Is this improper to imagine: "Traffic control to all planes in flight: We're having problems with traffic logistics and don't know when they will be unsnarled, to be quite honest. Please proceed to and augment the nearest holding pattern, remain aloft, and observe VFR until further notice."

[Unfortunate recording of what she said? "It usually takes a while to be quite honest." It should NEVER take any time to be honest. We presume that what she said orally should have been transcribed as "It usually takes a while, to be quite honest." But commas are seldom COMMAndeered orally. PGN]

✂ Commuter Flights Grounded Thanks To Bumbling TSA Inspector

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

Wed, 20 Aug 2008 17:17:11 PDT

Total Air Temperature (TAT) probes on nine American Eagle regional jets were damaged because "an overzealous TSA employee attempted to gain access to the parked aircraft" by using the TAT probes as would-be handholds. [Source: Aero-News.Net, 20 Aug 2008; PGN-ed; see the follow-up analysis by Jim Campbell, ANN E-I-C, who says "This was an extraordinarily dangerous incident, folks."]

<http://www.aero-news.net/index.cfm?ContentBlockID=340a79d6-839a-470d-b662-944325cea23d>

✂ Computer viruses make it to orbit

<Gabe Goldberg <gabe@gabegold.com>>

Thu, 28 Aug 2008 09:09:43 -0400

A computer virus is alive and well on the International Space Station (ISS). NASA has confirmed that laptops carried to the ISS in July were infected with a virus known as Gammima.AG. The worm was first detected on Earth in August 2007 and lurks on infected machines waiting to steal login names for popular online games. NASA said it was not the first time computer viruses had traveled into space, and it was investigating how the machines were infected.

Source: BBC NEWS, Technology

<http://news.bbc.co.uk/2/hi/technology/7583805.stm>

✂ Ohio Voting Machines Contained Programming Error That Dropped Votes

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

Thu 21 Aug 2008 14:47:12 PDT

Premier (formerly Diebold) has admitted to a software flaw in its GEMS system used in 34 states that can cause votes to be dropped while being transferred from memory cards to a central tallying point. This flaw has existed for at least 10 years, and because it is in the back-end counting software, it affects both touch-screen and optical-scan systems. [Source: Mary Pat Flaherty, *The Washington Post*, 21 Aug 2008; PGN-ed]

[Premier had previously asserted that this anomaly was the result of interference from the anti-virus software, which as I noted in my comment at the end of jared's post in [RISKS-25.29](#), seemed totally bogus to me.]

✂ States throw out costly electronic voting machines

<vim@duncan.cx>

Tue, 19 Aug 2008 18:03:50 -0700

The demise of touch-screen voting has produced a graveyard of expensive corpses: Warehouses stacked with thousands of carefully wrapped voting machines that have been shelved because of doubts about vanishing votes and vulnerability to hackers.

What to do with this high-tech junkyard is a multimillion-dollar question. One manufacturer offered \$1 a piece to take back its ATM-like machines. Some states are offering the devices for sale on eBay and craigslist. Others hope to sell their inventories to Third-World countries or salvage them for scrap.

Much money could have been saved had those bureaucrats just been subscribers to The Risks Digest.

Full AP Story here:

<http://ap.google.com/article/ALeqM5jej6XIWrQn6-gw5O5bJa1ELx78DgD92LLDO00>

✂ Risks of going on Internet record

<Spamcop <...>>

Thu, 21 Aug 2008 10:09:03 +0100

Even China can't remove the old or cached links fast enough:

> Chinese Gold Medalist Too Young To Compete, Finds Security Consultant

> InformationWeek Wed, 20 Aug 2008 1:42 PM PDT

> Mike Walker's Web search turned up an official Chinese Excel spreadsheet that indicates that gymnast He Kexin is only 14 years old.

http://www.informationweek.com/news/internet/policy/showArticle.jhtml?articleID=210102137&cid=RSSfeed_IWK_All

Blogging under the name Stryde Hax, Mike Walker, a principal consultant for the security group, has posted screenshots of an Excel spreadsheet that was removed from an official Chinese government Web site but was still available through Baidu, China's most popular search engine. The file appears to show that He Kexin is not old enough for Olympic competition.

<http://strydehax.blogspot.com/2008/08/hack-olympics.html>

Google returns about 36,700 for "He Kexin" AND "1994". (0.31 seconds)

The risk is also claiming the success of youth when it suits the PR in one case but not the other.

http://en.wikipedia.org/wiki/He_Kexin

✂ And here we go off the rails: "spam hunter"

<[Identity withheld by request]>

Tue, 05 Aug 2008

A large amount of spams were sent out in the name of a well known "spam hunter" in Switzerland, alleging he was about to commit suicide (Article in German at <http://www.20min.ch/digital/webpage/story/19754588>).

The attack (according to the media and interview with the person involved) appears to bear signs of the "Russian Internet mafia", and appears to herald a change into personal territory by the criminals involved. This attack has already had effect in that the subject is reconsidering what he does for a living. It's not a new idea to go personal, especially Spamhouse has suffered its share over the years.

The ensuing discussion on a security mailing list was interesting. It started with a simple observation that it maybe was a drive-by attack with infected websites, but there are some deeper implications. I've compiled the observations below.

- - - first response - - -

> AFAIK no DriveBy download, as the domains are not responding at all.

That may have more to do with actions of ISPs in the chain or there may be irony at work - the serving DNS may have been poisoned, thus having one evil canceling out another.

> but according to 20min.ch (article in German)

> <http://www.20min.ch/digital/webpage/story/19754588>

> it was, as assumed, some unhappy spammer who thought that its funny to
> send suicide letters.

Calling it that way ignores the real issue IMHO..

> Apparently several people contacted the police to report a possible
> suicide, and they promptly went and ringed the guy out of his bed at
> his apartment.

What happened here was that the spammers got personal, and with a large degree of success as the guy is now reconsidering what he's going to do professionally.

Let me translate this for you:

1 - he was obviously successful in what he did or whoever did this would not have bothered;

2 - a couple of published successes like that will ensure this to become a frequent event. The good news is that the effect will diminish over time, the bad news is that this will take time. Are you prepared to have family and friends threatened in this way - YOU may know it's mostly air, but most non-professionals don't., and it won't stop here.

- - - next response - - -

yep. try to explain THAT to your friends, customers, business contacts, etc. IF they are on the recipient list for that kind of spam. It could take you out of business, if people read that kind of crap and probably believe it. Even worse: Who are you going to inform about the faked story? If you inform all of your contacts, you will alert also those who did not even know about the SPAM problem.

✶ Educational "testing firm" flunks Internet Security 101

*<danny burstein <dannyb@panix.com>>
Tue, 19 Aug 2008 14:55:39 -0400 (EDT)*

The Princeton Review, the test-preparatory firm, accidentally published the personal data and standardized test scores of tens of thousands of Florida students on its Web site, where they were available for seven weeks. ...

One folder on the Web site gave unusual insight into how test preparation companies use older exams to prepare their practice tests. The folder contained digital scans of eight official SATs and six PSAT exams from 2005 through 2007. The tests are created by the Educational Testing Service, a nonprofit organization in Princeton, N.J.

<http://www.nytimes.com/2008/08/19/technology/19review.html?em>

✂ A cellphone bill roams to the stratosphere

<Gabe Goldberg <gabe@gabegold.com>>

Thu, 28 Aug 2008 10:17:18 -0400

Santa Monica resident Aurelie Foucaut traveled last month to Paris with her two kids. During a brief stopover in Montreal, she made six calls on her BlackBerry to friends and family members, each lasting less than three minutes.

Foucaut's wireless bill from T-Mobile arrived a few weeks ago. It included \$59.77 in ordinary usage charges. It also included a \$2,367.40 "data service roaming charge" for nearly 158 megabytes' worth of Internet access while in Montreal -- the equivalent of downloading about 80 novels.

"How is this possible?" Foucaut, 41, wanted to know. "I never go on the Internet with my phone. I don't download into my BlackBerry. I don't even know how to do it."

Los Angeles Times, 27 Aug 2008

<http://www.latimes.com/business/la-fi-lazarus27-2008aug27,0,7630867.column>

✂ Weird Clock Issue

<"Steven J. Greenwald" <sjg6@gate.net>>

Mon, 18 Aug 2008 21:06:36 -0400

At the moment, we experience tropical storm Fay here in the Miami area. It does not seem too bad compared to past tropical storms, and we have only experienced some few power outages that got fixed fairly quickly (typical). We've had some pretty impressive wind gusts (I'd guess about 40-50MPH). However, I noticed something really weird.

I have a battery operated clock that syncs via radio signal reception with the atomic clock in Boulder (very common - made by Oregon Scientific). It currently shows the correct time (as of writing: 9:05 PM EDT) but shows the date as Saturday September 27th 2008 instead of the correct date of Monday August 18, 2008!

I have no idea why this has happened. Perhaps some weird electromagnetic effect due to the storm (I have noticed things like compasses giving 180

degree wrong readings and spinning during storms)? Perhaps just some other glitch that just coincidentally happened during the storm?

Risks of omitting off-site backups?

*<"C.Y./J.E. Cripps" <cycmn@nyct.net>>
Thu, 21 Aug 2008 23:26:15 -0400 (EDT)*

Victor M. Deeb is wondering why 20 years of his work was thrown away. At 71, he had been experimenting in his basement laboratory. When firemen came in to put out a fire in a window air conditioner, they found 1500 vials, jars cans, bottles, and boxes of chemicals in his basement when they went to turn off the power. The Massachusetts state hazardous materials team reacted by having everything that was deemed hazardous removed and disposed of. So, 45 years of his research in polymer chemistry went down the drain (so to speak). However, all of his materials were approved by the U.S. FDA and seemingly nonhazardous. City officials maintain he was violating zoning laws. They also maintain he was given opportunities to recover his 20-years worth of notes, which were apparently seized. [Source: Priyanka Dayal, Chemist considers legal action over materials seized, *Worcester Telegram & Gazette News*, 16 Aug 2008]

<http://www.telegram.com/article/20080816/NEWS/808160346/1116>

The need for backups is not emphasized enough in this much-discussed story. (In this instance, photocopies of the mss notes would suffice.)

Telephone banking password /in/security

*<Tim Bradshaw <tfb@tfeb.org>>
Thu, 28 Aug 2008 00:24:33 +0100*

See this story in the BBC news: <http://news.bbc.co.uk/1/hi/england/hereford/worcs/7585098.stm>

The story raises at least two questions.

Firstly, if we are to believe the story, the person found out what his password had been altered to. So the whole text of the password was available to him (and probably to members of bank staff also). This should not be the case for obvious reasons.

Secondly, the story itself is extraordinary, as the BBC seem to have no notion that there might be a serious problem here, rather than just an amusing story.

It's tempting to add that this must mean that telephone banking passwords are held in plain-text equivalent, and that this is obviously a huge security problem. It does mean that they must be in plain-text equivalent, but things are not quite so simple: given the common "tell me characters a, b, and c of your password" approach, a conventional one-way hash of the

password does not work. I suppose you could create hashes for every possible subset of (say) 3 characters (so for "password", hash "pas-----", "pa-s-----" & so on), but that may be quite a lot of hashes (I think it is the number of combinations, so for 3-from-10 it would be 120 hashes, for 3-from-20 it would be 1140), and might also give an attacker a way into guessing the whole password. Still, that would probably be a lot better than keeping it in clear, which seems to be what is happening here.

✂ Boston judge tosses MIT students' gag order (Re: [RISKS-25.28](#))

<Richard Forno <rforno@infowarrior.org>>
August 19, 2008 1:54:46 PM EDT

[From Dave Farber's IP distribution]

[Source: Kim Zetter's WiReD blog, Federal Judge Throws Out Gag Order Against Boston Students in Subway Case, 19 Aug 2008; PGN-ed]
<http://blog.wired.com/27bstroke6/2008/08/federal-judge-t.html>

U.S. District Judge George A. O'Toole, Jr., vacated the temporary 10-day gag order that another judge had instituted against the three MIT students who were prevented from presenting a talk on security vulnerabilities in the Boston subway's fare tickets and cards. The judge also threw out a request by the MBTA to expand the restraining order. [[RISKS-25.28](#) and 25.29]

Dave's IP Archives: <https://www.listbox.com/member/archive/247/=now>

✂ Re: DNA Database Searches ([RISKS-25.25](#))

<Hal Murray <hmurray@megapathdsl.net>>
Tue, 19 Aug 2008 13:53:09 -0700

From:

<http://articles.latimes.com/2008/jul/20/local/me-dna20>

> The FBI laboratory, which administers the national DNA database
> system, tried to stop distribution of Troyer's results and began an
> aggressive behind-the-scenes campaign to block similar searches
> elsewhere, even those ordered by courts, a Times investigation found.

> No one knows precisely how rare DNA profiles are. The odds presented
> in court are the FBI's best estimates.

There is another risk in here. The FBI is tarnishing their reputation and with it the reputation of our whole justice system.

The FBI has (had?) a reputation for doing good science. Why are they dragging their feet because somebody wants to double check their work? What are they trying to hide?

I'm not a wizard on DNA matching or statistics, but I think I'm smart enough to understand a good white paper discussing this topic. I'm surprised the FBI hasn't written one and squashed this discussion.

Maybe The National Academy of Sciences should be asked to review this tangle.

✉ Re: How reliable is DNA ([RISKS-25.27-29](#))

<KCKnowlton@aol.com>

Tue, 19 Aug 2008 10:21:22 EDT

RISKS readers should be quite aware of the troublesome February 29th. Rather special statistics apply to about one of 1461 people who are born on Feb 29.

Recall: Leap-Year software bug gives "Million-dollar glitch" ([RISKS-18.74](#))

On the last day of a leap year in 1996, an aluminum plant in New Zealand triggered a software flaw that failed to account for the year having 366 days. It caused an enormously expensive event on the 366th day of the year. And there must be many similar incidents I don't remember. [PGN-ed]

✉ Re: Couple of On-Line Travel Booking Risks ([RISKS-25.28](#))

<"Chris Drewe" <e767pmk@yahoo.co.uk>>

Sat, 23 Aug 2008 21:53:49 +0100

There's a sort-of follow-up to this item in the travel section of today's newspaper (23 Aug 2008):

> A reader comments that the US Electronic System for Travel Authorisation
> application site at <https://esta.cbp.dhs.gov> didn't accept his passport
> because it was valid for more than 10 years.

Several readers have reported being charged \$49.95 for a permit application, which is a pain as the previous paper I-94W forms were free. As far as I can tell, applying via the official ESTA web site is free, but it appears that doing a Google (or similar) search for the site will match on some commercial agency sites which do charge for handling applications. These agencies may be offering some sort of value-added service, but the RISK is that people may be persuaded to pay a third party unnecessarily for something that they could do themselves, because of web search results.

✉ Re: Germany's New Unified Tax Identification Codes ([RISKS-25.29](#))

<"Ralf Fritsch" <Ralf.Fritsch@baw.de>>

Wed, 27 Aug 2008 10:14:40 +0200

It seems definite that obviously white spaces in the original data were misinterpreted during data transfer. Technical reasons remain until now unknown.

In the between, all 46000 inhabitants of Stade (Lower Saxony) received new letters from the Federal Central Tax Office regarding their Tax Identification Codes. As far as I can speak for myself and my family, for now the information is correct :-)

Nevertheless, the question who or what was responsible for the mess-up, remains unanswered.

Re: P2P Data Breach affects SCOTUS (Ashworth, [RISKS 25.24](#))

<Hal Murray <hmurray@megapathdsl.net>>
Tue, 19 Aug 2008 12:18:06 -0700

> People would be inclined to say "but it's not reasonable to believe that
> large corporate sites would be involved in this sort of collusion!".

Maybe things outside the USA are better, but around here anybody who is at all concerned about their privacy knows that our advertising companies collect all the information that they can get their hands on. Consider credit bureaus. Many years ago they may have been in the credit business. Today, they are in the information business.

Besides, it's not just corporate America that wants to collect your info. How many times has TSA been mentioned on RISKS?



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 31

Wednesday 10 September 2008

Contents

- [FAA redundancy -- or the lack thereof](#)
[Tessler and Robertson via PGN](#)
 - [Corrupt File Brought Down Flight Planning System](#)
[Gabe Goldberg](#)
 - [UK software upgrade issues](#)
[John Sawyer](#)
 - [JPMorgan Chase: The Bank Account That Sprang a Leak](#)
[Monty Solomon](#)
 - [Software problems affect the bottom line at J. Crew](#)
[Steven M. Bellovin](#)
 - [Google ads and language](#)
[Erling Kristiansen](#)
 - [Worditudinality](#)
[Rob Slade](#)
 - [Control-C vs. Bourne-Again SHell](#)
[jidanni](#)
 - [Control-C Control-C vs. gnus](#)
[jidanni](#)
 - [Risks of better security and "smarter" users](#)
[Ron Garret](#)
 - [BNY Mellon Data Breach Potentially Massive](#)
[George Hulme via Monty Solomon](#)
 - [Student hacker exposes Carleton U cash, ID card security holes](#)
[Sergei Patchkovski](#)
 - [Whit Diffie and Susan Landau: Internet Eavesdropping](#)
[Randall Webmail](#)
 - [US .gov website asks for personal info without https protection](#)
[Jonathan Thornburg](#)
 - [Re: Germany's New Unified Tax Identification Codes](#)
[Kevin Pfeiffer](#)
 - [Re: Firefox 3's Step Backwards ...](#)
[Dimitri Maziuk](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ FAA redundancy -- or the lack thereof

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

Sat, 30 Aug 2008 15:12:08 PDT

The FAA computer problem on 26 Aug 2008 ([RISKS-25.30](#)) "served as a reminder that the U.S. flight system is waiting for a modernizing overhaul." The FAA is apparently using "computing practices that would be considered poor in credit card networks or power plant operators -- relying on only the Atlanta and Salt Lake City centers for flight planning. For example, power and water utilities can be find a million dollars a day if they are willfully negligent. [Source: Joelle Tessler and Jordan Robertson, FAA outage reveals odd computing practices, AP item, 29 Aug 2008; PNG-ed]

<http://www.washingtonpost.com/wp-dyn/content/article/2008/08/29/AR2008082902088.html?hpid=sec-tech>

✂ Corrupt File Brought Down Flight Planning System

<Gabe Goldberg <gabe@gabegold.com>>

Fri, 29 Aug 2008 14:17:58 -0400

Strike 1: A corrupt file wasn't caught by validation?

Strike 2: It took 2 1/2 hours to restart after the failure?

Strike 3: The "backup" computer couldn't handle the failover load?

Strike 4: The restored-to-service computer couldn't clear the accumulated backlog until new transactions were suppressed?

Corrupt File Brought Down Flight Planning System A corrupt file contained in a normal software upload brought down the FAA's main flight planning computer on Tuesday, delaying hundreds of flights and prompting questions about the inevitability of it happening again. FAA spokesman Paul Takemoto told eWeek the corrupt file stopped flight plans from being filed at the FAA's Hampton, Ga. facility, which is the principal flight planning computer. "Basically, all the flight plans that were in the system were kicked out," Takemoto said. "For aircraft already in the air, or had just been pushed back from the gate, they had no problems. But for all other aircraft, it meant delays."

The system switched to the FAA's backup flight planning computer in Salt Lake City, which was quickly overwhelmed by airlines trying in vain to enter flight plans. "They just kept hitting the 'Enter' button. So the queues immediately became huge," Takemoto said. "On top of that, it happened right during a peak time as traffic was building. Salt Lake City just couldn't keep up." The Georgia computer was fixed in two-and-a-half hours but it wasn't until the FAA asked airlines to stop filing flight plans that the backlogs started to clear. All was reported normal on Wednesday but eWeek is

openly wondering how much longer the "a creaky old IT system" can continue. The system is more than 20 years old and the company that built it has been out of business most of that time, eWeek reported.

UK software upgrade issues

*<John Sawyer <jpgsawyer@googlemail.com>>
Sat, 30 Aug 2008 01:33:07 +0100*

Yet another example of UK government not testing software properly before upgrading!

<http://news.bbc.co.uk/1/hi/england/cambridgeshire/7588551.stm>

They want us to trust them with more information?

Dr John Sawyer, Wiltshire England.

JPMorgan Chase: The Bank Account That Sprang a Leak

*<Monty Solomon <monty@roscom.com>>
Sun, 31 Aug 2008 10:04:21 -0400*

Surely customers of the elite private banking operation at JPMorgan Chase, serving only the bank's wealthiest clients, are safe from such problems, right? Wrong, says Guy Wyser-Pratte, an activist investor on Wall Street for more than 40 years who uses his hedge fund's war chest of roughly \$500 million to wage takeover fights and proxy battles in the United States and Europe. In May, he learned that someone had siphoned nearly \$300,000 from his personal account at the private bank through many small electronic transfers over a 15-month period. Then he was told by the bank that he could stop the theft only by closing his account and opening a new one. And then JPMorgan Chase told him that the bank would cover only \$50,000 of his losses. ... [Source: Diana B. Henriques, *The New York Times*, 30 Aug 2008; PGN-ed]

<http://www.nytimes.com/2008/08/30/business/yourmoney/30theft.html?partner=rssuserland&emc=rss&pagewanted=all>

Software problems affect the bottom line at J. Crew

*<"Steven M. Bellovin" <smb@cs.columbia.edu>>
Sat, 30 Aug 2008 10:31:22 -0400*

According to the Wall Street Journal's Business Technology blog, software problems from a "botched system upgrade" caused earnings for the third quarter to drop by 12% from a year earlier. Problems included outages,

performance, botched orders, return problems, call center issues, and more.
<http://blogs.wsj.com/biztech/2008/08/27/j-crew-blames-software-for-its-bad-quarter/>

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

#Google ads and language

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>

Wed, 03 Sep 2008 20:09:26 +0200

Googling something in one language while accessing from another language environment can give rather amusing ads.

I looked for "SOA SWIM" (SOA = Service oriented architecture; SWIM = System wide information management. Both terms are related to network architecture). The first half-dozen hits were spot on, and gave me what I was looking for.

But the ads somehow caught my eye: Cures for chlamydia.
Explanation: SOA is the Dutch abbreviation for sexually transmitted disease.

So it seems that, while the search engine tries to match as many search terms as possible, the ads go for single words.

At first, I had a good laugh. But, thinking a bit more about what happened, what if somebody was trying to make a profile of me based on single words?

Some time ago (actually, quite a longtime ago), I was googling for "EROS data centre", a professional repository of Earth resource imagery.

Put EROS and SOA together, and you might get the wrong idea of what I had been up to, and what were the consequences.

#Worditudinality

<Rob Slade <rMslade@shaw.ca>>

Thu, 4 Sep 2008 18:25:35 -0800

Go look up the term rootkit on Wikipedia. (Go ahead, I'll wait.) Lovely entry, isn't it? Lots of information. Trouble is, there's lots of misinformation, too.

A rootkit is **not** "a program ... designed to take fundamental [or] ... `root' access" for a system. It's designed to **keep** that access, once you broken into the system and grabbed it. (And rootkits were around before 1990, etc, but we'll let that go for the moment.)

Or, at least, it used to be defined that way. Recently, all kinds of people have been redefining what rootkit means, to the point that it may no longer

mean anything.

Wikipedia is a wonderful tool, and the English encyclopedia made with it is a wonderful resource. For the most part. But when you get to the real specialty areas you start running into problems. As John Lawton has pointed out, the irony of the information age is that it has given new respectability to uninformed opinion. And Wikipedia is susceptible to that problem.

Now the Wikipedia people are aware of the problem, and have provided ways to address it. There is the fact that anyone can correct errors, when errors have been made. There are technical controls in terms of limits on changes. There are administrative controls in the granting of elevated privileges to editors. But occasionally you get a breakdown, such as the fact that an editor can be, him or herself, in error. And then you get entries like the one for rootkit.

But Wikipedia is not what I really want to talk about. I want to talk about words. Specifically, the jargon that we use, and create, in technical fields, and in the field of information security in particular. Because language is kind of like a giant Wikipedia, where anyone at all can make an entry. And anyone at all can try and modify that entry.

Lots of people like to talk about computer security. It's quite likely that more people like to talk about security than actually *do* anything about security. So it's not hard to see that a lot of the people who are talking, and writing, about security often talk about things that, well, they are not quite certain about.

If I say that Alan Turing was a homosexual, I might be right, or I might be wrong. But it would be fairly easy to check whether I was right or wrong. However, if I say that a Turing Machine is a universal computer because it can be implemented on any computer, I am making a different kind of assertion, and one that it harder to check. Someone who hears me say that, and knows that I'm wrong, might not challenge it immediately, because it's partly right, and the error I've made may not be important to the point that I'm making. But the people who hear me make that statement, and who do not know why the statement is in error, are probably going to assume and generate various kinds of mistaken ideas about Turing machines. And if I make the statement frequently enough, and in enough different places, it starts being taken as true. And eventually we'll have people saying that a universal computer is any entity that can be implemented on any platform. Which had nothing at all to do with what Turing was doing and proving.

So it is with a number of the specialized terms that we have been using in infosec. A lot of people are getting hold of them, and using them in sloppy ways. Now, a great many people say that language is living, and you have to make allowances for that growth. Fair enough: much of the vocabulary that we use every day in computer security didn't even exist fifty years ago, so it would be hard to argue the point. However, if the terms can be changed by anyone, at any time, then they lose meaning. If I use the word virus to mean one thing, and you use it to mean something quite different, then we aren't going to come to any agreement. We can't communicate. And, in all of these rapidly changing technical fields, communication is vitally

important.

So, in the blort, I just want to regrify you to smetnicate all forms of antrifact.

Yelth you for your fesculant.

victoria.tc.ca/techrev/rms.htm blogs.securiteam.com/index.php/archives/author/p1/

✂ Control-C vs. Bourne-Again SHell

<jidanni@jidanni.org>

Mon, 01 Sep 2008 02:04:01 +0800

Naturally I only use orthodox Free Software, like bash, the GNU Bourne-Again SHell, to control my household projects.

\$ sleep 55; launch_rocket

The problem is if one discovers a missing O-ring etc., then a Control-C interrupt will not cancel the whole launch as it does in other leading brand SHells, but instead just cancel the countdown -- VROOM. Next time use an && operator instead of a ;.

✂ Control-C Control-C vs. gnus

<jidanni@jidanni.org>

Mon, 01 Sep 2008 02:52:22 +0800

We continue our Control-C adventures with gnus.

As you know I only use the highest pedigree Free Software, Stallman->emacs->gnus, wherein lies

C-c C-c runs the command message-send-and-exit

I told them 13 times this was too easy to hit by accident, and rigged up my own Child Safety Cap macro.

Well, just the other day I was attempting to hit

C-c C-f C-c runs the command message-goto-cc

to merely add somebody important to the CC: header,

<http://news.gmane.org/group/gmane.emacs.gnus.general/thread=67308>

but guess which key I pressed too lightly? Imagine me sending half baked messages out the door before they are complet

✂ Risks of better security and "smarter" users

<Ron Garret <ron@flownet.com>>

Tue, 19 Aug 2008 11:28:19 -0700

The other day I visited the site of a well known issuer of SSL certificates

to look up some information in my account. I was shocked to realize that I was able to access this information without going through a login procedure. All I did was click the "login" button, and my account information came up. This behavior persisted across a browser restart, and even a machine reboot.

I was shocked. Here's a company whose business is security, but their site (apparently) issues login cookies that don't expire! Worse, there didn't seem to be a "logout" button!

(Spoiler alert: it makes an interesting exercise to see if you can figure out how this happened, other than that the web site designers were idiots. Here's a hint: I use a Mac.)

Most "secure" (I've been reading RISKS far too long not to put that in scare quotes) web sites follow a common motif: there's a login page where you type your user name and password into an HTML form. That information gets sent to the server, which verifies your credentials and issues a session cookie. After you've done your business you log out, which either removes the session cookie from your browser or invalidates it at the server. Usually the session cookie expires after some period of inactivity.

But there is another method of authentication on the Web: HTTP authentication. This is the kind of authentication that makes a browser dialog pop up to ask for your user name and password rather than entering it into an HTML form. There are different kinds of HTTP authentication. The most common one is "basic" authentication, because it's the easiest to set up. It is also fairly insecure because it sends passwords in the clear (usually with an accompanying warning in the browser dialog). Because of this, HTTP authentication is generally frowned up for "serious" security, despite the fact that there are variants that are more secure than "basic" authentication.

The site in question was using one of these more advanced HTTP authentication schemes. The first time I ever logged into the site, the login dialog popped up and, without really thinking about it, I marked the checkbox next to "remember this username and password in my keychain."

Now, this alone should not have produced the behavior that I saw because normally in order to access the OS X keychain an application has to ask permission, and my browser wasn't. But it turns out that the OS X keychain has a handy-dandy convenience "feature" that allows you to permanently grant access to a particular keychain item to a particular application, and Safari had "helpfully" added itself to this list when it created the keychain item.

So here we have a security risk that is a confluence of three circumstances, two of which are the result, arguably, of too much knowledge. They are:

1. The web site used a secure authentication scheme that behaves almost identically to a less secure scheme
2. I am familiar with the more common design of secure sites and
3. OS X and Safari conspire to subvert the security of HTTP authentication in a very subtle way in order to make things more convenient for the user

I find myself at a loss to suggest how this particular risk might have been avoided.

#BNY Mellon Data Breach Potentially Massive (George Hulme)

<Monty Solomon <monty@roscom.com>>

Sat, 30 Aug 2008 01:24:54 -0400

http://www.informationweek.com/blog/main/archives/2008/08/bny_mellon_data.html

BNY Mellon Data Breach Potentially Massive

Posted by George Hulme, Aug 29, 2008 10:09 PM

It was in May when we noted an investigation launched by the authorities in the state of Connecticut into a backup tape lost by the Bank of New York Mellon. The results of that investigation are in, and they don't look good.

First, some background (which is available in my earlier post, here). A backup 10 unencrypted backup tapes with millions of customers' information had gone missing on Feb. 27, and the Connecticut authorities wanted to know more, as there were up to half-million Connecticut residents private information place at risk.

Here's what those (unencrypted) tapes contained, according to Attorney General Blumenthal's letter:

BNY representatives informed my office that the information on the tapes contained, at a minimum, Social Security numbers, names and addresses, and possibly bank account numbers and balances.

That's just great, isn't it.

At first, we thought there were 4 million whose private financial information was on those tapes; turns out now that there could be up to 10 million. Here's what Connecticut Gov. M. Jodi Rell has to say in a statement released yesterday:

"It is simply outrageous that this mountain of information was not better protected and it is equally outrageous that we are hearing about a possible six million additional individuals and businesses six months after the fact," Governor Rell said. "We fear a substantial number of Connecticut residents are among this latest group."

I couldn't agree more. There is absolutely no acceptable excuse as to why this information was not encrypted on these tapes. None.

The BNY Mellon has set up this Web site for those who may have been affected by this incident.

Student hacker exposes Carleton U cash, ID card security holes

<Sergei Patchkovski <serguei.patchkovskii@sympatico.ca>>

Tue, 09 Sep 2008 12:09:33 +0000

On 9 Sep 2009, CBC News carried a report of a security breach of the Carleton University student ID cards. The Ottawa-based university issues the barcode and magnetic stripe-equipped cards to the students. The cards can be used to access on-campus buildings (including some of the residences), pay for services on-campus, and access university e-mail systems. According to the news report, a student (it is not clear from the report whether this was a student at Carleton, or at the Ottawa U - the other large university in the area) has compromised the security of the card by writing a piece of software "in a few hours" and installing it on a computer lab terminal. The attacker was able to collect the e-mail login credentials of at least 32 Carleton students. He/she then proceeded to report the breach to the victims and the university authorities, under an alias "Kasper Holmberg". In the report, he/she suggested that the system in its present form lacks the most basic safeguards against misuse, and should be suspended. University authorities has issued new ID cards to the affected students, and assured campus ID card users that "the campus e-mail system and campus card network are safe". The university is further considering calling in the police and charging "Karsper Holmberg" criminally for taking "a very odd way to draw attention to the security of the system", according to the university spokes-person, Christopher Walters.

The complete news story can be found at:

<http://www.cbc.ca/canada/ottawa/story/2008/09/08/ot-security-080908.html>

Whit Diffie and Susan Landau: Internet Eavesdropping

<Randall Webmail <rvh40@insightbb.com>>

August 30, 2008 1:32:46 AM EDT

[From several other groups that I see, including Dave Farber's IP. PGN]

<http://www.sciam.com/article.cfm?id=internet-eavesdropping>

As telephone conversations have moved to the Internet, so have those who want to listen in. But the technology needed to do so would entail a dangerous expansion of the government's surveillance powers

By Whitfield Diffie and Susan Landau

As long as people have engaged in private conversations, eavesdroppers have tried to listen in. When important matters were discussed in parlors, people slipped in under the eaves -- literally within the `eaves drop' -- to hear what was being said. When conversations moved to telephones, the wires were tapped. And now that so much human activity takes place in cyberspace, spies

have infiltrated that realm as well.

Unlike earlier, physical frontiers, cyberspace is a human construct. The rules, designs and investments we make in cyberspace will shape the ways espionage, privacy and security will interact. Today there is a clear movement to give intelligence activities a privileged position, building in the capacity of authorities to intercept cyberspace communications. The advantages of this trend for fighting crime and terrorism are obvious.

The drawbacks may be less obvious. For one thing, adding such intercept infrastructure would undermine the nimble, bottom-up structure of the Internet that has been so congenial to business innovation: its costs would drive many small U.S. Internet service providers (ISPs) out of business, and the top-down control it would require would threaten the nation's role as a leader and innovator in communications.

Furthermore, by putting too much emphasis on the capacity to intercept Internet communications, we may be undermining civil liberties. We may also damage the security of cyberspace and ultimately the security of the nation. If the U.S. builds extensive wiretapping into our communications system, how do we guarantee that the facilities we build will not be misused? Our police and intelligence agencies, through corruption or merely excessive zeal, may use them to spy on Americans in violation of the U.S. Constitution. And, with any intercept capability, there is a risk that it could fall into the wrong hands. Criminals, terrorists and foreign intelligence services may gain access to our surveillance facilities and use them against us. The architectures needed to protect against these two threats are different.

Such issues are important enough to merit a broad national debate. Unfortunately, though, the public's ability to participate in the discussion is impeded by the fog of secrecy that surrounds all intelligence, particularly message interception ('signals intelligence'). [...]

<http://tinyurl.com/6oolcn>

IP Archives: <https://www.listbox.com/member/archive/247/=now>

[Beware of the Adamant Eaves Drop. PGN]

US .gov website asks for personal info without https protection

<Jonathan Thornburg <J.Thornburg@soton.ac.uk>>

Fri, 29 Aug 2008 08:34:40 +0100 (BST)

I recently used the US Immigration and Customs Enforcement Agency's SEVIS (Student and Exchange Visitor Information System) to pay the fee for a US visa. The online version of this lives at

<http://www.ice.gov/sevis/i901/index.htm>

This process requires typing a variety of personal information into web forms lined from the ice.gov site, including full name, place/date of birth, and passport number. If one wants to pay online, credit card

information (including CVV2) is also required.

The index page for this system links to https urls for the actual form (as javascript-activated popups), but disables browser titlebars on the popular windows, so for most users there's little evidence of https security. And indeed, those https urls aren't even under a .gov domain, but rather (outsourced?) under fmjfee.com. I also saw no warnings about the dangers of typing such sensitive information on a public computer.

The risks of identity theft, or even "just" credit-card fraud, seem very large.

Re: Germany's New Unified Tax Identification Codes (Fritzsch, [R-25.29](#))

<Kevin Pfeiffer <pfeiffer@tiros.net>>

Fri, 05 Sep 2008 11:15:10 +0200

> It seems definite that obviously white spaces in the original data were
> misinterpreted during data transfer. Technical reasons remain until now
> unknown.

Empty fields, not "white space"

Ralf Fritzsch repeats the error from the original posting: the German-language newspaper source quoted wrote "empty [data] fields", not "white spaces". (Shades of the children's game "Stille Post" -- "Telephone".)

Re: Firefox 3's Step Backwards ... (Barrett, [RISKS-25.29](#))

<Dimitri Maziuk <dmaziuk@bmr.b.wisc.edu>>

Wed, 20 Aug 2008 12:52:47 -0500

> ... I believe that the criticism of Firefox 3.0 was simply misguided and
> ill-informed. This is not helpful.

Side note #1: the obvious self-contradiction. State that argument was strictly about encryption, then list a bunch of things that have nothing to do with encryption, then conclude that argument is misguided and ill-informed.

Side note #2: from day one SSL's been criticized for mixing two different things: encryption and authentication in one protocol. This precisely why. It's a design problem, most of the time you can't fix those in an implementation.

Aside from those, three problems with this argument are:

1. Why would I ever trust a certificate signed by someone called GoDaddy?

Especially over the one I generated and signed myself?

2. Nobody expects browser developers to come up with a solution for design flaw in underlying protocol (see side note #2) that works well for every user. Yet,

> The general logic is that most users should never be presented with ... a
> choice and the browser should make the decision for them. [sic]

3. The problem is not that firefox complains, it's that it previously complained that *signature cannot be verified*. Now it complains about *invalid certificate*. Technically a properly self-signed cert -- "criminal" or not -- is "invalid" only because firefox developers say so. And thy shalt trust their judgment because they, like GoDaddy, Know Better(tm).

Side note #3: another annoying new feature is that you can't type or paste into file upload field anymore.

Dimitri Maziuk, BioMagResBank, UW-Madison -- <http://www.bmrb.wisc.edu>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 32

Thursday 11 September 2008

Contents

- [Google revives 6-year-old news story, sends United shared down 75%](#)
[Steven J Klein](#)
[Drew Dean](#)
[Scott Nicol](#)
- [How Steve Jobs' obit got published](#)
[Philip Elmer-DeWitt via Monty Solomon](#)
- [Internet Traffic Begins to Bypass the U.S.](#)
[John Markoff via Monty Solomon](#)
- [Global Trail of an Online Crime Ring](#)
[Brad Stone via Monty Solomon](#)
- [Automated Bill Payments Are a Cinch: Not So Fast](#)
[Ron Lieber via Monty Solomon](#)
- [Hackers prepare supermarket sweep](#)
[Gabe Goldberg](#)
- [Antivirus software in critical systems?](#)
[Erling Kristiansen](#)
- [Re: States throw out costly electronic voting machines](#)
[Peter Houppermans](#)
[Jim Haynes](#)
- [Risks of GPS Devices that we had Not Previously Heard Of](#)
[Mark Brader](#)
- [Over-reliance on automated real estate valuation](#)
[Jeremy Epstein](#)
- [Re: Control-Z vs. Bourne-Again SHell](#)
[David Chau](#)
- [Re: Weird Clock Issue - a single bit error](#)
[Chris Smith](#)
[Mark Lutton](#)
[Amos Shapir](#)
- [Re: Bruce Schneier on Airport Photo ID Checks](#)
[Andy Piper](#)
[Amos Shapir](#)
- [Re: Risks of better security and "smarter" users](#)
[Dag-Erling Smørgrav](#)
[Ron Garret](#)

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

***Google revives 6-year-old news story, sends United shared down 75%**

<Steven J Klein <steveklein@mac.com>>

Wed, 10 Sep 2008 16:24:28 -0400

An unfortunate series of events:

1. In 2002, UAL (parent company of United Airlines) filed for bankruptcy, an event covered at the time by the Chicago Tribune.
2. The story was in the database of the Sun Sentinel, a Florida newspaper owned by the same company..
3. This last Saturday, lots of people (for reasons unknown) viewed the story on the Sun Sentinel's website.
4. Enough people viewed the story that it appeared in their list of "Popular Stories: Business." That list is automatically generated based on page-views.
5. Google's News crawler saw the link in the "Popular Stories" list. The current date, September 8, 2008, appeared on the web page with the story. The story itself carried no date.
6. Users of Google's "email alert" service who had requested stories mentioning UAL were sent links to the story. Also, anyone searching Google News for "UAL" or "United Airlines" would have seen a link to the story.
7. The UAL story was circulated by Income Securities Advisors Inc., a stock research firm that publishes reports on the Bloomberg L.P., financial-news service.
8. On Monday, September 8, at approximately 10:45AM, a headline from the report flashed across Bloomberg screens.
9. In the next 15 minutes, UAL shares in UAL dropped from almost \$12.50/share to just \$3, before trading was halted. At least one block of 100 shares traded at 1 cent per share, though that trade was later voided.

Eventually UAL put out a press release clarifying that the story was almost 6 years old, and that they were not in bankruptcy. Later that day the stock (mostly) recovered to over \$10/share.

This could be a very clever method of market manipulation. If spammers sent out millions of messages with links to the story, and just a small fraction of recipients clicked the link, the story could easily move to the "popular stories" list. Or perhaps hackers controlling botnets just directed the computers they control to send a request to the server to load the story.

Among the risks I can spot (no doubt I'm missing some):

- A. The story was undated, making it appear current. Possible solution: The automated system that adds stories to the database could include the date the story was added to the database.
- B. The story was automatically spread by lots of systems doing exactly what they're supposed to do.
- C. Neither Income Securities Advisors nor Bloomberg have humans fact-check these automated stories.

The story was widely covered. I learned about it here:

<http://online.wsj.com/article/SB122100794359017593.html>

Steven J Klein, Your Mac & PC Expert (248) YOUR-MAC or (248) 968-7622

Google revives 6-year-old news story, sends United shared down 75%

<Drew Dean <ddean@csl.sri.com>>

Wed, 10 Sep 2008 23:09:56 -0700

There are (at least) two interesting points here:

(1) The current mystery is why this article became "popular" in the first place? How many HTTP requests did that take? Are the User-Agent: headers identical (in which case one should suspect a botnet) or not (which does not rule out a botnet, of course)? How are the IP addresses of requesters distributed? What time interval did the requests arrive in?

(2) What we really have here is a failure of composition: Google didn't see a date on the article, so picked up the date on the web site's front page -- something that the web site author didn't intend to imply the date of content linked to from the front page. Oops. Both parties did a reasonable thing, but the composition turned out to be completely unreasonable.

Google revives 6-year-old news story, sends United shared down 75%

<"Scott Nicol" <scott.nicol@gmail.com>>

Wed, 10 Sep 2008 13:51:55 -0400

Tribune, Bloomberg and Google unite to clobber United

A nice summary of the events, followed by Google's and Tribune's take on what happened.

<http://www.washingtonpost.com/wp-dyn/content/article/2008/09/08/AR2008090803063.html?hpid=moreheadlines>

<http://googlenewsblog.blogspot.com/2008/09/update-on-united-airlines-story.html>

<http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/09-09-2008/0004882072&EDATE=>

✂ How Steve Jobs' obit got published (Philip Elmer-DeWitt's blog)

<Monty Solomon <monty@roscom.com>>

Fri, 29 Aug 2008 13:50:06 -0400

Philip Elmer-DeWitt, How Steve Jobs' obit got published, 28 Aug 2008

The first rule of publishing is that anything that can go wrong, will go wrong. (A corollary favored at *Time Magazine*, where I labored for nearly three decades, is that all copy is guilty until proved otherwise.)

None of this excuses, but it does help explain, how Bloomberg News managed to publish an obituary on Wednesday afternoon of Apple (AAPL) CEO Steve Jobs, who is still quite alive.

Advance work on famous figures' obits is nothing new, and given Jobs' well-publicized brush with pancreatic cancer four years ago and recent concerns about his weight loss, it's understandable that Bloomberg might choose this moment to update its piece on Jobs, although the version that got published contains no details about his health that weren't already in the public record.

According to a Bloomberg spokesperson, however, it was a routine update of the kind regularly performed by the obit department. ...

<http://apple20.blogs.fortune.cnn.com/2008/08/28/how-steve-jobs-obit-got-published/>

[Boomberg or Bustberg? PGN]

✂ Internet Traffic Begins to Bypass the U.S. (John Markoff)

<Monty Solomon <monty@roscom.com>>

Sat, 30 Aug 2008 01:05:33 -0400

[Source: John Markoff, *The New York Times*, 30 Aug 2008]

The era of the American Internet is ending. Invented by American computer scientists during the 1970s, the Internet has been embraced around the globe. During the network's first three decades, most Internet traffic flowed through the United States. In many cases, data sent between two locations within a given country also passed through the United States.

Engineers who help run the Internet said that it would have been impossible for the United States to maintain its hegemony over the long run because of the very nature of the Internet; it has no central point of control.

And now, the balance of power is shifting. Data is increasingly flowing around the United States, which may have intelligence - and conceivably military - consequences. ...

<http://www.nytimes.com/2008/08/30/business/30pipes.html?partner=rssuserland&emc=rss&pagewanted=all>

Global Trail of an Online Crime Ring (Brad Stone)

<Monty Solomon <monty@roscom.com>>

Sun, 31 Aug 2008 10:33:32 -0400

Brad Stone, Global Trail of an Online Crime Ring, *The New York Times*, 12 Aug 2008

As an international ring of thieves plundered the credit card numbers of millions of Americans, investigators struggled to figure out who was orchestrating the crimes in the United States.

When prosecutors unveiled indictments last week, they made a stunning admission: the culprit was, they said, their very own informant.

Albert Gonzalez, 27, appeared to be a reformed hacker. To avoid prison time after being arrested in 2003, he had been helping federal agents identify his former cohorts in the online underworld where credit and debit card numbers are stolen, bought and sold.

But on the sly, federal officials now say, Mr. Gonzalez was connecting with those same cohorts and continuing to ply his trade, using online pseudonyms - including "soupnazi" - that would be his undoing. As they tell it, Mr. Gonzalez had a central role in a loosely organized online crime syndicate that obtained tens of millions of credit and debit card numbers from nine of the biggest retailers in the United States.

The indictments last week of 11 people involved in the group give a remarkably comprehensive picture of how the Internet is enabling new kinds of financial crimes on a vast international scale.

In interviews over the last few days, investigators detailed how they had tracked Mr. Gonzalez and other members of a ring that extended from Ukraine, where a key figure bought and sold stolen numbers over the Internet, to Estonia, where a hacker infiltrated the servers of a Dallas-based restaurant chain.

The criminals stored much of their data on computer servers in Latvia and Ukraine, and purchased blank debit and credit cards from confederates in China, which they imprinted with some of the stolen numbers for use in cash machines, investigators say. ...

<http://www.nytimes.com/2008/08/12/technology/12theft.html?partner=rssuserland&emc=rss&pagewanted=all>

Automated Bill Payments Are a Cinch: Not So Fast (Ron Lieber)

<Monty Solomon <monty@roscom.com>>

Sat, 30 Aug 2008 01:07:15 -0400

[Source: Ron Lieber, YOUR MONEY: Automated Bill Payments Are a Cinch (Not So Fast), *The New York Times*, 30 Aug 2008]

A few months ago, in my first column for this newspaper, I extolled the virtues of automated bill payments: Set them up once, let your utilities, phone and credit card companies pull what you owe from your bank account each month and never sit through the drudgery of a bill-paying session again.

And boy, did you let me have it. I heard from a number of readers who thought I was out of my mind for suggesting that they send money out automatically each month or give billers unfettered access to their credit cards and bank accounts. Horror stories poured in, as well as several specific questions and concerns.

So this week, we'll look at five reasons that people are wary of automating their financial lives this way. But first let's back up and define precisely what we're talking about.

Until the 1990s, most of us were stuck writing a whole bunch of checks each month to pay our various bills. Then came the early Web-based bill payment systems, where we'd go to a bank or biller's Web site and push a few buttons to move money to the right places.

Only more recently, however, has it become possible to pay each bill every month without lifting a finger. There are three basic ways to do this. You can give each biller permission to pull the full amount from your bank account. You can use the online bill system at your bank to push payments out automatically each month. Or you can charge every bill to your credit card and give only that card company permission to pull money from your bank account when the credit card bill is due.

Each of these methods has its potential shortcomings, which will become clear as we march through the hiccups that can occur when automating your payments. ...

<http://www.nytimes.com/2008/08/30/business/yourmoney/30money.html?partner=rssuserland&emc=rss&pagewanted=all>

Hackers prepare supermarket sweep

<Gabe Goldberg <gabe@gabegold.com>>

Fri, 29 Aug 2008 06:26:14 -0400

Self-checkout systems in UK supermarkets are being targeted by hi-tech

criminals with stolen credit card details. A BBC investigation has unearthed a plan hatching online to loot US bank accounts via the checkout systems. Fake credit cards loaded with details from the accounts will be used to get cash or buy high value goods.

The supermarkets targeted said there was little chance the fraudsters would make significant gains with their plan. With the help of computer security experts the BBC found a discussion on a card fraud website in which hi-tech thieves debated the best way to strip money from the US accounts.

<http://news.bbc.co.uk/2/hi/technology/7584258.stm>

✶ Antivirus software in critical systems? (Re: jared, [RISKS-25.29](#))

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>

Wed, 03 Sep 2008 19:00:56 +0200

> [...There should be no need for anti-virus software in a
> well-designed voting system. PGN]

This is exactly a point I have been trying to make in several discussions about critical systems for satellite telemetry and telecommanding:

If you think you need anti-virus software in a (safety) critical system, there is something wrong with your design. Such systems, and many other safety-critical systems, should not contain

- * known vectors for viruses and other malware
- * known targets for such malware

Said differently, any data entering the system should be in a format YOU define, and should have no accommodations for importing executable code. And there should be no software in the system that will attempt to execute any imported files.

So, no e-mail, no web servers or clients, no office packages, etc.

Actually, if the system has to undergo some kind of certification, I wonder whether anti-virus software would be certifiable. Its behavior is, after all, dependent on virus definition files updated regularly, and originating from uncertified sources. Anti-virus scanners do have false positives (I have seen at least one), so they may accidentally flag legitimate data as malicious, and may endanger the proper operation of the system.

The reaction I mostly get is something like : You might be right, but let's keep it just in case... Which means they didn't get the point.

✶ Re: States throw out costly electronic voting machines ([RISKS-25.30](#))

<Peter Houppermans <peter@houppermans.com>>

Fri, 29 Aug 2008 10:56:24 +0200

Hmm, a lack of creativity here, methinks.

Innocent question: no chance of supplying a few to researchers to see if an acceptable alternative can be developed? If a company has the choice between

- a. flogging dead stock
- b. trying to make something acceptable of the remnants (i.e. get at least a return on the junk) by developing a new approach that can be audited, is open and can be proven to be safe (assuming that such is possible)

... wouldn't that be an excellent argument to supply a few systems to researchers for better, open developments? I refuse to accept that such systems are completely useless. Maybe sponsoring of an open, auditable project would be a better investment of government and corporate funds than parking the lot forever or scrapping it, and even the Company Formerly Know As Diebold (we know who you were) could then at least retain some market value.

Or is that a far too sensible idea?

Re: States throw out costly electronic voting machines ([RISKS-25.30](#))

<Jim Haynes <jhhaynes@earthlink.net>>

Fri, 29 Aug 2008 17:05:41 -0500 (CDT)

It seems that what's needed here is for one of these jurisdictions to make some of the machines available to some public-spirited open source people, who could reverse engineer the thing and then write open source software that would make them perform correctly.

Risks of GPS Devices that we had Not Previously Heard Of

<msb@vex.net (Mark Brader)>

Fri, 29 Aug 2008 17:11:42 -0400 (EDT)

The instructions for a certain GPS device are excerpted in the October issue of Consumer Reports:

When you are directed to press a key, you should press and quickly release the key. (You may need to be held down for a period of time to start a secondary function, when the instructions tell you to do so.)

Mark Brader, Toronto, msb@vex.net | "Fast, cheap, good: choose any two."

[If you are held down long enough, you might have been a martyr with your Heldenleben (Heldownleben?). PGN]

#Over-reliance on automated real estate valuation

<Jeremy Epstein <jeremy.j.epstein@gmail.com>>

Sat, 30 Aug 2008 16:55:10 -0400

Background: most of the major lenders in the US are in deep financial trouble, and are trying to reduce their risks. One of the ways they're doing that is to cut back on HELOCs (Home Equity Line of Credit, aka "second mortgages") - telling existing customers that even though they have a loan that says they're allowed to draw against the equity in their house, the homeowner is no longer allowed to draw money out because (the lenders claim) the value of the house is no longer enough to support the loan amount. This is being done in a blanket fashion - hundreds of thousands of people are getting these letters, based on generalized trends, not individual assessments.

My situation is similar to that of hundreds of thousands of other people, but I'm being bitten by the Automated Valuation Method (AVM) used by Homecomings Financial. Basically, they have a secret formula that gives a "value" to a house - and if you disagree with their conclusion, you have to pay for an appraisal to challenge it. In my case, I claim the value of the house is about \$X, they say it's between 39% and 51% of \$X (the most recent sale in my neighborhood was 1.1X, so I'm definitely in the right neighborhood). But because "the answer came from the computer", it's nearly impossible to fight - the ability of the paper-pushers to look beyond the computer has been taken away.

I've recently been listening to some old Isaac Asimov Robot stories, where he talks about "the positronic machines" which make all of the financial decisions, including adjusting production, based on gathering every possible data point and even accounting for human desires to ignore the machines' instructions. At some point, the humans in the story become impossible of operating without the Machines, and no longer even understand how the Machines make their decisions. Dealing with Homecomings makes me think that Asimov's prediction has already come true, at least in some domains!

#Re: Control-Z vs. Bourne-Again SHell (jidanni, [RISKS-25.31](#))

<David Chau <davidchau@figmentsrus.com>>

Thu, 11 Sep 2008 00:10:37 -0400

> \$ sleep 55; launch_rocket
> The problem is if one discovers a missing O-ring etc., then a Control-C
> interrupt will not cancel the whole launch ... Next time use an &&
> operator instead of a ;.

Unfortunately, && doesn't work so well either if one needs to temporarily put the launch on hold, but not abort it altogether:

```
$ sleep 55 && launch_rocket
<Control-Z>
[1]+ Stopped sleep 55
$ fg
... Hey, how come my rocket's still sitting there?
```

✉ Re: Weird Clock Issue - a single bit error ([RISKS-25.30](#))

<Chris Smith <smith@vex.net>>

Mon, 1 Sep 2008 21:02:19 -0400 (Eastern Daylight Time)

Steven Greenwald's radio synced clock error is not so weird once you understand more pieces of the puzzle.

<http://tf.nist.gov/timefreq/stations/wwwbtimecode.htm>

If you check the above site for the time code format used by WWVB, you will get the information you need to figure out the problem.

The time code format uses a "day of the year" system, where days are counted from 1 to 365 during the regular year. August 18th, 2008 (a leap year - days will count to 366) is day 231. September 27th is day 271.

The difference is 40 days, AND both days are in the same "100", and under 80 -- one date is between 00 and 39 and the other is between 40 and 79. Because WWVB uses a BCD representation, such a pattern means that the error corresponds to a single bit error.

Normally, clocks will try some form of validation on the received data to prevent problems like this. They might try to receive several minutes worth of data and see if the results are consistent. If you read the spec carefully, you will see that this is necessary because there are no error detection capabilities in the format.

Although this may seem like an oversight when you are used to internetworking protocols, it's much more common in the industrial design space, where designers may have a final budget of only half a dollar for all of the electronics in such a clock.

It is certainly possible that your location (in Miami, FL - not close to Boulder, CO) and the storm create conditions sufficient to consistently have your clock read wrong by one bit. I expect that by this time, your clock is back to normal.

[Also noted by F. Barry Mulligan. PGN]



Re: Weird Clock Issue (Greenwald [RISKS-25.30](#))

<Mark Lutton <mlutton@acquiremedia.com>>

Fri, 29 Aug 2008 11:25:58 -0400

This happens frequently. The signal is transmitted by extremely-low-frequency radio, and if you are far from the nearest transmitter the signal can be faint or erratic. There is just barely enough bandwidth in the signal to send the time as a series of bits with no error correction and no redundancy. I've seen the wrong time and date on my own atomic clock.

You should use a quartz clock (or a plug-in electric clock if your 60Hz house current is dependable enough) as your primary reference and set it once a day from the atomic clock but only if the time shown on the atomic clock is reasonable. Under no circumstances should any automated process be controlled directly by a radio atomic clock.

Re: Weird Clock Issue (Greenwald, [RISKS-25.30](#))

<Amos Shapir <amos083@hotmail.com>>

Tue, 2 Sep 2008 18:08:23 +0300

This very subject had been discussed in [RISKS-25.08](#); I quote my post (under the subject "Risks of Leap Years and Dumb Digital Watches", <http://catless.ncl.ac.uk/Risks/25.08.html#subj14>), about a similar device by LaCrosse:

(...) It sets itself by listening to a radio time signal, so theoretically it should never have to be set at all, but every now and then it glitches and displays a wrong time, date or year; the difference is always a power of 2 in one of the digits, which looks like it's getting the data in some sort of BCD format, without any checksum or sanity check (which is not news on RISKS). I wonder how many critical installations are using the same chip.

[What goes around comes around. That seems to be particularly true of nondigital clocks -- although not always correctly. PGN]

Re: Bruce Schneier on Airport Photo ID Checks ([RISKS-25.30](#))

<Andy Piper <andy@xemacs.org>>

Mon, 01 Sep 2008 13:53:40 +0100

The method described for subverting online checkin procedures must be airport / carrier / destination dependent to a certain extent. I usually checkin online and the printed boarding pass invariably carries a barcode that is scanned at security. A quick peek at the screen appears to show my checkin information, so only a very lax official would miss differing

names. This happens at least at SFO and LHR.

[This is apparently a checkin-and-the-egg problem. I don't want to egg Andy on, but the boarding pass is usually scanned by the airline folks as you board the plane, not by security. The TSA security folks merely check that the name on the ID matches the name on the boarding pass. And that is the vulnerability that Bruce notes. Perhaps a computer program might later note a name mismatch when/if the name is linked by the airline to the barcode for the actual flight manifest, but the airline employee typically does not do this match -- not even at SFO. They typically just scan the barcode and reach for the next boarding pass to keep people moving. PGN]

Re: Bruce Schneier on Airport Photo ID Checks ([RISKS-25.30](#))

<Amos Shapir <amos083@hotmail.com>>
Sun, 31 Aug 2008 17:41:20 +0300

The newly formed U.S. TSA has a serious problem: they have to supply Security, but they have no idea how (and it seems that they are unaware that nobody else does, either). But they do know that Security causes Harassment, and they do know how to do Harassment. So the obvious logic is, the more Harassment they'd do, the more Security will be produced. QED

Re: Risks of better security and "smarter" users (Garret, [RISKS-25.30](#))

<=?utf-8?Q?Dag-Erling_Sm=C3=B8rgrav?=<des@des.no>>
Thu, 11 Sep 2008 09:48:42 +0200

Ron Garret <ron@flownet.com> writes:

- > 1. The web site used a secure authentication scheme that behaves almost
- > identically to a less secure scheme
- >
- > 2. I am familiar with the more common design of secure sites [...]

Are you? Then surely, you're aware that the common form-based login method *also* sends your password in the clear? The HTTP "digest" method is the only purely HTTP / HTML authentication method that doesn't.

I assume that you are also aware that this is all moot if the web site makes proper use of SSL.

Re: Risks of better security and "smarter" users (Dag-Erling)

<Ron Garret <ron@flownet.com>>
Thu, 11 Sep 2008 08:47:23 -0700

> Are you? Then surely, you're aware that the common form-based login
> method *also* sends your password in the clear?

Yes. That is why sites use HTTPS, and users are trained to look for little
padlock icons.

> The HTTP "digest" method is the only purely HTTP / HTML authentication
> method that doesn't.

Yes. Notwithstanding, it is hardly ever used, and I think my experience may
be one reason why.

> I assume that you are also aware that this is all moot if the web site
> makes proper use of SSL.

That depends on your definition of "proper use."

But yes, I am aware of all this, and I assumed that the article's readers
would be as well, so I left out some details in the interest of parsimony.
Perhaps I should not have.

The user experience that surprised me was the following:

1. Restart my browser. Clear the cookie cache.
2. Go to the web site in question. Navigate to the page with the LOGIN
link. This page was not secure.
3. Click on the LOGIN link, expecting to be taken to a secure page with a
form to enter my credentials. I wasn't. Instead I was taken directly to my
account information. This page was secure, but since I was not aware that
my browser was silently accessing my keychain it appeared that I had just
logged in without providing any credentials. The fact that the process
started on an insecure page and ended on a secure one didn't seem relevant.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 33

Monday 15 September 2008

Contents

- [Antivirus software in critical systems?](#)
[Rob Diamond](#)
[Robert P Schaefer](#)
[PGN](#)
- [Re: States throw out costly electronic voting machines](#)
[Patrick J Kobly](#)
- [Re: FAA redundancy -- or lack thereof](#)
[Mike Martin](#)
- [Misleading headline: 'Big bang' experiment is hacked](#)
[Gabe Goldberg](#)
- [Change name, get off no-fly list](#)
[David Magda](#)
- [Re: Amos Shapir on Airport Photo ID Checks](#)
[Danny Lawrence](#)
- [iPhone Takes Screenshots of Everything You Do](#)
[Brian X. Chen via Monty Solomon](#)
- [Re: UAL, Automated trading gets spoofed!](#)
[Howard Israel](#)
- [San Francisco officials looking for hidden network device](#)
[Gabe Goldberg](#)
- [PayPal phishes their own customers](#)
[Andrew Pam](#)
- [Re: Risks of better security ...](#)
[Chris Adams](#)
[Ron Garret on David Bliss](#)
- [Re: Control-Z vs. Bourne-Again SHell](#)
[Philippe Pouliquen](#)
- [Re: Weird Clock Issue -- a single bit error](#)
[David Magda](#)
- [Re: Risks of GPS Devices ...](#)
[Sergei Patchkovski](#)
- [Re: Automated Bill Payments Are a Cinch: Not So Fast](#)
[CBFalconer](#)
[Sten Carlsen](#)
[Erling Kristiansen](#)

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

Antivirus software in critical systems? (Re: jared, [RISKS-25.29](#))

<Rob Diamond <robd@spin.net.au>>

Mon, 15 Sep 2008 23:14:28 +1000

I've worked in real-time (SCADA) software and related areas for years. More and more vendors are using Windoze, for the client UI machines and often for the servers as well (when *will* they learn ?). Last year I saw a Denial of Service attack on some client machines by the anti-virus and configuration management/license checking software. The user might be in the middle of dispatching a tech. to a job when the anti-virus software would start up -- the client machine would (almost completely) freeze for several minutes, until the anti-virus or conf. management software had finished running. It's incredible that the anti-virus software vendors have no idea about co-operative multi-tasking -- their software grabs the disk by the short hairs and gets its almost undivided attention until it's finished -- while the shortcomings of the OS task and I/O scheduler are pretty obvious.

Even funnier (you have to laugh or you'd cry) was the initial attitude of the IT outsourcer -- "What's the problem ? *Our* job is to protect the machines we supply from viruses and manage the software configuration and OS updates -- and that's what we're doing. If the machines are a bit busy for a while that's the user's problem. Or buy a more powerful machine." Eventually the problem was reduced, but not completely eliminated, by reducing run frequency and cutting back on the checks carried out.

Since this was a public utility with over a million customers the risks of not being able to dispatch a (possibly safety-critical) job while anti-virus software runs are pretty obvious.

Rob D. <robd@spin.net.au> +61-412-607-361

Antivirus software in critical systems? (Re: jared/pgn, [R-25.29](#))

<"Schaefer, Robert P \ (US SSA)" <robert.p.schaefer@baesystems.com>>

Mon, 15 Sep 2008 11:07:07 -0400

Virus installation is not needed for the use of the application, but it is needed for the development of the application.

What may be going on is the way systems are developed today which perhaps was not so true 10 years ago. Many critical systems and embedded systems are Windows based, you can get Windows on a single card computer, or an industrial PC, etc. The principal driver is familiarity and cost. For software development, the critical system is connected to the corporate LAN and the Internet, for many reasons, particularly file sharing, corporate configuration management. Access to the Internet allows access to vendor's device drivers, documentation and to register third party code. You can

even test the system on the LAN from your corporate desktop, once you've walked over to the lab to flip the power-on switch. (All sorts of risks internal to the corporation here with visible IP addresses providing access to embedded and shared devices.)

Corporate policy for responsible corporations is, if your computer is on the LAN or the Internet, then Virus protection must be installed, no ifs, ands, or buts. The sneaker-net still exists where LAN access is not available for embedded systems in the corporate world, but today the memory device is the thumb-drive and no longer the floppy disk.

✶ Antivirus software in critical systems? (Re: Schaefer, [R-25.33](#))

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

There is usually a huge gap between theory and practice. It clearly dominates this discussion.

In principle, voting systems and other critical systems should not be developed on untrustworthy operating systems with unreliable development tools and flawed software engineering.

Even more important, election systems should not have to rely on easily compromisable operating systems -- especially when there is essentially no accountability, poor configuration control, poor documentation, and perhaps even some Internet access for distributing results or even for voting, as well as unaudited devices for special user needs or for real-time operational maintenance.

Anyone with access to such an OS can completely compromise elections -- in the development process, in configuration and set-up, and in execution. More than anything else, we need trustworthy operating systems and trustworthy application software with thorough accountability. But that is still nowhere near enough, considering all of the extrinsic problems in registration, voter authentication, and so on.

Similar concepts should apply to critical infrastructure systems -- many of which somewhat surprisingly have live direct or indirect Internet connections. By contrast, consider gambling systems -- which are held to an enormously higher standard.

Antivirus software should be unnecessary by construction of those systems. HOWEVER, in practice, Robert implies, well, that's impossible because that's just the way it is. That is a terrible state of affairs.

✶ Re: States throw out costly electronic voting machines ([RISKS-25.30](#))

<Patrick J Kobly <patrick@kobly.com>>
Thu, 11 Sep 2008 20:02:35 -0600

One of the frustrating things about this discussion has always been how few people who comment on the subject are actually aware of the history.

I would suggest that anybody who thinks that open source will be able to provide the solution to the disaster that is eVoting read about why Jason Kitcat shut down the GNU.FREE (Free Referenda & Elections Electronically) project in 2002.

http://www.free-project.org/files/free_software_odyssey.pdf

As an aside, the suggestion that jurisdictions ought to provide existing equipment to researchers is a non-starter. Contractual (and legislative) restrictions on the jurisdictions exclude them from providing access to this equipment.

Patrick Kobly, 56 388 Sandarac Dr NW, Calgary, Alberta T3K 4E3
<http://www.kobly.com> 1-403-274-9033

[The contractual restrictions may get changed sooner than you think, at least in certain states. PGN]

Re: FAA redundancy -- or lack thereof (PGN, [RISKS-25.31](#))

<"mike martin" <mke.martn@gmail.com>>
Sun, 14 Sep 2008 09:35:11 +1000

The outage on 26 August in the FAA Flight Planning System was more likely due to a design deficiency than, as reports claimed, lack of capacity or redundancy.

I struck a similar issue some years ago with a real-time system that drove a large number of NCR automatic teller machines. The machines were capable of processing withdrawal transactions while off-line to the central computer, a measure intended to provide a degree of customer service in the event of central computer or communication link failure.

As first implemented, if the central computer went down for any length of time it was virtually impossible to bring it back up again. Every time we tried it would collapse under the onslaught of accumulated off-line transactions in the ATMs that were waiting to be posted.

The subsequent report from Gabe Goldberg suggests that something similar happened with the FAA system. He quotes FAA spokesman Paul Takemoto:

"Basically, all the flight plans that were in the system were kicked out," Takemoto said... The system switched to the FAA's backup flight planning computer in Salt Lake City, which was quickly overwhelmed by airlines trying in vain to enter flight plans. "They just kept hitting the 'Enter' button. So the queues immediately became huge," Takemoto said. "On top of that, it happened right during a peak time as traffic was building. Salt Lake City

just couldn't keep up." The Georgia computer was fixed in two-and-a-half hours but it wasn't until the FAA asked airlines to stop filing flight plans that the backlogs started to clear.

Yes, you could build in sufficient capacity and redundancy to handle the anomalous peak. Or you could do what we did with the ATM system, and sequence the start-up so that communication links were brought online progressively, presenting a load that remained within maximum processing capacity.

Presumably the next generation flight planning system will be design to fail-over seamlessly, thus avoiding an accumulation of backlog transactions. Then this problem will never happen again -- until it does.

Misleading headline: 'Big bang' experiment is hacked

*<Gabe Goldberg <gabe@gabegold.com>>
Mon, 15 Sep 2008 11:25:53 -0400*

After hackers inserted a message onto the CERN website, a spokesman for CERN (which houses the Large Hadron Collider, LHC) said that "The computer is used to monitor one of the experiments at the LHC, it's nothing to do with the LHC accelerator itself or any of the control systems."

<http://news.bbc.co.uk/2/hi/technology/7616622.stm>

So the collider wasn't hacked. But was the Web site hacked or was an experiment control system hacked? Unless they're experimenting with Web servers, those are different...

[Well, the monitoring system is only a Collide-O-Scope, so perhaps what you see is only an apparition anyway?]

Change name, get off no-fly list

*<David Magda <dmagda@ee.ryerson.ca>>
Fri, 12 Sep 2008 09:19:48 -0400*

And this illustrates just how completely useless no-fly lists are:

The U.S. Department of Homeland Security wrote a letter to Labbé in 2004, saying he had been placed on their watch list after falling victim to identity theft. At the time, the department said there was no way for his name to be removed.

Although Labbé wrote letters to the U.S. department, his efforts were in vain, prompting him to legally change his name. "So now, my official name is François Mario Labbé," he said.

"Then you have to change everything: driver's license, social insurance,

medicare, credit card--everything."

Although it's not a big change from Mario Labbé, he said it's been enough to foil the U.S. customs computers.

<http://www.cbc.ca/canada/montreal/story/2008/09/11/nofly-name.html>

<http://www.boingboing.net/2008/09/12/canadian-man-changes.html>

Re: Amos Shapir on Airport Photo ID Checks (RISKS-25.32)

<"Danny Lawrence" <dantemann@gmail.com>>

Mon, 15 Sep 2008 10:08:26 -0400

> The newly formed U.S. TSA has a serious problem: they have to supply
> Security, but they have no idea how (and it seems that they are unaware
> that nobody else does, either). But they do know that Security causes
> Harassment, and they do know how to do Harassment. So the obvious logic
> is, the more Harassment they'd do, the more Security will be produced. QED

Another problem is the blind reliance on "The Rules" without understanding why "The Rules" are there and what they are supposed to prevent. Case in point, a woman with pierced nipples tries to board a plane, and sets off the metal detector. The TSA screeners insist that she must pass through the metal detector without setting it off, instead of noting the nipple rings and realizing that they aren't a threat.

Admittedly in this case the TSA admitted that its "procedures were faulty", but didn't seem to think that the screeners did any thing wrong.

<http://cbs2.com/local/nipples.piercings.rings.2.686169.html>

[The rules can also be questioned, For example, confiscating a toothpaste tube that is 90% empty because the label says 5 ounces seems rather silly. But I suppose rules of that kind are intended to prevent screeners from using any intelligence. PGN]

iPhone Takes Screenshots of Everything You Do (Brian X. Chen)

<Monty Solomon <monty@roscom.com>>

Sat, 13 Sep 2008 22:03:37 -0400

iPhone Takes Screenshots of Everything You Do
By Brian X. Chen September 11, 2008 | 1:26:34 PM

Your iPhone is watching you.

If you've got an iPhone, pretty much everything you have done on your handset has been temporarily stored as a screenshot that hackers or forensics experts could eventually recover, according to a renowned

iPhone hacker who exposed the security flaw in a webcast Thursday. ...

<http://blog.wired.com/gadgets/2008/09/hacker-says-sec.html>

Re: UAL, Automated trading gets spoofed! (Re: [RISKS-25.32](#))

<Howard Israel>

Mon, 15 Sep 2008 10:47:15 -0400

"As Tribune Co. and Google Inc. pointed fingers at each other over the glitch that cratered UAL's stock [on 8 Sep 2008,] blame spread to the computers that robotically troll the Web for news stories and execute stock trades automatically." [Source: Shira Ovide and Jessica E. Vascellaro, UAL Story Blame Is Placed on Computer, *The Wall Street Journal*, 10 Sep 2008; PGN-ed]

http://online.wsj.com/article/SB122100794359017593.html?mod=3Dhpp_us_whats_news

San Francisco officials looking for hidden network device

<Gabe Goldberg <gabe@gabegold.com>>

Fri, 12 Sep 2008 15:09:45 -0400

As Deep Throat (Woodstein's, not the movie star) almost said, "Follow the packets..."

San Francisco officials are trying to find a device on the city's computer network that was allegedly left there by an IT worker who was jailed for refusing to divulge passwords to the city network, the IDG News Service reported on Thursday.

San Francisco network administrator Terry Childs was arrested in July on four felony charges of taking control of the city's computer network and locking administrators out. He remains in jail on \$5 million bail despite giving up the passwords to the mayor in a secret jail cell meeting a week later.

The device, which appears to be a router providing remote access to the city's fiber Wide Area Network, was discovered on August 28, the report says.

However, officials didn't know where the device was located and didn't have the user name and password to access it. When they tried to log in, a message was displayed that said the system was the "personal property of Terry S. Childs," according to a screenshot officials filed with the court.

http://news.cnet.com/8301-1009_3-10039650-83.html

[Earlier items on this case in [RISKS-25.24-25](#)). PGN]

✂ PayPal phishes their own customers

<Andrew Pam <xanni@glasswings.com.au>>

Mon, 15 Sep 2008 12:25:35 +0930

... Your monthly account statement is available anytime; just log in to your account at <https://SECURE.UNINITIALIZED.REAL.ERROR.COM/au/HISTORY>. To correct any errors, please contact us through our Help Centre at <https://SECURE.UNINITIALIZED.REAL.ERROR.COM/au/HELP>.

The error.com domain does not belong to PayPal.

Andrew Pam Serious Cybernetics <http://www.sericyb.com.au/>

✂ Re: Risks of better security ... (Garret, [RISKS-25.32](#))

<Chris Adams <chris@improbable.org>>

Thu, 11 Sep 2008 19:21:39 -0400

> The fact that the process started on an insecure page and ended on a
> secure one didn't seem relevant.

I'm a bit surprised that this is considered risks-worthy: this is how web security should work. It allowed a legitimate user access to a network resource without distracting away from the actual task they wanted to perform. It didn't provide a password which had not previously been sent to the remote server, would not have blindly continued had the x509 checks not passed, etc.

The drawback appears to be that Ron's Keychain didn't have one of the extra confirmation options enabled. Password managers have various permutations on this theme but with the exception of locking when the system is suspended to disk they're largely false security: if someone untrusted gets physical access to your computer they might not be able to login to etrade immediately but they can still trivially install malware, a physical keyboard sniffer, etc.

Usability is a security feature and I think this is the right balance: more prompts would lead many users to either disable them entirely or blindly hit okay, even when they get the one legitimate warning in the flood of false-positives. The major security improvement I'd make would be adding a password generator into the browser to make the use of site-specific passwords even easier.

✂ Re: Risks of better security ... (Garret, [RISKS-25.32](#))

<Ron Garret <ron@flownet.com>>

Thu, 11 Sep 2008 14:57:49 -0700

[In response to a message from David Bliss <david@dbsi.org>, interstitiated here to simplify reading. PGN]

>> I find myself at a loss to suggest how this particular risk might have
>> been avoided.

> Really? How about "prohibit the provision of features to 'remember'
> passwords, the entire point of which being to verify the identity of
> *people*, not *software*"?

Prohibit? How?

> Or at the very least refuse to use such features. I do.

This "feature" is enabled by default on OS X. I was not aware of its existence until this incident. As soon as I figured out what had happened I disabled it (which was in itself a non-trivial exercise).

> I don't think the web designers are the ones guilty of idiocy.

Indeed not. I never meant to imply that they were.

> (yes, yes, I know you thought you understood how that "feature" worked and
> thought it would prompt you for a different password before helping
> itself. Surely someone of your experience should know better than to have
> any faith in any software, ever?)

Please read:

<http://cm.bell-labs.com/who/ken/trust.html>

and then explain to me how you propose to get along in today's world without some faith in some software sometimes.

✉ Re: Control-Z vs. Bourne-Again SHell (jidanni/chau, [RISKS-25.31-32](#))

<Philippe Pouliquen <philippe@alpha.ece.jhu.edu>>

Fri, 12 Sep 2008 08:44:56 -0400 (EDT)

jidanni@jidanni.org wrote that

\$ sleep 55; launch_rocket
causes the "launch_rocket" application to run immediately if Ctrl-C is used during the sleep period, and that replacing the "," with "&&" cures the problem.

However, David Chau replied that the "&&" has its own problem with respect to stopping the sleep command (if the intent is to temporarily halt the count-down sequence).

It seems to me that this problem can be solved by putting the two commands

into a shell script, so that the Ctrl-C or the Ctrl-Z applies to the script as a whole, not the individual commands.

This can also be performed on the command-line with:

```
$ ( sleep 55 ; launch_rocket )
```

The caveat is that I only tested this on a FreeBSD and on a Linux system, and that job-control may be somewhat operating-system dependent...

To go a little further, I use the following script for playing music (I have stripped out the code comments in the interest of brevity):

```
for song in *.mp3
do
  /usr/local/bin/mpg123 "${song}" &
  trap "kill $! ; sleep 1" SIGQUIT
  wait
done
```

With the above code, Ctrl-C stops playback completely, Ctrl-Z pauses playback (fg resumes) and Ctrl-\ (SIGQUIT on FreeBSD) skips to the next song. Note that the "sleep 1" after the kill is a hack to allow the sound card buffer to drain, otherwise the next mpg123 may abort if the sound resources appear to be already in use.

[Similar comment noted by Michael Loftis. PGN]

✶ Re: Weird Clock Issue -- a single bit error (Greenwald, [RISKS-25.32](#))

*<David Magda <dmagda@ee.ryerson.ca>>
Sat, 13 Sep 2008 11:40:19 -0400*

> I have a battery operated clock that syncs via radio signal reception with
> the atomic clock in Boulder ... It currently shows the correct time (as
> of writing: 9:05 PM EDT) but shows the date as Saturday September 27th
> 2008 instead of the correct date of Monday August 18, 2008!

If you want to know the time, use a clock:

<http://www.radiocontrolledclock.com/radconwalclo1.html>

If you want to know the date, use a calendar:

<http://www.calendars.com/>

Which day it is only changes once a day, so you only have to check in the morning and not have to worry about it changing until midnight. :) Ditto for day of the week.

[Well, a caveat is needed. The date changes somewhere on the planet every hour (and in some places on the half-hour). PGN]

Re: Risks of GPS Devices ... (Brader, [RISKS-25.32](#))

<"Sergei Patchkovski" <serguei.patchkovskii@sympatico.ca>>
Fri, 12 Sep 2008 17:24:03 +0000

- > When you are directed to press a key, you should press and quickly
- > release the key. (You may need to [hold it] down for a period of time
- > to start a secondary function, when the instructions tell you to do so.)
[Bracketed PGN correction to simplify the discussion.]

Given the right circumstances, this may be the right design choice to make, odd as it sounds. A similar approach is often taken on wrist-mounted dive computers -- a short press of a button would activate a more common function -- such as switching between the current and maximum depth display, or advancing to the next page of the dive log. A two-second sustained push would activate a less common function -- such as setting the oxygen content or the surface altitude.

The rationale is simple -- making an externally-protruding push button waterproof is not easy, especially if they have to operate at a few bar external pressure in a salt-water environment. Having too many of those buttons may significantly increase the chances the device will leak and ruin your dive (or worse).

Re: Automated Bill Payments Are a Cinch: Not So Fast ([RISKS-25.32](#))

<CBFalconer <cbfalconer@yahoo.com>>
Thu, 11 Sep 2008 20:36:24 -0400

I have a simpler, and, I believe, safer system. My bank (and others) allow you to set up delayed payments from your account, or regular at stated intervals. These create checks from me to an organization, identified with my account number, etc. This handles everything without any fuss, except the telephone, which doesn't allow you to set up a constant monthly payment. The other outlays go on one of two credit cards. So, each month, I only need to set payments to the credit cards and the phone co. I pay the credit cards off entirely, so they don't have any interest involved.

Re: Automated Bill Payments Are a Cinch: Not So Fast ([RISKS-25.32](#))

<Sten Carlsen <sten@s-carlsen.dk>>
Sat, 13 Sep 2008 13:40:26 +0200

In Denmark the normal function of this system is different:

After the setup of this agreement:

Every month the bank will send you (paper or electronic form) a list of payments that have been reported by those covered by the agreement and will be due during the next month.

When this is received you have about 10 days to protest any payment to the bank; if you do, the payment will not be made and you have to settle the matter with the other party by other means.

In my case the agreement with the bank is such that if the bank makes an error, the bank will pay to correct it, if I make the error, I have to take the consequences. Seems reasonable to me.

Example: you have an account with your hairdresser (usually not big amounts), one month he has reported to your bank that he wants 20,000.00\$ from you. If you sleep and do not read your statement, he will be paid; if you notice that this is wrong and ask the bank to stop the payment, he is not paid but you will have to go down there and ask him what ... he is thinking.

This is a simplified version, there are of course more details to it than this but this is how it works. This has been available from before online banking was even possible in roughly the same shape.

The risks of this are not so big specially compared with who takes the penalty if errors occur. We very rarely hear that this goes wrong.

✶ Re: Automated Bill Payments Are a Cinch: Not So Fast ([RISKS-25.32](#))

*<Erling Kristiansen <erling.kristiansen@xs4all.nl>>
Sat, 13 Sep 2008 19:18:10 +0200*

An automatic payment scheme like the one described has been in operation in The Netherlands for many year, to almost everybody's satisfaction. There was some reluctance in the beginning, but it subsided rather quickly.

I think the key to success is that you have one month to ask your bank to undo the transaction, no questions asked. You need not give a reason, you need not prove that anybody made a mistake. You may, of course, have to fight it out later with the company that charged you, if they think you owe them money. You can file the cancel request through on-line banking, or go to your bank branch.

I barely hear about any mishaps or incidents with the scheme. If people know that transactions can be reversed, the incentive for wrong-doing is greatly reduced.

An additional advantage is that you avoid the mistakes you might make if you do the transfer yourself. I recently typed the wrong account number on a rather large transfer. The bank said they could not reverse the transaction, and I had to rely on the good will of the erroneous recipient. To my great relief, he returned the money promptly.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 34

Sunday 21 September 2008

Contents

- [SciAm article on Smart Grid](#)
[William P.N. Smith](#)
 - [Wall Street; where nothing can go wrong wrogn wrgn0....](#)
[David Leshner](#)
 - [Mortgage loan crisis due to wishful thinking, Garbage In Garbage Out](#)
[Geo Swan](#)
 - [BNY Mellon data breach now at 200K in Mass, 12M in U.S.](#)
[Monty Solomon](#)
 - [Risks of financial systems too complex to understand](#)
[Daniel P. B. Smith](#)
 - [Risks of not using check digits in bank account numbers](#)
[Toby Douglass](#)
 - [Risks of banking in Holland](#)
[Toby Douglass](#)
 - [Re: PayPal phishes their own customers](#)
[Sidney Markowitz](#)
 - [Re: Automated Bill Payments Are a Cinch: Not So Fast](#)
[Huge](#)
 - [Capability creep strikes again](#)
[Jay R. Ashworth](#)
 - [Expiration of cryptographic certificate killed airline ticket](#)
[Kenji Rikitake](#)
 - [Antivirus software in critical systems?](#)
[Martyn Thomas](#)
 - [Re: Antivirus software in critical systems? Aurora!](#)
[Al Mac Wheel](#)
 - [Re: Control-Z vs. Bourne-Again SHell](#)
[jidanni](#)
 - [Re: Risks of GPS Devices ...](#)
[Richard Grady](#)
 - [USENIX Annual Tech '09 Call For Papers](#)
[Lionel Garth Jones](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ SciAm article on Smart Grid

<"William P.N. Smith" <w_smith@compusmiths.com>>

Fri, 19 Sep 2008 09:17:15 -0400

I was just reading a great article on the need for a Smart electric Grid at <http://www.sciam.com/article.cfm?id=preventing-blackouts-power-grid> but found myself hoping that the people designing it are Risks readers.

Running the grid on a fly-by-wire system, and getting better efficiencies out of it by running it closer to the edge of stability are pretty scary concepts for long-time Risks readers. The thought of replacing every device (switch, circuit breaker, etc.) with a computerized version makes my brain want to explode.

Not that it _can't_ be done, any more than the ATC system can't be upgraded, but exhortations to do so make me want to ensure I'm current on my generator maintenance.

✂ Wall Street; where nothing can go wrong wrogn wrgno....

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

Thu, 18 Sep 2008 18:06:10 -0400 (EDT)

Saul Hansell's blog, How Wall Street Lied to Its Computers, 18 Sep 2008, <http://bits.blogs.nytimes.com/2008/09/18/how-wall-streets-quants-lied-to-their-computers/?pagemode=print>

I called some old timers in the risk-management world to see what went wrong. I fully expected them to tell me that the problem was that the alarms were blaring and red lights were flashing on the risk machines and greedy Wall Street bosses ignored the warnings to keep the profits flowing.

But she and others say there is more to it: The people who ran the financial firms chose to program their risk-management systems with overly optimistic assumptions and to feed them oversimplified data. This kept them from sounding the alarm early enough.

a) In other words, "Tell ourselves what we want to hear..."

b) Quis custodiet ipsos custodes

✂ Mortgage loan crisis due to wishful thinking, Garbage In Garbage Out

<Geo Swan <gswan@globalserve.net>>

Fri, 19 Sep 2008 10:14:04 -0700

Saul Hansell, writing his *The New York Times* blog on 18 Sep 2008, offered a detailed account of how the mortgage loans crisis was due to wishful

thinking in the entry of data to the automated tools bankers now count on to warn them of risky loans.

While the principle of "Garbage In, Garbage Out" is old news to RISKS readers, I thought this article was a useful reminder that the risks of GIGO still has not penetrated to the general public.

<http://bits.blogs.nytimes.com/2008/09/18/how-wall-streets-quants-lied-to-their-computers/?em>

✂️ BNY Mellon data breach now at 200K in Mass, 12M in U.S. (Re: [R-25.31](#))

<Monty Solomon <monty@roscom.com>>

Sat, 20 Sep 2008 09:55:18 -0400

Continuing the saga re: BNY Mellon noted in [RISKS-25.31](#), earlier reports indicated that perhaps 200,000 Massachusetts consumers and 4.5M people nationwide may have been affected. The corrected numbers now exceed 400,000, in Massachusetts and 12,000,000 nationwide according to the NY state Attorney General Martha Coakley. [Source: Jonnelle Marte, Bank's data loss may hit 400,000 Mass. customers, *The Boston Globe* online, 19 Sep 2008; PGN-ed]

http://www.boston.com/business/articles/2008/09/19/banks_data_loss_may_hit_400000_mass_customers/

✂️ Risks of financial systems too complex to understand

<"Daniel P. B. Smith" <usenet2006@dpbsmith.com>>

Wed, 17 Sep 2008 10:16:09 -0400

The Boston Globe, 17 Sep 2008:

"_Bottom to crisis nowhere in sight_. The root of the panic on Wall Street is that investors have lost \$350 billion from their securities backed by subprime mortgages. But on top of that, Wall Street holds tens of trillions in other arcane securities that were based on these mortgages. These mortgage securities are so complex that it's hard to calculate the value of these investments because owners do not clearly disclose their holdings. As a result, analysts and economists can't grasp how widespread the problem is... [A professor said] 'You know there are securities linked to the value of mortgages. You don't know how much those securities are worth...' Any attempts to gauge the size of these markets are 'an estimated guess,' said [an analyst]. 'When you zero in on the number, we don't know what the real risk is in there. It could be small or large. We just don't know,' he said. 'It's breathtaking.' [An economist said] 'it's hard to figure out who owes what to whom, and when that becomes a problem, markets don't function properly.'"

"Wall Street firms... packaged mortgages together in pools, issued securities backed by the pools, and then sold them to investors. In addition, they created and traded complex securities known as 'credit

default swaps...' The insurance contracts form an unseen but tangled web of connections linking AIG and Wall Street investment banks to hedge funds and even countries that invested in them. They are also one item in a smorgasbord of similar contracts - many of them based on corporate debt, credit cards, automobile loans, and commercial property loans - that is an unfathomable \$63 trillion."

Plenty of blame to go around, but where do computers come in?

Data processing made it possible to manage mutual funds with more than a few dozen stocks in them, like the first S&P index fund. Computer networking made it possible to interconnect financial products from different companies and create multilevel financial products, like Fidelity's Dynamic Strategies Fund. This "fund of funds" invests, not in stocks, but in other mutual funds and ETFs... _over a hundred of them_.

What would happen if you asked Fidelity for an inventory of the certificate numbers of all of the stocks in that fund?

Computer technology made it possible to build multilevel pyramids of financial products. These products contain many so investments, all many steps removed from the product's owner, that the owner cannot possibly have an intuitive grasp of them, or make any kind of reality check on their risk. They are so distant from the actual investments that underlie them that last November a federal judge in Ohio dismissed 14 foreclosure cases brought on behalf of mortgage investors, because the investors were unable to prove they actually owned the properties.

I once considered driving out to take a look at one of the commercial properties whose address was listed in the TIAA Real Estate Fund's quarterly report, just to see whether it was really there. I doubt that such a thing has even crossed the mind of the people who trade credit default swaps.

It might turn out that, without anyone really noticing, the global financial system has gradually turned into something that is mostly a MMORPG.

✂ Risks of not using check digits in bank account numbers

*<"Toby Douglass" <trd@45mercystreet.com>>
Tue, 16 Sep 2008 11:10:40 +0200 (CEST)*

Re: Automated Bill Payments Are a Cinch: Not So Fast, Erling Kristiansen
([RISKS-25.32](#))

It should be statistically practically impossible to accidentally enter a valid account number. If account numbers have no check digits, the bank has made a fundamental design error.

I have been living in Amsterdam now for four months (previously I lived in the UK). In the UK, my banks accounts are described by an eight digit account number and a six digit sort code (I believe this is true for all UK

banks). There are no check digits, but the account number must match the sort code, which provides a useful validation. In Holland, an account with ABN AMRO is described by a single nine digit number. There are no check digits. If you enter the wrong number, the bank will accept it, since it cannot detect your mistake.

Risks of banking in Holland

<"Toby Douglass" <trd@45mercystreet.com>>

Tue, 16 Sep 2008 12:03:47 +0200 (CEST)

Four months ago, I emigrated from Cambridge, England to Amsterdam, Holland.

Emigration requires at the destination the resumption of the organised necessities of life - such as, for example, a bank account.

There are three main banks in Holland - ABN AMRO, Postbank and Rabobank. (My commiserations to any banking entity not making my list).

On the basis of an almost nonexistent set of reviews for these banks and their services, I chose ABN AMRO.

Fast-forward nearly four months to this most recent weekend.

I unfortunately suffer from a hopefully transient neurological deficit which means my working memory is seriously impaired. (Something that happens naturally, it seems to me, to people as they move toward the slower realms of advancing age, so I think I am not alone in this deficit.)

As such, I forgot my Dutch PIN.

I wanted to phone ABN AMRO, to ask them to change my PIN. Unfortunately, where the rental market in Amsterdam is nonexistent (State intervention in the market has eliminated the market), I have not yet settled into a place of my own and so do not have a fixed land line - only a Dutch SIM mobile.

ABN AMRO offer two customer service numbers; one for use inside Holland, one for use internationally. The internal number cannot be called from my mobile. I do not know why. The international number detects you are calling from Holland and after a short, polite, Eddiesque message - "you're calling from Holland! I have to disconnect you immediately! share and enjoy!" *click* - and so I cannot phone the bank.

This is of course a risk; don't needlessly eliminate redundancy in your systems.

So, I have to travel, physically, to a branch. Fortunately, I'm young and healthy in body and traveling is not an issue.

I arrive at the bank -- on Saturday, naturally, since I do not wish to take a day off work just to visit.

I queue for a while. Dutch banks like that. I'm eventually approached by a Rutger Hauer look-a-like. I ask to change my PIN.

"Oh no, no...you're thinking you can change your PIN? no."

"I can't change my PIN? but then how do I make my card work again?"

"All we can do is issue you a new card. It takes three days. There's a charge."

I note in the UK, card issuing is free and you can change your PIN over the phone. Perhaps if card issuing here was free, you would also miraculously suddenly be able to change your PIN.

"Well, I need some money now - I don't have any cash on me and I need to do shopping and I can't use my card."

"Oh no, no...you're thinking you can withdraw money? no."

"I can't withdraw MONEY?!?"

"Not on the weekend. You have to come during the week. To this branch or one of two others in Amsterdam. No other branches provide money. And no branches provide money on the weekend."

(At this point, Rutger was looking at me as if I was slightly insane. Clearly, I had picked up in the UK some dangerous Anglo-Saxon notions of banking service, along the lines of being able to withdraw my money from my account).

"Look, I need to pay my rent. Can I transfer some money?"

"Oh no, no...you're thinking you can transfer money? no."

"I can't transfer money!?"

"No. You can only transfer money on-line and you must have your card and PIN. Also, there's a charge."

"So...I can't withdraw money and I can't transfer money?"

"That's right."

(I looked around, warily, to check I had not fallen into a re-enactment of The Castle and was being mistaken for the protagonist. Alas, it was just an ABN AMRO branch.)

"Okay, let me think...okay - if I closed my account, it has money in it now, what would happen to that money? you'd have to send it somewhere?"

"Yes. If you close your account, we will transfer the money to the account you specify. It'll take a few weeks."

"A FEW WEEKS??!?!?"

"Yes. The account is closed immediately of course, but there are checks and so on that we need to do. There is much bureaucracy that must be done. It takes a few weeks before the money is transferred."

At this point I realised that I was reflexively clenching and unclenching my fist and it seemed a prudent time to depart, lest the headlines --
"Embittered AMRO customer slays ten in money withdrawal horror!" "AMRO says -- we never expected people to forget their PIN!"

RISKS? single point of failure upon an entirely plausible failure mode (losing the PIN) with no fallback behaviour. If for any reason you forget your PIN, you can find yourself absolutely shut out of your account -- unable to withdraw money, unable to transfer money and even closing the account, the final recourse, is arranged such that your funds are sequestered. You literally have no access to your money. Like most people, I need to eat and get grumpy when I'm starved for two days.

Furthermore, I now have the choice of paying a charge for a new card, which I will use exactly once, to transfer my funds to my new Rabobank account before closing my ABN AMRO account, or actually physically withdrawing a couple of thousands euros and *walking* it across to my new bank to deposit it.

BTW, depositing cash into a Dutch bank? there's a charge.

Re: PayPal phishes their own customers ([RISKS-25.33](#))

<Sidney Markowitz <sidney@sidney.com>>
Tue, 16 Sep 2008 10:24:23 +1200

A web search for SECURE.UNINITIALIZED.REAL.ERROR.COM shows that this is neither phish nor phowl, it's a bug, not a pheature, though perhaps a bug most phoul. Apparently an error message about an uninitialized variable is being substituted where a URL is supposed to go in a template for the e-mails.

This has been happening at least for almost a year.

<http://www.tamebay.com/2007/10/genuine-paypal-emails-with-spoof-urls.html>

Luckily whoever owns error.com has not set up a phishing website to take advantage of the bug. But the bug may not be as benign as simply producing a bogus URL in the e-mail. This report indicate that it may be associated with PayPal transactions that the user aborts being completed anyway:

<http://discussionboard.prostores.com/showthread.php?t=7795>

This one is even worse. Not only does it seem to be associated with a bogus charge to the PayPal account, but it demonstrates the bug showing up as bad links in e-mail from a presumably live PayPal customer service representative

sent to a customer:

<http://forum.skype.com/index.php?showtopic=192431>

Sidney Markowitz <http://www.sidney.com>

✂ Re: Automated Bill Payments Are a Cinch: Not So Fast (RISKS-25.32)

<Huge <huge@huge.org.uk>>

Thu, 18 Sep 2008 10:22:56 +0100

I'm surprised no-one has mentioned the Direct Debit scheme which operates in the UK, mostly very successfully;

"Over 75% of adults in the UK have at least one Direct Debit and around 100,000 organisations use Direct Debit for collecting a variety of regular and occasional bills including utility payments, insurance, council tax, mortgages, loans and subscriptions."

<http://www.bacs.co.uk/BACS/Consumers/Direct+Debit/>

The "Direct Debit Guarantee" covers your rights;

"If an error is made by the organisation or your bank or building society, you are guaranteed a full and immediate refund from your branch of the amount paid."

To our (UK) eyes, US retail banking is very old-fashioned (*). I haven't written a cheque (US: check) for a utility bill (or any other regular payment) for years. Indeed, cheques are fading from use at an accelerating rate and a number of large organisations no longer accept them. Cheque processing was out-sourced by most UK retail banks some years ago as no longer economic to keep in-house.

(* Given recent events, I am no longer sure if this is a good or bad thing.)

✂ Capability creep strikes again

<"Jay R. Ashworth" <jra@baylink.com>>

Wed, 17 Sep 2008 16:35:18 -0400 (EDT)

Of course, it's being sold as a plan to Protect The Chillluns:

<http://www.thenewspaper.com/news/25/2537.asp>

Private companies in the US are hoping to use red light cameras and speed cameras as the basis for a nationwide surveillance network similar to one that will be active next year in the UK. Redflex and American Traffic Solutions (ATS), the top two photo enforcement providers in the US, are quietly shopping new motorist tracking options to prospective state and local government clients. Redflex explained the company's latest developments in an August 7 meeting with Homestead, Florida officials.

"We are moving into areas such as homeland security on a national level and on a local level," Redflex regional director Cherif Elsadek said. "Optical character recognition is our next roll out which will be coming out in a few months -- probably about five months or so."

The technology would be integrated with the Australian company's existing red light camera and speed camera systems. It allows officials to keep full video records of passing motorists and their passengers, limited only by available hard drive space and the types of cameras installed. To gain public acceptance, the surveillance program is being initially sold as an aid for police looking to solve Amber Alert cases and locate stolen cars.

I don't, at the moment, see any way around this problem: corporations are in it only for the money; if they can make that money by selling to governments capabilities that it would be illegal for the governments to implement on their own, they will.

It's a slippery slope, in the reverse of the usual direction.

And remember: if that database exists, your wife's divorce attorney will be able to subpoena it.

Nice to know Al Queda doesn't need to take away our freedoms; like the citizens of the Weimar Republic, we're doing a bang up job of it ourselves.

Jay R. Ashworth, Ashworth & Associates, St Petersburg FL USA 1 727 647 1274
Baylink <http://baylink.pitas.com> jra@baylink.com

✶ Expiration of cryptographic certificate killed airline ticket

*<Kenji Rikitake <kenji.rikitate@acm.org>>
Thu, 18 Sep 2008 21:47:40 +0900*

All Nippon Airways (ANA) made a public announcement on September 19, 2008 that the check-in system trouble for the domestic flights happened on September 14, 2008 was caused by expiration of the cryptographic certificate issued for access authentication of check-in terminals for the ticket agents.

The company told that:

- * the certificate was expired on September 14, 2008;
- * the expiration was direct cause of the errors of the check-in terminals when the terminals were booted on September 14, 2008;
- * the company knew when they first installed the certificate on 2005;
- * they didn't activate the certificate until September 2007; and
- * no one in the company did notice the expiration during the development of the terminal subsystem.

Sources: ANA public announcement (in Japanese)
<http://www.ana.co.jp/topics/notice080914/index.html>

The risks are obvious:

- * If you depend on something which will expire, such as PKI certificates and domain name subscription, failure of the renewal may kill the whole subsystems depending on the expired objects;
- * If you depend on something which will expire, a warning system (of pre-expiration notice) should be installed to tell you about the expiration, or you will forget about it and may cause the system trouble; and
- * You should always be aware of the *unused* functions of a system and how they work, especially when you decide to activate some of them.

✉ Antivirus software in critical systems? (Re: PGN, [RISKS-25.33](#))

<Martyn Thomas <martyn@thomas-associates.co.uk>>
Tue, 16 Sep 2008 09:32:28 +0100

Self-evidently, fitness for purpose should trump cost of development in this discussion, because the incremental cost of carrying out the final stage of development (and then operation) in an environment that does not require the system to include its own protection against virus infection is fairly small, and the examples that have been given describe systems that are clearly not fit for purpose as implemented.

On the other hand, if cost is more important to you than fitness for purpose, I have a system waiting for you that costs 10% less than the lowest estimate anyone else has given you. Give me a call.

Martyn Thomas CBE FREng <http://www.thomas-associates.co.uk>

✉ Re: Antivirus software in critical systems? Aurora!

<Al Mac Wheel <macwheel99@wowway.com>>
Tue, 16 Sep 2008 12:19:15 -0500

Aurora is US Gov name for the mischief hackers' malware can do when targeted directly at electric utilities. Here's a link to a couple of recent Aurora incidents:

- (a) \$ 1 million generator blown up by hacking = DHS proof of concept.
- (b) Vancouver Canada insider crime as union negotiating
<http://www.militaryphotos.net/forums/showthread.php?t=121081>

US Congress hearings last week into what it takes to protect against this.

- (a) Public Utilities complain that by US making Aurora details top secret, even from their industry, they cannot mitigate against all

threats known to gov.

- (b) US gov agencies say solution is for Congress to give them unfettered authority to meddle in industry, with zero accountability for how that authority is used.

Here's a link to those hearings.

http://energycommerce.house.gov/cmte_mtgs/110-eaq-hrg_091108.Cybersecurity.shtml

Re: Control-Z vs. Bourne-Again SHell (jidanni/chau, [RISKS-25.31-32](#))

<jidanni@jidanni.org>

Wed, 17 Sep 2008 07:17:59 +0800

The problem with commands like
\$ sleep 666; destroy_planet
is that Dr. Evil can type them on your VT100 terminal and walk gleefully away, while you try to find the bash page in the manual racks to see if there are any safe control or break keys you can press short of yanking the terminal out of the wall as time runs out... but it was all a bad 1980's dream, as the librarian tugs your shoulder "Sir, your half-hour is up and there are a lot of people waiting to use a terminal."

Re: Risks of GPS Devices ... (Brader, [RISKS-25.32](#))

<Richard Grady <richard@richbonnie.com>>

Tue, 16 Sep 2008 12:02:12 -0700

This is standard behavior on most amateur radio transceivers, because there are many more functions needed than there are keys on the device.

One of my transceivers (Yaesu FT-8100R, a mobile 2-meter/70-cm unit) triples up on some keys:

1. Press the key to activate the Normal function.
2. Press the F/M key (similar in concept to a shift or control key) and then press the key to activate the Alternate function.
3. Press the F/M key for 1/2 second or more and then press the key to activate the Super-Alternate function.

I have memorized some of the Alternate functions, but I usually have to refer to the manual for the Super-Alternate functions.

[Incidentally, in [RISKS-25.34](#), Sergei apparently completely missed the humor that Mark Brader had very amusingly noted ("to be held down"), which my comment highlighted to make sure our readers did not miss it. However, Sergei apparently did miss it. I seem to have compounded the silliness by evidently oversimplifying the repetition of the gaffe that Mark quoted by trying to correct it, because Sergei had responded not to the humor that had amused Mark and that had inspired me to run Mark's item in the first

place. If that perhaps mistakenly gave anyone the impression that Mark would have disagreed with Sergei, I profoundly apologize to Mark. This is a case where the humor should have been obvious to readers of Mark's item in [RISKS-25.32](#), not the details of the implied corrected statement. PGN]

USENIX Annual Tech '09 Call For Papers

<Lionel Garth Jones <lgj@usenix.org>>

Wed, 17 Sep 2008 11:37:46 -0700

2009 USENIX Annual Technical Conference

June 14-19, 2009, San Diego, CA

Paper Submissions Deadline: January 9, 2009, 11:59 p.m. PST

<http://www.usenix.org/usenix09/cfpb/>

On behalf of the 2009 USENIX Annual Technical Conference program committee, we request your ideas, proposals, and papers for tutorials, refereed papers, and posters.

Authors are invited to submit original and innovative papers to the Refereed Papers Track of the 2009 USENIX Annual Technical Conference. Papers can be either full papers of at most 14 pages or short papers of at most 6 pages. Authors are required to submit papers by 11:59 p.m. PST, Friday, January 9, 2009. (Note new deadline.)

In full papers, we seek high-quality submissions that further the knowledge and understanding of modern computing systems, with an emphasis on implementations and experimental results. Short papers should describe early ideas, advocate a controversial position, or present interesting results that do not require a full-length paper. We encourage papers that break new ground or present insightful results based on practical experience.

The USENIX conference has a broad scope. Specific topics of interest include but are not limited to:

- Architectural interaction
- Cloud computing
- Deployment experience
- Distributed and parallel systems
- Embedded systems
- Energy/power management
- File and storage systems
- Mobile, wireless, and sensor systems
- Networking and network services
- Operating systems
- Reliability, availability, and scalability
- Security, privacy, and trust
- System and network management and troubleshooting
- Usage studies and workload characterization
- Virtualization
- Web technology

More information on these and other submission guidelines is available on our Web site:

<http://www.usenix.org/usenix09/cfpb/>

On behalf of the 2009 USENIX Annual Technical Conference organizers,
Geoffrey M. Voelker, University of California, San Diego
Alec Wolman, Microsoft Research

2009 USENIX Annual Technical Conference Program Co-Chairs
usenix09chairs@usenix.org



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 35

Monday 22 September 2008

Contents

- [Sydney road tunnel closed by computer 'glitch'](#)
[John Colville](#)
- [DC Primary votes don't add up... even with a fudge factor](#)
[David Leshner](#)
- [Hurricane Ike](#)
[Les Denham](#)
- [Hacker claims Palin e-mail hacked via password reset](#)
[Rob McCool](#)
- [Re: Wall Street; where nothing can go worng wrogn wrngo....](#)
[Martin Ward](#)
- [Re: Risks of financial systems too complex...](#)
[Jim Horning](#)
- [Re: Risks of not using check digits](#)
[Erling Kristiansen](#)
[Paul van Keep](#)
- [Re: capability creep on red-light cameras](#)
[Paul Wallich](#)
- [Info on RISKS \(comp.risks\)](#)

✉ Sydney road tunnel closed by computer 'glitch'

<"John Colville" <colville@it.uts.edu.au>>
Tue, 23 Sep 2008 08:39:12 +1000 (EST)

The M5 East tunnel is a 4-km tunnel on a major motorway leading into Sydney. On 22 Sep 2008 the tunnel was closed for 2 3/4 hours starting at about 0900, due to the failure of a backup computer. It caused serious disruption to traffic in that area of Sydney. "... the tunnel had to be closed to traffic because its safety equipment was disabled when the computer system was down."

[`It is the sixth time the \$800 million project has been shut since it opened in late 2001." Previous failures included a different "computer

glitch" in Feb 2002; lighting systems failed 11 months later; a "combined power failure" occurred in Mar 2004; the CCTV system failed in Dec 2004; and another computer crash caused as five-hour closure on 25 Jun 2008. PGN] The company which operates the tunnel has now agreed to have a staff member on duty at all times.

<http://www.smh.com.au/news/national/oh-baby-m5-tunnel-takes-its-toll/2008/09/22/1221935513625.html?page=fullpage#contentSwap1>

John Colville, Faculty of Engineering & IT; University of Technology, Sydney
Honorary Associate + 61 2 9514 1854 colville@it.uts.edu.au

✶ DC Primary votes don't add up... even with a fudge factor

<"David Leshner" <wb8foz@panix.com>>
Mon, 22 Sep 2008 16:17:32 -0400 (EDT)

Nikita Stewart and Elissa Silverman, *The Washington Post*, 22 Sep 2008; B01
<http://www.washingtonpost.com/wp-dyn/content/article/2008/09/21/AR2008092102344_pf.html>

As District officials continue to investigate errors in the early vote tallies from the Sept. 9 primary, one number stands out: 1,542. That number appeared in the category for "overvotes" in 13 separate races when the D.C. Board of Elections and Ethics released early results on election night. But those votes inexplicably vanished shortly after midnight, when officials posted what they identified as corrected results. ...

The elections board initially blamed the discrepancies on a single defective computer memory cartridge at the Precinct 141 polling site on U Street NW in the Dupont Circle area. Sequoia has said the cartridge was not defective and suggested that tabulation errors might have been triggered by workers or by a static or electrical discharge.

[The article goes on about problems within Board, including the fact the CTO does not have a claimed BS degree, and the ExDir's departure.]

Static discharge? At least they are not saying swamp gas was to blame.

[I was going to reference this to a past voting Risks post, but there are so many to choose from...]

✶ Hurricane Ike

<Les Denham <les@iiandt.com>>
Mon, 22 Sep 2008 16:03:36 -0500

Along with about 4 million other residents of this area, I experienced Ike ten days ago. And am still experiencing it. Many of the problems are computer related.

The first problem was that my home DSL service stopped when Ike was still 200 miles away (Friday evening). I suspect that my phone service stopped about the same time. Shortly afterwards, my electricity stopped.

On Saturday afternoon, after the winds died down, I found I had phone service, but still no electricity. I tried to get my DSL working by plugging the DSL modem into a UPS which still had some charge, but that didn't work. A little later, the phone service stopped working. And the cell phone service.

Next morning, I tried the phone, and it worked. Later in the day, when the electricity came on, I tried my DSL, and it worked. In my email, I found a message from my ISP apologizing for the interruption in service: the co-location site had the backup generator for the servers function correctly, but the backup generator for the air conditioning failed to start. Of course, this did not matter to me, because at the time I had neither power, nor internet, nor phone. By evening, the phone and the internet had stopped working again, but I had found that by walking about a mile from the house I could get a cell phone signal. On one of these walks I saw an AT&T truck and flagged the driver down. I asked what the problem was: we had power, and damage in my subdivision was minimal. He explained that each subdivision had a remote unit or subexchange with its own battery backup, which was charged from the exchange -- and the exchange was still running on backup generators, which did not have enough reserve to power all the subexchanges.

By Monday afternoon, AT&T had their act together, and I had a landline, DSL, and cell phone signal.

For me, the most significant point of failure appeared to be that AT&T has engineered their backup power supplies to only cope with about twelve hours of power failure. With hurricane Ike, we had over 90% failure of electricity supply to the fourth largest city in the U.S.A. The first repairs were not completed for about 24 hours; it was a week before 50% of power was restored; and ten days later we still have over 30% of electricity customers without power.

Les Denham, Vice President, Interactive Interpretation & Training, Inc.
1500 Citywest, Suite 800, Houston, TX 77042, U.S.A. 1-713.840.3326

Hacker claims Palin e-mail hacked via password reset

*<Rob McCool <robm@robm.com>>
Sun, 21 Sep 2008 22:38:16 -0700 (PDT)*

<http://blog.wired.com/27bstroke6/2008/09/palin-e-mail-ha.html>

This blog entry refers to an anonymous hacker who claims to have been the one behind the widely publicized breach of VP candidate Sarah Palin's Yahoo e-mail account. The interesting part is that the claimed attack was not

based on a weak password, but instead based on a weak password-reset mechanism. The hacker claimed that with a few searches in Google and some information (Palin's birthday) from Wikipedia, along with some guesses of phrasing, he was able to gain access to her email account.

Re: Wall Street; where nothing can go wrong wrong....

<Martin Ward <martin@gkc.org.uk>>

Mon, 22 Sep 2008 12:32:52 +0100

A lot of the comments in [RISKS-25.34](#) seem to imply that the people running the financial firms were stupid and/or careless in not doing a correct risk analysis.

These people are not stupid or careless, merely greedy, unscrupulous and irresponsible. They did a careful risk analysis all right, and then made the decision to deliberately feed false information into the computer models and deliberately create massively complex financial instruments.

Their risk analysis looked like this:

Success: My company hands off the package before it blows up. My company makes a massive profit and I end up fabulously wealthy. (Other companies make massive losses and have to be bailed out by the government, but that is incidental).

Failure: My company ends up holding the package when it blows up. My company makes a massive loss and ends up having to be bailed out by the government. I end up extremely wealthy.

After careful consideration of all the risks and benefits, I decide to go ahead!

In an ideal world, the risk analysis would look like this:

Success: My company hands off the package before it blows up. My company makes a massive profit and I become fabulously wealthy. Other companies make massive losses and have to be bailed out by the government. My company, and all the others, gets investigated and I end up bankrupt and jailed for many years.

Failure: My company ends up holding the package when it blows up. My company makes a massive loss and ends up having to be bailed out by the government. I become extremely wealthy. My company, and all the others, gets investigated and I end up bankrupt and jailed for many years.

Quote: "There was a willful designing of the systems to measure the risks in a certain way that would not necessarily pick up all the right risks" If an engineer, for personal gain, willfully designed (say) a sewage monitoring system so that it did not pick up the right risks, and as a result thousands of homes were flooded with sewage and destroyed, that engineer would (I

hope) end up in jail. But in the financial world, people can get away with doing much more damage, for personal gain, with no personal risk to themselves.

martin@gkc.org.uk <http://www.cse.dmu.ac.uk/~mward/>
G.K.Chesteron web site: <http://www.cse.dmu.ac.uk/~mward/gkc/>

Re: Risks of financial systems too complex ,, (Smith, [RISKS-25.34](#))

<"Jim Horning" <jhorning4@comcast.net>>
Sun, 21 Sep 2008 23:27:33 -0700

I thoroughly agree with Daniel's main point, but let's not blame computers too much.

This is the result of financial creativity driven by greed, both of which have been around for quite a bit longer than computers. Many of the securities at the heart of the 1929 market crash were very nearly as complex as those you describe. See, for example, John Kenneth Galbraith's insightful 1955 book, *The Great Crash 1929* (<http://www.amazon.com/Great-Crash-1929-Kenneth-Galbraith/dp/0395859999/>). An ironic side note is the role of Goldman Sachs in some of the most highly-leveraged creations.

[And PLEASE read Jim's very insightful blog all the way to the end:
<http://horning.blogspot.com/2008/09/economy-is-fundamentally-sound.html>
PGN]

Re: Risks of not using check digits (Re: Douglass, [RISKS-25.34](#))

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>
Mon, 22 Sep 2008 20:13:48 +0200

It is not correct that Dutch bank account numbers do not use check digits. I have an account with ABN-AMRO, and I just did the check: I changed one digit of an otherwise correct number. (I was prepared to accept the risk of sending 1 cent to the wrong recipient.) The transaction was rejected by the on-line banking service. According to one source I found (in Dutch): <http://cgi.dit.nl/bank.cgi> the check is that a specified weighted sum of the 9 digits must be divisible by 11.

There is one exception: The Postbank. Postbank account numbers don't even have a fixed length, very short (3-4 digits) numbers typically being given to major charities and other high-profile customers. There is no intrinsic check of validity, as far as I know. The Postbank is supposed to check the name of the recipient, but I have positive evidence that this does not always happen, even for a rather large transaction.

Re: Risks of not using check digits (Re: Douglass, [R 25.34](#))

<Paul van Keep <paul@vankeep.com>>

Mon, 22 Sep 2008 14:16:03 +0200

... The 9-(and 10-)number system has an 11-test that ensures a sparse usage of the available number space. The formula is pretty simple: The total of 9 times digit1 plus 8 times digit2 etc. should be divisible by 11. The account number 123456789 for instance is a valid number.

[Note: Paul's formulation of the formula is for the nine-digit number system, where digit9 is the unit's digit. The extension to ten digits is more obvious with the equivalent mathematical formula given on the wiki below, using the sum from $i=0$ (to $N=9$ or 10) of the i th digit times $i+1$, where the right-most digit is the $i=0$ th digit. (Elf is 11 in Dutch, and does not imply a mischievous creature carrying out the arithmetic.) PGN]

See the Dutch Wikipedia entry for a more complete description:

<http://nl.wikipedia.org/wiki/Elfproef>

Re: Capability creep on red-light cameras (Ashworth, [RISKS-25.34](#))

<Paul Wallich <pw@panix.com>>

Sun, 21 Sep 2008 20:45:38 -0400

> Jay R. Ashworth" <jra@baylink.com> writes:

> And remember: if that database exists, your wife's divorce attorney will be
> able to subpoena it.

If that were the only problem. If that database exists, your employer, your employer's competitors and the stores you shop at will be buying soft-realtime access to it.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 36

Tuesday 30 September 2008

Contents

- [Mersenne-aries receive benevolence](#)
[PGN](#)
- [Wall Street's Collapse May Be Computer Science's Gain"](#)
[ACM technews](#)
- [BBV: Two-Minute warning on voting machines](#)
[Steve Kelem](#)
- [Online flight bargains not as good as they seemed](#)
[Donald Mackie](#)
- [Risks of all-encompassing backups](#)
[Peter Gutmann](#)
- [ATM reprogramming scam; Two arrested](#)
[Kevin Poulsen via PGN](#)
- [Default passwords and gasoline thefts](#)
[Jim Haynes](#)
- [ATM bug](#)
[Phil Smith III](#)
- [Re: Sydney tunnel: When is a backup not a backup?](#)
[Martin Ward](#)
- [Sydney Australia or Sydney Nova Scotia?](#)
[Rick Gee](#)
- [Too big to fail = single point of failure?](#)
[Bill Hopkins](#)
- [Flooded computers disposed of?](#)
[Marty Brenneis](#)
- [Burning wheelchair almost destroys airplane](#)
[Andrew Koenig](#)
- [Re: Risks of financial systems too complex...](#)
[Robert P. Schaefer](#)
- [Re: Hacker claims Palin e-mail hacked via password reset](#)
[Scott Miller](#)
- [Re: Risks of not using check digits](#)
[Toby Douglass](#)
- [Risks in Networked Computer Systems, Andre' N. Klingsheim](#)
[PGN](#)
- [Study on InSecurity of Social Networks](#)

[LinkedIn et al. via Klaus Brunnstein](#)

• [Estonian Cyber Security Strategy document](#)

[Gadi Evron](#)

• [Info on RISKS \(comp.risks\)](#)

✂ Mersenne-aries receive benevolence

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

Sat, 27 Sep 2008 19:49:34 PDT

[Thanks to Phil Porras for spotting this one.]

As part of the Great Internet Mersenne Prime Search (GIMPS), UCLA mathematicians led by Edson Smith discovered (on 23 Aug 2008) the first verified Mersenne prime number with more than 10 million digits -- indeed, 13-million digits long:

$$p = 2^{(43,112,609)} - 1.$$

The Electronic Frontier Foundation prize is \$100,000. This is the eighth Mersenne prime "discovered" at UCLA, using spare cycles of many machines (as is also done with the SETI project -- the search for extraterrestrial intelligence).

[Source: Thomas H. Maugh II, *Los Angeles Times*, 27 Sep 2008; PGN-ed]

<http://www.latimes.com/news/science/la-sci-prime27-2008sep27.0.2746766.story>

[Note that this discovery does not greatly advance the quest for rapid factoring of arbitrary large prime products. However, it is once again a reminder of the potential power of highly distributed computing.

The prize is on the order of eight-tenths of a penny per prime-number digit. The first multi-million-digit prime,

$$2^{(6,972,593)} - 1,$$

had only 4,197,919 digits, and received \$50K from EFF a decade ago:

<http://primes.utm.edu/notes/6972593/PressAnnouncement.html>

I wonder if EFF will now spring for the first 100-million-digit Mersenne prime to fall?]

✂ "Wall Street's Collapse May Be Computer Science's Gain"

<technews@HQ.ACM.ORG>

Fri, 26 Sep 2008 13:45:04 -0400

Patrick Thibodeau and Todd R. Weiss, *Computerworld*, 26 Sep 2008

The recent collapse on Wall Street may make a career in computer science or IT more attractive to students, who largely left those fields following the dot-com bust of 2001. Stanford University computer science department chairman William Dally says students are returning to computer science because they like the field and not necessarily because it can make them rich. Boston College professor John Gallagher says he has already seen a change in student interest, with many students contacting Gallagher and expressing an interest in switching from finance. Following the dot-com

bust, computer science enrollment declined until it reached a low of 8,021 last year, down from 14,185 in 2003-2004, according to the Computer Research Association (CRA). Meanwhile, offshore outsourcing also scared students into avoiding technology careers. Now, companies are suffering from a shortage of technology professionals, and the looming baby boomer retirements will only add to the problem. CRA analyst Jay Vegso says economic conditions appear to impact the choice that students make when choosing a major, and students currently choosing majors may be looking for safer alternatives. Stevens Institute of Technology's Howe School of Technology Management associate dean Jerry Luftman says the major difference between today and the late 1990s is the type of student that businesses need. While technical skills are important, Luftman says companies also want students with management and industry training, strong communications abilities, and marketing and negotiations skills. The U.S. Bureau of Labor Statistics reports that IT jobs are among the fastest growing; openings for networks systems and data communications analysts are expected to reach 402,000 this year, up from 262,000 in 2006.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115616&intsrc=news_ts_head

BBV: Two-Minute warning on voting machines

<Steve Kelem <steve@kelem.net>>

Tue, 30 Sep 2008 10:23:53 -0700

This message is from Black Box Voting, a non-profit that monitors voting irregularities and fraud. Steve Kelem, Los Altos Hills, CA

- ----- Original Message -----

Subject: From BBV: Two-Minute warning on voting machines

Date: Thu, 11 Sep 2008 02:55:21 -0700

From: Black Box Voting <blackboxvoting@worldnet.att.net>

Reply-To: crew@blackboxvoting.org

TWO-MINUTE WARNING ON VOTING MACHINES: Welcome to "SPEED VOTING"

Permission to reprint or excerpt granted, with link to blackboxvoting.org

Diebold/Premier says it's too late to fix a new voting machine 2-minute warning and "time-out" feature, which can kick voters off the machine, forcing them to accept a provisional ballot. At least 15 voters were booted off the machine in Johnson County, Kansas recently, and Diebold/Premier says this is due to a software upgrade which sets a timer on voter inactivity. According to the company, the machines receiving the upgrade are used in 34 states and 1,700 jurisdictions.*

*This seems inflated, though. Unless the optical scan machines are also outfitted with a 2-minute warning, which doesn't make sense, it would seem that this should only apply to the DRE states and locations.

JOINING THIS PROBLEM TO MAKE IT BIGGER:

A study on DRE allocation from Ohio indicates that it takes an average of four to nine minutes per voter to cast an average-length ballot, and ballots in many locations will be longer than average this fall. Each additional ballot question can add 30 seconds to the time a voter must monopolize the DRE.

Diebold's 2-minute timeout kicks in when the voter does not make a selection quickly enough. (Welcome to 21st Century literacy tests.)

According to a Sept. 10 Kansas City Star Article, Johnson County upgraded touchscreen voting machines with a new software release from Diebold subsidiary Premier Election Solutions Inc. Buried in the release notes was a mention of a new "time out" feature that makes the voting machine eject a voter card if there has been no activity for 150 seconds. The machine emits a warning sound at 120 seconds.

You can read the full article here:

<http://primebuzz.kcstar.com/?q=node/14307>

You can add your insights and ask questions here:

<http://www.bbvforums.org/forums/messages/7659/78057.html>

The Black Box Voting TOOL KIT 2008

(<http://www.blackboxvoting.org/toolkit2008.pdf>)

recommends that citizens, like you, obtain the voting machine allocation plans for your jurisdiction. This is going to become critical for locations that use touch-screens, or DREs. Unlike optical scan voting machines, DREs require voters to monopolize a machine the whole time they are voting.

The Ohio study linked below provides concrete guidelines for how many machines are needed:

<http://www.bbvdocs.org/OH/franklin/gen2008-voting-machine-allocation.pdf>

(3,023 KB)

[See also: Wisconsin cheese more nimble than voting list. PGN]

<http://www.bbvforums.org/forums/messages/176/78042.html>

✶ Online flight bargains not as good as they seemed

<Donald Mackie <donald@iconz.co.nz>>

Tue, 30 Sep 2008 22:06:17 +1300

As we get increasingly used to booking travel online - and also seeing bargain fare offers - this had to happen sometime. Of course - if it's too good to be true...

Apparently the airline was altering the fares - the intended increase became the sale price. Normally NZ-Europe costs around NZ\$2300.

This from the *New Zealand Herald* is fairly self-explanatory:

http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10534492

"More than 100 New Zealanders who snapped up extremely cheap airfares yesterday will have their money refunded and tickets voided.

One-way tickets from Auckland to Europe through airline KLM started at just \$50 on its website yesterday. Return business trips were priced at \$500. But the fares were a result of a filing error, KLM spokeswoman Elizabeth Vangalen told the Weekend Herald from Amsterdam last night.

"It's a filing mistake, a human error," she said. "The tariffs vary a lot from day to day, so there are a lot of chances for human error."

The airline did not have the final number of tickets bought at the reduced price, but already more than 100 tickets had been identified. The number could rise to as high as 300, she said. Full refunds would be made "as soon as possible".

The bookings had already been canceled, Ms Vangalen said, and the airline believed there was no chance any travelers wanting to have their tickets honoured would get their way.

But simply voiding the tickets when it was realised a mistake had been made was not good enough, one angry traveler said last night.

David Smith, who had been planning a trip to London with his partner for some time, bought two return tickets on his credit card yesterday. When taxes, surcharges and reservation fees were added the cost was \$660. Mr Smith said he had given his employer the dates of his trip, and had booked accommodation in London.

"I'm a professional myself and if I make a mistake I'm held accountable for it. I don't just say to a customer, 'I cocked up, now give me the money back'," he said."

Don Mackie, Auckland, New Zealand

✶ Risks of all-encompassing backups

*<pgut001@cs.auckland.ac.nz (Peter Gutmann)>
Tue, 30 Sep 2008 21:02:35 +1300*

With users squirreling their data away in ever more obscure locations (this "disk drive" is an iPod, that "disk drive" is a cellphone, the other "disk drive" is an SD card, ...) it's necessary for backup software to be very methodical in what it backs up or face the risk of losing user data. So what happens when your software to uses a comprehensive backup policy? Here's one example, with identifying marks deleted:

This programme, always running in the background, monitors files on your

computer and notices when they have been modified. It then copies the files, compresses and encrypts them, and sends them through the net to a backup computer. This system reads and preserves ALL FILES on each computer. Users are not allowed to restrict files from being read and backed up.

If you have a laptop, you may have noticed that this programme uses huge amounts of bandwidth initially, because it starts out by dumping all the files on your disk. I discovered this when most of my ISP monthly allocation was used up over one weekend, largely by this backup. I quickly learned to put the application on "pause" whenever it was plugged in at home. I don't always remember to "unpause" it when I am at work, and I'm having second thoughts about whether I even want to.

After some consultation, I was assured that the bandwidth for uploading files would decline rapidly once all the files had been transferred, but the high upload rate continued for over a month. I was mystified why it should be taking so long to finish this initial task for an 80GB drive until I discovered that the programme is not simply monitoring the internal hard disk, but all memory devices accessible to the computer. So when I took it home, it was, among other things, backing up the 300MB drive I use for family and personal matters, and another 500MB drive that I used as a "hot backup". In fact, apparently, every time you drop a CD or DVD into a drive, or connect a memory stick, it also grabs those files and uploads them. Even connecting a camera, apparently will result in your pictures being uploaded and saved. I haven't yet been able to determine whether it is also accessing remote disks that are available to my computer at home through my network behind a firewall, where sharing is wide open, and other members of my family have information they definitely do not want uploaded.

It seems the vendors are stuck between a rock and a hard place. If they miss some obscure storage location, then customers get upset. But if they do scour every piece of storage media, then other customers get upset. You can't even exclude "obvious" media like CDs/DVDs because with packet-writing software you don't know whether what's in there isn't being used as general R/W data storage and therefore in need of backup.

ATM reprogramming scam; Two arrested (Kevin Poulsen)

*<"Peter G. Neumann" <neumann@csl.sri.com>>
Wed, 24 Sep 2008 9:39:40 PDT*

In what Kevin Poulsen reports are the first felony charges for hacking ATMs, two men in Lincoln, Nebraska used default passcodes to reprogram privately owned cash machines to believe they were dispensing ones instead of twenties. Kevin notes that a gas station cash machine in Virginia Beach VA had been similarly reprogrammed in 2006 to believe it was dispensing fives, using default administrative passcodes that were printed in owners' manuals by Tranax and Triton -- whose newer ATMS require default passcodes to be changed on first use. [Source: Kevin Poulsen, Two Arrested in First Bust

for ATM Reprogramming Scam, 23 Sep 2008; PGN-ed]
<http://blog.wired.com/27bstroke6/2008/09/two-arrested-in.html>

Some folks wonder why voting machines cannot be trustworthy if ATMs are secure. But ATMs have cameras, audit trails, printed receipts, money (which is evidently more important than votes), and constrained development and operation -- and still aren't secure. Of course, all-electronic voting machines don't have those things, and are much less secure. PGN

✂ Default passwords and gasoline thefts

*<Jim Haynes <jhhaynes at earthlink dot net>>
Tue, 23 Sep 2008 11:36:26 -0500 (CDT)*

An article in today's **Arkansas Democrat-Gazette** tells of 1500 gallons of gasoline stolen from a station. It seems the gasoline pumps are shipped with a default key-code and the station owners are failing to change the codes. "Thieves can sometimes purchase a key and the factory default codes on the Internet. If the station owner has not changed the default code, then the thief can manually enter the codes to put the machine in stand-alone mode and steal gasoline." Tells how after the particular station had closed for the night someone had reprogrammed it and the police discovered long lines of cars waiting there to fill their tanks for free. All but two got away.

✂ ATM bug

*<"Phil Smith III" <risks0908@akphs.com>>
Tue, 23 Sep 2008 10:00:07 -0400*

Last week I was making a largish deposit using a touch-screen ATM (US; bank probably isn't relevant, since I assume they use COTS software).

I started the transaction, including entering the amount, then signed the check and wrote my account number on it. Then I fed the check into the deposit envelope. By this time, the display was asking, "Do you need more time?" (an existential question if ever I saw one!).

I either brushed the "No" button or hit "No" -- I'm not sure which (I've noticed before that the buttons don't make good use of screen real estate -- they should be as widely separated as possible, and aren't). In any case, it said "Transaction canceled" and that was it. But meanwhile, it had happily eaten the envelope containing my check!

I'm still waiting for the bank to find it. I had written the account number on the back, so hopefully that will do it. Turns out the branch doesn't process ATM deposits, so they can't help (I of course spoke with them immediately after it happened), and &bank Galactic keeps saying to wait another day. Meanwhile, I've filed a "dispute" with them; everyone agrees

that it's not rational that whoever processed the deposits, finding an orphaned check *with an account number on the back that matches the payee's name*, wouldn't have just processed it.

Actually, what I probably should have done, is redone the transaction, putting *an empty envelope* in the slot. Then things would have been much, much clearer to whoever processed the envelopes.

In any case, this is clearly a software bug: as I pointed out to the bank, if it's going to let me cancel a deposit after it's accepted the envelope, it should let me cancel a withdrawal after it's dispensed the cash. They didn't seem to think that was funny.

✂ **When is a backup not a backup? (Re: Colville, [RISKS-25.35](#))**

<Martin Ward <martin@gkc.org.uk>>
Tue, 23 Sep 2008 11:43:22 +0100

"The M5 East tunnel is a 4-km tunnel on a major motorway leading into Sydney. On 22 Sep 2008 the tunnel was closed for 2 3/4 hours starting at about 0900, due to the failure of a backup computer."

We have had systems fail because the backup system was not able to handle the peak load on the main system: in other words, the "backup" turned out to be unable to take over when most needed. So it wasn't a "backup" at all.

Now we have a system which fails because the "backup" computer failed. So this "backup", instead of dealing with a single point of failure, adds another single point of failure to the system!

martin@gkc.org.uk <http://www.cse.dmu.ac.uk/~mward/>

✂ **Sydney Australia or Sydney Nova Scotia?**

<Rick Gee <RGEE@okanagan.bc.ca>>
Tue, 23 Sep 2008 10:47:19 -0700

A woman planning to fly on Air Canada to Sydney, Australia would up in Sydney, Nova Scotia. [And it reportedly had happened to two other people, in 2002.]

<http://www.cbc.ca/canada/nova-scotia/story/2008/09/19/sydney-argentina.html>

Rick Gee, Chair, Computer Science, Okanagan College www.okanagan.bc.ca/cosc
people.okanagan.bc.ca/rgee

✂ **Too big to fail = single point of failure?**

<"Bill Hopkins" <whopkins@wmi.com>>

Tue, 23 Sep 2008 14:26:33 -0400

In designing reliable systems, we generally try to identify and avoid any single points of failure: components that, if they fail, bring down the system.

I haven't seen a lot of discussion about avoiding "too big to fail" components in our financial system. One is a comment by James Pinkerton (with whom I generally don't agree on much) in Politico's Arena:

<http://www.politico.com/arena/archive/25.html>

✂ Flooded computers disposed of?

<Marty Brenneis <marty@sparkology.com>>

Mon, 22 Sep 2008 19:20:31 -0700

There was a photo in a recent **San Francisco Chronicle** of workers piling up flooded computer equipment from one of the hospitals in the path of hurricane Ike. It got me to thinking of how much tracking there is of the IT equipment with data stored in them that goes astray in a scene like that.

In many cases the power is out long before the equipment gets flooded. I'd bet that a large number of the hard drives have recoverable data in them.

How many flooded systems are there in the disaster area? How many have sensitive data on them? How many workers toss the flooded machines in the trash thinking they are unrecoverable.

Food for thought for the risks readers out there.

Marty Brenneis, Kerner Studios, Making Chaos for the CG World

✂ Burning wheelchair almost destroys airplane

<"Andrew Koenig" <ark@acm.org>>

Tue, 23 Sep 2008 15:34:34 -0400

A holiday jet carrying 229 passengers narrowly avoided disaster when a wheelchair stored in the hold burst into flames shortly after landing at Manchester airport. The chair was removed from the Boeing 727-200 jet and placed on a vehicle - where it immediately burst into flames and was destroyed. <http://www.timesonline.co.uk/tol/travel/news/article4810663.ece>

Further commentary is superfluous.

Re: Risks of financial systems too complex ,,, (Smith, [RISKS-25.34](#))

<"Schaefer, Robert P \{US SSA\}" <robert.p.schaefer@baesystems.com>>
Thu, 25 Sep 2008 13:38:22 -0400

As long as we are citing references to the crash of 1929, one may want to read:

Garet Garrett, Ouroboros or The Mechanical Extension of Mankind,
E.F. Hutton, 1926
<http://mises.org/books/ouroboros.pdf>

The focus of Garrett's text expands on Horning's list, in particular the fourth "weakness":

4) The dubious state of the foreign balance

[NOTE: For RISKS readers less inclined to mythology, ouroboros (literally, tail-eater, with numerous alternative spellings in its transliteration from Greek) refers to a serpent devouring its own tail, symbolizing cyclicity or cyclicality. Maybe the serpent inhabited the Cycladic Islands, one of which is Eschati -- which might in turn be related to Eschatology but not E-scatology, which we find a lot of on the Internet. (See my treatise on the use and misuse of the hyphen, The Hyphenater's Handbook or The Hyphen-Haters Handbook, on why I prefer 'E-mail' to 'email' and related thoughts.) PGN]

Re: Hacker claims Palin e-mail hacked via password reset ([RISKS-25.35](#))

<Scott Miller <SMiller@unimin.com>>
Tue, 23 Sep 2008 08:26:11 -0400

Gotta call "bollocks" on this one, or at least make an accusation of information withheld. I "own" three Yahoo! email accounts, and I created a fourth in the interests of fact checking this claim (in case something had changed since I set up the other three). After testing, it does not appear to be possible to complete the Yahoo! password reset function without knowing either the Yahoo! ID or the alternate email address. No purported analysis of the alleged hack that I have seen (including the alleged description by the alleged hacker himself) has mentioned knowing either of those two items. So, has essential information been omitted from the description of the hack by all parties (and why?), is the claim entirely falsified, or is there a third possibility that escapes me at the moment?

Re: Risks of not using check digits ([RISKS-25.35](#))

<"Toby Douglass" <trd@45mercystreet.com>>
Wed, 24 Sep 2008 19:22:50 +0200 (CEST)

My apologies for the factual error regarding check digits in Dutch bank account numbers.

I obtained this information by phoning ABN AMRO and reaching what I believe in the end was third-line support.

[I am always grateful to RISKS readers for incremental fact-checking!
PGN]

***Risks in Networked Computer Systems, Andre' N. Klingsheim**

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

Fri, 26 Sep 2008 11:33:45 PDT

My SRI colleague Ulf Lindqvist has just returned from Bergen, Norway, where he was a member of the examining committee for the defense of Andre Klingsheim's PhD thesis -- which Ulf has shared with me. The thesis is a collection of eight of Klingsheim's published papers in English, ranging from analyses of the Norwegian national security infrastructure, their ATM system, potential man-in-the-middle attacks (why do women never get implicated?) and flawed authentication in Internet banking, mobile risks, vulnerabilities in E-governments, identity theft, and open wireless nets. Klingsheim's introduction to the thesis identifies various common threads that will be familiar to RISKS readers, particularly risks relating to security, privacy, and judicial matters. What is perhaps most worth noting here is the pervasive nature of the problems throughout so many application areas. Although this should be no surprise to you all, it is still a useful reminder of how far we need to go in the future.

<http://www.nowires.org/Thesis-PDF/AndreKlingsheim.pdf>

***Study on InSecurity of Social Networks (LinkedIn et al.)**

<"Klaus Brunnstein" <brunnstein@informatik.uni-hamburg.de>>

Fri, 26 Sep 2008 14:08:45 +0200

RISKS readers may be interested to read details of a study just published by Fraunhofer SIT (Institute for Secure Information Technologies, SIT, situated in Darmstadt, Germany) addressing Security problems of several highly frequented social networks, including facebook, myspace, LinkedIn and Xing (plus 3 German platforms: studiVZ, wer-kennt-wen and lokalisten). The author Andreas Poller analysed acces protection, traffic protection using crypto (hardly available) as well as registration; with facebook being slighly less insecure than myspace, and LinkedIn (which supports pseudonymity which is though hardly useful in business applications) slightly better than Xing, no platform satisfies essential security requirements.

The study which was developed for the German market, is presently only available in German but will be translated when sufficient international

interest is experienced:

German title: "Soziale Netzwerke gefaehrden Privatsphaere"

http://www.sit.fraunhofer.de/fhg/Images/SocNetStudie_Deu_Final_tcm105-132111.pdf

(engl): "Social Networks dangerous for private sphere"

The study addresses technical issues only. In addition, it would be helpful not only requirements and availability of security functions but also the enforcement of privacy in related laws. In addition to the (technical) insecurity of globally operating social networks, differences in legal protection of privacy (e.g. between US and European laws) should be addressed.

Klaus Brunnstein, Prof. em. University of Hamburg, Germany (9/26/2008)

✶ Estonian Cyber Security Strategy document -- now available online

<Gadi Evron <ge@linuxbox.org>>

Fri, 26 Sep 2008 08:43:09 -0500 (CDT)

The Estonian cyber security strategy document is now available online. I must say once again the concept of a national cyber security stance is quite interesting.

Those who wish to download the document:

<http://www.mod.gov.ee/?op=body&id=518>

My contact there specified she'd be happy to answer any questions. To avoid spam of her inbox, email me for her address.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 37

Thursday 2 October 2008

Contents

- [NASDAQ's Google surprise](#)
[PGN](#)
- [Computer Failure Hobbles Hubble, Derails Shuttle Mission](#)
[Sharon Gaudin](#)
- [Amazon multiple account weirdness](#)
[Graham Bennett](#)
- [Alarm sounded on second-hand kit](#)
[Gabe Goldberg](#)
- [Seeking tales of IT gone wrong](#)
[Andrew Brandt](#)
- [Re: Risks of financial systems too complex ...](#)
[Robert P Schaefer](#)
- [Re: When is a backup not a backup?](#)
[Mark F](#)
- [The folly of retaining default settings](#)
[Ken Knowlton](#)
- [Weak password reset procedures](#)
[identity withheld](#)
- [New castle rules in chess?](#)
[Andy Walker](#)
- [Re: Hacker claims Palin e-mail hacked ...](#)
[Rob McCool](#)
[Scott Miller](#)
[Allen Hainer](#)
- [Info on RISKS \(comp.risks\)](#)

NASDAQ's Google surprise

<"Peter G. Neumann" <neumann@csl.sri.com>>
Wed, 1 Oct 2008 8:29:35 PDT

In the last three minutes of NASDAQ trading on 30 Sep 2008, an amazing event occurred relating to Google stock. It was not reported in the 1 Oct issue

of **The New York Times** and mentioned only in passing in a very brief detail-free summary in the **San Francisco Chronicle**. This is an excerpt from NASDAQ.com after the market close:

GOOG: Stock Quote & Summary Data

Last Sale \$320.50

Change Net \$60.50 -15.89%

Today's High/Low \$483.63 / \$39 [NOT A TYPO. PGN]

In a "glitch" that apparently remains to be explained, the stock price took a horrendous dive in the last few minutes. Although some people tried to profit from it, NASDAQ **canceled** all transactions with Google shares above \$425.29 or below \$400.52, and the closing value was readjusted to \$400.52.

TheAustralian.news.com.au blames "Erroneous trades" routed to Nasdaq that sent Google shares tumbling. Shares rebounded in after-hours trading to \$413.06.

NASDAQ is also investigating trades in Rohm & Haas during the same three-minute window.

Conceivably, the \$39 transaction could have resulted from an erroneous entry such as \$390. [As I edit this, my old home laptop has suddenly developed a sticking "a" key.] And recent studies seem to show that the market is driven more by rumor and innuendo than by external events. However, some sort of range checking would seem to have long ago been in place to prevent such wild outliers. In any event, hopefully an insider will be able to let us know what really happened.

Computer Failure Hobbles Hubble, Derails Shuttle Mission

<technews@HQ.ACM.ORG>

Wed, 1 Oct 2008 14:11:21 -0400

NASA scientists announced that a data formatter and control unit on the Hubble Space Telescope has "totally failed," preventing data from being sent to Earth and delaying a shuttle mission. The Science Data Formatter is designed to collect information from five onboard instruments, format the data into packets, put headers on the packets, and send the packets to Earth. Hubble Space Telescope program executive Michael Moore says the Hubble's problematic computer, which has been in orbit for more than 18 years, is a simple but vital part of the telescope's communications system. NASA scientists are now working to switch the Hubble to onboard redundant systems to resume services until a space shuttle arrives with a replacement system. NASA postponed the space shuttle's planned October repair mission so a replacement computer system can be obtained. Hubble manager Preston Burch does not know what caused the failure, but notes that the unit runs at a relatively high temperature compared to other components, and high temperatures tend to accelerate the degradation process. Moore says switching over to the redundant systems should take about 10 hours, and

technicians and scientists expect to complete the process at the end of the first week of October. NASA's Ed Weiler says the switchover and subsequent installation of new redundant systems should add another five to 10 years to Hubble's life. [Source: Sharon Gaudin, *Computerworld*, 30 Sep 2008, via ACM TechNews, Wednesday, October 1, 2008]

<http://www.computerworld.com/action/article.do?command=3DviewArticleBasic&articleId=3D9115903>

Amazon multiple account weirdness

<Graham Bennett <graham@simulcra.org>>

Tue, 30 Sep 2008 20:54:49 +0100

The other day, I logged in to Amazon and got as far as checking out, when I noticed that my address book only had very old addresses in it (from circa 2001/2002) and the order history stopped around the same time. After thinking for a bit I realised that I'd accidentally used an old password that I don't really use for anything important any more to log in, so I logged out and logged back in with the correct (newer) password and exactly the same e-mail address. Lo and behold, I got my up to date account information and recent order history.

Now, I don't think I'm alone in expecting that when I create an account with a website, the e-mail address or login id will be the primary key, and not the login and password combined. So I was a bit surprised by this.

I sent Amazon e-mail asking them how this could have happened, and asking them a couple of awkward questions like "What if I change the passwords on both accounts to be the same?" and "If I delete one account does it delete both?". They couldn't really provide satisfactory answers to that and said I must have inadvertently created the second account (which is probably the case).

Discussing this with some colleagues at work, it became evident that this is the usual behaviour - you can create as many accounts as you like for the same e-mail address, as long as the passwords are different. Moreover, creating the account does not require the email address to be confirmed! So this means anyone can create an account on Amazon with my e-mail address.

Now, I don't think this in itself is a massive security hole since the new account doesn't have access to any privileged data, but at the very least someone malicious could try to do some nasty things. For example, they could create a lot of accounts against a target e-mail address with common passwords, and hope that the victim accidentally logs in with the wrong one and, not realising their mistake, re-enters their details and makes a purchase. The user probably wouldn't notice since the confirmation will get sent to their e-mail address as expected.

I put these points to Amazon in a customer services enquiry, and for the most part I got the expected fob-off:

"Please rest assured that Your Account is secure.

"In the event of Malicious creating accounts with obvious passwords in the hope that someone will accidentally type the wrong one and enter their credit card details into an account, Our secure server software encrypts all your personal information including credit or debit card number, name and address. The encryption process takes the characters you enter and converts them into bits of code that are then securely transmitted over the Internet.

"Secondly, An attacker registering many passwords against the e-mail address of a victim, even if the attacker was to get access to the customer's account, Please know that if someone was able to log in to your account, they would still not have access to your payment card details, as they are not displayed anywhere on the site.

"None of the customers who have shopped at Amazon.co.uk have reported fraudulent use of a payment card as a result of purchases made with us. In fact, we are so confident about the transaction security we offer on our site that we back every purchase with a security guarantee."

Well, I'm glad that I've got all those 'bits of code' protecting me! Unfortunately, they'll be protecting the attacker too... They do make the valid point that you can't extract credit card details even if you can log into an account, but you can still make purchases and read or change addresses.

I have seen posts on the Web saying that the reason for this functionality is so that people sharing the same e-mail address can have their own accounts. This might have been an issue in the early days of online shopping, but now in the days of widely available free e-mail accounts, I don't think this is necessary. Even then, why not have an e-mail verification step when creating a new account? I don't think this would be a barrier for people signing up.

It seems strange to me that such a well-known Web presence as Amazon would operate a confusing system like this, the disadvantages seem to far outweigh the advantages. I'm sure security experts would say that the simpler a system is, the simpler it is to secure it.

<http://graham33.wordpress.com/2008/09/14/amazon-multiple-account-weirdness/>

Alarm sounded on second-hand kit

<Gabe Goldberg <gabe@gabegold.com>>

Thu, 02 Oct 2008 10:50:03 -0400

For less than a pound (UK), a security expert obtained front-door access to a council's internal network. Andrew Mason from security firm Random Storm bought some network hardware from auction site eBay for 99p. When he switched it on and plugged it in, the device automatically connected to the internal network of Kirklees Council in West Yorkshire. Kirklees council

called the discovery "concerning", but said its data had not been compromised.

<http://news.bbc.co.uk/2/hi/technology/7635622.stm>

Seeking tales of IT gone wrong

<Andrew Brandt <risks_inquiry@amishrabbt.com>>

Thu, 25 Sep 2008 02:14:46 -0600

As a sporadic reader of your list, I'm familiar with the kinds of stories that end up gracing each issue of the ACM Risks Digest. I've come to ask you, all of you, for some help.

I'm a freelance reporter, currently on assignment to write a story for *Infoworld*. The gist of the story is "Greatest IT Mistakes," where I hope to relate true anecdotes of people who -- perhaps in an ill-advised, well-intentioned state of mind -- set off a cascade of errors that resulted in serious computer downtime, lost data, or other notable information technology failures or problems.

As opposed to the typical story in RISKS, I'm searching for the stories about problems that, while they may have been aggravated or magnified by automated systems, were initiated by humans.

Many such historical events (e.g., the Morris Worm) are well known. Many more end up in the Snopes urban legend archive. I'm looking for examples that fall outside the parameters of the well-known events of this type, and I won't print anything the veracity of which I cannot authenticate. Please send me true stories, preferably where you have direct, personal knowledge of the details and parties involved.

The goal of the story is not to humiliate a person, or call attention to a company with poor IT policies. This isn't a name-and-shame piece. I'd like the story to serve as a cautionary tale to others, with a humorous angle, if that's possible. And I think it is. To that end, I'm willing to anonymize what anyone cares to share with me to whatever extent is necessary to avoid such humiliation. Of course, if the person or people responsible for, by way of entirely hypothetical example, deleting a company's entire e-mail archive in the process of performing a backup are willing to have their identities disclosed, I'd be more than happy to oblige.

I'll be searching the archives for stories dating back no further than about 18 months that suit the needs of my article; if you know of a particularly juicy tidbit, please contact me directly with anecdotes. You can use the risks_inquiry@amishrabbt.com e-mail address, with the word "risks" somewhere in the subject line.

Thanks very much in advance for your assistance.

[I suggested to Andrew that he cull through the RISKS archives and my annotated index (<http://www.csl.sri.com/neumann/illustrative.html>),

especially those with the descriptor "h" (for human) and "i" (for interface). PGN]

Re: Risks of financial systems too complex ,,, (Schaefer, [R-25.36](#))

<"Schaefer, Robert P \{(US SSA)\}" <robert.p.schaefer@baesystems.com>>
Tue, 30 Sep 2008 15:55:58 -0400

PGN missed my follow-up correction. Ouroboros was written in 1926, before the crash. A good read though. The book I meant to cite was:

Garet Garrett, The Bubble that Broke the World, 1932
<http://www.mises.org/books/bubbleworld.pdf>

Re: When is a backup not a backup? (Ward, [RISKS-25.36](#))

<Mark F <mark49607@gmail.com>>
Wed, 01 Oct 2008 20:13:38 -0400

> We have had systems fail because the backup system was not able to handle
> the peak load on the main system: in other words, the "backup" turned out to
> be unable to take over when most needed. So it wasn't a "backup" at all.

I've been on commercial flights that weren't permitted to take off because they had only 2 of 3 navigational devices functioning.

The irony is that only 2 were required, but the airline had decided that it wanted the extra reliability of having 3, not realizing that the FAA rules said that ALL of the installed units had to be working.

(This was in about 1965, so the rules may have changed.)

The folly of retaining default settings (Re: Haynes, [RISKS-25.36](#))

<Ken Knowlton <KCKnowlton@aol.com>>
Wed, 1 Oct 2008 10:16:03 EDT

[Re: Jim Haynes [RISKS 25.36](#): Default passwords and gasoline thefts, and George Santayana's "Those who cannot remember the past..."]

Sixty five years ago Richard Feynman created a minor ruckus by opening several filing cabinets containing super-secret info at Los Alamos simply by dialing the standard factory setting of their combination locks.

#

Weak password reset procedures

<[Identity withheld by request]>

Wed, 1 Oct 2008 11:52:58

There's always a tradeoff in making password resets easy vs. secure. I ran into what (to me) was a new low point today.

At Starwood.com, if you forget your account info, you can type in your e-mail address. It then gives you a choice of e-mailing you a temporary password (the normal approach), or recovering it using your "secret" question - which I did. So the answer to my "secret" question is as good as my password.... but most people's secret question is probably *less* secure than a password, since it's more likely to be something that can be recovered from a credit report, or at least brute force guessed. (I don't know if there are limits as to how many failures you can have before they lock you out.)

OK, that's pretty weak. But then the big surprise - once I logged in (again, having only provided the answer to my secret question), I changed passwords - and the profile screen displays all 16 digits of my credit card number, plus the expiration date. Not the usual twelve stars and the last four digits, but the full 16 digits.

The risk? Making recovery easy for customers (and hence increasing revenue and reducing help desk costs) can increase the risk to customers, even those who don't lose their passwords!

✂ New castle rules in chess? (Re: [RISKS-25.36](#))

<anw@cuboid.uk (Andy Walker)>

Thu, 2 Oct 2008 00:13:40 +0000 (UTC)

We've become used to confusions between assorted Sydneys, Gibaltars and so on. "Right Move", an organ of the English Chess Federation, reports on one between Newcastles. To cut quite a long story short, lady wants to find a chess club in Newcastle for her son, and quite sensibly googles for "junior chess Newcastle". The organiser in Newcastle-under-Lyme, a modest town, is quite used to this confusion, and passes her on to his counterpart in Newcastle-upon-Tyne, a large city whose university is well-known to readers of these articles. Said organiser finds her some nearby schools with chess clubs. Slightly puzzled mother says those schools are across the city, and aren't there any in nearby suburbs? Turns out [of course] that she is in Newcastle NSW, Oz -- yet another of the 33 Newcastles (and more variants) listed by Wiki.

I suppose it shouldn't be a surprise that emigrants to new countries name not only their towns and cities but also some of their suburbs, streets and schools after those in their old countries. The problem is, of course, that Google and other computerised tools are international in scope, and locals

don't always recognise the need for disambiguation.

[I've just run the same google, and the Lyme one is not only now fifth (behind two Tynes and two NSWs) but is also clearly a Lyme rather than a random Newcastle, so either the web pages have changed or else the lady was somewhat careless.]

[I have a personal interest in this confusion, as my house was once owned by the Duke of Newcastle, the "most hated man in England" at the time of the Reform Act riots (when his home, Nottingham Castle, was burned down). As Lyme is much too small to have a proper Duke, I always assumed he was a Tyne. But I found out fairly recently that the Tynes had died out, the title had had to be re-created, and they had used the Lyme version as a figleaf to give a different name but allow the same abbreviation.]

Re: Hacker claims Palin e-mail hacked ... (Miller, [R-25.36](#))

*<Rob McCool <robm@robm.com>>
Tue, 30 Sep 2008 20:23:12 -0700 (PDT)*

I think Scott Miller raises an interesting question, which is how did the hacker know to look for her e-mail at Yahoo to begin with.

I agree that it's unlikely that he knew her alternate e-mail address. I would think only an insider would know that.

Yahoo IDs can be public, although I can't remember if it's opt-in or opt-out, at <http://members.yahoo.com/>

Since the Yahoo ID was deleted after the incident, we don't know if her ID was listed or not. But that's one way her Yahoo ID could have been found. For fun, try looking for Arnold Schwarzenegger or Gray Davis in that directory. But then again, some of those accounts may have been created by mischief makers as a result of this incident.

It's also possible that the Yahoo ID recovery process was changed after this incident and that the mechanism we're looking at isn't the one that was in place at the time. This may have only been the most high-profile of cases where the prior mechanism was abused and the Yahoo security team may have enhanced it since then.

All these possibilities are there, and while I agree that they're slim chances, I'm not willing to conclude that it's BS yet. But the question remains, how did this person know that the real Sarah Palin was using Yahoo e-mail?

Re: Hacker claims Palin e-mail hacked ... (McCool, [RISKS-25.37](#))

*<SMiller@unimin.com>
Wed, 1 Oct 2008 09:10:25 -0400*

Rob, Well, regardless of the accuracy of these reports, there's your risk: Using a "something you know" factor as part of the recovery authentication that could in fact be "something that you and everyone else in the Internet universe knows or can trivially discover". It is indeed possible that Yahoo! changed recovery methods after (and as a result of) the incident, but my observation after over a year of using Yahoo! mail is that they seem to have a _lot_ of trouble replicating any behavior changes across their server farm, so I am somewhat skeptical that such a revision was successfully completed within 48 hours of the initial published reports. I created the new account to see if there was some option to allow additional recovery questions (e.g., the "high school" data mining allegation) that was only available at set-up time - there was not. I doubt that the reports are without a germ of truth, but I think that two things are obvious: The reports as they stand are at best incomplete; The media (unfortunately including many IT specialty sites and bloggers) embarrassed itself (again unfortunately, as usual) with its complete inability to do even rudimentary fact checking. Although perhaps I need to check my assumption that anyone working in the media remains capable of embarrassment...

✂ Re: Hacker claims Palin e-mail hacked ... ([RISKS-25.36](#))

<Allen Hainer <risks@hain-veilchen.de>>
Wed, 01 Oct 2008 15:55:36 +0200

Scott Miller raises the question of whether a yahoo account can be reset without knowing the yahoo ID. The yahoo ID in question can easily be found using yahoo advanced search:

<http://members.yahoo.com/interests?.oc=a>

Enter the first and last name. The picture was last updated in 2006, so I don't think it is a recent spoof.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 38

Tuesday 14 October 2008

Contents

- [Investigator: Computer likely caused Qantas plunge](#)
[Paul Saffo](#)
- [Qantas A330 accident](#)
[Martyn Thomas](#)
- [B-2 crash on takeoff](#)
[Ken Knowlton](#)
- [Illinois high-speed trains](#)
[Jon Hilkevitch](#) via [David Lawver](#)
- [D10T: National Debt Clock is out of digits](#)
[Mark Brader](#)
- [Passport RFID attack: missing validation](#)
[Aaron Emigh](#) via [PGN](#)
- [Missing hard drive "not encrypted" because it was "secure"](#)
[John Carlyle-Clarke](#)
- [Russian researchers achieve 100-fold increase in WPA2 cracking speed](#)
[Monty Solomon](#)
- [Defective news submission website](#)
[Steven M. Bellovin](#)
- [Risks of a new laptop](#)
[Nick Brown](#)
- [Researcher Liuba Belkin: Workers more prone to lie in e-mail](#)
[Monty Solomon](#)
- [Thomas Crown escape, revisited](#)
[Peter Houppermans](#)
- [Re: Sydney NS vs. Sydney NSW](#)
[Steve Schafer](#)
- [Oyster card hack details revealed](#)
[Gabe Goldberg](#)
- [Re: Remarkable -- United Airlines Stock](#)
[Russ Nelson](#)
- [Info on RISKS \(comp.risks\)](#)

✉ **Investigator: Computer likely caused Qantas plunge**

<Paul Saffo <paul@saffo.com>>
Tue, 14 Oct 2008 07:55:32 -0700

[Brings back memories of the early A320 accidents caused in part by a stubborn fly-by-wire system... -p]

Investigator: Computer likely caused Qantas plunge
Rod McGuirk, Associated Press, 14 Oct 2008

A faulty computer unit likely caused a Qantas jetliner to experience two terrifying midair plunges within minutes last week. More than 40 people were injured when the Airbus A330-300 briefly nose-dived twice during a flight from Singapore to the western Australian city of Perth last Tuesday.

Julian Walsh, chief air investigator at the Australian Transport Safety Bureau, said an initial investigation indicated the cause was a computer unit that detects through sensors the angle of the plane against the airstream. He said one of the plane's three such units malfunctioned and sent the wrong data to the main flight computers.

The flight data recorder indicated the plane, carrying 303 passengers and 10 crew, climbed about 200 feet from its cruising level of 37,000 feet and then went into a nose-dive, dropping about 650 feet in 20 seconds, before returning to cruising level, the safety bureau said last week. The sharp drop was quickly followed by a second of about 400 feet in 16 seconds.

[The Air Data Inertial Reference Unit (ADIRU) was sending "erroneous, spike" data to the Flight Control Primary Computers ("PRIM", comparable to the A320's ELACs), which event disconnected the autopilot. A short while later the ADIRU sent "very high, random, incorrect" values to the PRIM, causing a pitch-down command. The same occurred again another short while later. See the ASTB press release:

http://www.atsb.gov.au/newsroom/2008/release/2008_43.aspx

Incidentally, early suspicions centered on air turbulence, which were incorrect. I have disregarded many of the earlier postings from RISKS readers, but thank you for them. PGN]

The problem is the latest in a series of malfunctions and near-misses for Australia's flagship carrier in recent weeks.

Australian authorities are still investigating an explosion aboard a Qantas 747-400 aircraft carrying 365 people over the South China Sea in July that ripped a hole in the fuselage. That explosion caused rapid loss of pressure in the passenger cabin but no one was injured.

Walsh said the French manufacturer Airbus had notified all operators of A330 and A340 aircraft, which are equipped with the same sensors, about how crews should respond to such a malfunction. But aircraft are unlikely to be grounded over a malfunction that had never happened before, he said. "It is probably unlikely that there will be a recurrence, but obviously we won't dismiss that," Walsh told reporters, saying they would investigate the problem further.

The faulty unit will be sent to the U.S. component manufacturer for testing, he said. A report on the accident is to be released next month. Qantas said the preliminary findings showed that the fault lay with the manufacturer rather than the airline. "This is clearly a manufacturer's issue and we will comply with the manufacturer's advice," the airline said in a statement.

<http://sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/10/14/international/i053943D69.DTL>

✈ Qantas A330 accident

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

Tue, 14 Oct 2008 14:44:11 +0100

The ATSB report raises a few questions:

(http://www.atsb.gov.au/newsroom/2008/release/2008_43.aspx)

- * Why wasn't the fault in ADIRU 1 screened out by comparison with the other two ADIRUs?
- * Why were "spikes" treated as valid input by the primary flight computers?
- * Was the possibility of erroneous input to the primary flight computers from the ADIRU considered in the hazard analysis? If so, with what result? If not, why not?

The pilots deserve credit for their prompt recovery.

Martyn Thomas CBE FREng <http://www.thomas-associates.co.uk>

✈ B-2 crash on takeoff (Bob Charette, Re: [RISKS-25.19](#))

<Ken Knowlton <KCKnowlton@aol.com>>

Mon, 13 Oct 2008 16:28:36 EDT

[Bob Charette's item amplifies what was summarized in Paul Saffo's item in [RISKS-25.19](#), and is included here for archival purposes. Bob is a well-known authority on risk analysis, but has not been a regular RISKS contributor. PGN]

Bad Data into Computers Caused B-2 Crash

Posted to *IEEE Spectrum* online by Robert Charette on June 9, 2008 5:00 AM

The US Air Force reported that the February crash on take-off of the \$1.4 billion B-2 stealth bomber called the Spirit of Kansas was caused by moisture interfering with the operations of 3 of the aircraft's 24 air pressure sensors. The sensors were all on the port side of the aircraft. The moisture problem was found to skew the data being fed into the aircraft's flight control computers.

According to news reports, "The aircraft crew believed the bomber had reached the takeoff speed of 140 knots when in reality it was traveling ten knots slower and rotated for takeoff. The malfunction also meant that the sensors showed the plane to be in a nose down position, causing it to command a high level of pitch, around 30 degrees. This, combined with the low takeoff speed, caused the aircraft to stall and veer to the left."

The pilot and co-pilot ejected successfully, although the co-pilot was hurt.

What the Air Force noted was that the crash could have prevented by more effective risk communications.

Again, according to the story, "The vulnerability of the sensors to moisture was first detected by air crews and maintenance staff in 2006, at which time it was discovered that turning on the 500 degree pitot heat prior to sensor calibration would evaporate the water and cause a return to normal readings. However, this was never formally noted and so the pilots of the aircraft were unaware of the potential problem or its solution."

In fact, another B-2 had to abort a takeoff at the same base because of the same problem apparently last year, but the pilots of the B-2 that crashed hadn't been briefed about it.

On a personal side, the B-2 belong to the 509th bomb wing, my old outfit. I was an avionics tech back in the early 1970s, and I find it strange that the problems with the sensors were not logged, nor that when an abort happened, the causes were not formally briefed. I also find it interesting that the information about heating the pitot at the very least wasn't informally spread among the very small B-2 pilot community. If memory serves me correctly, the problem back when I was in the Air Force was that pilots complained about everything - even if a system worked as designed but didn't work the way they wanted it to - on their aircraft during after-flight debriefs, which were all noted, filed, cataloged and analyzed. No issue was too small not to make note of.

✈ Illinois high-speed trains

<David Lawver <dlawver@doit.wisc.edu>>

Thu, 2 Oct 2008 15:41:46 -0500

Jon Hilkevitch, **Chicago Tribune**, 1 Oct 2008

Improvement in train-control mechanisms on the corridor through Illinois to St. Louis will give Amtrak engineers precise information in the locomotive cab that reinforces what the signals along the tracks are saying and indicates track conditions ahead. For instance, sensors indicating that gates and warning lights are operating properly at railroad crossings and no vehicles are blocking the tracks will enable approaching trains to maintain top speeds through the crossings, officials said.

The system is considered fail-safe, even at high speeds. If an engineer violates the signals, the system will stop the train. The new signal system is being installed on about 25 miles of track, from Joliet to Mazonia, to improve the safety and reliability of passenger service, according to the Federal Railroad Administration.

The improved technology will also boost train speeds from 79 m.p.h. to 110 mph on sections of 118 miles of track between Mazonia and Ridgely, near Springfield.

[And we know this fail-safe system is implemented by computers, of course, so we all feel reassured that Nothing Can Go Wrong.]

Full article at:

http://www.chicagotribune.com/news/local/chi-amtrak-funding_01oct01,0,7784079.story

David Lawver, UW-Madison DoIT/SNCC-SM Operational Process Coordinator
1-608/262-8159 3108 CS&S dlawver@doit.wisc.edu

✶D10T: National Debt Clock is out of digits

<msb@vex.net (Mark Brader)>

Wed, 8 Oct 2008 13:21:09 -0400 (EDT)

[Search Google News for "debt clock".]

In a sign of the times, the National Debt Clock in New York has run out of digits to record the growing figure. The government's current debt at about 10.2 trillion dollars. The organisation that runs the sign said it plans to update it next year by adding two digits to make it capable of tracking debt up to a quadrillion dollars.

http://ukpress.google.com/article/ALeqM5h_QzfbREUJ7Nlu72_cisVDT3envQ

[Mark added subsequently:]

Say, if this is the first time this has happened, does that make it 1D10T? :-)

✶Passport RFID attack: missing validation (Aaron Emigh)

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

Sat, 11 Oct 2008 19:31:26 PDT

[Aaron Emigh sent me an article that discusses generally the issue of the absence of validation of 35 out of 45 countries' public keys used to validate data in RFID passport chips.

<http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece>

(Note: The PKD participants' list [1] lists only nine participants:

Australia, Canada, Germany, Japan, New Zealand, Singapore, Korea, the UK,

and the USA. Either the reported number is incorrect, or another country has begun participating since the list was published in April of this year.)

The ICAO seems to understand the issue; the PKD's 2007 report [2] states "The business case for validating ePassports is compelling: border control authorities can confirm that the document held by the traveler: was issued by a bona fide authority, has not been subsequently altered, is not a copy." In the ICAO PKD Procedures [3], it says (section 7.2): "The Country Signing CA Certificate (Ccsca) must be disseminated by the Participant prior to eMRTD [electronic machine readable travel document] issuance." So it does seem that this was understood, and that the way to enable validation of ePassport data is to participate in the PKD.

The article implies that Secunet Golden Reader accepts self-signed certs from countries that have not filed a Ccsca, and that this data could be accepted by border patrol agents. It would obviously seem a better choice to force border personnel to validate the printed documents, where they presumably have some expertise in rejecting fraudulent credentials, in lieu of accepting any digital data that can't be validated. Does anyone know whether there are processes that capture a requirement for manual review for non-PKD-participating countries' passports? I don't have a copy of ICAO 9303.

1. http://www2.icao.int/en/MRTD/Downloads/PKD%20Documents/PKD_Board_-_Participants_list_v_1.1.pdf
2. http://www2.icao.int/en/MRTD/Downloads/PKD%20Documents/PKD_Board_-_Annual_Report_2007.pdf
3. http://www2.icao.int/en/MRTD/Downloads/PKD%20Documents/PKD_Procedures_Final_Version.pdf

Missing hard drive "not encrypted" because it was "secure"

*<John Carlyle-Clarke <john@wormdrive.net>>
Mon, 13 Oct 2008 22:57:34 +0100*

This form of story is becoming depressingly familiar at the moment in the UK to the point where numbness is setting in.

http://news.bbc.co.uk/1/hi/uk_politics/7667507.stm

"Up to 1.7m people's data missing. A missing computer hard drive may have contained details of 1.7 million people who had enquired about joining the armed forces, the government has said."

What made this story stand out for me was a quote in it from EDS, via Bob Ainsworth, the government minister with responsibility. They said:

"EDS assesses that it is unlikely that the device was encrypted because it was stored within a secure site that exceeded the standards necessary for restricted information."

To paraphrase: there was no way this could go missing, so we didn't bother

to encrypt it.

✂ Russian researchers achieve 100-fold increase in WPA2 cracking speed

<Monty Solomon <monty@roscom.com>>

Sun, 12 Oct 2008 18:21:47 -0400

Russian security company Elcomsoft posted a press release on 12 Oct 2008 detailing a new method to crack WPA and WPA2 keys:

With the latest version of Elcomsoft Distributed Password Recovery, it is now possible to crack WPA and WPA2 protection on Wi-Fi networks up to 100 times quicker with the use of massively parallel computational power of the newest NVIDIA chips. Elcomsoft Distributed Password Recovery only needs a few packets intercepted in order to perform the attack. ...

<http://securityandthe.net/2008/10/12/russian-researchers-achieve-100-fold-increase-in-wpa2-cracking-speed/>

<http://www.prweb.com/releases/wi-fi/cracking/prweb1405954.htm>

http://securityandthe.net/wp-content/uploads/2008/10/elcom_pressrelease_wpa.pdf

✂ Defective news submission website

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Mon, 6 Oct 2008 10:31:22 -0400

My department is hosting a distinguished lecturer, so I went to the university web site for submitting important campus news items. I described the talk and the speaker, clicked submit -- and was presented with a request to log in with my university login and password. A bit odd, I thought, but perhaps not unreasonable -- maybe only faculty can submit news items. So I logged in -- and got a web form for administering database access control lists and tables...

This would be Just Another Buggy Web site, but there's one final detail that elevates this incident to a classic: the distinguished lecturer is Peter Neumann...

(http://calendar.columbia.edu/sundial/webapi/get.php?vt=detail&id=25765&con=embedded&br=ais_featured)

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

[Very amusing. My talk was given one-half hour after Steve sent that message, on Integrity of Elections. I suppose examples of voting machines (and ATMs) showing a blue screen of death or an operating system login prompt would also tickle Steve's fancy. PGN]

✂ Risks of a new laptop

<Nick Brown <Nick.BROWN@coe.int>>

Thu, 9 Oct 2008 13:36:02 +0200

I've just received a flyer from Dell which, among other things, describes a whole range of new services for which I can sign up when I buy a new PC.

1. "Recovering your data". For 60 Euros, during 3 years, Dell will "help me recover my data following flood, fire, or other incident". No indication is given of how likely this is to be physically possible, nor exactly how much effort Dell will put into this before declaring my disk to be dead. I'll still be making my own backups, thanks.
2. "Tracking down your stolen laptop" (55 Euros). If, during the first 3 years, my laptop is stolen and connected to the Internet, "its location can be determined" and "local law enforcement agencies will help you get it back". I'd be interested in seeing Dell's worldwide agreement with "local law enforcement agencies", and what the penalty clauses are if said agencies fail to return my laptop. I'd also be interested to know what other mechanisms Dell has planned to track where my laptop was used *before* I reported it stolen. Naturally, we will be assured that "strict safeguards are in place to stop this happening". (I'd be interested to know how this works... do they use some form of ID built into the CPU, or is there an open port on the firewall, or are the MAC addresses of the network cards - Ethernet and WiFi - piggybacked into network packets in some way?)
3. (The best one) "Formatting your data remotely" (70 Euros). Note that I'm translating from French here; what I presume they mean is "formatting your disk [partitions] remotely", not some service whereby they right-justify your paragraphs for you. The description of the service is breathtaking: "Dell can remotely format (sic) your sensitive data if your PC is lost or stolen. Your critical data will not fall into the wrong hands".

Wow. So if I buy this service (and probably, even more worryingly, if I don't), my Dell laptop will have software on it which will listen for a message from the mother ship which will tell it to "format the data".

The RISks are beyond enumeration, but let's start with:

- If your PC is stolen and the thief is sufficiently clever to backup the data before connecting it to the Internet, then not only does she have all your data, but you might naively think she doesn't.
- If the guy I met at the airport last week, to whom I lent my laptop for a minute so he could check his webmail after we swapped business cards, happened to note the service tag of the PC, and it turns out that he works for a rival company, he will likely have all the info he needs to ensure that I have a very bad day.
- If Joe in Cincinnati calls Dell to say his laptop has been stolen, and his serial tag is off by one from mine, and someone presses the wrong key in the mother ship, how much is Dell's liability for my data?

However, all (data) may not be lost. Because Dell also offers:

4. "Certified data destruction" (18 Euros). When the time comes to get a

new PC, Dell will take my old one and guarantee the secure destruction of all the data on the hard drive, and recycle its components. So apparently a simple format (remote or otherwise) isn't enough to keep your data out of the hands of the bad guys. I'm confused. I would also be very interested to have a list of people who are so serious about the need for their data to be securely destroyed, that they are prepared to pay in advance for it. I wonder if a disgruntled former call-center employee might sell me that data? No, surely not. And the people in charge of actually destroying the data wouldn't take a copy, either.

Nick Brown, Strasbourg, France.

Researcher Liuba Belkin: Workers more prone to lie in e-mail

<Monty Solomon <monty@roscom.com>>

Fri, 10 Oct 2008 08:48:03 -0400

In two studies co-authored by Lehigh's Liuba Belkin, people using e-mail lied almost 50 percent more often than those using pen-and-paper. Workers are significantly more likely to lie in e-mail messages than in traditional pen-and-paper communications, according to two new studies co-authored by Lehigh's Liuba Belkin.

More surprising is that people actually feel justified when lying using e-mail, the studies show. "There is a growing concern in the workplace over e-mail communications, and it comes down to trust," says Belkin, an assistant professor of management in the College of Business and Economics. "You're not afforded the luxury of seeing non-verbal and behavioral cues over e-mail. And in an organizational context, that leaves a lot of room for misinterpretation and, as we saw in our study, intentional deception."

The results of the studies are reported in the paper, "Being Honest Online: The Finer Points of Lying in Online Ultimatum Bargaining." Belkin and her co-authors-Terri Kurtzberg of Rutgers University and Charles Naquin of DePaul University-presented their findings at the annual meeting of the Academy of Management held in August. ...

http://www3.lehigh.edu/News/V2news_story.asp?iNewsID=2892

Thomas Crown escape, revisited

<Peter Houppermans <peter@houppermans.com>>

Fri, 3 Oct 2008 13:26:43 +0200 (CEST)

A crafty bank robber in America made a Thomas Crown style escape from the scene of his crime by recruiting a crowd of unsuspecting identically-dressed accomplices on the Internet. King5.com reports that the well-organised villain struck as an armoured van was picking up cash from the a Bank of

America branch in Monroe, Washington. Wearing a dust mask, safety goggles, dayglo vest and a blue shirt, he pepper-sprayed a security guard and grabbed a bag of cash before fleeing briskly.

Responding plods were hampered in their pursuit by the fact that a dozen other dayglo-vested, masked, goggled and blue-shirted men had congregated in the vicinity -- just as the legion of bowler-hatted suits assembled in New York's Metropolitan Museum in the latest Thomas Crown film [to?] fatally embugger the authorities' efforts to bracelet the eponymous billionaire blagger.

In this case, it appears that the anonymous miscreant recruited his unsuspecting dupes on Craigslist. ...

[Source: The Register, 3 Oct 2008. The rest of the story is good too. PGN]

http://www.theregister.co.uk/2008/10/03/craigslist_thomas_crown/

Re: Sydney NS vs. Sydney NSW (25.36)

<Steve Schafer <steve@fenestra.com>>

Fri, 03 Oct 2008 09:41:06 -0400

I live in Athens, Ohio. One of the local newspapers is the *Athens News* (<http://www.athensnews.com/>). As it turns out, there is also an English-language *Athens News* in the other Athens (<http://www.athensnews.gr/>).

Not surprisingly, electronic correspondence intended for one *Athens News* sometimes ends up at the other. This happened in July, with a letter mistakenly sent to our local *Athens News*. The editor decided to print it anyway:

<http://www.athensnews.com/opinion/letters/2008/jul/03/letter-abandoned-dogs-ask-wheres-odysseus-when-you/>

This set off a chain of events that eventually led to a successful trans-Atlantic resolution of the situation:

<http://www.athensnews.com/news/2008/jul/07/dogs-rescued-greek-island/>
<http://www.athensnews.com/news/local/2008/jul/10/letter-editor-sparks-international-dog-rescue/>
<http://www.athensnews.com/news/2008/jul/14/greek-dogs-safely-placed-homes-europe/>

I am also reminded of when, several years ago, I was walking past the gates at Dallas-Fort Worth International Airport, I noticed that American Airlines flights to "San Jose CA" and "San Jose CR" were departing from adjacent gates. The scheduled departure times were less than two hours apart.

Oyster card hack details revealed (Re: [RISKS-25.22,24](#))

<Gabe Goldberg <gabe@gabegold.com>>

Tue, 07 Oct 2008 10:43:53 -0400

The Oyster card is used on London's travel network. Details of how to hack one of the world's most popular smartcards have been published online. The research by Professor Bart Jacobs and colleagues at Radboud University in Holland reveals a weakness in the widely used Mifare Classic RFID chip. This is used in building entry systems and is embedded in the Oyster card used on London's transport network. Publication of the research was delayed by legal action taken by the chip's manufacturer.

Paper chase

Prof Jacobs and his team first identified the vulnerability in a research paper that was due to be published in March 2008. However, the release of the article was delayed after chip manufacturer NXP attempted to secure a court injunction against its publication. The paper was finally released on Monday at the European Symposium on Research in Computer Security (Esorics) 2008 security conference held in Malaga, Spain.

Sensitive data stored on the Mifare Classic chip is protected by a unique number that acts as a key. When the chip, or a card bearing it, is placed near a reader it transmits and receives information based on its key. The security of the system depends on the key remaining secret. [Source: Peter Price, BBC]

http://news.bbc.co.uk/2/hi/programmes/click_online/7655292.stm

Re: Remarkable -- United Airlines Stock

<Russ Nelson <nelson@crynwr.com>>

October 1, 2008 8:27:02 PM EDT

[From Dave Farber's IP group. PGN]

> PGN wrote (see [RISKS-25.37](#)) : TheAustralian.news.com.au blames "Erroneous > trades" routed to Nasdaq sent Google shares tumbling. Shares rebounded in > after-hours trading to \$413.06.

It's not necessarily erroneous trades. A number of stockholders will have a stop on their shares, so that they automatically sell if the price drops below a certain amount, typically 10% or whatever they think is outside the normal day's range of stock trading.

Other people are interested in buying the stock once its price climbs out of its normal range. There's a whole theory ("technical trading") which tries to predict what is normal, and when a stock is going to exceed its normal price range. They have set a limit on the price they're willing to buy. When the price goes above that, they buy the stock.

Sometime mean people will buy a bunch of shares of a stock, then sell them all at once. Depending on market conditions, they can depress the price of the stock enough to hit people's stops, at which point they sell, which drives the price down further, and further. The mean people then buy all

the stock back (which takes a lot of cash, obviously), which sends the price of the stock zooming.

If they're lucky, again, they'll send the price up so high that they'll start to hit limits, and more and more people will buy the stock. The mean people are happy to sell the stock to them.

And when all of this winds down and the price returns to approximately its original value, both the people with stops and limits are screwed and the mean people make a lot of money. Sounds like NASDAQ saw that happen, and undid it. Usually the effect is small and the mean people get away with it.

--my blog is at <http://blog.russnelson.com>
521 Pleasant Valley Rd. Potsdam, NY 13676-3213 +1 315-323-1241

IP Archives: <https://www.listbox.com/member/archive/247/=now>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 39

Friday 17 October 2008

Contents

- [NSA posts secrets to writing secure code](#)
[Joab Jackson via Jim Innes](#)
- [Excel error leaves Barclays with extra Lehman assets](#)
[Gabe Goldberg](#)
- [LAPD blames fingerprint errors for false arrests](#)
[PGN](#)
- [Maryland Police Put Activists' Names On Terror Lists](#)
[David Hollman](#)
- [Airport baggage screener charged with stealing passengers' stuff](#)
[Peter Houppermans](#)
- [Credit card readers compromised](#)
[Peter Houppermans](#)
- [More Smart Card Cracking](#)
[Gene Wirchenko](#)
- [Stolen Votes and Stolen Elections](#)
[Mark E. Smith](#)
[PGN](#)
- [Online health records](#)
[David Magda](#)
- [New Data Privacy Laws Set For Firms](#)
[Ben Worthen via Monty Solomon](#)
- [New Massachusetts Regulation Requires Encryption of Portable Devices ...](#)
[Monty Solomon](#)
- [Amazon e-mail accounts](#)
[Steve Loughran](#)
- [Security questions with unacceptable answers](#)
[Earl Truss](#)
- [Worrisome money transfer](#)
[Martin Cohen](#)
- [Stallman vs. Cloud Computing](#)
[jidanni](#)
- [A comment on "outliers"](#)
[Ken Knowlton](#)
- [The Risks of "Something you know"](#)
[Steve Taylor](#)

- [Re: D10T: National Debt Clock is out of digits](#)
[Andrew Raybould](#)
 - ["Sydney NS vs. Sydney NSW" and popup adds!](#)
[Paul D.Smith](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ NSA posts secrets to writing secure code

<"Jim Innes" <james.innes@carrierclasstowers.com>>
October 14, 2008 11:58:28 AM EDT

[Recall that RISKS has always sought to include success stories on approaches that can avoid the types of risks that continually reappear here. Here is one example of something that might be educationally worth considering. PGN]

[From Dave Farber's IP group. PGN]
Archives: <https://www.listbox.com/member/archive/247/=now>

Joab Jackson, Tokeneer case study serves as an example of writing low-defect, highly-reliable code, researchers claim, *Government Computer News* weekly newsletter.

The National Security Agency has released a case study showing how to cost-effectively develop code with zero defects. If adopted widely, the practices advocated in the case study could help make commercial software programs more reliable and less vulnerable to attack, the researchers of the project conclude.

The case study is the write-up of an NSA-funded project carried out by the U.K.-based Praxis High Integrity Systems and Spre Inc. NSA commissioned the project, which involved writing code for an access control system, to demonstrate high-assurance software engineering.

With NSA's approval, Praxis has posted the project materials, such as requirements, security target, specifications, designs and proofs.

The code itself, called Tokeneer, has also been made freely available.

"The Tokeneer project is a milestone in the transfer of program verification technology into industrial application," said Sir Tony Hoare, noted Microsoft Research computer scientist, in a statement. "Publication of the full documents for the project has provided unprecedented experimental material for yet further development of the technology by pure academic research."

Developing code with very few defects has long been viewed as a difficult and expensive task, according to a 2006 paper by Praxis engineers describing the work that was published in the International Symposium on Signals, Systems and Electronics.

For this project, three Praxis engineers wrote 10,000 lines of code in 260

person-days, or about 38 lines of code per day.

After the project was finished, a subsequent survey of the code found zero defects.

Moreover, Tokeneer meets or exceeds the Common Criteria Evaluation Assurance Level (EAL) 5, researchers said. Common Criteria is an ISO-recognized set of software security requirements established by government agencies and private companies. Industry observers have long concluded that it would be too expensive for commercial software companies to write software programs that would meet EAL 5 standards.

According to the 2006 paper, the engineering team used a number of different techniques for writing the code, all bundled into a methodology they call Correctness by Construction, which emphasizes precise documentation, incremental developmental phases, frequent verification and use of a semantically unambiguous language.

The developers wrote the code in a subset of the Ada programming language called SPARK, which allows for annotations that permit static analysis of the program. They used the GNAT Pro integrated developer environment software from AdaCore.

"This case study has shown that software-based security products can be built that are reliable, verifiable and cost effective against Common Criteria guidelines," the paper concluded. "The bar has been raised for both procurers and suppliers."

✂ Excel error leaves Barclays with extra Lehman assets

<Gabe Goldberg <gabe@gabegold.com>>

Tue, 14 Oct 2008 19:35:22 -0400

A reformatting error in an Excel spreadsheet has cropped up in the largest bankruptcy case in U.S. history, prompting a legal motion by Barclays Capital Inc. to amend its deal to buy some of the assets of Lehman Brothers Holdings Inc. The law firm representing Barclays filed the motion (download PDF) on Friday in U.S. Bankruptcy Court for the Southern District of New York, seeking to exclude 179 Lehman contracts that it said were mistakenly included in the asset purchase agreement. The firm -- Cleary Gottlieb Steen & Hamilton LLP -- said in the motion that one of its first-year law associates had unknowingly added the contracts when reformatting a spreadsheet in Excel. [Source: Excel error leaves Barclays with more Lehman assets than it bargained for, *Computerworld*, Oct 14 2008]

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117143>

[Another Excel-lent risk report, also noted by Chris Leeson, who observed that there should be fireworks at the hearing scheduled for 5 Nov, which will be just in time for Guy Fawkes Night! PGN]

✂ LAPD blames fingerprint errors for false arrests

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

Fri, 17 Oct 2008 10:40:13 PDT

Police have arrested innocent people due to faulty fingerprint analysis but have not determined how many cases were affected by such errors. The *Los Angeles Times* has obtained an internal police report that notes two cases in which charges were dropped after problems with the fingerprint analysis were discovered, blamed on "shoddy work and poor oversight". One fingerprint analyst, who was involved in both the mishandled cases, was fired and three others were suspended and two supervisors replaced. "This is something of extraordinary concern," said Michael Judge, public defender for Los Angeles County. "Juries tend to afford the highest level of confidence to fingerprint evidence. This is the type of thing that easily could lead to innocent people being convicted." [Source: AP item, 17 Oct 2008; PGN-ed, thanks to Lauren Weinstein]

http://www.dailynews.com/breakingnews/cj_10743941

✂ Maryland Police Put Activists' Names On Terror Lists

<"David Hollman" <david.hollman@gmail.com>>

Wed, 15 Oct 2008 20:25:05 +0100

The Washington Post, 7 Oct 2008

<http://www.washingtonpost.com/wp-dyn/content/article/2008/10/07/AR2008100703245.html>

"[Some of the involved officials] said the activists' names were entered into the state police database as terrorists partly because the software offered limited options for classifying entries." (from the second page).

The gist of it is that the MD police added names of people who were nonviolent protesters to a terrorist watch list/database; their names were also included on a federal database as well.

While there may be software design and use issues involved (such as: did the database admins have an incomplete grasp of all the "use cases" to be tracked? Were the choices deliberately limited for some political or statistical purpose?) the most potent risk may be that "computer problems" can be used as an excuse for a much more serious human error.

✂ Airport baggage screener charged with stealing passengers' stuff

<Peter Houppermans <peter@houppermans.com>>

Wed, 15 Oct 2008 13:01:27 +0200

From http://www.theregister.co.uk/2008/10/14/tsa_screener_theft/:

A baggage screener for the US Transportation Security Administration has confessed to brazenly stealing a trove of electronics gear from the luggage of passengers he was sworn to protect, federal prosecutors said.

Pythias Brown, 48, of Maplewood, New Jersey, regularly sold the high-priced video cameras, laptop computers, and global positioning systems on eBay using the handle "alirla," according to a criminal complaint filed in federal court in Newark. Brown told investigators he began stealing the items in September 2007 while screening luggage at Newark Liberty International Airport.

✶ Credit card readers compromised

<Peter Houppermans <peter@houppermans.com>>

Wed, 15 Oct 2008 13:07:49 +0200

This is a biggie:

http://www.theregister.co.uk/2008/10/10/organized_crime_doctors_chip_and_pin_machines/

In a nutshell, criminals installed mobile phone kit INSIDE credit card readers before they arrived at merchants and shops, thus sending details of every card used on those terminals to criminals in Pakistan. Not sure how this was discovered, but the scale is breathtaking.

[Followup: I requested more details, and Peter replied. PGN]

You should watch a BBC program, available on YouTube. In part 2, my favourite news reported, Jeremy Paxman, goes into grilling mode, and he tears strips off the credit card suppliers who are trying to pretend it's not a big deal. Well, it is. See <http://www.youtube.com/watch?v=L7QzOcZAwbg>, part 2 is <http://youtube.com/watch?v=pHdX3ZYEvXw>. It's quality TV. (Paxman can be incredibly obnoxious if he doesn't get a straight answer, enjoy.) Also features Ross Anderson from Cambridge, oh, and they managed to get a terrorist angle on it (grin).

OK, below an elaboration. I have omitted by part 2 that I'm one of the two principal authors of an algorithm that addresses that mutual authentication problem in full (which will become part of our token firmware Q1 2009 or maybe earlier), I didn't really want to blow my own horn (or be seen to), nor do i want to play the marketing buffoon. I solve problems, not flog gadgets - and I will get back to you with something new there too. FYI, www.axsionics.ch, happy to send you docs.

Interesting challenge to discover..

1 - it's an add-on, so the electronics won't detect changes as inputs are tapped before they get to the tamperproofing.

2 - if you block mobile comms there will be another way. You're fixing the

wrong problem (more on that later). The good news is that the method they used caused interference, eventually leading to discovery. It sort of radiated trouble..

A disclosure before I start: I actually work for the company that solved this whole problem about a year ago (well, actually several years ago, but the startup has grown into a "real" company :-). Who wants to know will find out easily enough, but my reply is not for marketing.

Transaction challenges (also by banks):

1 - ensure that, as a payment provider, you're talking to the actual account holder

2 - assure to the account holder that you are, indeed, the payment handler

3 - secure this whole process to ensure authentication, authorisation, confidentiality and integrity of the process

(bonus challenge: 4 - ensure that a transaction is actually as expected by the client and get an approval that supports non-repudiation)

Point 1 is done by PIN. The above hack destroys that assurance, but it was IMHO weak to start with, even though most of my cards have 6 digits. The ones with signatures have my face next to the signature (given the quality of the picture mainly to frighten people). How do I know as provider that "owner" and card are together when this happens? I don't - at a point of sale Chip & PIN has driven the assumption that "it must be so", and merchants no longer have any means to check other than picture cards which nobody examines other than with a signature.

Point 2 is where both ATMs and credit card terminals fall down, as well as banks that call their customers - how do you know it's really the bank? How do I know I'm entering my PIN safely? Nothing assures the user of the rightful recipient of their always-the-same PIN..

Point 3 is inadequately dealt with by the "secure shell" approach a("secure" network and "secure" terminal, which means a rogue insider -network or hardware- nulls your whole approach). It is moderately OK from a risk management point of view as you contain the fraud ability to a limited audience, but as soon as someone gets *really* creative many will follow the new path - QED above. With Internet banking there is a dependency on the user terminal being moderately safe, something you can never ensure as a bank. In addition, OTP lacks feedback, challenge - response devices work with cleartext so a Man In The Middle or Man In The Browser remains possible. Note that we started this discussion with a credit card which has NOTHING apart from a secure terminal - if it isn't you thus have a major problem.

Point 4 is now dealt with with out-of-band methods - get a display and confirmation via another route, typically mTAN. But do you really want transaction details travel via an insecure network which principally has no SLA for SMS? SMS traffic is the first that gets dropped if the cell gets busy.. In credit cards PIN entry is assumed to function both as

authentication and authorisation, but the above hack would have worked even if those steps were with different PINs.

There are a few solutions to the whole picture, but keep in mind that the base assumption should always be that the system the card is used on is infected/hacked/tampered with, which rather reduces the number of options. In addition, improving security has normally a tendency to make life harder for the poor end user who has to go through more ritual, incantations and incense burning on behalf of the relevant issuer to keep things safe.

More Smart Card Cracking

<Gene Wirchenko <genew@ocis.net>>

Tue, 14 Oct 2008 18:54:58 -0700

http://www.infoworld.com/article/08/10/07/Researchers_show_how_to_crack_popular_smart_cards_1.html?source=NLC-SEC&cgd=2008-10-13

Stolen Votes and Stolen Elections

<"Mark E. Smith" <mymark@gmail.com>>

Tue, 14 Oct 2008 22:46:47 -0700

<http://globalpundit.org/2008/10/13/oped-stolen-votes-and-stolen-elections/>
<http://www.opednews.com/articles/OpEd-Stolen-Votes-and-Sto-by-Mark-E-Smith-081014-17.html>

Stolen Votes and Stolen Elections

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

Fri, 17 Oct 2008 10:40:13 PDT

Mark Smith's message reminds me of a book I just received:

Richard Hayes Phillips
Witness to a Crime: A Citizen's Audit of an American Election
Canterbury Press, Rome NY, March 2008
ISBN 978-0-9798722-3-5

This is an extraordinarily detailed analysis of the 2004 presidential election in Ohio, and perhaps a harbinger of things to come. PGN]

Online health records

<David Magda <dmagda@ee.ryerson.ca>>

Fri, 17 Oct 2008 10:02:46 -0400 (EDT)

This needs to proceed very, very carefully:

- > The Progressive Conservative government plans to start slowly, at first
- > offering only a bit of information such as vaccination records. However,
- > the end goal is to post everything, including prescriptions, X-rays and
- > laboratory test results. [...]

>

- > Mr. Brisson said addressing security and privacy concerns will be
- > paramount as the province builds the new e-health service. He's hopeful
- > that 'an incremental approach' will not only build up confidence but also
- > usage.

>

- > He said Alberta is in a position to take this step because it's already
- > developed an electronic medical record system accessible exclusively to
- > health-care providers. Every other province and territory is now setting
- > up similar paperless systems.

<http://tinyurl.com/6755ak>

<http://www.theglobeandmail.com/servlet/story/RTGAM.20081017.health17/BNStory/National/home>

The whole "exclusively to health-care providers" bit sounds a bit naive, given the reports out of the US of hospital and IRS employees accessing records of celebrities.

Maher Arar is probably glad that the Syrians couldn't get his medical records:

http://en.wikipedia.org/wiki/Maher_Arar

Can government agencies request (warrant or not) a copy of your medical records if it's in a central database?

We generally know how to secure paper records, I don't think we've quite figured out how to do the same with electronic records.

✂ New Data Privacy Laws Set For Firms (Ben Worthen)

<Monty Solomon <monty@roscom.com>>

Fri, 17 Oct 2008 00:06:43 -0400

Ben Worthen, New Data Privacy Laws Set For Firms, *The Wall Street Journal*, 16 Oct 2008

Alicia Granstedt, a Las Vegas-based hair stylist who works for private clients and on movie sets, never worried about conducting most of her business through e-mail. Ms. Granstedt regularly receives e-mails from customers containing payment details, such as credit-card numbers and bank-account transfers. Since she travels frequently, she often stores the e-mails on her iPhone. But a Nevada law that took effect this month requires

all businesses there to encrypt personally-identifiable customer data, including names and credit-card numbers, that are transmitted electronically.

After hearing about the new law, Ms. Granstedt started using e-mail encryption software, which requires her clients to enter a password to read her messages and send responses. It is a hassle, "but I can't afford to be responsible for someone having their identity stolen," she said.

Nevada is the first of several states adopting new laws that will force businesses -- from hair stylists to hospitals -- to revamp the way they protect customer data. Starting in January, Massachusetts will require businesses that collect information about that state's residents to encrypt sensitive data stored on laptop computers and other portable devices. Michigan and Washington state are considering similar regulations. ...

<http://online.wsj.com/article/SB122411532152538495.html>

✂ New Massachusetts Regulation Requires Encryption of Portable

<Monty Solomon <monty@roscom.com>>

Fri, 17 Oct 2008 09:13:37 -0400

Devices and Comprehensive Data Security Programs

Miriam Wugmeister and Charles H. Kennedy, Morrison & Foerster, Sep 2008

<http://www.mofo.com/news/updates/bulletins/14495.html>

Randy Gainer, New State Laws Require Extensive Data Security Plans and Encryption, Davis Wright Tremaine LLP, Sep 2008

http://www.dwt.com/practc/privacy/bulletins/09-08_DataSecurityPlans.htm

201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth

<http://www.mass.gov/?pageID=ocaterminal&L=4&L0=Home&L1=Consumer&L2=Privacy&L3=Identity+Theft&sid=Foca&b=terminalcontent&f=reg201cmr>

Ben Worthen, New Data Privacy Laws Set For Firms,

The Wall Street Journal, 16 Oct 2008

<http://online.wsj.com/article/SB122411532152538495.html>

✂ Amazon e-mail accounts

<"Steve Loughran" <steve.loughran@gmail.com>>

Thu, 2 Oct 2008 19:56:00 +0100

Regarding the issue about Amazon allowing >1 login per e-mail address, its a historical legacy that they probably hate. Remember back in 1995 when the

whole family had one compuserve or AOL e-mail address? That's when Amazon was created, and that is where they came up with the fact that an Amazon user does not have a 1:1 mapping of e-mail->userID. What they do have is a mapping of (e-mail,password)->userID; you can create two accounts with the same e-mail address, but you will get into trouble if you try and give them the same password. I'm not sure what happens, so try it and see.

The newer Amazon services, such as the Amazon Web Services, have a stricter "one e-mail address" per account rule. Clearly their support organisation has learned the error of the original design decision.

Security questions with unacceptable answers

*<"Earl Truss" <etruss@gmail.com>>
Fri, 3 Oct 2008 10:05:05 -0500*

My wife recently bought a new car and the dealer arranged financing through a local credit union. This credit union has a web site that allows one to check on their accounts and do transfers between accounts and such. I wanted to use the site to make sure the first payment was credited correctly so I attempted to log in. First off, the owner of the account has to call them so they can send out a password to be used for the initial log in so we did that. When I received the password, I again went to the web site and it required me to change the default password. So far, so good. It then required me to set up some security questions by choosing from a fixed list of perhaps ten questions. One of the first was "What was the color of your first car?" I picked that one since I thought that was easy for me to remember but difficult for anyone else to know or find out so I typed in the answer - "red". I was told that I had to enter at least four characters for the answer to the question. I really had no idea what to do except laugh at the programmer who came up with this one. Figuring that this was the case for all of them, I tried again ... "What is your father's middle name?" "Bud" "You must enter at least four characters for the answer to this question." Obviously we must distort reality to pass this test.

Worrisome money transfer

*<martin cohen <mjc_q@yahoo.com>>
Thu, 2 Oct 2008 13:16:09 -0700 (PDT)*

I wanted to transfer some money between two of my IRAs (banks unnamed). I logged into the one where the money was to go (I prefer pull to push). I anticipated having to go to the source, print out a form, signing it, and mailing it in.

Instead, all I had to do was, at the receiving site, enter the source account number, and request a transfer. No authentication of any type was asked for. Less than a week later, the money was transferred.

I don't know if this is common, but this worries me. Can anyone withdraw money from my account just by knowing the account number? I did not see any matching of names between the accounts.

✶ Stallman vs. Cloud Computing

<jidanni@jidanni.org>

Wed, 15 Oct 2008 05:52:31 +0800

Stallman cautions against the "cloud computing" myth:

<http://lists.gnu.org/archive/html/bug-findutils/2008-10/threads.html>

<http://techblog.dallasnews.com/archives/2008/10/cloud-computing-is-stupidity-s.html>

<http://blogs.zdnet.com/carroll/?p=1880>

<http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman>

http://blogs.computerworld.com/rms_hates_cloud_computing_says_you_should_too

and also <http://www.osnews.com/thread?332053> if you have the right browser.

I just want to add a warning that one day when one's Gmail breaks, one will attempt for the first time in one's life to contact the massive Google Corporation. Whereupon one will discover that despite their best intentions, due to their massive scale, there is little chance one will get a personal reply. "No problem" you might say, "there will certainly be many others in the same boat, so it will get fixed". Well, yes that's usually how it works with power outages and the electric company, if not at least you can still always just call their local service center.

[When Gmail breaks? What about the complaints that repeated failed login attempts (a simple type of denial-of-service attack) results in YOUR Gmail account being disabled, with no easy way to get it reactivated? PGN]

✶ A comment on "outliers" ([RISKS-25.37](#))

<Ken Knowlton <KCKnowlton@aol.com>>

Fri, 3 Oct 2008 16:54:04 EDT

PGN mentions "outliers" ([RISKS-25.37](#)) -- leading me to muse on the automatic elimination of aberrant points. In some sporting events, a common practice is to eliminate the highest and lowest judges' scores, and to average the rest. But now consider generalizing on the idea: It may not be generally known, for example, that there are configurations of equally-weighted points in 3-D space for which the pair of points that are farthest apart from each other are the two points that are closest to the center of gravity of the lot!

[I guess that very few RISKS readers will identify Ken with one of his most delicious innovations (if I remember correctly from our Bell Labs days in the 1960s): the 17-sided unistable uniform solid that will always roll over onto the same side: the ultimately loaded-but-unloaded die.

Very dicey matter. PGN]

#The Risks of "Something you know" (Re: Miller [RISKS-25.37](#))

<"Steve Taylor" <staylor@intelematics.com.au>>

Fri, 3 Oct 2008 12:15:00 +1000

A recent article ([RISKS-25.37](#)) mentioned the danger that the "something you know" used to authenticate an account may sometimes be "something everybody knows".

This brings to mind a newspaper article I once read on computer security. While for the most part it was a pretty decent article, I winced when the reporter mentioned that his own e-mail account had once been broken into, even though he'd carefully chosen the extremely obscure password "THX1138".

While that looks pretty much like a random string of letters, it is in fact the name of George Lucas's first film, from his student days.

I don't know what the overlap is between hackers and science fiction fans, but I'm sure it's substantial. "THX1138" is probably more secure than "Gandalf", but it's still nothing to feel safe with.

The moral: choose a **really** secure password. I suggest "Picard" or "Skywalker".

#Re: D10T: National Debt Clock is out of digits

<"andrew raybould" <stop.posting.addresses@gmail.com>>

Thu, 16 Oct 2008 22:56:48 -0400

This is one integer-overflow problem where it seems an opportunity was lost by not using a signed integer... Oh, well, the timing is fortuitous: just when this counter needs another digit, one has become available from the Dow Jones Industrial Average.

#"Sydney NS vs. Sydney NSW" and popup adds! (Re: [RISKS-25.36-38](#))

<"Paul D.Smith" <paul_d_smith@hotmail.com>>

Wed, 15 Oct 2008 09:17:21 +0100

I tried to read the story from the "Athens News" but every single link takes me into a popup add zone for domains. I presume the "Athens News" website has something hacked into it because I see the story briefly but then I'm thrown elsewhere.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 40

Tuesday 21 October 2008

Contents

- [Treasury Office Faults IRS Computer Security](#)
[AP via PGN](#)
- [Springer: Open for all to see](#)
[Debora Weber-Wulff](#)
- [TBS leaves baseball championship game viewers in the dark](#)
[Jim Reisert](#)
- [Drunk, and Dangerous, at the Keyboard](#)
[Alex Williams via Monty Solomon](#)
- [Thousands Face Mix-Ups in Voter Registrations](#)
[Mary Pat Flaherty](#)
- [Ohio Secretary of State's Web Site Hacked; voter suppression tactics](#)
[Steve Kelem](#)
- [From BBV: Two-Minute warning on voting machines](#)
[Steve Kelem](#)
- [Unbelievable security violation](#)
[Identity withheld](#)
- [Re: More Password Reset Procedures](#)
[Identity withheld](#)
- [Risks: Unlock your house via the Internet](#)
[Gabe Goldberg](#)
- [Re: Remarkable -- United Airlines Stock](#)
[Martin Gregorie](#)
- [Re: Outliers](#)
[Jurek Kirakowski](#)
- [Re: Investigator: Computer likely caused Qantas plunge](#)
[Peter Rieden](#)
[Ron Garret](#)
- [Re: Sydney NS vs. Sydney NSW](#)
[Chuck Charlton](#)
- [Re: Illinois high-speed trains](#)
[Joseph Brennan](#)
- [Re: Risks of a new laptop](#)
[Scott Miller](#)
- [Correction/disclaimer re unistable polyhedron](#)
[Ken Knowlton](#)

- [Re: The folly of retaining default settings](#)
[Mark Thorson](#)
 - [Re: D10T: National Debt Clock is out of digits](#)
[Mark Hull-Richter](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Treasury Office Faults IRS Computer Security

<"Peter G. Neumann" <neumann@csl.sri.com>>
Mon, 20 Oct 2008 15:55:16 PDT

Two new IRS computer systems that will eventually cost taxpayers almost \$2 billion are being put into service despite known security and privacy vulnerabilities, a Treasury watchdog said in a report coming out Thursday. The office of the Treasury Inspector General for Tax Administration said Internal Revenue Service officials failed to ensure that identified weaknesses had been addressed before putting the new systems into use. Inspector General J. Russell George said it was "very troublesome" that the IRS "was aware of, and even self-identified, these weaknesses."

The IRS, in a statement, said security of taxpayer data "is of paramount importance" to the agency and that, as noted in the report, it had implemented many of its recommendations and taken steps to improve security. It stressed that no taxpayer data has been harmed and numerous security safeguards were in place.

The report focused on the Customer Account Data Engine, which will provide the foundation for managing all taxpayer accounts, and the Account Management Services system, which will provide faster and improved access by employees to taxpayer account data.

Both systems are gradually being put into use. CADE, expected to cost more than \$1 billion through 2012 to develop and operate, this year processed about 20 percent of the 142 billion returns filed. The Account Management Services system, AMS, still in its initial stages, will cost more than \$700 million to develop and maintain through 2024. [Source: AP item, 16 Oct 2008]
<http://www.nytimes.com/aponline/washington/AP-IRS-Computer-Security.html>

✂ Springer: Open for all to see

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>
Sun, 19 Oct 2008 21:14:44 +0200

The German weekly magazine *Der Spiegel* 19 Oct 2008 reports on the data protection problems that a large rival publishing house, Springer, has had in the past few days.

It turned out that people who had submitted ads for their local ad papers online had all of their data -- name, address, mobile telephone, bank account info -- available online, helpfully indexed by Google.

It was especially problematic for people who had put in, shall we say, rather delicate, anonymous ads. One example was the retired gentleman looking for men to play stripping card games with him; another person was looking for a bisexual playmate. And there they were, searchable and unencrypted on the open Internet.

It was discovered by a system administrator who was doing an ego search in September. He was shocked to find his mobile telephone number cheerfully delivered by Google. He investigated and found the data to be from an ad he had placed about a year and a half ago with a Springer newspaper for selling his apartment.

Springer reacted quickly, removing the data, but it has taken ages to purge it from the Googlebanks. The system administrator is a bit angry at Springer, as they have not offered to pay him damages for having to get a new phone number.

I googled the admin's name, I still get a hit on "Visual Form Maker - Admascript" for the Hamburger Abendblatt, but the cache data is gone and the Link only returns a 404.

http://www.hamburgerwochenblatt.de/php/edit_table.php?order=mwst&sort=ASC&sw=j&tbl=kleinanzeigen

The tool is advertised as offering forms for web pages that can be created in an uncomplicated way for people without knowledge of programming.

Perhaps people who cannot program should not be entrusted with making forms for web pages with sensitive data?

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Treskowallee 8, 10313 Berlin GERMANY +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

TBS leaves baseball championship game viewers in the dark

<Jim Reisert AD1C <jjreisert@alum.mit.edu>>

Sat, 18 Oct 2008 23:05:40 -0600

Said the TBS network statement: "Two circuit breakers in our Atlanta transmission operations tripped, causing the master router and its backup -- which are necessary to transmit any incoming feed outbound -- to shut down. This impacted our live feed from being distributed to any of the other networks in the Turner portfolio and caused the delay in our coverage. Both our primary and backup routers were impacted by this problem. We apologize to baseball fans for this mishap that caused a delay in our coverage."

According to Pomeroy, the failure of the routers was unprecedented and prevented TBS from broadcasting a live message of any kind, including an informational scrawl at the bottom of the screen. Pomeroy said the network had no choice but to put on taped programming, which resulted in "The Steve Harvey Show" at least temporarily ending up in the slot reserved for Game 6.

http://www.boston.com/sports/columnists/massarotti/2008/10/tbs_leaves_viewers_in_dark.html

Jim Reisert AD1C/Ø, <jjreisert@alum.mit.edu>, <http://www.ad1c.us>

Drunk, and Dangerous, at the Keyboard (Alex Williams)

<Monty Solomon <monty@roscom.com>>

Sun, 19 Oct 2008 19:03:31 -0400

[Source: Alex Williams, *The New York Times*, 19 Oct 2008]

ANYONE who has spent more than a few minutes over the last couple of weeks trolling tech blogs or cocktail lounges has probably heard about Mail Goggles, a new feature on Google's Gmail program that is intended to help stamp out a scourge that few knew existed: late-night drunken e-mailing.

The experimental program requires any user who enables the function to perform five simple math problems in 60 seconds before sending e-mails between 10 p.m. and 4 a.m. on weekends. That time frame apparently corresponds to the gap between cocktail No. 1 and cocktail No. 4, when tapping out an e-mail message to an ex or a co-worker can seem like the equivalent of bungee jumping without a cord.

Mail Goggles is not the first case of a technology developed to keep people from endangering themselves or others with the machinery of daily life after they have had a few. For years, judges have ordered drunken-driving offenders to install computerized breath-analyzers linked to their car's ignition system to prevent them from starting their vehicles when intoxicated.

But as the first sobriety checkpoint on what used to be called the information superhighway, the Mail Goggles program also raises a larger question: In an age when so much of our routine communication is accomplished with our fingertips, are we becoming so tethered to our keyboards that we really need the technological equivalent of trigger locks on firearms?

In interviews with people who confessed to imbibing and typing at the same time - sometimes with regrettable consequences - the answer seems to be yes. ...

<http://www.nytimes.com/2008/10/19/fashion/19drunk.html?partner=rssuserland&emc=rss&pagewanted=all>

Thousands Face Mix-Ups in Voter Registrations

<technews@HQ.ACM.ORG>

Mon, 20 Oct 2008 13:20:51 -0400

[Source: Mary Pat Flaherty, *The Washington Post*, 18 Oct 2008, P. A1, from ACM TechNews, Monday, October 20, 2008]

New state voter registration systems across the U.S. are incorrectly rejecting voters and threatening to disrupt the election process. The problems are occurring in states that switched from locally managed lists of voters to statewide databases, a change required by the Help America Vote Act. Although the switch is supposed to be a more efficient and accurate way to keep lists up to date, the transition is causing the systems to question the registrations of thousands of voters when discrepancies occur between their registration information and other official records. In Alabama, for example, dozens of voters are being labeled as convicted felons due to incorrect lists, and Michigan is scrambling to restore thousands of names it illegally removed from voter rolls due to residency questions. In Wisconsin, tens of thousands of voters could be affected, as officials admit that their database is wrong one out of every five times it flags a voter, often due to data discrepancies such as a middle initial or a typo in a birth date. Herbert Lin, who is studying the issue for the federal Election Assistance Commission, says that states are not using the "best scientific knowledge known today," as required by law. One of the problems with Wisconsin's database, which has been in place since August, is that 95,000 voters are incorrectly listed as being 108 years old. If no birth date was available when names were moved into the electronic system, it automatically assigned 1 Jan 1900. By federal law, anyone whose name is flagged must be notified and given a chance to prove his or her eligibility, but voting rights experts say voters are not always alerted, and some, even if they are notified, may simply decide to skip the election as a result.

<http://www.washingtonpost.com/wp-dyn/content/article/2008/10/17/AR2008101703360.html>

✂ Ohio Secretary of State's Web Site Hacked; voter suppression tactics

*<Steve Kelem <steve@kelem.net>>
Tue, 21 Oct 2008 10:25:49 -0700*

Ohio Secretary of State Jennifer Brunner cut back on the accessible functionality of their website after apparent penetration efforts. This was reportedly not the first such attack. [Source: Sarah Lai Stirland, WiReD blog, 20 Oct 2008]

<http://blog.wired.com/27bstroke6/2008/10/ohio-secretary.html>

✂ From BBV: Two-Minute warning on voting machines

*<Steve Kelem <steve@kelem.net>>
Tue, 30 Sep 2008 10:23:53 -0700*

This message is from Black Box Voting, a non-profit that monitors voting irregularities and fraud. Steve Kelem, Los Altos Hills, CA

- ----- Original Message -----

Subject: From BBV: Two-Minute warning on voting machines [...]
Date: Thu, 11 Sep 2008 02:55:21 -0700

From: Black Box Voting <blackboxvoting@worldnet.att.net>

TWO-MINUTE WARNING ON VOTING MACHINES: Welcome to "SPEED VOTING"

Permission to reprint or excerpt granted, with link to blackboxvoting.org

Diebold/Premier says it's too late to fix a new voting machine 2-minute warning and "time-out" feature, which can kick voters off the machine, forcing them to accept a provisional ballot. At least 15 voters were booted off the machine in Johnson County, Kansas recently, and Diebold/Premier says this is due to a software upgrade which sets a timer on voter inactivity. According to the company, the machines receiving the upgrade are used in 34 states and 1,700 jurisdictions.*

* This seems inflated, though. Unless the optical scan machines are also outfitted with a 2-minute warning, which doesn't make sense, it would seem that this should only apply to the DRE states and locations.

Unbelievable security violation

<[Identity withheld]>

Fri, 17 Oct 2008 23:56:36 -0400

My cable TV provider allows on-line access to accounts and major changes to services can be made on-line. If you forget the password, you can request a reset. They reset and e-mail you the temporary password. This is done by many and is reasonable. However, this hi-tech company mails out the same password every time -- the name of the company. That means that I can attempt to login as an "enemy", claim that I have forgotten the password. They mail him the temporary password but I already know what it is. After a brief pause while they send him an e-mail, I log in with the universal password and change it. I can then do things like order services, cancel services, etc. and, in general, be a real pest. The true owner cannot login and will have just received a misleading message telling him to use the new temporary password.

Talk about dumb!

Re: More Password Reset Procedures

<[identity withheld]>

02 Oct 2008

The Civil Air Patrol, an auxiliary of the US Air Force, runs a website where members can access their membership and qualification status. Of course it is password protected, and of course I had forgotten mine.

The site provides the normal "forgot your password?" link which takes you to a page where you enter your member number and email address, and then a

"submit" button that is supposed to trigger an email with your login details.

This submit button, however, triggered an obscure and lengthy error message, something to do with the output of the server can't be parsed maybe because of println's or whatever. I am a webmaster for several sites and even I couldn't figure out exactly what it was complaining about. In any case, it wasn't working.

Before I continue, let me add that in the process of logging in members are reminded of a recent administrative requirement to take a brief online course on OPSEC (operational security) and agree to the OPSEC rules. Apparently, someone had released the new radio frequency lists, which had been changed because the old lists were publicly available. I took the online course (it did not require logging in!) and submitted a form with the "I agree to abide by the OPSEC requirements" box checked. In brief, I agreed not to tell things to people who didn't need to know them.

I went to the helpdesk page and submitted a problem report. In the problem report I had to enter both my member number and email address. That's the same data the "forgot password" form required.

In response, I was requested to provide my SSN and another piece of information. The request arrived by email, but with instructions not to answer by email, but to POST THIS INFORMATION AS A RESPONSE ON A PROBLEM REPORT WEBPAGE. A web page that required no login to reach. My response was "yeah, right."

By e-mail, I received a followup response. "Please provide your daytime phone number and we will call you to get the information."

Keep in mind, this is an auxiliary to the US Air Force, a government operation, at a .mil address, where I had just been required to certify that I would follow OPSEC rules to protect their data. They expected that I would tell my SSN to anyone who calls on the phone asking for it. I don't tell the magazine subscription people my true "month of birth" or other bit of personal data they want to "verify they'd spoken to me", I sure as heck am not going to tell Joe Random Caller my SSN. (But this is the same CAP that routinely sells my membership data to credit card companies, who want me to get my special "CAP logo credit card" at their special usurious rate.)

In my response I asked first if they were kidding me, or if this was some kind of test to see if I understood the meaning of OPSEC. I pointed out that the "forgot password" page required only my id number and email address, both of which they already had, and maybe they should just trigger the "forgot password" action using the data they already had. They had no need for anything more. Or, barring that, fix the original problem and I would get the update myself.

This response got me passed off to someone else who realized (I hope) the stupidity of what they had asked me to do, or at least the futility (I expect) of getting me to cooperate, and an email with my login credentials arrived shortly thereafter.

The final nail? They did not reset my password to a new value and then force me to change it upon the next login. They sent me my EXISTING PASSWORD IN PLAINTEXT. WITH MY USERNAME.

This is YOUR government at work, folks.

✂ Risks: Unlock your house via the Internet

<Gabe Goldberg <gabe@gabegold.com>>

Thu, 16 Oct 2008 21:51:22 -0400

What could possibly go wrong?

<http://www.theinquirer.net/gb/inquirer/news/2008/09/04/unlock-house-via-internet>

✂ Re: Remarkable -- United Airlines Stock (Nelson, [RISKS-25.38](#))

<Martin Gregorie <martin@gregorie.org>>

Wed, 15 Oct 2008 00:42:46 +0100

Russ Nelson is correct in supposing that automated trading takes place, but I think he has his trading operations backward: surely its 'sell' if the price exceeds an upper limit and 'buy' if its below the lower limit. After all, the purpose of the program is to make money, not to give it away!

The usual term for his "mean people" is short sellers. They don't need money to operate: if they are well regarded enough, many markets will let them sell what they don't have in the expectation that the price will drop and they can then acquire the stock at a lower price before they have to complete the bargain by delivering it to the purchaser. Needless to say, if they go short on a large enough amount of stock, the expected price fall becomes a self-fulfilling prophesy.

A similar thing happened in Australia during the Poseidon bubble, when more shares than existed in a mining stock were short sold when the bubble burst, but there was no bail-out for those gamblers. Trading in the stock was suspended and the short sellers were forced to complete their bargains no matter how much money they lost in the process. Needless to say, the stockholders made a killing and the short sellers lost their shirts. Then short selling was banned completely and trading resumed.

✂ Re: Outliers

<Jurek Kirakowski <jzk@ucc.ie>>

Mon, 20 Oct 2008 12:11:06 +0100

Outliers have been mentioned recently (25.37 and 25.39). One should take

care to distinguish between an outlier and an unexpected reading.

1. When the target is moving, you can never be sure whether an unexpected reading is an error (therefore trim it) or true but the start (worsening, etc.) of a trend. Making *either* assumption on a priori grounds can be dangerous to your health and is risky.
2. When the target is static and the measurement process is relatively uncontaminated then you may use the normal distribution assumptions -- variation is error -- and identify unexpected readings as "outliers" (ie you claim to know the distribution and therefore can consider this reading "lies outside.") But the onus is on you to establish the two first conditions are met. Not to do so is also risky.

Ratings from a dozen or so judges, some of which may be biased either way? Simple. Use medians. If there is no bias then the mean = median. If there is, the median process removes the biases (including the horrible thought that there may be a coalition of judges.)

✂ Re: Investigator: Computer likely caused Qantas plunge ([RISKS-25.38](#))

<"Rieden, Peter (UK)" <Peter.Rieden@baesystems.com>>
Fri, 17 Oct 2008 12:14:59 +0100

Perhaps this should be re-titled "Risk of Inflammatory reporting".

To quote from the piece:

1. "A faulty computer unit likely caused a Qantas jetliner to experience two terrifying midair plunges within minutes last week"
2. "and then went into a nose-dive, dropping about 650 feet in 20 seconds"

A 650-foot drop in 20 seconds gives a vertical velocity of 22mph. Taking a conservative estimate of cruise speed at 600mph, simple geometry tells us that this "terrifying mid-air plunge" amounted to a 2.1 degree dive - something which even the most attentive of passengers would be unlikely to have noticed. Whilst I fully accept that the failure to hold altitude has significant concerns for air-traffic safety, I suggest that this "terrifying plunge" stuff is tabloid baloney which should be ridiculed rather than repeated.

✂ Re: Investigator: Computer likely caused Qantas plunge ([RISKS-25.38](#))

<Ron Garret <ron@flownet.com>>
Thu, 16 Oct 2008 11:40:52 -0700

It should be pointed out that these rates of descent (~2000 fpm) are quite typical for a jetliner even during normal operation. Even a small plane can safely descend at these rates, though that would feel fairly dramatic.

Re: Sydney NS vs. Sydney NSW (Schafer, [RISKS-25.38](#))

<Chuck Charlton <charlton@gmail.com>>
Tue, 14 Oct 2008 20:21:28 -0700

The three-letter codes for those two airports are SJC and SJO respectively. My sister once booked the wrong one. I told her that she should have just flown into SFO. [Chuck Charlton, San Francisco]

Re: Illinois high-speed trains ([RISKS-25.38](#))

<Joseph Brennan <brennan@columbia.edu>>
Tue, 14 Oct 2008 20:38:05 -0400

> The improved technology will also boost train speeds from 79 m.p.h.

Cool. The reason this will allow train speeds above 79 m.p.h is that the Interstate Commerce Commission made a rule in *1922* that required cab signals like this for speeds of 80 and up.

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

Joseph Brennan, Columbia University Information Technology

Re: Risks of a new laptop (Brown, [RISKS-25.38](#))

<SMiller@unimin.com>
Tue, 14 Oct 2008 17:03:43 -0400

There seem to be a number of unfounded or otherwise curious assumptions in M. Brown's inquiry. Regarding items 2 & 3 - Dell is re-labeling Absolute Software's (<http://www.absolute.com/>) Computrace service, which I happen to use extensively on behalf of my employer. A Computrace equipped laptop will attempt to "phone home" via Internet connection once per day. Obviously, there does need to _be_ a connection. The computer is identified via an ESN (a 16 x 36-value [0-9; A-Z] unique string assigned by Absolute when the product is registered). The ESN is correlated in Absolute's database with the hardware MAC address and other hardware items to establish a "fingerprint" for the computer. Regarding relationships with law enforcement, Absolute does pretty well, in my experience. The issue in recovery lies mostly with the requirements to have a judge authorize a search warrant (or local equivalent) to serve on the ISP, and yet again for the physical location of the stolen computer. That can be a pain, but to make it easier would only further threaten our Liberty; I recommend leaving that as is, thank you very much. A small piece of Computrace code that is capable of reinstalling the main program at next Internet connection is loaded on ROM on compatible (all Dells, most models of other brands)

computers. So the hard drive may be formatted or replaced and the tracking program will reinstall itself. A computer was stolen from my employer's premises in 2006, and the very first thing that the thief did was swap out the hard drive. That computer was calling in again within 36 hours. Regarding Data Delete, see the above constraints on computer identification. In addition, Absolute requires that computer owners pre-register any administrators to be authorized for Data Delete (at a substantial cost per admin), and the log in requires two factor authentication using a password and a time-based RSA key issued to registered admins. Lastly, initiating Data Delete costs 250 USD, and Absolute wants assurance about where the money is coming from before they nuke the computer. Is it impossible that a black hat could maliciously trigger this function? Hardly, but there would seem to be many ways to inflict equivalent damage that are a darned sight easier (not to mention cheaper) to effect. I am mystified why any thinking human would assume that it was impossible for data to be stolen before the Data Delete function was invoked. I wouldn't, and Absolute has never stated or implied otherwise (although it sadly doesn't much surprise me to find that Dell seems to have dumbed down the description of the service). So the alternative of giving a potential data hijacker an unlimited time window to conceive of and execute theft of data is preferable to an imperfect, less-than-real-time deletion in exactly what way? Regarding the certified destruction of data (#4), I can't quite make out whether M. Brown is trying to belittle the perceived need for this service, or its implementation by Dell. We also use this service as part of Dell's Asset Recovery Services, of which the more important part to us is their certification that the computer has been disposed of in compliance with all applicable environmental laws and regulations. We do a 7-pass DOD wipe (DBAN) before such a computer is sent to Dell, however the data destruction service does provide some additional assurance in the event that our in-house wiping procedure has quietly failed. In the case of the typical consumer, the admitted risk is no doubt offset by the probability that most users would not know or care to even attempt to purge data on their own, and those who did would probably do no more than a Windows delete operation on files.

Correction/disclaimer re unistable polyhedron

<Ken Knowlton <KCKnowlton@aol.com>>

Fri, 17 Oct 2008 21:37:21 EDT

[... the 17-sided unistable uniform solid that will always roll over onto the same side ... PGN]

Not quite. (1) The question, lying around for years, was "What convex polyhedron with least number of faces, cut from uniform material, can be demonstrated to be gravitationally stable on only one face? Mine had 19, not 17, faces. (2) on submitting this for publication, I learned that Richard Guy already had the very same design in the galleys, with the presses running, having found it two months earlier (he was gracious enough to say that I had independently discovered it).

[Ken, TNX for the correction. Tangential to RISKS, but we always strive

for correctness. PGN]

Re: The folly of retaining default settings

<Mark Thorson <eee@sonic.net>>
Fri, 03 Oct 2008 15:24:39 -0700

Ken Knowlton incorrectly recounts Richard Feynman's exploits. Feynman opened the file cabinets by guessing that the combination chosen by Frederic de Hoffman was based on a natural constant. It was e (the base of the natural logarithms).

The Captain's safe was opened by the Los Alamos locksmith, who told Feynman how he did it. He knew the default combinations were usually 25-0-25 or 50-25-50. It was the latter.

You can read about it here:

<http://www.gorgorat.com/>

Search down for "Safecracker Meets Safecracker".

Re: D10T: National Debt Clock is out of digits (Brader, [RISKS-25.38](#))

<MHR <mhullrich@gmail.com>>
Tue, 14 Oct 2008 13:34:54 -0700

If the clock is out of digits, can't they just print some more?

Mark Hull-Richter, Linux Software Developer, Registered Linux User #472807
[sign up at <http://counter.li.org/>]



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 41

Thursday 23 October 2008

Contents

- [Re: Computer likely caused Qantas plunge](#)
[Peter Bernard Ladkin](#)
[Dag-Erling Smørgrav](#)
[Guy Dawson](#)
[Chris Kuan](#)
- [U.S. Government to Take Over Airline Passenger Vetting](#)
[PGN](#)
- [IEEE Spectrum review process upgrade curiosity](#)
[PGN](#)
- [Dan Wallach's report on a vote-flipping examination](#)
[PGN](#)
- [Deceptive practices in elections](#)
[PGN](#)
- [Straight Party Voting Issues](#)
[Leonard Finegold](#)
- [GAO report on Social Security Numbers](#)
[PGN](#)
- [Re: More Password Reset Procedures](#)
[Ralph Jacobs](#)
- [Re: Amazon e-mail accounts](#)
[Dimitri Maziuk](#)
[Klaus Johannes Rusch](#)
- [2 of 3 navigational devices functioning](#)
[Daniel P. B. Smith](#)
- [Info on RISKS \(comp.risks\)](#)

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

Wed, 22 Oct 2008 10:48:19 +0200

Re: Rieden and Garret ([RISKS-25.40](#))

I don't think it helps to suggest that the manoeuvre would be something

passengers are "unlikely to have noticed" (Rieden) or "typical" (Garret). It's not the vertical speed that mattered, it is the acceleration used to get there.

The vertical acceleration was -0.8g according to the Airbus All-Operators-Telex, enough to throw unbelted people against the ceiling (but with not quite their full weight) and 14 people were injured seriously enough to be transported by medical helicopter to hospital. The ATSB has classified it as an accident. Their preliminary report is on their WWW site.

It was more than a "terrifying plunge", it was one sufficient to break people's bones.

Peter Bernard Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

[We received a slew of messages on this topic. The following three are more or less representative of different key points. PGN]

✂ Re: Investigator: Computer likely caused Qantas plunge ([RISKS-25.40](#))

<=?utf-8?Q?Dag-Erling_Sm=C3=B8rgrav?= <des@des.no>>
Wed, 22 Oct 2008 12:02:35 +0200

> Rieden: Perhaps this should be re-titled "Risk of Inflammatory reporting".

Or perhaps "risk of becoming so cynical that you dismiss the story out of hand instead of doing your own research and finding out that the reporter left out a zero, and that more than forty passengers sustained injuries, fifteen of them serious, in a 6,500-foot drop".

Dag-Erling Smørgrav - des@des.no

✂ Re: Computer likely caused Qantas plunge ([RISKS-25.40](#))

<Guy Dawson <guy@crossflight.co.uk>>
Wed, 22 Oct 2008 13:30:40 +0100

What does not appear to be considered is that descent during the 20 seconds may not have been linear. There may have been an initial rapid descent followed by a recovery phase.

I know that if I were sitting in my airliner seat and suddenly found the cabin seat coming down to meet me at 22mph I'd be pretty scared!

Guy Dawson, I.T. Systems Manager, Crossflight Ltd guy@crossflight.co.uk

✈️ Re: Computer likely caused Qantas plunge ([RISKS-25.40](#))

<Chris Kuan <mrgazpacho@hotmail.com>>

Thu, 23 Oct 2008 08:54:01 +1000

In reply to both Peter and Ron, it seems that while misreporting is to blame here, it is merely vaguely imprecise rather than deliberately misleading.

At a press conference, the Australian Transport Safety Bureau played an animation of the incident -- based on recorded flight data. It clearly shows that while the entire incident lasted about 20 seconds, the most severe event was a change in the aircraft's pitch from +2.1 degrees to -8.3 degrees over a period of approximately 1 second.

✈️ U.S. Government to Take Over Airline Passenger Vetting

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

Thu, 23 Oct 2008 10:19:42 PDT

[RISKS has previously reported on the overly aggressive name matching in use of the no-fly list (e.g. David Nelson and Senator Kennedy, [RISKS-22.80](#), 22.81, 25.15). This might minimize those problems. However, any error in the databases used for matching may now be even more difficult to surmount in time to catch your plane.]

The Department of Homeland Security will take over responsibility for checking airline passenger names against government watch lists beginning in January, and will require travelers for the first time to provide their full name, birth date and gender as a condition for boarding commercial flights, U.S. officials said Wednesday. Security officials say the additional personal information -- which will be given to airlines to forward to the federal agency in charge -- will dramatically cut down on cases of mistaken identity, in which people with names similar to those on watch lists are wrongly barred or delayed from flights.

The changes, to be phased in next year, will apply to 2 million daily passengers aboard all domestic flights and international flights to, from or over the United States. By transferring the screening duty from the airlines to the federal government, the Secure Flight program marks the Bush administration's long-delayed fulfillment of a top aviation security priority after the Sept. 11, 2001, terrorist attacks.

Homeland Security Secretary Michael Chertoff and Transportation Security Administration (TSA) chief Kip Hawley said yesterday that, except in rare situations, passengers who do not provide the additional information will not be given boarding passes.

... DHS has received more than 43,500 requests for redress since February 2007 and has completed 24,000 of them, with the rest under review or awaiting more documentation, TSA spokesman Christopher White said. But the

number of people who actually match the names on the watch lists is minuscule, officials acknowledged. On average, DHS screeners discover a person who is actually on the no-fly list about once a month, usually overseas, and actual selectees daily, Hawley said.

To bolster their case for the new program, U.S. officials for their first time disclosed that the no-fly list includes fewer than 2,500 individuals and the selectee list fewer than 16,000. Ten percent of those named on the no-fly list and fewer than half on the selectee list are U.S. citizens, Chertoff said. [Source: Spencer S. Hsu, *The Washington Post*, 23 Oct 2008; PGN-ed]

[Of course, if the TSA database information is as riddled with errors and other variations as are the voter registration databases, the employment eligibility verification databases, and so on, there will still be many false positives on would-be fliers.]

IEEE Spectrum review process upgrade curiosity

<"Peter G. Neumann" <neumann@csl.sri.com>>
Wed, 22 Oct 2008 11:36:02 PDT

I just received a note saying that my review of a submitted paper that was due on 22 Nov 2006 was now overdue. To make matters worse, when I tried to bring up the details on their website, my browser found itself in an infinite loop. I clearly thought I had submitted my evaluation two years ago, and queried Elizabeth Bretz -- who does an excellent job overseeing the review process. This is her response:

``Peter -- no worries. They upgraded the peer review system, and a queue of old papers suddenly sprang to life. There's no need for you to do anything, except disregard the e-mails. Apologies for the interruption and aggravation. Elizabeth''

As the RISKS graybeard, I feel Upgraded by just one more example of an upgrade that did not work as expected.

Dan Wallach's report on a vote-flipping examination

<"Peter G. Neumann" <neumann@csl.sri.com>>
Thu, 23 Oct 2008 10:17:59 PDT

See Dan Wallach's analysis of vote-flipping in the Hart Intercivic e-slate systems.

<http://accurate-voting.org/2008/10/22/vote-flipping-on-hart-intercivic-eslate-systems/>

Deceptive practices in elections

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

Tue, 21 Oct 2008 10:40:50 PDT

Remember that many of the problems with elections are not directly related to the voting systems themselves. For example, two reports were released yesterday that should be of interest to those of you who are not fed up with risks in voting, relating to deceptive campaign practices:

E-Deceptive Campaign Practices

Electronic Privacy Information Center and The Century Foundation

20 Oct 2008

http://votingintegrity.org/pdf/edeceptive_report.pdf

Deceptive Practices 2.0: Legal and Policy Responses

Common Cause, The Lawyers Committee for Civil Rights under Law,
and the Century Foundation

20 Oct 2008

<http://www.tcf.org/print.asp?type=PR&pubid=149>

Straight Party Voting Issues

<Leonard Finegold <L@drexel.edu>>

Tue, 21 Oct 2008 17:34:47 -0400

[This is forwarded by Leonard from someone else, who says:] Lest any of you think this is a hoax, i just checked and it is verified as TRUE on Snopes-- <<http://www.snopes.com/politics/ballot/straightticket.asp>> <http://www.snopes.com/politics/ballot/straightticket.asp> Unbelievable! I rarely like to pass on stuff but this one i encourage everyone to pass on to EVERYONE so we don't have another 8 years of DISASTER. just got this from a friend of mine, pass it on:

"Straight Party Voting" Trap. Here are the details and what to do about it:

THE PROBLEM: "Straight party voting" on voting machines is revealing a bad pattern of miscounting and omitting your vote, especially if you are a Democrat. Most recently (Oct. 2008), a firm called Automated Election Services was found to have miscoded the system in heavily Democratic Santa Fe County, New Mexico such that straight party voters would not have their presidential votes counted.

STRAIGHT PARTY VOTING is allowed in 15 states. Basically, it means that you can take a shortcut to actually looking at who you are voting for and instead just select a party preference. Then the voting machine makes your candidate choices, supposedly for the party you requested.

HOW TO PROTECT THE COUNT against the Straight Party Vote trap:

1) NEVER CHOOSE THE STRAIGHT PARTY VOTE OPTION, because it alerts the computer as to your party preference and allows software code to trigger whatever function the programmer has designed.

2) SEND THIS INFORMATION OUT TO AS MANY PEOPLE AS YOU CAN, blog it, root n' toot it out there to get the word out.

3) ESPECIALLY GET THE WORD OUT TO PEOPLE IN THE FOLLOWING STATES, which have straight party voting options:

Alabama, Indiana, Iowa, Kentucky, Michigan, New Mexico, North Carolina, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Texas, Utah, West Virginia, Wisconsin

4) DEMAND COMPLETE AND CAREFUL TESTING OF THE STRAIGHT PARTY OPTION IN LOGIC & ACCURACY TESTS

5) LOOK FOR UNDERVOTES (high profile races with lower-than-average number of votes cast) and flag them, post them, bring them to the attention of others for additional scrutiny.

Voting machine miscounts of straight party votes were proven by California researcher Judy Alter in the 2004 New Mexico presidential election; in Alabama Democrat straight party votes were caught going to a Republican, and Wisconsin a whole slew of straight party votes disappeared altogether. Both DRE and optical scan machines are vulnerable. Private contractors are involved; private firms like LHS Associates, Automated Election Services, Harp Enterprises, Casto & Harris and others will program almost all systems in the USA this November. ES&S scanners were involved in examples cited, but Diebold has also issued a cryptic Product Advisory Notice in 2006 about unexpected results from certain Straight Party option programming practices.

[Incidentally, I wandered into a voting station in Vancouver, Canada, a couple of weeks ago. They use paper ballots; I asked if they're counted manually, reply "you bet ". They handled more people much more expeditiously than in my PA, USA station, 'cos we have only a couple of voting machines, and they had effectively lots more, and simpler ones...aka ballot boxes. And results were available certainly by next morning (and prob. earlier). LF]

Leonard X. Finegold, Physics, Drexel University, 3141 Chestnut Street
Phila. PA 19104 1-215.895.2740 L@drexel.edu

GAO report on Social Security Numbers

<"Peter G. Neumann" <neumann@csl.sri.com>>
Wed, 22 Oct 2008 11:42:02 PDT

Social Security Numbers Are Widely Available in Bulk and Online
Records, but Changes to Enhance Security Are Occurring
GAO-08-1009R September 19, 2008
<http://www.gao.gov/products/GAO-08-1009R>

Summary

Various public records in the United States contain Social Security numbers (SSN) and other personal identifying information that could be used to commit fraud and identity theft. For the purposes of this report, public records are generally defined as government agency-held records made available to the public in their entirety for inspection, such as property and court records. Although public records were traditionally accessed locally in county courthouses and government records centers, public record keepers in some states and localities have more recently been maintaining electronic images of their records. In electronic format, records can be made available through the Internet or easily transferred to other parties in bulk quantities. Although we previously reported on the types of public records that contain SSNs and access to those records, less is known about the extent to which public records containing personal identifying information such as SSNs are made available to private third parties through bulk sales. In light of these developments, you asked us to examine (1) to what extent, for what reasons, and to whom are public records that may contain SSNs available for bulk purchase and online, and (2) what measures have been taken to protect SSNs that may be contained in these records. To answer these questions, we collected and analyzed information from a variety of sources. Specifically, we conducted a survey of county record keepers on the extent and reasons for which they make records available in bulk or online, the types of records that they make available, and the types of entities (e.g., private businesses or individuals) that obtain their records. We focused on county record keepers because, in scoping our review, we determined that records with SSNs are most likely to be made available in bulk or online at the county level. We surveyed a sample of 247 counties—including the 97 largest counties by population and a random sample of 150 of the remaining counties, received responses from 89 percent, and used this information to generate national estimates to the extent possible. Our survey covered 45 states and the District of Columbia, excluding five states where recording of documents is not performed at the county level (Alaska, Connecticut, Hawaii, Rhode Island, and Vermont). We used the information gathered in this survey to calculate estimates about the entire population of county record keepers.

Many counties make public records that may contain Social Security numbers (SSNs) available in bulk to businesses and individuals in response to state open records laws, and also because private companies often request access to these records to support their business operations. Our sample allows us to estimate that 85 percent of the largest counties make records with full or partial SSNs available in bulk or online, 3 while smaller counties are less likely to do so (41 percent). According to county officials and businesses we interviewed, SSNs are generally found in certain types of records such as property liens and appear relatively infrequently. However, because millions of records are available, many SSNs may be displayed. Counties in our survey cited state laws as the primary reason for making records available, and requests from companies may also drive availability, as several told us they need bulk records to support their businesses models. Counties generally do not control how records are used. Of counties that make records available in bulk or online, only about 16 percent place any restrictions on the types of entities that can obtain these records. We found that title companies are the most frequent recipients of these

records, but others such as mortgage companies and data resellers that collect and aggregate personal information often obtain records as well. Private companies we interviewed told us they obtain records to help them conduct their business, including using SSNs as a unique identifier. For example, a title company or data reseller may use the SSN to ensure that a lien is associated with the correct individual, given that many people have the same name. Information from these records may also be used by companies to build and maintain databases or resold to other businesses. Businesses we contacted told us they have various safeguards in place to secure information they obtain from public records, including computer systems that restrict employees' access to records. In some cases, information from these public records is sent overseas for processing, a practice referred to as offshoring. We were not able to determine the extent of offshoring, but both record keepers and large companies that obtain records in bulk told us that it is a common practice. In the course of our work, we found that public records data are commonly sent to at least two countries--India and the Philippines. State and local governments, as well as the federal government, are taking various actions to safeguard SSNs in public records, but these actions are a recent phenomenon. Based on our survey, we estimate that about 12 percent of counties have completed redacting or truncating SSNs that are in public records-- that is, removing the full SSN from display or showing only part of it--and another 26 percent are in the process of doing so. Some are responding to state laws requiring redaction or truncation, but others have acted on their own based on concerns about the potential for identity theft. For example, California and Florida recently passed laws that require record keepers to truncate or redact SSNs in their publicly available documents, while one clerk in Texas told us that in response to public concern about the vulnerability of SSNs to misuse, the county is redacting SSNs from records on its own initiative. In recent years, 25 states have enacted some form of statutory restriction on displaying SSNs in public records. Some states have also enacted laws allowing individuals to request that their SSNs be removed from certain records such as military discharge papers.

✉ Re: More Password Reset Procedures

*<"Ralph Jacobs" <ralph.jacobs@gmail.com>>
Tue, 21 Oct 2008 17:10:08 -0600*

In response to the Civil Air Patrol example and the statement "This is YOUR government at work, folks."...

The vast majority of the Civil Air Patrol is made up of volunteers. The few paid employees that exist work for CAP the non-profit corporation and are not government employees. That doesn't excuse any of the errors described during the password reset process; just that they weren't committed by the government in this case.

✉ Re: Amazon e-mail accounts (Loughran, [RISKS-25.39](#))

<Dimitri Maziuk <dmaziuk@bmrw.wisc.edu>>

Sat, 18 Oct 2008 13:49:33 -0500

> ... an Amazon user does not have a 1:1 mapping of e-mail->userID.

Counterpoint: back when PayPal was created, they came up with 1:1 mapping of credit card number->userID. Guess how that works for people with joint bank accounts.

(OK, we're weird: my wife kept her maiden name and we don't have 8 credit cards, we only have one. And has the same number for two different cardholder names, unlike our one debit card. Still, we can't be the only two people on the net with a joint visa account.)

I wonder if an analysis of my wife's PayPal/Ebay purchase history would get her diagnosed with multiple personality disorder...

Re: Amazon e-mail accounts (Loughran, [RISKS-25.39](#))

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

Sun, 19 Oct 2008 14:20:54 +0200

Amazon's approach to allow multiple accounts with the same e-mail address has advantages when it comes to e-mail address changes. A customer returning to Amazon years later can still login with the original account data, getting access to purchase history, gift certificates, reviews etc. and change the e-mail address from there even when another customer has used the same e-mail address in the meantime. The downside is that a customer can easily end up with multiple accounts, and merging those later requires manual intervention by Amazon staff.

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

2 of 3 navigational devices functioning

<"Daniel P. B. Smith" <usenet2006@dpbsmith.com>>

Sun, 19 Oct 2008 12:42:03 -0400

In [RISKS-25.37](#), Mark F wrote: "I've been on commercial flights that weren't permitted to take off because they had only 2 of 3 navigational devices functioning."

It was standard practice to equip sailing ships with three chronometers. This requirement forms a pivot for the plot in *Michael, Brother of Jerry*, a very bad and justly obscure 1915 novel by Jack London (better known for *The Call of the Wild*). Here's a key passage (with ethnic slurs redacted). (Needless to say the voyage ends in disaster due to the shipowner's pennypinching ways).

"It's a pity," he would suggest to Captain Doane, "that you have only one chronometer. The entire fault may be with the chronometer. Why did you sail with only one chronometer?"

"But I WAS willing for two," the owner would defend. "You know that, Grimshaw?"

The wheat-farmer would nod reluctantly and Captain would snap:

"But not for three chronometers."

"But if two was no better than one, as you said so yourself and as Grimshaw will bear witness, then three was no better than two except for an expense."

"But if you only have two chronometers, how can you tell which has gone wrong?" Captain Doane would demand.

"Search me," would come the pawnbroker's retort, accompanied by an incredulous shrug of the shoulders. "If you can't tell which is wrong of two, then how much harder must it be to tell which is wrong of two dozen? With only two, it's a fifty-fifty split that one or the other is wrong."

"But don't you realize--"

"I realize that it's all a great foolishness, all this highbrow stuff about navigation. I've got clerks fourteen years old in my offices that can figure circles all around you and your navigation. Ask them that if two chronometers ain't better than one, then how can two thousand be better than one? And they'd answer quick, snap, like that, that if two dollars ain't any better than one dollar, then two thousand dollars ain't any better than one dollar. That's common sense."



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 42

Friday 24 October 2008

Contents

- [Greenspan says computer input did it](#)
[CWmike via timothy via Wendell Cochran](#)
- [Vint Cerf: Big Changes Ahead for the Internet](#)
[TechNews](#)
- [UW researchers uncover gap in border security](#)
[Peter Gregory](#)
- [Re: Computer likely caused Qantas plunge](#)
[Dag-Erling Smørgrav](#)
[Cameron Simpson](#)
[Adrian Edmonds](#)
- [Re: Straight Party Voting Issues](#)
[David Phillips](#)
[Arthur Flatau](#)
- [Re: Remarkable -- United Airlines Stock](#)
[John Levine](#)
- [Info on RISKS \(comp.risks\)](#)

✉ Greenspan says computer input did it

<Wendell Cochran <atrypa@eskimo.com>>
Fri, 24 Oct 2008 06:24:27 -0700

Greenspan Tells Congress Bad Data Hurt Wall Street
Posted by timothy on Thursday October 23, @06:41PM
from the [but-all-this-looted-cash-won't-do-much-harm](#) dept.

Supercomputing The Almighty Buck United States Politics
CWmike writes "Former Reserve Bank chairman Alan Greenspan has long praised technology as a tool to limit risks in financial markets. In 2005, he said better risk scoring by high-performance computing made it possible for lenders to extend credit to subprime borrowers. But today Greenspan told Congress that the data fed into financial systems was often a case of garbage in, garbage out. Christopher Cox, chairman of the Securities and

Exchange Commission, told the committee that bad code led the credit rating agencies to give AAA ratings to mortgage-backed securities that didn't deserve them. Explaining in his testimony what failed, Cox noted a 2004 decision to rely on the computer models for assessing a decision that essentially outsourced regulatory duties to Wall Street firms themselves."

✂ Vint Cerf: Big Changes Ahead for the Internet

<technews@HQ.ACM.ORG>

Fri, 24 Oct 2008 13:42:26 -0400

Mikael Ricknas, IDG News Service, 21 Oct 2008, via ACM TechNews, 24 Oct 2008

Google vice president Vint Cerf predicts that 2008 and 2009 will be the most important years for the evolution of the Internet. "This year and the next year are probably the most significant years for Internet's evolution that I can remember," Cerf says. The most significant change will be the transition to IPv6, which will offer more address space for the Internet as the number of IPv4 addresses are expected to run out in 2010. Cerf notes that IPv6 also is required to comply with user's requests to go into encrypted mode. Another large change is the implementation of a more secure domain name system that uses Domain Name System Security Extensions (DNSSECs). DNSSEC ensures that users who use a domain name hookup receive the correct IP address instead of something from a hacker. The Internet also will soon support internationalized domain names with non-Latin character sets. "This is a big change, because for the last 30 years the only thing you could use was Latin characters, and just the letters a through z, digits 0 to 9, and a hyphen," Cerf says. He says other changes that would make the Internet more useful include broadcast and support for multihoming, which would make it easier for users to have more than one Internet service provider.

http://www.infoworld.com/article/08/10/21/Big_changes_ahead_for_the_Internet_says_Vint_Cerf-IDGNS_1.html

[This clearly has the potential to improve many things. However, case sensitive characters, cyrillic characters (e.g., "o") and others that might easily be confused with Latin characters are likely to provide some new opportunities for phishers (fissures in the dike?). PGN]

✂ UW researchers uncover gap in border security

<Peter Gregory <petergregory@yahoo.com>>

Fri, 24 Oct 2008 07:46:03 -0700 (PDT)

Perhaps RFID-passport/ID card cloning is making it into the mainstream media. Not that this is anything at all new to this esteemed audience.

The end of the article says that the WA dept of licensing is looking into the matter - as though they have never heard of any of the RFID risks. Based upon their implementation, this may in fact be the case.

<http://www.komonews.com/news/33205899.html>

Peter Gregory, CISA, CISSP, DRCE | Risk Analyst and Manager | Published
Author, Columnist petergregory@yahoo.com | www.peterhgregory.com

Re: Computer likely caused Qantas plunge (RISKS-25.40)

<Dag-Erling Smørgrav <des@des.no>>

Fri, 24 Oct 2008 02:31:12 +0200

> ... in a 6,500-foot drop.

I have to retract that... it seems that it was in fact 650 feet, and
the source *I* consulted (I believe it was Sky News) added a zero.

Re: Computer likely caused Qantas plunge (Rieden, RISKS-25.38)

<Cameron Simpson <cs@zip.com.au>>

Fri, 24 Oct 2008 14:12:34 +1100

Or the aircraft's horizontal speed might be utterly irrelevant to the effects.

Several people were injured in this incident. For example, at:

<http://www.news.com.au/couriermail/story/0,23739,24460989-952,00.html>

we see stuff like:

The "ghost in the machine" malfunction which caused a mid-air drama
leaving 46 people injured has puzzled air safety investigators who
cannot recall a similar incident in aviation history. [...]

Passengers on board the flight have described haunting images of
children and babies hitting the ceiling of the plane.

While the incident left some with spinal injuries and others with
broken bones and lacerations [...]

At least 30 passengers and crew aboard QF72 were seriously injured -
some with spinal injuries and others with broken bones and lacerations

650 feet in 20 seconds is about 10m/s descent. It is irrelevant how
shallow the absolute angle was if the descent started abruptly enough
because acceleration can still be immense. Analogy: if you're on a bus
and someone swings a nasty uppercut at you, does the speed of the bus
matter?

Cameron Simpson <cs@zip.com.au> DoD#743 <http://www.cskk.ezoshosting.com/cs/>

Re: Computer likely caused Qantas plunge (RISKS-25.40)

<Adrian Edmonds <Adrian.Edmonds@stryker.com>>

Thu, 23 Oct 2008 23:08:32 -0700

Whilst working for a UK company specialising in fire detection/extinguishing we regularly received incident reports from the CAA. Whilst our main concern was fuel tank vent and dump systems I was struck by the number of airborne accidents involving turbulence. Some of these incident reports caused much hilarity on a Friday afternoon, especially the ones showing just what can happen with a food trolley and sleeping passengers I have always flown since then with my seatbelt firmly attached around my body.

Just like they say on the inflight safety announcements, keep your seatbelt on at all times.

Adrian Edmonds, Stryker GI,8 Haeshel Street,PO Box 3534, Caeserea 38900 ISRAEL
+972-73 737 4772

Re: Straight Party Voting Issues (Finegold, [RISKS-25.41](#))

<"David Phillips" <skydaver@gmail.com>>

Fri, 24 Oct 2008 09:35:11 -0400

Leonard Finegold passed on information about problems with straight party voting issues, undercounting, etc.

I can only speak to North Carolina, where I have lived & voted for 24 years. While we do have straight party voting available, and all of the potential problems from Leonard's post do exist, it is well publicized during each election cycle that a straight party vote will NOT select a presidential candidate, or any judicial candidates, or any of the non-partisan races on the ballot. I cannot remember whether this has always been the case since I moved here, but believe that it has.

Re: Straight Party Voting Issues (Finegold, [RISKS-25.41](#))

<Arthur Flatau <flataua@acm.org>>

Fri, 24 Oct 2008 09:37:09 -0500

It seems the problem with straight party voting here in Austin is perhaps a poor user interface (I have not yet voted this year, so I can I am making some conjectures based on past experience as well as this article from the Austin American Statesman: Ignore straight-ticket voting rumors, clerk says <http://www.statesman.com/news/content/news/stories/local/10/23/1023voterscam.html>)

Travis County uses Hart InterCivic eSlates machine, I believe that these are used fairly widely throughout Texas. The problem is, I believe, that when you vote straight party (presumably for either Democratic or Republican, although all the rumors seem to be about the Democratic party), it seems the machine merely selects all the Democratic candidates. If you then try to

vote for the Democratic Party candidate (Obama) or presumably any other Democratic candidate, you unselect that person. I am not sure that is all that bad a design (assuming it does work as I think). You are given a chance to review all of you selections before pushing the button to cast your vote. In any case, although there are major problems with electronic voting, including the Hart InterCivic eSlates this seems like at best a minor issue. You do have to be careful to review who you actually voted for, but this is true for any voting system, including paper ballots.

✈ Re: Remarkable -- United Airlines Stock (Nelson, [RISKS-25.38](#))

<John Levine <johnl@iecc.com>>

24 Oct 2008 00:01:53 -0000

> surely its 'sell' if the price exceeds an upper limit and 'buy' if its
> below the lower limit. After all, the purpose of the program is to make
> money, not to give it away!

No, Russ got it right. That's known as momentum investing. I don't think it makes much sense, but there are definitely people who do it.

John Levine, johnl@iecc.com, Primary Perpetrator of "The Internet for Dummies", Information Superhighwayman wanna-be, <http://www.johnlevine.com>, ex-Mayor



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 43

Wednesday 29 October 2008

Contents

- [Driver hits NIPSCO pole; surge fries sewage treatment plant](#)
[Shawn Merdinger](#)
- [Risks of escalating complexity: AA757 electrical power loss](#)
[David Leshner](#)
- [Schlage BrightBlue wireless lock controllers](#)
[Shawn Merdinger](#)
- [Computer screens out distress call from kidnap victim](#)
[David Tombs](#)
- [Finnish E-Voting System Loses 2% of Votes](#)
[Pertti Huuskonen](#)
- [Article on voting through American history](#)
The New Yorker via Harlan Rosenthal
- [Poison-pill auto-disclosure for security vulnerabilities](#)
[Paul Robinson](#)
- [They got us coming and going: tire monitoring](#)
[Paul Wexelblat](#)
- [Holistic Systems](#)
[Pierre-Jacques Courtois](#)
- [Twitter Jitters](#)
[Zachary Tumin](#)
- [Info on RISKS \(comp.risks\)](#)

Driver hits NIPSCO pole; surge fries sewage treatment plant

<"Shawn Merdinger" <shawnmer@gmail.com>>

Tue, 28 Oct 2008 22:31:05 -0400

http://www.chestertontribune.com/Town%20of%20Chesterton/driver_hits_nipsco_pole_surge_fr.htm

Kevin Nevers, Driver hits NIPSCO pole; surge fries sewage treatment plant

When a motorist, at approximately 12:11 a.m. on Sunday, struck a NIPSCO pole on Woodlawn Ave. just west of North Eighth Street, he not only interrupted

electric service to the Chesterton wastewater treatment plant, he caused a power surge which zapped into oblivion the whole of the plant's automated computer system. [Added note in archive copy: Chesterton, Indiana, USA]

Since early Sunday morning, Superintendent Steve Yagelski told the Town Council at its meeting Monday night, operators have been working the plant by hand, after the computer system known as SCADA -- tasked with running the facility automatically -- was fried and failed. Yagelski hastened to add that no by-pass occurred, thanks to the fact that a backup alarm system not connected to SCADA activated and alerted staffers.

One backup system which did not work, however, was the emergency power supposed to be provided by two generators. Yagelski told the Chesterton Tribune after the meeting that the surge was so powerful and comprehensive that SCADA failed before it could send the activation message to that pair of generators. A NIPSCO crew subsequently got those emergency generators running and then restored electric service to the plant as a whole. Now Yagelski is performing triage, trying to assess the damage done to the most critical components of the facility. "This is an unusual thing," he said. "We lost the entire plant. Virtually every breaker in the facility was blown and had to be re-set."

Yagelski expects the cost of replacing damaged computers and electronics to be considerable. "I have no idea at this point what it will cost," he said. "But I'm sure we're in the thousands of dollars." Yagelski added that he is "hopeful" that insurance -- the plant's or the motorist's -- will reimburse at least part of the expense. Until systems can be restored, though, operators will continue to "walk the plant around the clock" to keep it in operation.

✶ Risks of escalating complexity: AA757 electrical power loss

<"David Leshner" <wb8foz@panix.com>>
Mon, 27 Oct 2008 11:27:36 -0400 (EDT)

On 22 Sept, 2008 a AA 757 diverted to ORD with an in-flight electrical issue. It landed, not on the longest runway, skidding on locked brakes for thousands of feet. The pilot opted to angle off the runway near the end; I assume seeking better braking action in sod. [It worked.]
There was a long delay in evacuation as the crew could not get the engines to shut down (!?!?!).

The NTSB preliminary report is out, and it's got almost enough Risks to fill a sequel to PGN's book by itself:

<http://ntsb.gov/ntsb/brief.asp?ev_id=20081007X03940&key=1>

NTSB Identification: CHI08IA292

Greatly shortened, they had a "AIR/GRD SYS" alert message, consulted the Quick Reference Handbook, changed to a standby power configuration and continued. This configuration was battery powered, and they appear to have

thought from what the QRH said that the battery charger was still working.

It wasn't... and they later lost multiple systems, including some flight controls, interphone, PA, antilock brakes, thrust reversers, spoilers, AND engine shutdown controls.

An 747 & 757-qualified pilot for another carrier remarked that the manuals have gotten simpler and simpler over the decades. While such is inevitable given the orders-of-magnitude complexity difference between say a 727's three paralleled generators, and the multiple power buses on a 757 [They lost four buses out of many.] there is a price to pay -- "too simple" is not better than too complex.

I have to wonder about external tech support. Boeing has a 24x365 support center for in-flight problems, but in their previous strike, it was at least impaired if not inoperative. Did the crew ask for help?

✂ Schlage BrightBlue wireless lock controllers

<"Shawn Merdinger" <shawnmer@gmail.com>>

Mon, 27 Oct 2008 03:18:48 -0400

... power panel with HTTP interface. Oh, and Telnet is enabled by default and not covered very deeply at all in the installation manual.

http://www.brightblue.schlage.com/pdf/bbmanual_hardware.pdf

✂ Computer screens out distress call from kidnap victim

<"David Tombs" <tombs@bigpond.net.au>>

Tue, 28 Oct 2008 21:57:22 +1000

This tragic case was reported in the UK press a couple of weeks ago. Broadly, a teenage girl was abducted and later murdered. Under duress, she secretly and very bravely called the 999 emergency number on her mobile, hoping the operator would hear and understand the situation and organise a rescue. Unfortunately there is a function in the emergency response software to screen out and terminate calls where the caller does not speak clearly to the operator within a given time, which is what happened here. A log of the call was recovered later and the girl was obviously in distress.

The screening function is valuable in stopping accidental emergency calls clogging up the system. However in a minority of situations, like this one, it is the wrong thing to do, with life-critical consequences. This case seems to present another situation where the decision-making of a machine is wrongly preferred over a human. How well was the screening function specified, and what analyses of failure modes were undertaken?

"Hannah Foster, the A-level student kidnapped and strangled in 2003, called

999 in a desperate attempt to get help after she was abducted from the street, a court heard today. The 17-year-old dialed the emergency services, hoping that the operator would be able to hear the conversation with a man alleged to be Maninder Pal Singh Kohli, who was accused of snatching her after a night out with friends in Southampton, Winchester Crown Court was told. But Nicholas Haggan QC, prosecuting, told the jury that the operator could not hear what was being said and there was a system which disconnected the call after a short time to stop accidental emergency calls clogging up the system."

<http://www.telegraph.co.uk/news/uknews/3196048/Hannah-Foster-murder-Student-dialled-999-after-abduction-but-was-cut-off.html>

✶ Finnish E-Voting System Loses 2% of Votes

<Pertti Huuskonen <pertti.huuskonen@uta.fi>>
Wed, 29 Oct 2008 10:14:47 +0200

Finland has for decades used a reasonably efficient and transparent paper-based election process. Now we are experiencing almost a total ignorance of the e-voting issues already discussed in RISKS for years.

There have been many warnings from the nerds and IT crowd towards the government, but they have still decided to push for e-voting machines. Classic mistakes include dismissing paper records to verify individual votes and sourcing the infra from closed-source contractors. There was even a strikingly ignorant comment from the Minister of Justice, Ms. Tuija Brax, dismissing the reported problems in electronic voting as "science fiction".

<http://www.hs.fi/politiikka/artikkeli/Oikeusministeri+Brax+kiist==+s=hk=F6isen+==+nestyksen+uhat/1135239194037>
(in Finnish)

Now this incident below (232 unexecuted votes) is little more than a minor usability glitch, not a security issue, but gives an idea of the sloppy attitudes. Sounds like the voting system involved was never tested *with actual users*, just experts. Besides RISKS, this contractor has not been reading their basic usability testing books, either.

<http://www.ffi.org/blog/2008-10-28-finnish-evoting-votes-lost.html>

EFFi (Electronic Frontier Finland) are doing their best to keep the public aware here, though.

<http://www.ffi.org/blog/2008-09-01-evoting-report-in-english.html>

-- Pertti Huuskonen (bertil@gmail.com)

"Finland piloted a fully electronic voting system in municipal elections last weekend. Due to a usability glitch, 232 votes, or about 2% of all electronic votes were lost. The results of the election may have been affected, because the seats in municipal assemblies are often decided by margins of a few votes. Unfortunately, nobody knows for sure, because the Ministry of Justice didn't see any need to implement a voter-verified paper

record. The ministry was, of course, duly warned about a fully electronic voting system, but the critique was debunked as 'science fiction.' There is now discussion about re-arranging the affected elections. Thanks go to the voting system providers, Scytl and TietoEnator, for the experience."

<http://news.slashdot.org/article.pl?sid=08/10/29/0137202&from=rss>

[Also noted in part by Matti Siivola, and by Ian Oliver -- who noted the role of proportional (preferential) balloting. PGN]

***Article on Voting through American history (*The New Yorker*)**

<Harlan Rosenthal <harlan.rosenthal@verizon.net>>

Mon, 27 Oct 2008 12:18:16 -0500 (CDT)

http://www.newyorker.com/reporting/2008/10/13/081013fa_fact_lepore

includes discussion of "voter-fraud fraud" - and how parties in power try to change the vote by changing the voter lists.

<http://www.newyorker.com/online/blogs/hendrikhertzberg/2008/10/voter-fraud-fra.html>

Sounds suspicious -- unless you know that despite all the hysteria, from 2002 to 2005, only twenty people in the entire United States of America were found guilty of voting while ineligible and only five of voting more than once. By contrast, consider the lede on this story www.nytimes.com/2008/10/09/us/politics/09voting.html, published a week ago today: "Tens of thousands of eligible voters in at least six swing states have been removed from the rolls or have been blocked from registering in ways that appear to violate federal law, according to a review of state records and Social Security data by *The New York Times*."

***Poison-pill auto-disclosure for security vulnerabilities**

<Paul Robinson <paul@paul-robinson.us>>

Mon, 27 Oct 2008 02:15:20 -0700 (PDT)

I have thought of something regarding researchers who have made security discoveries, and I thought of a way in which they might legally develop, in effect, a 'poison pill' to those who would want to silence them. I'm not a lawyer and I don't know all of the exact requirements but I thought of an interesting way to cause "blowback" on those who try to browbeat others into silence.

A poison pill refers to a provision in a corporation's bylaws or charter that makes a takeover attempt by a suitor which management does not agree with to trigger a provision which essentially would cause the company to be too expensive for the acquirer. Sometimes done by allowing others than the acquirer to buy company stock at a much lower price, which requires the acquirer to buy even more stock of the company and raises the cost dramatically. So my thought was, why can't security researchers do that, so

that an attempt to do a 'hostile takeover' of the information triggers the poison pill defense, making the hostile takeover attempt of their information backfire worse than if they had tried to be civil and not institute legal proceedings.

Here's one way I think it can be done. My effort here is to make all actions legal so that nobody gets cited for contempt or commits a crime or otherwise violates the law in doing so..

Bob discovers some security hole in something, and sends a document with full and complete disclosure of the entire explanation including how to exploit, to Alice, who is not part of his team but is simply a third-party. His instructions are, as long as he keeps re-sending the full instructions to her, every day, to do nothing, but as soon as he stops sending the full instructions, to publish and disseminate the information as widely as possible. To ensure he has not been, say, grabbed by criminals, she is to presume any order from him to change this which does not include full disclosure to be a false order given under duress or to ignore unread any order not accompanied by the full, complete disclosure document..

Bob then publicizes the security hole either to the vendor to give them time to find a patch or makes a public announcement in a less than full manner.

Bob and his team are sued with a restraining order not to give out details to anyone else..

As a result, Bob is legally prohibited from sending Alice any documents because he can't send a full disclosure. As Bob has set up the instructions to Alice before he had any idea he would be sued, he isn't violating the order with what he sent because he sent it before the case was even filed or he was aware of it. So the only way that Bob can comply with the order, is to not send anything to Alice or not send the same document, which triggers the poison pill and she then posts the information everywhere she can.

The company suing can't come after Alice later, she's not releasing a trade secret nor was she under any obligation to do so. If it's Bob's paper, it's his copyright so she hasn't violated anything relating to the vendor either. Nor did she have any knowledge of the lawsuit, presuming that the lawsuit would have anything to do with her or that she would be a party to the lawsuit anyway.

Thus, if the vendor or the other party is civil and polite, either disclosure is delayed, or only a partial disclosure at the conference occurs, but a lawsuit causes automatic and unpreventable full disclosure.

If Alice is not an employee of Bob and has no legal responsibility to him, I don't see where she has any obligation to remain silent. She hasn't been served with any court order, only Bob has. She has no knowledge of why Bob stopped, only that he has. And if she's in another jurisdiction, the court might not even have authority to issue an order to her.

Or we can push this further by her doing the same thing and handing it off to a third party herself, so that if she doesn't continue to do so, or she AND Bob do not continue to send the complete document, that the third party

is to publish it.

Do this with two or three third parties each, and you essentially create a web of poison 'pill boxes' so that attempts to stop information do the exact opposite.

As I see it, the company wanting the information has to (1) sue bob; (2) get him to reveal whom he gave copies of the paper to; (3) find them and get service on them; (4) get them to reveal whom they gave copies to; and so on, and do this before the promise expires. And some of these people can be such that they are only reachable by e-mail, and despite what some people would like to have, one can't be served a court order by e-mail; there is no proof of delivery nor proof that the recipient saw it.

In some cases the vendor would have to go back to court, get a summons, serve it on Alice's ISP, get her information - if the ISP or mail service provider has any - then use that to find where Alice is and try to get good service on her. And do all of this before Bob's original request to her expires and she publishes.

Could even be done using a web site in which you have to keep re-uploading the same paper to prevent its publication. Once you've been served with a gag order, you can't do that any more and you have no means to stop the publication from taking place. In order to stop it, the company suing would, again, have to contact their ISP or look up the Whois page of the website owner (if it's theirs and not simply a nominee acting as party for service of process, or even simply a page seller who sells web space to people), contact them, and, presuming the company is in the same jurisdiction and can reach them - they have no legal obligation to answer the phone or read e-mail - to get them to stop the automatic publication. It's only if they can actually get good service on someone in person that it would really be significant to be able to force them to stop. Or have proven evidence that someone was notified of a legal proceeding where the court could have or get jurisdiction over them.

And if the party who answers for the website is simply an answering service or it's an answering machine, the party who gets the message might not get notice until after the document is published. As their website is automatic, they don't need to monitor it unless it reports something wrong. And if the website owner is in one jurisdiction but their webserver is in another then it may mean the company suing has to try to find yet someone else to stop that website.

Seems like an interesting scheme to thwart threats and from what I am aware of, legally sound although again, I'm not a lawyer.

They got us coming and going: tire monitoring

*<Paul Wexelblat <wex@cs.uml.edu>>
Sat, 25 Oct 2008 17:52:12 -0400*

I just bought a new car. When I went to Tিরerack.com to look at winter tires, I was informed of the TPMS (Tire Pressure Monitoring System) that appears mandatory as of 2007. This system typically includes an RFID-attached sensor in each wheel that sends data to a sensor that...

The issue is that it seems, according to <http://www.hexview.com/sdp/node/44> each one of these has a unique ID that would allow tracking of an individual vehicle. Unsubstantiated - by me, so far- research indicates that it is illegal to disconnect this system (federal) and that some states actually check operation at state inspections.

Vehicle tracking - speeding - big brother - sheer nosiness.

I'm sure that there is no need to further enumerate the risks to this audience.

P.M. Wexelblat PhD, Erst of the Dept. of Computer Science
University of Massachusetts Lowell, One University Ave, Lowell, MA 01854

[Are you *tired* of items on monitoring and the age of surveillance? If not, check out the extremely well-done five-part British series, "The Last Enemy" (with a massively cross-coupled database system called TIA), which concludes this Sunday on PBS's Masterpiece Theater. If you missed the first four episodes, don't start with the fifth. The plot is much too convoluted to grasp from the end, but should be quite relevant for RISKS readers. The series will apparently be available online "for a limited time" only. PGN]

<http://www.pbs.org/wgbh/masterpiece/lastenemy/index.html>

Holistic Systems

<Pierre-Jacques Courtois <pierre-jacques.courtois@uclouvain.be>>
Wed, 29 Oct 2008 12:07:51 +0100

PGN,

Looking through old issues of SIGSOFT, I just come across your 2006 article

<http://www.csl.sri.com/neumann/holistic.pdf>

(sorry for my slowness...), and just wish to let you know how much I agree with its conclusions and recommendations. It happens that I have a book just published:

<http://www.springer.com/engineering/production+eng/book/978-1-84800-371-2>

a main theme of which is precisely to advocate an hologrammatic approach to computer dependability justification. You are referenced in it, as an author, but for another of your contributions!

However, now that this book is completed, I have the feeling that a holistic approach for embedded computer systems may not be, as you cautiously suggest at the very end of your article, an "easier" challenge than in other disciplines. One reason perhaps is that the huge number of variables to be kept under control includes all those of the application supported by the computer system, and not only those, but also all those of the detailed inner levels of the software and hardware implementation.

Pierre-Jacques Courtois BEL V (Fed. Agency for Nuclear Control Subsidiary)
Rue Walcourt, 148, B-1070 Brussels, Belgium <http://www.belv.be/> +32 2 5280 268
Louvain School of Engineering Universite' catholique de Louvain B-1348
Louvain - la -Neuve, Belgium, Phone: +32 10 47 31 50
Home page <<http://www.info.ucl.ac.be/Bienvenue/PagesPersonnelles/courtois/>>

[P-JC, I think it is an enormous challenge practically speaking. But it might be aided by being somewhat less obscured by politics; also in the research communities at least, some of the architectural and software engineering issues and other precursors are perhaps less contentious.
PGN]

Twitter Jitters

<zachary_tumin@harvard.edu>
Wed, 29 Oct 2008 09:37:38 GMT

Last week a report by the US Army's 304th Military Intelligence Battalion roiled government social web (web 2.0) advocates. The microblogging service Twitter, it found, can be used as a potent tool by terrorists. There followed some handwringing on Twitter and among journalists, and even some thinking across the river -- here at Harvard.

Will this dustup affect the move to the social web in the defense and intelligence communities -- wikis, blogs, Facebook, and the like? After all, there's been good movement in recent months, impressive gains, and some major wins. But there's been little enterprise wide embrace. To many, the current position feels unstable. [... Long item truncated. Read the rest of Zachary's blog item at <http://www.lnwprogram.org/blog/>. PGN]

REVIEW: "Security Engineering", Ross Anderson

<"Rob, grandpa of Ryan, Trevor, Devon & Hannah" <rMslade@shaw.ca>>
Mon, 27 Oct 2008 12:20:02 -0800

BKSECENG.RVW 20080929

"Security Engineering", Ross Anderson, 2008, 978-0-470-06852-6,
U\$70.00

%A Ross Anderson ross.anderson@ieee.org rja14@cam.ac.uk

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

%D 2001

%G 978-0-470-06852-6 0-470-06852-3

%I John Wiley & Sons, Inc.

%O U\$70.00 416-236-4433 fax: 416-236-4448

%O <http://www.cl.cam.ac.uk/~rja14/book.html>

%O <http://www.amazon.com/exec/obidos/ASIN/0470068523/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0470068523/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0470068523/robsladesin03-20>

%O Audience i+ Tech 3 Writing 2 (see revfaq.htm for explanation)

%P 1040 p.

%T "Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition"

Anything written by Gene Spafford is important. Anything written by Bruce Schneier is readable, and, even if you disagree with it, worth thinking about. Anything written by Ross Anderson is important, readable, worth considering, and correct.

The preface states that this book is intended as a text for self-study or for a one term course, a reference for professionals, an introduction to the underlying concepts, and an original scientific contribution in terms of the foundational principles for security engineering. In addition, the preface to the second edition notes that these concepts now need to be understood by legal investigators, managers, and, in the wake of 9/11, everyone. A very tall order to fulfill, but one which, for once, seems to have been accomplished. I have often been asked, in regard to these reviews, whether there are, in fact, any books that I do like. Well, I like this one. If you are involved with security and you haven't read "Security Engineering," you should. And you have no excuse if you haven't. This is the second edition to be printed, and the first edition is available online, in its entirety.

(And, if the first edition is available online for free, why should you buy the second? Because the second edition has more, in almost every respect.)

Part one deals with the basic concepts of engineering and security. Chapter one presents four example situations of security needs. Protocols are not limited to the precise but limited structures with which computer people are familiar. Security is a people problem, and chapter two, entitled "Usability and Psychology," addresses this issue up front, along with a set of more conceptual, but more formal, authentication problems and protocols. It is unlikely that the models presented exhaust the field, but some thought indicates that they are pertinent to a wide variety of applications. Much the usual thoughts and advice on passwords is issued in chapter three, although the research is better documented, and some additional research (passphrase generated passwords are as secure as randomly assigned ones, and as memorable as naively chosen ones) is presented. (Anderson's writing is clear enough, but he does betray a taste for symbolic logic that might limit the audience for the book. Still, perseverance on the part of the reader will be amply rewarded.) It is strange not to see any mention of the work factor of passwords overall. Chapter four reviews access control, but primarily from the perspective of system and hardware internals. Cryptography, in chapter five, is covered reliably and well, although the structure and flow of the material is not always in developmental order. The problems of distributed systems are examined; in terms of concurrency, failure resistance, and naming; in chapter six. Economics can be used to examine a great many aspects of security (and insecurity). Chapter seven looks at a number, but I was disappointed to note that risk analysis was not one of them.

Part two uses a number of applications of secure systems to introduce

particular concepts or technologies. Chapter eight discusses multilevel security, which encompasses most of the formal security models such as Bell-LaPadula. Medical (and census) databases are used, in chapter nine, as examples of multilateral, or compartmented, security: the need to deal with information of equal sensitivity, but restricted to different groups. Controls particularly related to the banking system and fraud are presented in chapter ten, although the material is long on anecdotes, and contains weaker analysis than the preceding text. A somewhat limited, but still interesting, review of physical security has been added in chapter eleven. Chapter twelve reviews monitoring systems, of both monitoring and metering types. In regard to nuclear command and control systems, chapter thirteen examines the tension between availability (the ability to fire a missile) and confidentiality (or authentication: making sure nobody else does). Various aspects of the technology for security printing and seals is dealt with in chapter fourteen. Biometrics, in chapter fifteen, gets a good, but fairly standard, treatment. Chapter sixteen delves into tamper-resistance in cryptographic gear and smartcards (expanding on the content of fourteen). The TEMPEST and Teapot (no, I'm not kidding) projects on emission security are reviewed in chapter seventeen. Chapter eighteen examines the security problems inherent in the use of application programming interfaces (APIs). There is good coverage of the basics of traditional electronic warfare in chapter nineteen, although the material on information warfare is not as thorough. Chapter twenty looks at telecommunications system security, with some material on phone phreaking and lots on cellular encryption. Network attack and defense, in chapter twenty-one, is less focused than other chapters, and adds malware. Copyright and DRM (Digital Rights Management) systems are examined in chapter twenty-two, with solid coverage of recent controversies. Gaming, social networks, elections, and other complex applications are discussed in chapter twenty-three.

Part three turns to politics, management, and assurance. Chapter twenty-four, under the title of "Terror, Justice, and Freedom," has a fascinating discussion of major issues in public policy. Management issues, in chapter twenty-five, are presented in an interesting but generic manner. The discussion of system evaluation and assurance asks the usual question in regard to how we know our systems are secure. In a sense, though, the subtitle of the book is wrong: much of the material points out how **not** to build dependable systems, and chapter twenty-six is a bit disheartening. The conclusion, in chapter twenty-seven, is that we need more engineers and engineering.

Although the material is presented in a very formal way, the writing is usually quite readable, and the exceptional stilted passages are still accessible to the determined reader. On occasion, one could hope for additional explanations of some items that are mentioned briefly and passed over. The constant emphasis on how security protections have failed can be depressing, but the examination of the errors of others does provide the basis for better designs in the future.

copyright Robert M. Slade, 2002, 2008 BKSECENG.RVW 20080929
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
victoria.tc.ca/techrev/rms.htm blogs.securiteam.com/index.php/archives/author/p1/



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 44

Saturday 8 November 2008

Contents

- [U.K. NHS computer system "grinds to a halt"](#)
[Richard Cook](#)
- [Risk of repairing Hubble too soon](#)
[Ted Blank](#)
- [New GPS satellite may crash some receivers](#)
[William P.N. Smith](#)
- [Risks of unilingual vacation-reply messages](#)
[Mark Brader](#)
- [US court throws out most software patents](#)
[John Oram via Monty Solomon](#)
- [Beware: T-Mobile's Voicemail Paging Trap](#)
[Lauren Weinstein](#)
- [Re: BBC Domesday Project](#)
[Mike Tibbetts](#)
- [Re: Treasury Office Faults IRS Computer Security](#)
[Paul Robinson](#)
- [Computers Freedom & Privacy Conference 2009 - Request For Proposals](#)
[Bruce R Koball](#)
- [REVIEW: "Handbook of Research on Technoethics", Luppicini/Adell](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

U.K. NHS computer system "grinds to a halt"

*<Richard Cook <ri-cook@sbcglobal.net>>
Mon, 03 Nov 2008 11:11:07 -0600*

The Financial Times reports that implementation of the National Health Service's enormous healthcare information technology (HIT) system has been halted after incapacitating difficulties with a few installed sites. The 12.8 billion-pound (~US\$21 billion) system has been plagued by difficulties including the withdrawal of one chief supplier, Accenture, in 2006 and the dismissal of a second, Fujitsu, in May of this year. The FT's report was

denied in a carefully worded statement from Ms.

Christine Connelly, the U.K.'s CIO for Health, who has been in her present position for just one month. She noted that the system was still be tested and that its deployment needed to be delayed it was possible to "fix technical issues but also to manage the impact on working practices". The government side of the project has been remarkable for senior staff changes.

The Tory opposition has been quick to point out the project's shortcomings. Mr. Stephen O'Brien, shadow minister for health, is described the program as "hugely expensive" and "desperately behind schedule". MP Nick Clegg questioned PM Gordon Brown about "an NHS computer system that doesn't work" in the House of Commons but Mr. Brown's reply included only a lukewarm defense of the system. The government's Department of Health referred questions to "Connecting for Health" (previously identified as *NPfIT* for The National Programme for IT) which reportedly claimed that "things are moving, but slowly".

According to the FT, the National Audit Office has said that the program is four years late. More importantly, key portions of the system have not been field tested and only a few hospitals are actually using the system for patient care. Only one "big acute care hospital has turned on a version of the new system since May." An internal NHS document reportedly titled "Lessons Learnt from the Royal Free Hospital Emergency Department" reveals many, unaddressed problems with the clinical system intended to support emergency services.

In 2005, Fujitsu and Cerner were contracted to supply key portions of the system, replacing software vendor IDX because of poor performance. Fujitsu was fired in May of this year, a move which may have cost the company as much as 300 million pounds of its 896 million pound contract. Cerner's software was "bred in the US market... as a billing system that was being turned into a Patient Administration System" according to one critic quoted in the Inquirer.

Another key element of the system is the Lorenzo Patient Management System, developed by iSoft. Problems with Lorenzo have delayed its go live in U.K. hospitals. The software is being built mainly in India for Computer Sciences Corporation (CSC) and its subcontractor IBA Health which acquired iSoft. According to ComputerWeekly.com, NHS Connecting for Health staff said in June that "Lorenzo is being rigorously tested at early adopter sites with differing care settings and geographies to ensure it meets the necessary quality criteria and is relevant to the needs of diverse healthcare communities prior to going live within a working healthcare environment." According to The Guardian, Lorenzo was at the time of the statement "mired in development glitches and is still struggling to get out of the technical design phase".

A major point of contention has been the tough contracts that prevent suppliers from being paid until the systems are working. Major suppliers, including BT, CSC, Fujitsu, Cerner, iSoft and others had earned only 1.29 billion pounds despite a business plan that expected them to have been paid 2.819 billion pounds by March.

Perhaps not surprisingly, despite the widely acknowledged failure of the system itself the main suppliers and Connecting for Health continue to tout the benefits of IT. On October 22nd, Connecting for Health announced that standardized, electronic records will improve patient safety. According to the CSC website "NPfIT will improve the NHS and benefit all those who work in it and who use it by ensuring that the right information about a patient is available to the right people at the right time. It will improve the quality of time spent with patients by significantly reducing the administrative burden on clinicians and healthcare professionals."

✂ Risk of repairing Hubble too soon

<"Ted Blank" <tedblank@gmail.com>>
Thu, 30 Oct 2008 18:47:16 -0400

Perhaps the operators on the Hubble should roll the dice and engage in some maneuvers which stress the vehicle slightly outside of normal limits to see what else is close to breaking so it can also be fixed on the repair mission. Of course if this goes too far, the only choice for Hubble repair might be long tow to the ISS (International Service Station) for its tune-up. Who has their AAA card?

✂ New GPS satellite may crash some receivers

<"William P.N. Smith" <w_smith@compusmiths.com>>
Sat, 01 Nov 2008 10:03:15 -0400

In the November 2008 issue of *BoatU.S.* magazine, there's a reference to a new GPS satellite being switched on. It uses the identifier "PRN 32", which causes some [...] Northstar GPS units to "become confused" and "shut down".

Fortunately, there are firmware updates available, though in some cases they cost money. Unfortunately, most boaters wouldn't know a firmware update if they hooked one, so there will undoubtedly be accidents and other problems, and GPS units "acting flakey" (they only crash when that particular satellite is in view) that will be replaced unnecessarily.

Oops!

✂ Risks of unilingual vacation-reply messages

<msb@vex.net (Mark Brader)>
Fri, 31 Oct 2008 15:45:44 -0400 (EDT)

The council of Swansea, Wales, decided to have a certain road posted "No entry for heavy goods vehicles. Residential site only". Official road signs

in Wales today must be in Welsh as well as English, so the English text was emailed to the council's translation office.

And in due course a sign was erected with text in Welsh -- whose meaning was: "I am not in the office at the moment. Please send any work to be translated."

See <http://news.bbc.co.uk/2/hi/uk_news/wales/7702913.stm>.

(Note incidentally the comment in the article to the effect that they should have consulted an expert. Well, that's what they *were* doing -- the real problem was that a person who translates things into a certain language has no business having a vacation notice that's only in that language. In other words, the failure notice failed to be identifiable as out-of-band.)

This all reminds me of the restaurant in Beijing whose name in English is apparently signposted as "Translate Server Error". (Pictures of it have been circulating on the Internet for a while, but I don't know if they are genuine.)

[Also noted by Peter Zilahy Ingerman. PGN]

✂ US court throws out most software patents, John Oram

<Monty Solomon <monty@roscom.com>>

Fri, 31 Oct 2008 22:29:43 -0400

John Oram, Microsoft has a problem, *IT Examiner*, 31 Oct 2008

Much of the patent portfolio of some of the world's biggest software companies has become worthless overnight, thanks to a ruling yesterday by the US patent court.

The US Court of Appeals for the Federal Circuit (CAFC) in Washington DC has decided that in the future, instead of automatically granting a patent for a business practice, there will be a specific testing procedure to determine how patentable is that process.

The decision is a nearly complete reversal of the court's controversial State Street Bank judgment of 1998, which started the stampede for patenting business practices.

<http://www.itexaminer.com/us-court-throws-out-most-software-patents.aspx>

<http://www.groklaw.net/pdf/07-1130.pdf>

✂ Beware: T-Mobile's Voicemail Paging Trap

<Lauren Weinstein <lauren@vortex.com>>

Sun, 26 Oct 2008 11:18:33 -0700

Beware: T-Mobile's Voicemail Paging Trap

<http://lauren.vortex.com/archive/000448.html>

Greetings. Longtime users of T-Mobile may already be familiar with this issue that I'm about to describe, but with many persons now moving to T-Mobile from AT&T to get hold of the Google Android G1 phone, lots of these new subscribers may be in for a disappointing surprise, especially if you use your phone for business purposes and rely on a clear and concise outgoing voicemail announcement.

One of the basic rules of human interface design is that you don't want to ever offer callers options that don't actually work as described. T-Mobile violates this concept big time for the overwhelming majority of calls into their voicemail system, and in a manner that could have potentially very serious results.

The problem is essentially simple. All callers who hear your personalized voicemail outgoing message are then offered the opportunity to send a numeric page ("press 5"). Unfortunately, this paging prompt is presented to everyone hearing your voicemail message, *even when you have paging turned off* -- which is in fact the default state.

This is more than an annoyance to callers who sit through additional verbiage waiting for a beep, it can result in misunderstandings and worse:

"I entered my number for a page -- I needed to reach you right away! Why the blazes didn't you call back?"

"Oh, I have paging turned off."

"Then why the hell did the system offer me a page and have me waste my time entering my call back number? Who designed that blasted thing? The Three Stooges?"

Actually, that's unfair to Larry, Moe, and Curly -- I'm sure they could have done a better job of voicemail system design than T-Mobile's vendor.

This isn't rocket science. Don't jerk callers around telling them that they can page and then put them through the motions of entering call back numbers in a useless exercise reminiscent of the Mad Tea Party from "Alice in Wonderland," especially since we can be sure that only a tiny percentage of subscribers ever actually want to use paging at all.

It's notable that AT&T Mobility does this right. You can always configure an AT&T cellular line so that if paging is off, there is no prompting for paging call backs. In fact, AT&T's cellular voicemail system can be configured just to play your outgoing message and beep without any prompting verbiage at all being added onto the end -- which is the ideal situation in most cases.

It's incredible for T-Mobile to operate a voicemail system that makes it impossible for them to avoid confusing callers with false prompting options and actions that are at best ineffectual -- and can easily lead to serious

problems indeed when assumed paging actions never actually take place.

Achtung T-Mobile! You pride yourself on your customer service. But this behavior of your voicemail is sloppy, consumer-unfriendly, and in some situations perhaps even dangerous. You can do much better.

Lauren Weinstein, +1 (818) 225-2800 <http://www.pfir.org/lauren>
Co-Founder People For Internet Responsibility - <http://www.pfir.org>
Co-Founder NNSquad Network Neutrality Squad - <http://www.nnsquad.org>
<http://lauren.vortex.com> lauren@vortex.com or lauren@pfir.org

Re: BBC Domesday Project (Leeson, [RISKS-21.93](#))

*<"Mike Tibbetts" <Mike.Tibbetts@scotent.co.uk>>
Tue, 4 Nov 2008 12:44:47 -0000*

By chance I came across PGN's list of risks "Illustrative Risks to the Public in the Use of Computer Systems and Related Technology" (<http://www.csl.sri.com/neumann/illustrative.html>) on the Internet and found a reference to the BBC Domesday Project and the public reports that the Laservision discs produced in the 1980s were no longer readable and so the data is lost. As have other commentators, Nick Leeson cites this as another example of the risks to the public interest in the use of computer technology.

I'd like to put the record straight - about the BBC Domesday Project, at least.

I was one of the two people who conceived the BBC Domesday Project which began in 1984 and completed in the Autumn of 1986. I was in overall charge of its practical realisation. I do not intend any criticism of you or any of the other academics who have highlighted our project as an example of lack of foresight but I have been repeatedly stung by such criticisms because, in fact, nothing could be further from the truth. However, it is not my personal pique which is the important issue here but the fact that dismissing us as unthinking technocrats with no forward vision or sense of national heritage actually masks what I believe to be the real problem about data preservation and of which I think the BBC Domesday Project is indeed a good exemplar, but not as currently presented.

At the time we put the Domesday Project together in 1984, we in the BBC did our utmost to ensure that what we were doing could be preserved for the future, irrespective of technological evolutions. From the very first we worked in close collaboration with the UK National Data Archive which was funded by the UK's Economic and Social Research Council and housed at the University of Essex in East Anglia. The Director of the National Data Archive at that time was Professor Howard Newby, now Vice-Chancellor of Liverpool University. From day one, Professor Newby was one of four senior academics we invited to be on a steering committee which was the main source of guidance on policy and academic rigour for the project.

As you probably know, the BBC Domesday Project successfully completed the compilation and publication of two twelve-inch Laservision discs. In a world which still awaited the introduction of usable Wintel PCs, CD-ROM, MP3 audio, M/JPEG video or Internet technology, we had to innovate much of the technology which made our venture possible. We collaborated with Philips to adapt their Laservision technology to allow digital data to be encoded in the stereo soundtrack of their analogue videodisks. We used the BBC Microcomputer which, as a previous collaboration between BBC TV engineers and Acorn Computers, had a 625-line video output and was therefore uniquely conformable with an analogue PAL TV signal. The material on the disks contains a massive collection of material to portray every aspect of the UK in the early 1980s, including 10,000 Ordnance Survey maps, 200,000 photographs, local descriptions and survey returns from an estimated 1 million members of the UK population, hundreds of video clips from the BBC and other media archives, newspaper and magazine front pages, commissioned essays from key experts, the contents of virtually every government department's computer archive statistically re-structured into datasets to provide maximum intercomparability, surrogate journeys through a whole range of environments from council flats to rural farms. All this was catalogued and indexed by a massive system designed and implemented by the then-chairman of the UK Society of Indexers.

Enough, already. I could bore for Britain about those two years in the mid-eighties.

In sharp contrast to the way we are portrayed now by some commentators, we were always acutely aware of the volatility of the hardware and software we had used to implement the Domesday Project and the need to preserve this unique archive for the future. Knowing that our project was coming to an end we transferred the master tapes and server files for everything we had compiled, including all our working documents and enabling software to ... the National Data Archive under the supervision of Professor Newby.

Following the completion of the Domesday Project the BBC attempted to continue the work on interactive media by converting our team into a new unit to be called the Interactive Television Unit and I was offered the position of being its first Editor. However, in common with others, I had come to realise how far ahead of our general time the Domesday Project was and therefore likely to be marginalised within a traditional broadcasting organisation. I moved on from the BBC and a couple of years later the ITU was disbanded.

Eighteen or so years later I began to hear about a project instigated by a Northern UK university to "rescue" the Domesday Project data because, as we had always known, our idiosyncratic Philips "LV-ROM" player (of which only about a thousand were ever sold thanks to Philips' exorbitant end-user price) had virtually ceased to exist and copies of the plastic disks were approaching unreadability. I immediately went to the National Data Archive website to assure myself that our original masters had been preserved, only to find no record of them! Although I was not personally involved in the "Camileon" rescue project, I understand that those people also failed to find any trace of the original material in the National Archive and work began to try and re-create methods to retrieve the data from remaining copies of the disks and bits and pieces of resource in personal collections.

The rescue in conjunction with the UK National Archives (the old UK Public Records Office and different to the National Data Archive) was partially successful and a reconstruction of the material on one of the two Domesday disks was completed and made available as an online resource. This was the part of the Domesday Project where a large number of local volunteers (including 50% of ALL the primary and secondary schools in the country) collaborated to survey, comment on and photograph their local communities and compile entries for the "Community Disk". This material covered over 100,000 square kilometers of the UK land surface and accounted for over 60% of the populated areas of the UK. I assumed that this web-based reconstruction of the Community Disk would be carefully preserved by the National Archives at Kew in London who had part-funded the reconstruction.

But no.

I hear that the instigator of the Community Disk rescue project has sadly died and his web-page which used to link through to the web-enabled reconstruction no longer functions. I have asked other members of the original team and no-one seems to know where, if anywhere, this can now be accessed.

Neither of the websites of the National Data Archive nor the National Archives contain any reference to substantial holdings of the Domesday Project material, either in its original or reconstructed form. The National Archives only refer to some digi-beta tapes holding some of the imagery from the Community Disks.

So, after this extended diatribe, what's my point?

Basically that the fault in all this lies not in the lack of vision or foresight by the technologists but that, at least in the UK, the national systems of data preservation and heritage archiving simply don't work reliably or consistently. We lodged our original material with the official national conservators and, so far as I can tell, they seem to have lost it! More importantly the fruits of a major national effort to retrieve some of the material also seems to have disappeared from the public radar after only a year or two, even though relevant national bodies were involved in the reconstruction.

Referring to the risks in the title of PGN's list, I respectfully suggest that, for the Domesday Project at least, the risks do not really trace to the use of computers but in the inadequate procedures for effective national curation and conservation of information assets. More importantly, blaming the technocrats shifts the focus away from where, in my opinion, probing questions from authoritative people like yourself might more properly be directed.

This e-mail has extended far longer than I intended and I apologise for taking up your time (if you have persisted to the end!). If you care to respond I would be very interested in your thoughts.

Mike Tibbetts, 62 Prestonfield, Milngavie, Glasgow G62 7PZ

+44 (0)141 570 1782 :mike.tibbetts@scotent.co.uk

Re: Treasury Office Faults IRS Computer Security (PGN, [RISKS-25.40](#))

<Paul Robison <rfc1394@yahoo.com>>
Sun, 2 Nov 2008 11:35:16 -0800 (PST)

> Both systems are gradually being put into use. CADE, expected to cost more
> than \$1 billion through 2012 to develop and operate, this year processed
> about 20 percent of the 142 billion returns filed.

142 Billion pages, would mean a tax return averaging 473 pages each for every man, woman, and child in the U.S. (300 million people).

142 Billion returns, about 20 times the entire world population!

142 Million returns, completely believable.

Computers Freedom & Privacy Conference 2009 - Request For Proposals

<Bruce R Koball <bkoball@well.com>>
Sun, 2 Nov 2008 19:08:23 -0800 (PST)

Request For Proposals, Washington, DC, June 1-4, 2009

The 19th annual Computers, Freedom, and Privacy conference is now accepting proposals for panels, workshop sessions, and other events.

CFP is the leading policy conference exploring the impact of the Internet, computers and communications technologies on society. It will be taking place in June 2009, just months into a brand new U.S. administration - an exciting moment in history, as we look into the future and ask, "Where do we go from here?" For more than a decade, CFP has anticipated policy trends and issues and has shaped the public debate on the future of privacy and freedom in an ever more technology-filled world. CFP focuses on topics such as freedom of speech, privacy, intellectual property, cybersecurity, telecommunications, electronic democracy, digital rights and responsibilities, and the future of technologies and their implications.

We are requesting proposals and ideas for panels, plenaries, debates, keynote speakers, and other sessions that will address these and related topics and how we can shape public policy and the public debate on these topics as we create the future.

We especially encourage proposals that:

- * Take advantage of our Washington, DC location
- * Shed light on what we can expect from the new administration
- * Incorporate a global and international perspective
- * Focus on the future and what we can expect in the years to come in technology and policy

- * Include debates or otherwise present challenging points of view
- * Inform attendees about cutting-edge technologies and issues

However, we encourage proposals in all areas. The more complete and fleshed out a proposal, the more likely it will be accepted - but we welcome the submission of all good ideas.

To submit a proposal or idea for CFP 2009, please go to <http://www.cfp2009.org/submissions/subguide.html>

Many thanks and we look forward to your ideas and your participation!

CFP 2009 co-chairs, Jay Stanley and Cindy Southworth

REVIEW: "Handbook of Research on Technoethics", Luppicini/Adell

<Rob Slade <rmslade@shaw.ca>>
Mon, 3 Nov 2008 11:08:37 -0800

BKHRTCET.RVW 20081002

"Handbook of Research on Technoethics", Rocci Luppicini/Rebecca Adell,
2009, 978-160566022-6, U\$495.00

%E Rocci Luppicini

%E Rebecca Adell

%C Suite 200 701 E. Chocolate Ave., Hershey, PA 17033-1117

%D 2009

%G 978-160566022-6

%I IRM Press/Idea Group/IGI Global

%O U\$495.00 800-345-432 717-533-8845 cust@idea-group.com

%O <http://www.amazon.com/exec/obidos/ASIN/1605660221/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/1605660221/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/1605660221/robsladesin03-20>

%O Audience n Tech 1 Writing 1 (see revfaq.htm for explanation)

%P 1028 p. (2 volumes)

%T "Handbook of Research on Technoethics"

The (very brief) preface states that the work is for students, instructors, researchers, ethicists, technology scholars, and just about everybody.

Unfortunately, all it has to say about the topic is that it is broad.

Ultimately, this is a compendium of papers related to ethics related to technology (sometimes).

Even in the more detailed attempt to define technoethics, in the first article, the authors have to admit that there is little agreement on the term: that some see it as the special responsibility of technologists and engineers, while others extend it to behavioural standards for the new global community. A "conceptual map" of the topic is presented at one point. In some attempt to be cute the topics are overlaid on a map of Europe, but the specific subjects are laid out in almost random fashion, primarily covering computer ethics and related ideas, but extending somewhat

into biomedical areas. (One of the more interesting papers examines the ethics of performance enhancement technologies in sports.)

The essays are divided into broad categories: theoretical frameworks, areas of research, case studies, emerging trends, and further reading. The titles of the sections do little to differentiate the contents of the pieces. In the section on theoretical frameworks, for example, one paper describes Lawrence Kohlberg's theory of moral development, while another briefly notes John Rawls' theory of social justice: the other five essays are generic introductions to ethics in technical arenas. (The article looking at Kohlberg is merely an overview of his philosophy, without any real relation to technology. Similarly, a later treatise is simply an explanation of podcasting, without any relevance to ethics at all.) There does not appear to have been any attempt to structure topics in advance, but rather to attempt to arbitrarily impose some kind of organization after the fact. Therefore, while some of the treatises are detailed and well written, most are vague and simplistic. There are different examples and focus in various papers, but there is an enormous amount of duplicate content, particularly in terms of basic concepts.

The range of examples might be interesting or useful for broad discussions of ethics in a technical environment. However, it is hard to imagine an audience that would benefit from this work, rather than a number of others that would be more valuable at less cost (even when considered in total). Deborah Johnson's "Computer Ethics" (cf. BKCOMPETH.RVW) is limited to information technology, true, but it is more complete in that field. Herman Tavani's "Ethics and Technology" (cf. BKETHTECH.RVW) is more structured and foundational. The addition of a decent text on bioethics would equal or exceed the content of these volumes, and be easier on the pocketbook. (Or is it immoral to contemplate such base considerations?)

copyright Robert M. Slade, 2008 BKHRTCET.RVW 20081002
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
victoria.tc.ca/techrev/rms.htm blogs.securiteam.com/index.php/archives/author/p1/



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 45

Monday 17 November 2008

Contents

- [Chinese hackers breach white house computer systems](#)
[PGN](#)
- [Hacker Tool Targeting MS08-067 Vulnerability](#)
[Websense via Monty Solomon](#)
- [Lose the BlackBerry? Yes He Can, Maybe: President-Elect Obama](#)
[Jeff Zeleny via Monty Solomon](#)
- [Texas Suspends Massive Outsourcing Contract](#)
[Keith Price](#)
- [Driver Blames GPS System For Car-Train Collision](#)
[Paul Saffo](#)
- [Stop! Buses only! --What do you mean, you ARE a bus?](#)
[Mark Brader](#)
- [Martian deep freeze: NASA's Mars Lander dies in the dark](#)
[Sharon Gaudin via PGN](#)
- [The "Two Focaccia Buttons Defense"](#)
[Robert Hall](#)
- [Risks of assuming constant hours in a day](#)
[Toby Gottfried](#)
- [Excel auto-formatting](#)
[David Magda](#)
- [Texting bug hits the Google phone](#)
[Amos Shapir](#)
- [Vintage IBM tape drive in Apollo moon dust rescue](#)
[Chris Leeson](#)
- [gnus-mime-print-part vs. Mom's room](#)
[jidanni](#)
- [False security from privacy screens](#)
[David Alan Gilbert](#)
- [Re: BBC Domesday Project](#)
[Martin Ward](#)
[Theo Bucher](#)
- [Re: Poison pill auto-disclosure](#)
[Terje Mathisen](#)
[Al Macintyre](#)
[Richard O'Keefe](#)

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

Chinese hackers breach white house computer systems

<Peter G. Neumann" <neumann@csl.sri.com>>
Sun, 16 Nov 2008 18:44:23 PST

Chinese hackers have penetrated the White House computer network on multiple occasions and obtained e-mails between government officials, a senior US official told the *Financial Times*. On each occasion, the attackers accessed the White House computer system for brief periods, allowing them enough time to steal information before US computer experts patched the system. US government cyber intelligence experts suspect the attacks were sponsored by the Chinese government because of their targeted nature. But they concede that it is extremely difficult to trace the exact source of an attack beyond a server in a particular country. "We are getting very targeted Chinese attacks so it stretches credulity that these are not directed by government-related organisations," said the official. [Source: The *Financial Times* website has items by Demetri Sevastopolu, dated 7, 8, and 17 Nov 2008. The above text is an excerpt from the most recent. PGN-ed]

Hacker Tool Targeting MS08-067 Vulnerability

<Monty Solomon <monty@roscom.com>>
Tue, 11 Nov 2008 12:37:35 -0500

Websense Security Labs has noticed a special hacker tool in China. In the past few weeks, Microsoft has announced and released a patch for the MS08-067 vulnerability, and a hacker tool named "wolftooth bot catcher" has been widely used by hackers to attack machines running Windows operating systems without the KB958644 patch. Our write up of the original vulnerability details can be found here. 11 Nov 2008.

<http://securitylabs.websense.com/content/Blogs/3237.aspx>

<http://securitylabs.websense.com/content/Alerts/3218.aspx>

Lose the BlackBerry? Yes He Can, Maybe: President-Elect Obama

<Monty Solomon <monty@roscom.com>>
Sun, 16 Nov 2008 15:53:42 -0500

President-elect Barack Obama will have to give up his habitual use of his BlackBerry when he becomes president -- largely because of the Presidential Records Act (but presumably also because of its inadequate security). His use of e-mail is likely to also be constrained. However, he apparently intends to be the first president with a laptop on his desk. [Source: Jeff Zeleny, *The New York Times*, 16 Nov 2008; PGN-ed]

<http://www.nytimes.com/2008/11/16/us/politics/16blackberry.html>

[Recall previous items (RISKS [RISKS-19,29,32,33](#)) regarding the ban against laptops on the Senate floor: fears of surfing, lobbyists, spamming, real-time on-line influence, etc., eschewing possible benefits of being able to search through pending legislation and to better communicate! PGN]

✶ Texas Suspends Massive Outsourcing Contract

<Keith Price <price@usc.edu>>
Thu, 30 Oct 2008 15:12:40 -0700

Late last week, the *Dallas Morning News* ran a story about a massive computer crash that destroyed hundreds of Texas Attorney General Greg Abbott's confidential documents which may prevent scores of Medicaid fraud prosecutions. ...

This was noted in the IEEE Spectrum Risks blog --
http://blogs.spectrum.ieee.org/riskfactor/2008/10/late_last_week_the_dallas.html

✶ Driver Blames GPS System For Car-Train Collision

<Paul Saffo <paul@saffo.com>>
Tue, 11 Nov 2008 08:34:24 -0800

On the evening of 10 Nov 2008, a man's car got stuck on the Metro-North tracks in Bedford Hills, N.Y. in Westchester County because he said his GPS told him to make an immediate right turn. Police blamed Jose Silva's overdependence on GPS. He was cited for driving on the tracks and not obeying signs. Metro-North spokeswoman Marjorie Anders said, "You don't turn onto train tracks. Even if there are little voices in your head telling you to do so. If the GPS told you to drive off a cliff, would you drive off a cliff?"

The same thing had happened in Jan 2008. Apparently the safety features that were added then were not enough to deter Silva. [Source: KPIX; PGN-ed]
<http://cbs5.com/watercooler/gps.beford.hills.2.829797.html>

✶ Stop! Buses only! --What do you mean, you ARE a bus?

<msb@vex.net (Mark Brader)>
Sun, 2 Nov 2008 03:43:29 -0500 (EST)

In some British cities, restricted-traffic lanes such as bus-only lanes are protected by bollards that automatically lower themselves into the street when a permitted vehicle is detected, and rise again behind it.

The other day in Manchester, though, a bollard rose *while* a bus was passing over it. The bus was brought to an abrupt stop and several passengers were injured.

http://www.manchestereveningnews.co.uk/news/s/1077219_six_hurt_as_bus_hits_bollards

I was hoping to find a BBC story on this, as they have shorter URLs and I know they don't expire quickly, but there doesn't seem to be one at present. However, while looking for it, I came across this item

<http://news.bbc.co.uk/1/hi/england/cornwall/7220833.stm>

about bollards in the city of Truro rising suddenly under the feet of pedestrians, which they also aren't supposed to do, earlier this year.

[Later note added:]

Here's a followup story link, although the cause is still unknown:

http://www.manchestereveningnews.co.uk/news/s/1077703_call_for_bollards_inquiry

♣ Martian deep freeze: NASA's Mars Lander dies in the dark

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

Sun, 16 Nov 2008 12:00:37 PST

After five months digging up and analyzing soil samples on Mars, verifying the existence of ice, and noting that snow falls from Martian skies, NASA's Phoenix Mars Lander has gone silent -- because the nights have grown longer and there is less sun to recharge the solar batteries. [Source: Sharon Gaudin, Computerworld, 11 Nov 2008] <http://www.computerworld.com>

♣ The "Two Focaccia Buttons Defense"

<Robert Hall <bob-3FA86EQ8EH-@channels.research.att.com>>

Tue, 11 Nov 2008 17:22:18 -0500

I had lunch today at a local bakery/sandwich place, ordering a sandwich and drink. The bill seemed high to me, even for that place, so I looked at the computer-generated register receipt:

6.29 [Sandwich]
1.59 [Drink]
8.77 Subtotal
0.61 Tax
9.38 Amount Due

The prices seemed consistent with the menu, and computers never make arithmetic errors, right?

Oops, wrong. ($6.29 + 1.59 = 7.88$, NOT 8.77)

When I went back to point this out, the response was "Sorry, sir, but our system was reprogrammed recently and we have two focaccia buttons now. That's the problem."

My first reaction was to want to understand better how it could make sense for *any* number of "focaccia buttons" to make $6.29+1.59 = 8.77$. But then I remembered the Indiana Legislature and decided to accept my refund with grace. (In case you were wondering, I decided it was too risky to order pi for dessert.)

Observations:

1. Check your receipts. Don't assume the computer never makes arithmetic errors; don't even assume it is doing the same arithmetic problem displayed on the paper.
2. Verify your paper optical-scan ballot.
3. Why does anybody trust Internet gambling sites (or any software based gambling machines of any kind, for that matter) to play fair?

Robert J. Hall, AT&T Labs Research

✂ Risks of assuming constant hours in a day

<<toby@gottfriedville.net>>

Sat, 1 Nov 2008 23:50:31 -0700

I am reporting [on] myself in this instance. I recently developed a small application for a group to sign up for some activities.

As such, it involves date calculations.

I made the (altogether reasonable, I thought) assumption that if you take a timestamp and add 24 hours, it becomes the same time on the following day.

Well, not always. Such as when clocks change for Daylight Savings Time.

24 hours after 00:30 on Sunday Nov 2, it is 23:30 on Sunday Nov 2. (In local time that is.)

In this case, the problem self repaired after the clocks were changed - it was only a bug during the 24 (23 ? 25? 2?) or so hours immediately before the hour the clocks changed.

I guess that is one of the reasons that we do the clock changes late at night during the weekend. It minimizes the Risks.

✂ Excel auto-formatting

<"David Magda" <dmagda@ee.ryerson.ca>>
Mon, 17 Nov 2008 13:18:49 -0500 (EST)

Auto-formatting in Excel has reared its head again:

- > Some of these details on various trading contracts were marked as hidden
- > because they were not intended to form part of Barclays' proposed deal.
- > However, this "hidden" distinction was ignored during the reformatting
- > process so that Barclays ended up offering to take on an additional 179
- > contracts as part of its bankruptcy buyout deal, Finextra reports. [...]
- > It's unclear what the financial ramifications of the formatting error
- > might be. Excel spreadsheets might seem a fairly unsophisticated method of
- > logging multi-billion pound trading positions, but they are quick to
- > produce and easy to understand--vital consideration in a financial
- > market--which makes them widely used.

http://www.theregister.co.uk/2008/10/15/lehman_buyout_excel_confusion/

Texting bug hits the Google phone

<Amos Shapir <amos083@hotmail.com>>
Wed, 12 Nov 2008 17:53:54 +0200

A text conversation has revealed a big problem with the G1 mobile phone - powered by Google's Android software. The newly discovered bug causes the phone to restart when owners type in the word "reboot" soon after starting up the device. Full story at:

<http://news.bbc.co.uk/2/hi/technology/7722367.stm>

This reminds me of a bug/feature of a popular model of phone modem, which would hang up the line whenever it encountered the words NO CARRIER (I hope nobody is reading this edition of Risks over a phone line...)Amos Shapir

Vintage IBM tape drive in Apollo moon dust rescue

<Chris Leeson <Chris.Leeson@atosorigin.com>>
Tue, 11 Nov 2008 11:16:52 -0000

Yet another data recovery exercise

http://www.theregister.co.uk/2008/11/11/vintage_ibm_tape_drive_moon_dust_data/

A day after reading Mike Tibbetts post about the Domesday project, I came across this article on The Register.

Data on Moon Dust from Apollo 11, 12 and 14 was stored on a number of tapes requiring a "1960s-era IBM 729 Mark V tape drive". The tapes were archived

by NASA and Sydney University. Alas, due to an "archiving error", the NASA copies were disposed of. The Sydney ones are, however, still available.

SpectrumData, a data recovery firm, have managed to track down a tape drive in the Australian Computer Museum Society, and will be borrowing it to try and read the tapes. They hope to have the hardware working by January, and to extract the data from the tapes then.

The tapes were stored in a climate-controlled environment, so may still be viable (although there are lots of things that can wreck tapes). On the other hand, the restoration job is described as "It's going to have to be a custom job to get it working again. It's certainly not simple, there's a lot of circuitry in there, it's old, it's not as clean as it should be, and there's a lot of work to do."

#gnus-mime-print-part vs. Mom's room

<jidanni@jidanni.org>

Tue, 11 Nov 2008 01:50:04 +0800

'Twas the night before Christmas, when all through the house,
not a creature was stirring... except the old printer up in Mom's room:
In the "gnus" news reader, usually

p runs the command `gnus-summary-prev-unread-article`
Select unread article before current one.

Except when the cursor happens to be resting on an image, whereupon

p runs the command `gnus-mime-print-part`
Print the MIME part under point.

<http://news.gmane.org/group/gmane.emacs.gnus.general/thread=67574>

No problem. Trip the house circuit breaker, then go upstairs with a flashlight. "Paper jam, blew a fuse, I'll take care of it!" better than Mom: "So that's what you've been browsing! I'm returning the computer to the department store. You can have a new one when you're 18."

#False security from privacy screens

<"Dr. David Alan Gilbert" <dave@treblig.org>>

Sat, 1 Nov 2008 18:03:09 +0000

A major phone shop here in Manchester has just been redecorated; they've now got a nice clean glass wall into the rest of the shopping centre. That would be the wall against which they have the PCs they take your information and do credit checks on.

I explained to one of the shop workers that I thought it insecure and he said 'It's ok, we've got privacy screens'.

A lot of places seem to treat privacy screens as silver bullets, they indeed do stop people seeing the screens from off angle - but where you can stand straight in front of the machine (e.g. when someone has just put a glass wall up or as is common in new open plan banks when you can just stand a bit further back) they are completely useless.

I took the assistant outside the shop and showed him; and he referred me to the shop manager, who unfortunately just said 'well what can I do - I didn't design the shop'. So much for security. I suggested he put a poster up on the glass wall.

✂ Re: BBC Domesday Project (Re: Tibbetts, [RISKS-25.44](#))

*<Martin Ward <martin@gkc.org.uk>>
Sun, 9 Nov 2008 13:04:43 +0000*

> so far as I can tell, they seem to have lost it!

Not completely lost. The whole Domesday Project appears to be available on the web here: <http://www.domesday1986.com/>

martin@gkc.org.uk <http://www.cse.dmu.ac.uk/~mward/>

✂ Re: BBC Domesday Project (Tibbetts, [RISKS-25.44](#))

*<theo.bucher@computer.org>
Sun, 9 Nov 2008 21:28:03 +0100*

Writing History as a Pioneer is Taking a Risk

I sympathize with Mike Tibbetts, as I think it unfair to cite 'lack of foresight' as a cause of the loss of the Domesday data. Lack of knowledge may be closer. But anyone claiming anything like that today has the benefit of 20/20 hindsight. It's not a fair comparison.

Who was to blame? Well, perhaps nobody, unless naivety is a sin. The Domesday Project was a pioneering feat. Pioneers sometimes pay a high price for their achievements. In this case no one really suffered, although it is sad that the collection disintegrated. History should be viewed in the light of the times of its happening.

I submit that the outcome of this project and other such experiences were inevitable, contemplating the sociotechnomics (sociology in the space between technology and economics).

Consider the following probable or possible circumstances.

Conservation in public Archives works something like this:

1. Most archive holdings are on paper or photographic film.
2. The preservation of paper or photographic film requires a certain amount of knowledge, diligence and skill, but it's not extremely difficult.
3. Such know-how evolves only slightly over time, as, for example, new types of paper are used and new methods of conservation are developed. The know-how needed for conservation of conventional materials is therefore relatively stable, systematic and it is relatively easily learned and remembered, given a good general education in natural sciences. The basic information is freely available (and useful for all sorts of other purposes too). It remains available in a cheap and stable form: in Basic Object-Oriented Knowledge Systems (books), universally catalogued using a standard system (ISBN).
4. It is conventionally accepted that archives conserve their materials based mainly on controlling the environmental conditions and protecting from external influences.
5. The costs of preservation may rise slowly year on year. Not so slowly if the price of energy burgeons, but even that rise in costs will be accepted as essential to doing business; it impacts the complete conventional holdings of the archive. Incidentally, many public archives have collections of ancient historical documents in urgent need of restoration, lest they decay completely, but no funds for such a project.
6. The interest of a Chief Archivist will be mainly on keeping the gros of the inventory in good condition, and *accessible* and to provide good services to the customers of the day.
7. To hang on to their jobs, archivists will do what other people do. They put priority on keeping the overwhelming majority their customers happy, especially their top paying customers.

Now consider some not improbable circumstances of a set of hi-tech recordings on a rare or obscure hi-tech medium needing to be migrated in 1992 (take it with a pinch of salt):

1. The hi-tech holding acquired in 1986 is a single holding (or one of only a very few) among thousands of other holdings having significant historical value that you can feel (because some of them are falling apart).
2. The archivist is not a hi-technologist. (S)he has no idea what is needed to conserve the holding. Asks the single IT specialist on archive staff (an expert in DOS/Windows 2.0).
3. Migrating data on a rare medium to a new medium, or (oh horror!) to a new *data format* is a P-R-O-J-E-C-T. But it's not a project like restoring some ancient books. It can't be done by the usual staff, it needs IT specialists. The archivist has no such IT specialist on staff.
4. IT specialists are only very rarely conservationists. IT jobs are secured by constantly inventing new kinds of wheels, excuse me, I mean, of course, by innovation. Can't hire any IT conservationists in 1992 because top IT people are busy thinking about how to integrate Wind-OS 3.x into a conventional IT environment - enough to do, and it's a sellers' market. The archivist needs to hire a C-O-N-S-U-L-T-A-N-T. Consultants cost more than staff. Gritting teeth, the archivist hires a Consultant.
5. Much of the information that IT specialists will need for the project is

- in the system documentation. That's the *system* documentation (not the user manuals). The system documentation is unique knowledge in the hands of the manufacturer. New generations of hardware and software entail learning new programming languages, new programming tools, new concepts for structuring and manipulating data, also new workarounds for the bugs in the systems, and that includes the bugs (errors and omissions) in the documentation, which may have been hurriedly completed shortly before the custom product was shipped (if 'complete' documentation was written at all). The consultant tells the archivist (s)he needs additional documentation that is not available, and not easily obtained, and, especially in view of the circumstances - custom development - the documentation may also be incomplete or inaccurate. Success is not guaranteed (and keeping within budget, even less so).
6. Formal methods of project management for IT existed in 1992, but were not as well developed as they are now and were not so widely applied. Even so 30 to 50% of projects fail to deliver.
 7. The project is competing for funds with another project to restore high-profile irreplaceable tomes from 1066, to save them from complete annihilation. No customer has expressed any interest in this hi-tech holding since it was acquired.
 8. You are the archivist. What would you do?

That is maybe a generous scenario. With a little thought, a number of other kinds of SNAFU could probably be discerned as possible contributory causes.

I realise this was the National Data Archive, so some of the details that I filled in are to be taken as metaphors and no more. But it is conceivable that the contributing parties were not at fault, i.e. that they did not fail to learn from history, and they were certainly doing something useful: they were writing history for others to learn from.

✂ Re: Poison pill auto-disclosure (Robinson, [RISKS-25.43](#))

<Terje Mathisen <terje.mathisen@hda.hydro.com>>
Fri, 31 Oct 2008 09:14:41 +0100

This is very similar to the setup used by rsync.net (where I keep some (encrypted) backups of critical information):

They have a "canary" page which they promise to update every week:

<http://www.rsync.net/resources/notices/canary.txt>

It states, among other things, that

"rsync.net Warrant Canary

Existing and proposed laws, especially as relate to the US Patriot Act, etc., provide for secret warrants, searches and seizures of data, such as library records.

Some such laws provide for criminal penalties for revealing the warrant, search or seizure, disallowing the disclosure of events that would materially affect the users of a service such as rsync.net.

rsync.net and its principals and employees will in fact comply with such warrants and their provisions for secrecy.

rsync.net will also make available, weekly, a "warrant canary" in the form of a cryptographically signed message containing the following:

* a declaration that, up to that point, no warrants have been served, nor have any searches or seizures taken place

* a cut and paste headline from a major news source, establishing date

Special note should be taken if these messages ever cease being updated, or are removed from this page."

If this message ever stops being updated, I must assume it was because they either forgot to do so (hasn't happened yet), or some outside party have indeed served them with a warrant, but without also forcing them to continue making bogus updates to the canary message.

✂ Re: Poison pill auto-disclosure (Robinson, [RISKS-25.43](#))

<Al Macintyre <macwheel99@wowway.com>>
Thu, 30 Oct 2008 11:58:17 -0600

I heard a similar story, which may be urban legend.

A librarian sent notification each day to the library's Board of Directors. "We have not yet received any secret demand under the Patriot Act." Then when they got the first such demand, where the rules prohibit telling anyone about it, she stopped sending the notification, so now they all knew.

✂ Re: Poison pill auto-disclosure (Robinson, [RISKS-25.43](#))

<"Richard O'Keefe" <ok@cs.otago.ac.nz>>
Tue, 4 Nov 2008 13:42:50 +1300

Paul Robinson ([RISKS-25.43](#)) proposed a "Dead man switch" technique for forcing disclosure. I am not a lawyer of any kind, but there seem to be some flaws:

1. He assumes that it is legal for Bob to inform Alice about the defects. The contract under which he has access to the software may forbid this. According to the Wikipedia, UCITA has so far been passed in only two states, but wasn't it going to prohibit public criticism of bad software? Even in states or countries sans UCITA, specific software licences may

forbid this.

2. If there is a court order prohibiting Bob from publishing information about the defects, then his failure to effectively cancel his prior arrangement with Alice will almost certainly count as defiance of the court order.

3. If I'm wrong about 2, then the scheme might work once. But don't expect it to work twice; laws can be patched.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 46

Weds 26 November 2008

Contents

- [E-prescription for IT disaster](#)
[Tom Yager via Gene Wirchenko](#)
- [Computer virus shuts down three London hospitals](#)
[Patrick O'Beirne](#)
- [The Blackberry, the President, and Reality](#)
[Fred Cohen](#)
[Steve Wildstrom](#)
- [Choose too large a sample interval and look like an idiot](#)
[Max Power](#)
- [The Great RoHS/Tin Whisker Fiasco of 20??](#)
[Jay R. Ashworth](#)
- [ACMS helps recover lost Moon data](#)
[David Shaw](#)
- [Re: Vintage IBM tape drive in Apollo moon dust rescue](#)
[David Brunberg](#)
- [Re: BBC Domesday Project](#)
[Kees Huyser](#)
[Amos Shapir](#)
- [Re: NASA's Mars Lander dies in the dark](#)
[John Levine](#)
- [Excel user awareness](#)
[Patrick O'Beirne](#)
- [Info on RISKS \(comp.risks\)](#)

✉ E-prescription for IT disaster (Tom Yager)

<Gene Wirchenko <genew@ocis.net>>
Sat, 22 Nov 2008 16:28:04 -0800

Tom Yager, E-prescription for IT disaster, *Infoworld* Blog, 19 Nov 2008
http://weblog.infoworld.com/yager/archives/2008/11/eprescribing_mo.html?source=NLC-DAILY&cgd=2008-11-19

The federal paperless prescription mandate is a model for pathetic planning

that will leave users and IT blamed for failures

Researchers just finished mapping a patient's leukemia tumor genome, finding only eight differences between her tumor cells and normal ones taken from her skin. This breakthrough in medical technology was somehow accomplished while the American Medical Association and U.S. government health agencies are doing a rip and replace of the nation's medication distribution system. Taking the prescription system paperless has been on the national road map since timeshared mainframes were the rage, but up to now, those delivering, managing, regulating, and receiving health care always found wiser uses for the time and money required for a prescription system overhaul.

Now, in the final seconds before an administration sworn to reform health care takes office, e-prescribing is being lofted as a Hail Mary pass by interests with a mix of honorable and questionable intentions. It has not remotely begun to gel, but now it is poor planning made law, and it falls to practitioners, pharmacies, and IT to make it work. Make it work now, or the government will dock already inadequate reimbursement for treatment under Medicare and Medicaid. Company-paid insurance can't be handled any other way.

It probably seems that I'm casting too jaundiced an eye on the issue. Who could oppose the modernization of a paper system whose flaws exact tolls in lives and taxpayer dollars lost to fraud? Trouble is, e-prescribing is loaded with agendas, with conduits for control and work-arounds for potential future regulation and reformation (whatever those may be). It is being executed under the rubric of urgent social necessity, but the health care system has far more pressing issues to deal with. Doctors have less time to see patients, new reasons to refuse to treat patients on government assistance, and new levels of complication that tacitly discourage certain types of prescriptions.

Ain't broke

E-prescribing is sold as an essential modernization of a creaky, error-prone, inefficient, and costly paper system that cannot keep pace with the explosive growth of prescriptions. If you didn't know better, you might say they're right. This archaic system has its roots in simpler times when small-town pharmacists knew small-town doctors and their office staff personally. Pharmacists' experience and face-to-face dealings with patients red-flagged erroneous or suspicious prescriptions. [...]

Computer virus shuts down three London hospitals

*<Patrick O'Beirne <Mail3nospam@sysmod.com>>
Tue, 18 Nov 2008 16:13:25 +0000*

A computer virus infection has forced a number of London hospitals to shut down their IT systems, and revert to manual operation.

[Searching on this turned up many reports, naming St Bartholomew's, the Royal London Hospital, and the London Chest Hospital, all part of the Barts and London NHS Trusts. The URL Patrick gave me did not seem to work. PGN]

✶The Blackberry, the President, and Reality (Re: Solomon, [RISKS-25.45](#))

<Fred Cohen <fc@all.net>>

Mon, 17 Nov 2008 17:55:00 -0800

The Records Act does not prevent the use of a Blackberry - all you have to do is record what you send (and receive) - a relatively simple matter. The fact that sending classified over a blackberry is a problem is, of course, a limitation, but hardly a surprise. The other challenge relates to the traceability of the blackberry to a location and the ability to use this information to deliver smart weapons on target. And then there is the use of the voice part for recording conversations when it appears to be off. And of course the list goes on. But isn't this a good thing for computer security? After all, we can secure things like this if we want to, and the fact that so public an official has to deal with these sorts of issues should be an eye-opener for lots of folks. It's a good thing that it is being brought up, but it should not force him to stop using the device. Assuming it is properly managed.

That brings us to the real issue. The security of Federal systems and the measures taken to protect (and not protect) them are problematic, they tend to get low scores on relatively simple tests of security, and of course the White House computer systems have been broken into recently (according to the news stories) and emails revealed - blackberry not even involved. At the dawn of the information age, as it enters the highest parts of our government, we may actually see an executive who has to deal with these issues and a serious effect on notional policy and operational decisions. Change is coming, but will that change be change we can rely on?

Fred Cohen & Associates, 572 Leona Drive, Livermore, CA 94550 <http://all.net/>
1-925-454-0171 <http://tech.groups.yahoo.com/group/FCA-announce/join>

✶The Blackberry, the President, and Reality (Re: Solomon, [RISKS-25.45](#))

<Steve Wildstrom <steve_wildstrom@wdc.exchange.businessweek.com>>

Tue, 18 Nov 2008 13:25:35 -0500

Most of what has been written about the President-elect and his BlackBerry is nonsense. As President, he may not have time for as big a time-suck as a BlackBerry, but neither the Presidential Records Act nor security concerns (for unclassified material) should be an issue. A BlackBerry certainly meets all the retention requirements of the PRA (actually, these would be met by the underlying mail system-Exchange, Lotus Domino, or GroupWise.) With respect to security, the BlackBerry has picked up a long list of approvals,

including certification under FIPS for "sensitive but unclassified" information. BlackBerrys are widely used within the government, including by law enforcement agencies, as is a similar technology for Windows Mobile and Palm from Motorola Good Mobile Messaging.

Steve Wildstrom, Technology & You columnist, BusinessWeek, 1200 G St NW Suite 1100, Washington, DC 20005 www.businessweek.com/technology/wildstrom.htm

✂ Choose too large a sample interval and look like an idiot

<Max Power <dist23@juno.com>>
Wed, 19 Nov 2008 13:35:49 -0800

... Risks of using poorly customized map software ...
http://news.bbc.co.uk/2/hi/in_depth/629/629/7600053.stm

The BBC Box uses GPS based satellite transponder technology. The Box pings its location every 24 hours. The Box should ping its location every 11 hours, or some oddball number smaller than 24. Sadly, the sample ping sample interval is too small -- and the mapping software is not bright enough to use arcs between sample points to avoid clearly wrong map displays.

In this case The Box's trip around Taiwan looks totally wrong (19/10/2008 & 20/10/2008). The ship did not plow thru the Taiwanese mountains!

Also, the trip around Indonesia, and Malaya to Singapore looks totally wrong as well. And the trip skirting around Sri Lanka does not look right either. And Yemen, eeesh!

- * These nation's EEZ's are somewhat unsafe due to piracy, but that issue needs to be tackled by the UN.
- * I don't believe that a smaller ping interval is any less safe, if the new data point is delayed from being displayed by 120 minutes.

What other visual mapping gaffes will we have to tolerate for the next year? The Box project will last a year at least.

I actually hope the BBC inserts interpolated data points, or even better -- get a GPS log of the container ship's route.

The GPS unit in use here probably stores a data point every 15 minutes, and can probably send trip logs autonomously.

Max Power, CEO, Power Broadcasting, <http://HireMe.geek.nz>

✂ The Great RoHS/Tin Whisker Fiasco of 20??

<"Jay R. Ashworth" <jra@baylink.com>>

Thu, 20 Nov 2008 11:03:14 -0500 (EST)

Slashdot just ran a story about a lead substitute based on bisumth.

<http://tech.slashdot.org/article.pl?sid=08/11/19/2330241>

As I had expected, some of the commenters (me among them) noted that the removal of lead from solder to meet European RoHS requirements is causing problems with the formation of tin whiskers.

<http://www.siliconfareast.com/whiskers.htm>

So, now, the question you have to ask yourselves is: what happens when one of those tin whiskers shorts out a critical piece of avionics in the plane you're flying in?

And, more importantly... has that thought already occurred to people who build avionics, and make RoHS laws... and if so, why does Google have so much trouble finding evidence thereof?

<http://www.google.com/search?q=rohs+tin+whiskers+avionics>

Everybody seems to be trying to *fix* this potential problem, but the whole point of RoHS was, as I understand it, keeping lead out of landfills.

How many avionics and other such life-critical items end up in landfills in the first place?

Jay R. Ashworth, Ashworth & Associates, St Petersburg FL +1 727 647 1274

<http://baylink.pitas.com> <http://photo.imageinc.us>

✂ ACMS helps recover lost Moon data

<"David Shaw" <d.shaw@sport.usyd.edu.au>>

Thu, 20 Nov 2008 17:13:10 +1100

The risk of not being able to read aging storing media / formats is no doubt familiar to many RISKS readers, but this particular story seems like a textbook example.

"Scientists hope to recover lost data from the Apollo moon missions using a 40-year-old tape drive borrowed from the Australian Computer Museum Society (ACMS). NASA lost its original tapes - containing data from studies of lunar dust but thankfully back-ups were stored at Sydney University. Work is now underway to restore a 1960s-era IBM 729 Mark V tape drive so the tapes can be read."

More info at:

<http://www.abc.net.au/news/stories/2008/11/10/2415393.htm>

The real irony here is that the ACMS's valuable, historical collection of computers has been evicted twice and struggles for funding. I suspect we went awfully close to never being able to retrieve NASA's lost data.

Re: Vintage IBM tape drive in Apollo moon dust rescue ([RISKS-25.45](#))

<"David Brunberg" <dbrunberg@gmail.com>>
Mon, 17 Nov 2008 22:03:05 -0500

While the problem (loss of data due to obsolete formats/equipment) is real, consider this: the moon dust/rock samples have been carefully preserved and are available for analysis by qualified scientists. It would probably be cheaper to re-run the chemical and isotopic analyses. The analytic technology has progressed to be able to use much smaller masses and would probably offer more precision and flexibility.

It's been discussed thoroughly before, but a more significant problem, in my opinion, is the loss of data due to aging of storage media, and specifically the loss of time sensitive data. For instance, 30-year-old photographs that, when compared against current images, might lead to major astronomical findings by showing long-term changes in positions or conditions of celestial objects.

Re: BBC Domesday Project (Tibbetts, [RISKS-25.44](#))

<Kees Huyser <kees.huyser@nikhef.nl>>
Tue, 18 Nov 2008 09:31:20 +0100

Jeffrey Darlington of the Digital Preservation Department of the The National Archives wrote in 2003 about the rescue in an article in *Ariadne*, a magazine for information professionals in archives, libraries and museums: <http://www.ariadne.ac.uk/issue36/tna/>

Re: BBC Domesday Project (Tibbetts, [RISKS-25.44](#))

<Amos Shapir <amos083@hotmail.com>>
Wed, 19 Nov 2008 17:45:31 +0200

In other words, they have bound the data format from the start to specific hardware implementations, which were rare even then. This put an extra burden on the archivers who would necessarily have to convert it later. (Maybe this reflects the general attitude in a country where power is still measured by horses, and people are weighed by stones :-)) Once data is digitized, it would certainly fare much better if it was kept in the most simple form; I suspect it would have been easier to rescue even if it was all put on punched cards!



Re: NASA's Mars Lander dies in the dark ([RISKS-25.45](#))

<John Levine <johnl@iecc.com>>

18 Nov 2008 13:02:19 -0000

In fairness, that was always the plan. The original schedule when Phoenix landed in May was to operate for three months during the Martian summer, but it worked well enough that they extended the mission twice until it ran out of sunlight.

I wonder why they didn't design it to go to sleep and try waking it up when the days get longer. Perhaps they figure that by then there will be so much dust on it that it won't get enough sunlight to restart.

John Levine, johnl@iecc.com, <http://www.johnlevine.com>

Primary Perpetrator of "The Internet for Dummies",

✂ Excel user awareness (Re: Magda, [RISKS-25.45](#))

<Patrick O'Beirne <Mail3nospam@sysmod.com>>

Tue, 18 Nov 2008 08:47:06 +0000

It's not Excel auto-formatting. It's a breakdown in the communication of significance between those who know what something means and those who just manipulate spreadsheets without knowing what they mean; compounded by last-minute rush and pressure and lack of supervision. see

<http://www.sysmod.com/praxis/prax0811.htm>

Some of my comments are:

"A maximum of one minute checking time, then. If you delegate work, you have the responsibility to check it. Spotting 179 differences in 1000 rows is not that hard. Lawyers always work with paper evidence, so a simple check would have been to print the excel sheet as received, print the PDF, and visually compare the pagination. If they had had to do it by midnight, then at least the largest numbers could be checked in 15-20 mins. After all, even with the late submission by the client, counsel had nearly four hours just to look at it and convert it to PDF. If the check had been done on Sept 18, much embarrassment would have been spared."

"Let's look at the interface between client and lawyer. Clients should be able to expect well-paid lawyers to exercise vigilance and help protect the clients against themselves. As well as their first job which is to review the substantive content of documents, it should be standard practice in to review all received files for metadata and hidden data. It could be hidden text in a Word document, blacked-out text in a PDF, or file properties in an Office document that reveal identities. However, lawyers are rather expensive IT reviewers, so for one's own protection, one should review documents both in content and form before release. Form includes not just hidden data, but anything that is not manifestly clear to the parties

involved and could be a source of confusion. Is "Y/N" in column Z a sufficient indicator, and was its significance made plain?"

I have not read about the judgment yet on the case which was due Nov. 5

Patrick O'Beirne, Systems Modelling Ltd.

<http://www.sysmod.com/> (+353)(0) 5394 22294



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 47

Monday 8 December 2008

Contents

- [Chatsworth Wreck May be a Safety Failure](#)
[Chuck Weinstock](#)
- [Caltrain computer outage causes extensive schedule disruption](#)
[PGN](#)
- [Water pumps failed in Yorba Linda fire](#)
[Jim Geissman](#)
- [Dangerous Precedence Set - Federal Criminal Charges for Violation of Commercial Online ToS?](#)
[Stephen via Dave Farber](#)
- [A cyber-attack alarms the Pentagon](#)
[Jerry and Virgil Gligor via David Farber](#)
- [A secure version of reality](#)
[Andy Piper](#)
- [The recovery features of botnets](#)
[Peter Houppermans](#)
- [Fingerprints in South Africa](#)
[Heinz M. Kabutz](#)
- [Facebook and tracking people](#)
[David Magda](#)
- [How *not* to improve data quality](#)
[Richard O'Keefe](#)
- [Israeli Labor primaries postponed: electronic systems fail](#)
[Amos Shapir](#)
- [Re: Risks of assuming constant hours in a day](#)
[Curt Sampson](#)
- [Workshop on GENI and Security: Call for Participation](#)
[Matt Bishop](#)
- [MiniMetricon call for participation](#)
[Fred Cohen](#)
- [REVIEW: "The History of Information Security", de Leeuw/Bergstra](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

✶ **Chatsworth Wreck May be a Safety Failure**

<Chuck Weinstock <weinstock@sei.cmu.edu>>

Mon, 8 Dec 2008 17:59:40 -0500

Off the Newswire at www.trains.com

[Three different spellings of the conductor's name unified. PGN]

According to the **Los Angeles Times**, conductor Robert Heldenbrand, the lone surviving crew member of the Sept. 12 Metrolink wreck that killed 25 people, has told investigators the signal he passed prior to the crash was green.

Trackside signals are programmed to detect the presence of a train or other equipment within a block and turn red, telling approaching movements to stop prior to entering. If the signal truly displayed a green aspect when in fact a Union Pacific freight occupied the block, it would mean a signal failure. Such failures do occasionally occur, and are known as false clear indications.

Heldenbrand's account backs up that of three witnesses on the platform of the Chatsworth depot, who also say the light was green at the time of the crash. Still, the National Transportation Safety Board is standing by its account of the crash, saying the train's engineer, Robert Sanchez, passed a red signal before slamming head-on into the UP freight. It has, however, questioned how brightly lit the signal was.

Investigators had earlier asked why Sanchez hadn't called out the signal's indication on the radio, which Heldenbrand would have been required to repeat back if the signal wasn't green. But a green signal would have meant the two would not be required to call the signal.

✶ Caltrain computer outage causes extensive schedule disruption

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

Fri, 5 Dec 2008 14:15:50 PST

On 4 Dec 2008, Caltrain (the commuter line between San Francisco and San Jose/Gilroy) experienced significant delays due to the computer system that controls the signal system. The problem began at the end of the morning rush hour, and was still ongoing during the evening rush hour. Trains had to be controlled manually, including bullet trains overtaking local trains. Delays were further complicated by construction at Palo Alto's California Avenue station -- which requires only one train at a time in the station (even though the long-standing problem of having northbound passengers cross-over the southbound tracks has finally been resolved in the past week, with the completion of a northbound platform).

✶ Water pumps failed in Yorba Linda fire

<Jim Geissman <jimgeissman@socal.rr.com>>

Thu, 27 Nov 2008 13:31:15 -0800

The equipment failures caused fire hydrants to run dry in the highest neighborhood in the city and may explain why firefighters were unable to protect homes.

Water officials said [on 25 Nov 2008] that pumps designed to push water to the upper reaches of a hillside Yorba Linda neighborhood failed during a 15 Nov firestorm [so that] firefighters were forced to abandon the area and let homes burn....

Water officials believe the electric pumps shut off because the fire had burned through their electrical communication systems. The backup, they said, failed because of the heat.

Officials said that the reservoir has been on the to-do list since at least 2001, when developer Shapell Industries first submitted plans to build homes around Hidden Hills. The agency has recognized the need for more reservoirs in the eastern side of Yorba Linda for 30 years but depends on developers' building plans to determine where to locate the infrastructure.

[Interesting that residential development occurs before development of the infrastructure required to support it.]

<http://www.latimes.com/news/local/orange/la-me-water26-2008nov26,0,3919612.story>

✶ Dangerous Precedence Set - Federal Criminal Charges for

<Stephen <sdpoe@airmail.net>>
November 27, 2008 12:24:49 PM EST

Violation of Commercial Online ToS?

[From Dave Farber's IP list. PGN]

A very dangerous legal precedence was set today.

In the case of the 13-year-old who committed suicide supposedly over a MySpace hoax, the mother involved was found guilty on three federal counts. What of? Not of a serious criminal act.

She was found guilty on three criminal counts (misdemeanors), in a federal court, of violating the Terms of Service agreement. So now you can be accused, tried, and found guilty of a federal criminal offense not for breaking a Federal or even a state law, but rather for violating the Terms of Service of a click- through agreement of a commercial site you go to on the Web.

"Prosecutors alleged that Drew and her employee violated MySpace's "terms of service," which prohibit using fraudulent registration information, obtaining personal information about juvenile members, and using the service to harass, abuse or harm others...

The verdict underscores the complexities of the case. Some legal experts and civil liberties groups said a felony conviction would mean that millions of people who violate the terms of service of the Web sites they visit could become criminally liable. Experts also said that if violating such terms is a crime, then the sites that write the agreements essentially could function as lawmakers or prosecutors. " - from *The Washington Post*

<http://www.washingtonpost.com/wp-dyn/content/article/2008/11/26/AR2008112600629.html?hpid=topnews>

"The case was prosecuted under the federal Computer Fraud and Abuse Act, originally intended to prosecute hackers. Did Lori Drew effectively hack MySpace for nefarious purposes? Some people think it's quite a stretch.

"This was a very aggressive, if not misguided, theory," said Matt Levine, a New York-based defense attorney and former federal prosecutor. "Unfortunately, there's not a law that covers every bad thing in the world. It's a bad idea to use laws that have very different purpose." from ZDNet @ <http://government.zdnet.com/?p=4207>

Archives: <https://www.listbox.com/member/archive/247/=now>

[IP] Re: A cyber-attack alarms the Pentagon

<David Farber <dave@farber.net>>
Sun, 7 Dec 2008 09:34:29 -0500

>From: No-Name <labmanager@gmail.com>

I've heard a rumor about the way the WORM made it's way into the Pentagon computer network. If true, it was a simple but brilliantly effective method. Someone infected thumb drives with the WORM then dropped them around the Pentagon parking lot. The employees, picked them up, took them into their offices and plugged them into their office computers to determine the owner of the drive. Jerry

Date: December 4, 2008 8:36:03 PM EST
>From: Virgil Gligor <GLIGOR1@aol.com>
Subject: For IP: A cyber-attack alarms the Pentagon

Cyberwar: The worm turns, *The Economist*, 4 Dec 2008

A cyber-attack alarms the Pentagon

Battlefield bandwidth is low at best, making networks sticky and e- mails tricky. American soldiers often rely on memory sticks to cart vital data between computers. Off-duty, they use the same devices to move around music and photos. The dangers of that have just become apparent with the news that the Pentagon has banned the use of all portable memory devices because of the spread of a bit of malicious software called agent.btz.

This is a "worm", meaning that it replicates itself. If you have it on, say,

the memory card of a digital camera it will infect any computer to which you upload photos. It will then infect any other portable memory plugged into that computer (the cyber-equivalent, one might say, of a sexually transmitted disease). On any computer hooked up to the Internet, this variant tries to download more nasty stuff: in this case two programs that access the hard-drive. Was it a humdrum crime of trying to steal banking details? Or something more serious? The trail has gone cold.

In any case, the malicious software (malware in the jargon) penetrated at least one classified computer network. The problem was severe enough for Admiral Michael Mullen, the chairman of the joint chiefs of staff, to brief George Bush on it. Officials are saying little more than that.

Kimberly Zenz, an expert on cyberwarfare at VeriSign iDefense, a computer security company that is investigating the attack, notes that it is not clear that agent.btz was designed specifically to target military networks, or indeed that it comes from either Russia or China (two countries known to have state-sponsored cyberwarfare programmes that regularly target American government computer networks).

Indeed, she says, by the standards of cyberwarfare, agent.btz is pretty basic; it is a variant of a well-known bit of malware called the SillyFDC worm, which has been around for at least three years. By contrast, a government commission warned Congress last month that "since China's current cyber operations capability is so advanced, it can engage in forms of cyberwarfare so sophisticated that the United States may be unable to counteract or even detect the efforts."

The most remarkable feature of the episode may not be the breach of security, but the cost of dealing with it. In the civilian world, at least one bank has dealt with agent.btz by blocking all its computers' USB ports with glue. Every bit of portable memory in the sprawling American military establishment now needs to be scrubbed clean before it can be used again. In the meantime, soldiers will find it hard or outright impossible to share, say, vital digital maps, let alone synch their iPods or exchange pictures with their families.

A secure version of reality

*<Andy Piper <andy@xemacs.org>>
Wed, 03 Dec 2008 12:46:39 +0000*

A variation on a common RISKS theme, but one I have come across increasingly often. More and more websites are enforcing "secure" passwords and, it seems, security questions. For instance two websites I used recently, which front real services I use (credit card and pet insurance) enforce passwords that **must** contain at least one upper-case character, one digit and not bear any resemblance to your user id. So far, so secure. Unfortunately they also want an answer to a security question as a reminder. Mother's maiden name is usually the one I pick, but my mother has a double barreled maiden name and this time I get:

"Answer to security question is invalid, please correct"

Sorry? So the self-evidently correct answer is not, in fact, "correct" according to the website mafia. Ok, move along to the next one, place of birth. My place of birth is tripled barreled (one of those quaint English towns where the name is related to the river that runs through it).

"Answer to place of birth question is invalid, please correct"

Gah! I'm assuming that what the site doesn't like is the hyphen's in both names (or perhaps that they have two names, although for place names that seems entirely dubious). The problem is that I am beginning to have to enter information that is not only wrong, but which I have no hope of remembering correctly 6 months later. Increasingly the same is true for passwords. I use systems where the above rules are enforced *and* password aging takes place *and* the use of an old password is prohibited. So now I have to remember not only information that is incorrect but also a system for encoding passwords in my brain for these sites. Increasingly that system fails and I need to recover the password, but the recovery system is also failing me now!

Where will this madness end?

✂ The recovery features of botnets

<Peter Houppermans <peter@houppermans.com>>
Fri, 28 Nov 2008 11:36:17 +0100

Interesting read, was a submission by Thomas Lakofski to a mailing list.

Short summary: botnet code contains a semi-random domain name generator which it will contact for new instructions. This makes it impossible to shut down the controlling domains as the code will simply switch to a new name for instructions - which differs every single day. Let me put it another way: a shutdown is virtually impossible without catching the actual operator.

<http://blog.fireeye.com/research/2008/11/technical-details-of-srizbis-domain-generation-algorithm.html>

✂ Fingerprints in South Africa

<"Dr Heinz M. Kabutz" <heinz@jvaspecialists.eu>>
Fri, 05 Dec 2008 09:57:33 +0200

In South Africa, whenever you apply for an ID book, passport or driver's license, your fingerprints are taken. In the past, these were used to prevent identify theft. Of course, even that is flawed. I know someone whose skin flakes off his fingertips when he is under stress. He had a lot

of trouble renewing his passport, because his fingerprints did not match what was on file.

It would be fair to say that in South Africa, the Department of Home Affairs has a database of almost all the fingerprints in the country. You cannot do anything without an ID book.

Now someone has had the "brilliant" idea to open up this database to the police service, who are notorious for their low conviction rate. It horrifies me to think how many false positives there will be! Imagine being dragged out of bed at 3am by police special forces for murder and rape, because your fingerprint biometrically matched a serial killer's. The level of corruption at the South African Police Service is well known, so this is probably one of the worst news I have heard in years.

I'm sure fellow RISKS readers will agree ...

http://www.iol.co.za/index.php?art_id=vn20081205053045716C521775

Dr Heinz M. Kabutz (PhD CompSci), Sun Java Champion,
Author of "The Java(tm) Specialists' Newsletter" <http://www.javaspecialists.eu>

Facebook and tracking people

<"David Magda" <dmagda@ee.ryerson.ca>>
Thu, 27 Nov 2008 16:00:45 -0500 (EST)

Nowadays, once you have someone's name, it can be quite easy to track them down:

- > Leary was left with an unpaid bill for about \$520, and little hope of
- > recovering his money.
- >
- > "It was then I remembered that when the group arrived, one of them had
- > asked about one of our waitresses who was not working that night," Leary
- > said yesterday.
- >
- > The waitress gave him a name and then he thought of Facebook.
- >
- > "I searched the name and there he was, large as life," he said. "And he
- > was pictured with his girlfriend--the only girl who had been in the
- > group.
- >
- > "The site also gave me his place of employment, which was handy."

<http://tinyurl.com/68rfob>
<http://www.news.com.au/technology/story/0,25642,24714093-5014239,00.html>

It turns out the individual in question worked at another restaurant, from which he's now been fired.

✂ How *not* to improve data quality

<Richard O'Keefe <ok@cs.otago.ac.nz>>

Thu, 4 Dec 2008 16:52:21 +1300

A few days ago my wife and I bought a 2nd-hand station wagon to replace a vehicle that needed repairs for which parts are now hard to obtain. Part of the process is to change the registration for the new vehicle. As we were dutifully filling in all the details on the form, we came to a box for our phone number, and being unable to think of any reason why we wouldn't want the licensing authority to be able to reach us, were about to fill it in.

At that point the dealer stopped us and advised us not to. The reason? If your phone number changes (e.g., you drop your mobile in a toilet and have to get a new one -- happened to me once), you are legally obliged to tell the LTSA, but only if you told them your number in the first place. And most people never remember to do this.

So a rule "You must tell us if your phone number changes" that was presumably intended to ensure that the data would be more accurate has had the effect of making the data mostly unavailable.

✂ Israeli Labor primaries postponed: electronic systems fail

<Amos Shapir <amos083@hotmail.com>>

Mon, 8 Dec 2008 17:12:14 +0200

This is primary elections season in Israel, when political parties vote for their nominees for the upcoming general elections in February. The Labor party tried a fully electronic voting scheme which failed miserably, forcing them to delay the election by several days and go back to the old fashioned paper ballot method.

Full story at: <http://www.ynetnews.com/articles/0,7340,L-3631836,00.html>

Despite that, today the Likud right-wing party also held its primary elections electronically, and did face some trouble, though not as fatal.

Full story at: <http://www.ynetnews.com/articles/0,7340,L-3635022,00.html>

Unfortunately, there aren't many technical details about the systems involved.

✂ Re: Risks of assuming constant hours in a day (Toby, [RISKS-25.45](#))

<Curt Sampson <cjs@cynic.net>>

Sat, 6 Dec 2008 16:49:22 +0900

> I made the (altogether reasonable, I thought) assumption that if you take a

> timestamp and add 24 hours, it becomes the same time on the following day.
> Well, not always. Such as when clocks change for Daylight Savings Time.

And that's only the start. As we're all well aware, you can't even add sixty seconds to a time and assume it's then in the next minute.

We normally don't think much about this, but lately I've been doing a lot of programming in Haskell, and the folks who built the libraries being much too smart for their own (or, anyway, my) good, make this clear, not to mention push it a bit in your face:

<http://haskell.org/ghc/docs/latest/html/libraries/time/Data-Time-Clock.html>

Actually, though, as well as being more than a little pedantic, this is I think a fairly brilliant example of good risk management: by forcing programmers to stop and make a choice between a DiffTime (which includes leap seconds) and a NominalDiffTime (which more or less pretends they don't exist), it also forces them to think for a moment about what exactly they're doing.

So kudos to Ashley Yakeley, the rather smart author of this library.

Curt Sampson <cjs@starling-software.com> +81 90 7737 2974 Functional programming in all senses of the word: <http://www.starling-software.com>

✱ Workshop on GENI and Security: Call for Participation

<Matt Bishop <bishop@cs.ucdavis.edu>>
Thu, 4 Dec 2008 13:36:48 -0800

Workshop on GENI and Security
January 22-23, 2009
Davis, California, USA

The Global Environment for Network Innovations (GENI) is a suite of network research infrastructures now in its design and prototyping phase. It is sponsored by the National Science Foundation to support experimental research in network science and engineering. The goal of this workshop is to engage the security community in GENI's design and prototyping, to ensure that security issues are properly considered during its development.

First, what classes of security experiments should GENI support? What capabilities will GENI require to allow the conduct of these experiments? Second, how can GENI itself be adequately secured and protected from attack? What forms of authentication, authorization, and accountability would be most appropriate?

As the GENI Project Office expects to issue its 2nd solicitation for GENI analysis and prototyping subcontracts in the middle of December, with proposals due in mid-February, it is anticipated that topics discussed at the workshop will lead to proposals from the security community.

Participation. We invite short (1 paragraph preferably; at most 1 page) statements of ideas addressing these two issues. Submit your statement to geni-workshop@cs.ucdavis.edu by December 18. Please use either PDF or text.

For more information: <http://seclab.cs.ucdavis.edu/meetings/genisec>

Matt Bishop, UC Davis

MiniMetricon call for participation

<Fred Cohen <fc@all.net>>

Wed, 3 Dec 2008 16:21:03 -0800

For those interested in security metrics, here is the link to the Call for Participation for MiniMetricon 3.5. [20 April 2009, Moscone Center SF]

<http://www.securitymetrics.org/content/Wiki.jsp?page=Metricon3.5>

Fred Cohen & Associates 572 Leona Drive Livermore, CA 94550 1-925-454-0171
<http://all.net/>

[Frequent RISKS contributors Fred and Jeremy Epstein are on the PC. PGN]

REVIEW: "The History of Information Security", de Leeuw/Bergstra

<Rob Slade <rMslade@shaw.ca>>

Thu, 4 Dec 2008 11:03:07 -0800

BKHISCCH.RVW 20081020

"The History of Information Security", Karl de Leeuw/Jan Bergstra,
2007, 978-0-444-51608-4

%E Karl de Leeuw karl.de.leeuw@xs4all.nl

%E Jan Bergstra

%C 256 Banbury Road, Oxford, OX2 7DH

%D 2007

%G 978-0-444-51608-4

%I Elsevier Advanced Technology

%O +44 865 512242 Fax: +44 865 310981 books.elsevier.com

%O <http://www.amazon.com/exec/obidos/ASIN/0444516085/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0444516085/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0444516085/robsladesin03-20>

%O Audience i Tech 1 Writing 2 (see [revfaq.htm](#) for explanation)

%P 887 p.

%T "The History of Information Security: A Comprehensive Handbook"

Chapter one, which stands in for an introduction to the papers in this volume, already notes that the title is inaccurate. The editor admits

that this work is not a history, as such, but an overview from the perspective of different disciplines related to information security, taking a historical approach in examining the socio-political shaping of infosec. The authors ask whether technology influenced public policy and politics, and look for information security strategies (or the lack thereof) in politics. I found the selection of references disquieting, noting that the editor responsible for the choice of papers complained that there was no historical material addressing industrial espionage, administrative practices, disruption of communications with criminal intent, or other areas. No mention is made, in the references, to the works of Stamp (cf. BKINSCPP.RVW), Winkler (cf. BKCRPESP.RVW, BKSPAMUS.RVW), or Denning (cf. BKDENING.RVW) to name just a few.

I can agree with the emphasis on social aspects of security: security is, and always has been, a people problem. Information security, however, necessarily involves technology, and the authors of most of the papers included in this collection have concentrated so much on history (mostly in the form of dates and political rivalries) that the questions of influence of technology on politics, or politics on technology, can't really be analyzed. Additionally, enormous topical areas relevant to information security (such as risk management, intrusion detection, cryptographic infrastructure (PKI), physical security, computer architecture, application development, and malware) are notable by their absence.

Part one addresses intellectual property. Essay subjects include various forms of censorship and self-censorship (with no mention of the "full disclosure" debate), the German patent system, copyright, and the application of copyright and patent to software.

Part two looks at items related to identity management, with a highly abstract and impractical philosophy of identity, notes on document security, a review of identity cards, and a recent history of biometrics.

Although entitled "Communications Security," part three is about cryptography. The papers on Renaissance (1400-1650) and Dutch (up to 1800) cryptography, British postal interception up until the 1700s, the KGB crypto office, and the NSA (US National Security Agency) are of primarily political interest. The articles on rotor cryptography, Colossus, and the Hagelin machines have points of curiosity, but are still very thin on technical details. A final essay attempts a very terse overview of modern cryptographic concepts.

Computer security is in part four. Early US military evaluation standards, some of the basic formal information security models, an academic look at application security and auditing, a rough division of recent information technology into decade "periods," an equally unpolished history of Internet security, and a scattered review of computer crime make up this section.

For some reason questions of privacy and regulations governing the export of cryptography are seen to fit together in part five. Three

papers present US cryptographic export restrictions, a random and not completely successful attempt to define privacy, and various US undertakings at regulating the use of encryption.

Part five can't have been lumped together simply due to a lack of articles, since part six is a single piece providing a limited and incomplete overview of information warfare.

As a book this volume is disappointing. It is not "a history," merely a collection of papers, with little structure or linkage. The topics relate to security, but a work on infosec should have more technical content and understanding. It is certainly not comprehensive. And, at several kilograms in weight, it bears little resemblance to a handbook.

That said, a number of the essays do provide interesting historical points, anecdotes, and references. Therefore, those with the stamina to work through the material may be rewarded with historical nuggets, and pointers to further sources of information.

copyright Robert M. Slade, 2008 BKHISCCH.RVW 20081020
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
victoria.tc.ca/techrev/rms.htm blogs.securiteam.com/index.php/archives/author/p1/



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 48

Thursday 18 December 2008

Contents

- [Computer problem shuts down Toronto Stock Exchange for a day](#)
[Mark Brader](#)
 - ["Smart" vehicles - do they introduce new risks?](#)
[Mike Martin](#)
 - [An old clock arithmetic problem](#)
[Kees Huyser](#)
 - [Another translation adventure](#)
[Hal Murray](#)
 - [Cute piece of malware engineering](#)
[Drew Dean](#)
 - [Thieves Winning Online War, Maybe Even in Your Computer](#)
[John Markoff](#) via [Monty Solomon](#)
 - [CheckFree DNS hijacked](#)
[Hal Murray](#)
 - [Software Security Top-10 Surprises](#)
[Gary McGraw](#) via [PGN](#)
 - [iPhone thief thwarted by MobileMe sync](#)
[Nick Rothwell](#)
 - [Risks of data retention](#)
[Mark Armbrust](#)
 - [Password complexity? Not wiith LinkedIn](#)
[Leon Kuunders](#)
 - [Teacher Throws Fit Over Student's Linux CD](#)
[Mike Rechtman](#)
 - [FYI - !b404](#)
[Rob Slade](#)
 - ["Helpful" authentication](#)
[Erling Kristiansen](#)
 - [The Perfect Law: Re: Dangerous Precedence Set](#)
[Martin Ward](#)
 - [REVIEW: "The Business Privacy Law Handbook", Charles H. Kennedy](#)
[Rob Slade](#)
 - [Info on RISKS \(\[comp.risks\]\(#\)\)](#)
-

Computer problem shuts down Toronto Stock Exchange for a day

<msb@vex.net (Mark Brader)>

Thu, 18 Dec 2008 16:23:48 -0500 (EST)

This is not what it usually means to say "the stock market was down" or "the stock market crashed"!

Yesterday the Toronto Stock Exchange (TSX) and the affiliated TSX Venture Exchange were open for only 18 minutes after early trading revealed a problem with the quotes being sent out. This was reported as a "network firmware issue" that "resulted in complications with data sequencing"; the backup system also failed.

The problem was not rectified until late enough in the afternoon that it had already been decided to close for the day.

See: <http://www.cbc.ca/money/story/2008/12/18/tsxresumption.html>

Mark Brader, Toronto, msb@vex.net | "Fast, cheap, good: choose any two."

"Smart" vehicles - do they introduce new risks?

<"mike martin" <mke.martn@gmail.com>>

Sun, 14 Dec 2008 10:56:48 +1100

The Economist reports this week on technology-based measures that vehicle manufacturers are introducing to prevent or ameliorate traffic accidents:

"Many of these safety systems at first give warning of impending danger before taking over. Despite that potential delay they still provide what Rodolfo Schöneburg, Daimler's head of passive safety, has described as an "electronic crumple zone": applying the brakes a bit late rather than not at all will at least reduce the impact of a collision.

"Yet sometimes there is no room for any delay in avoiding an accident, for instance when a vehicle jumps a stop sign at a busy junction. This means safety systems will need to become even more autonomous in order to act faster -- faster, probably, than people can. But because cars will be acting independently of each other, this raises safety concerns of its own.

"Researchers worry, for example, about what might happen if a child ran into a busy road. If one car automatically slammed on its brakes and swerved, it could prompt others to take evasive action. The result of all these automatic, independent decisions could be a pile-up causing more deaths, injuries and damage than there would have been had drivers remained in charge. So some researchers are now looking at ways in which vehicles could co-ordinate their crash-avoidance manoeuvres. This means that in an emergency cars would have to tell each other at once what they were about to do, says Thomas Batz of the Fraunhofer Institute for Information and Data

Processing in Karlsruhe, Germany."

http://www.economist.com/science/displaystory.cfm?story_id=12758720

Collision avoidance (TCAS) technology has been generally beneficial in aircraft, although the 2002 mid-air collision of two planes over Switzerland resulted from conflict between a TCAS instruction and one from an air traffic controller ("July 2002 air collision revisited", [RISKS-23.23](#) <<http://catless.ncl.ac.uk/Risks/23.23.html#subj1>>). However motor vehicle drivers rarely have the same degree of training in how to handle emergencies as airline pilots. A study by an Australian university found that while vehicles equipped with ABS (anti-skid) brakes were less likely to be involved in multi-vehicle crashes compared with the same models lacking ABS brakes, they were 35% over-involved in single-car accidents, <http://www.racv.com.au/wps/wcm/connect/Internet/Primary/my+car/car+safety/safety+equipment/brakes/ABS/>.

Advanced technology protection systems may confuse drivers not used to their action in an emergency or may cause them to become over-confident and take risks that they otherwise would not. Paying hundreds, or perhaps thousands, of dollars extra for technology that allows a driver to feel safer may not result in that driver actually being safer. I haven't even started to speculate on risk of software defects in these systems.

✶ An old clock arithmetic problem

<Kees Huyser <kees.huyser@nikhef.nl>>

Tue, 9 Dec 2008 09:39:56 +0100

[Re: Risks of assuming constant hours in a day (Sampson, [RISKS-25.47](#))]

About 20 years ago my then-boss discovered a systematic difference in the time accounting software that was running on our mainframe computer. This accounting software would calculate for what length of time a user had been using a given resource on the computer.

The computer was running Unix and, since we had a source license, the boss started digging into the source code. He eventually found the error not in the accounting software, but on a lower level in the operating system where a programmer in the USA had assumed that the whole world did things the way they were done in America.

The error? Seconds = Hertz

[I presume that programmer would have been "in Dutch" with your then-boss, with some frequency! PGN]

✶ Another translation adventure

<Hal Murray <hmurray@megapathdsl.net>>

Thu, 11 Dec 2008 15:33:18 -0800

One of Europe's most prestigious scientific journals, the *Max Planck Forschung* (Research) journal had a special issue on China. The cover art in the German language edition was supposed to be an example of Chinese calligraphy, a poem, but actually was an ad for a Hong Kong strip joint. (It had been allegedly vetted by a respected Sinologist.) In the online and subsequent English print versions, the cover art was replaced with calligraphy written by a 16th-century Jesuit titled Illustrated Explanations of Strange Devices, as shown in the website, which also provides some translations of the original. [PGN-ed]

<http://www.smh.com.au/news/home/technology/eminant-scientific-journal-gets-hit-for-sex/2008/12/11/1228584998876.html>

✂ Cute piece of malware engineering

<Drew Dean <ddean@csl.sri.com>>
Tue, 9 Dec 2008 11:21:25 -0800

Recently, I've been receiving a number of obvious spams with a ZIP file attached, the zip file name being <my email address>.zip. Today, for amusement, I saved the download to take a look at it: there was one file in the ZIP archive, named with my email address: ddean@csl.sri.com . The Unix file(1) program told me everything I needed to know: it's a Windows executable. Now, the .COM extension denotes an ancient MS-DOS executable file format, which, IIRC, is restricted to 64KB of code and data, etc. (The file in question is 28KB or so, UPX compressed [whatever that is].)

But that's a beautiful attempt at social engineering: most people probably don't remember .com being an executable file format, and what harm could a file named with your email address do? Not having Windows handy, I couldn't easily find out, nor would I want to in any case....

✂ Thieves Winning Online War, Maybe Even in Your Computer (Markoff)

<Monty Solomon <monty@roscom.com>>
Tue, 9 Dec 2008 23:15:51 -0500

John Markoff, *The New York Times*, 6 Dec 2008

Internet security is broken, and nobody seems to know quite how to fix it.

Despite the efforts of the computer security industry and a half-decade struggle by Microsoft to protect its Windows operating system, malicious software is spreading faster than ever. The so-called malware surreptitiously takes over a PC and then uses that computer to spread more malware to other machines exponentially. Computer scientists and security researchers acknowledge they cannot get ahead of the onslaught.

As more business and social life has moved onto the Web, criminals thriving on an underground economy of credit card thefts, bank fraud and other scams rob computer users of an estimated \$100 billion a year, according to a conservative estimate by the Organization for Security and Cooperation in Europe. A Russian company that sells fake antivirus software that actually takes over a computer pays its illicit distributors as much as \$5 million a year.

With vast resources from stolen credit card and other financial information, the cyberattackers are handily winning a technology arms race.

"Right now the bad guys are improving more quickly than the good guys," said Patrick Lincoln, director of the computer science laboratory at SRI International, a science and technology research group.

A well-financed computer underground has built an advantage by working in countries that have global Internet connections but authorities with little appetite for prosecuting offenders who are bringing in significant amounts of foreign currency. That was driven home in late October when RSA FraudAction Research Lab, a security consulting group based in Bedford, Mass., discovered a cache of half a million credit card numbers and bank account log-ins that had been stolen by a network of so-called zombie computers remotely controlled by an online gang. ...

<http://www.nytimes.com/2008/12/06/technology/internet/06security.html>

✂ CheckFree DNS hijacked

<Hal Murray <hmurray@megapathdsl.net>>
Mon, 08 Dec 2008 20:07:15 -0800

Hackers Hijacked Large E-Bill Payment Site

http://voices.washingtonpost.com/securityfix/2008/12/hackers_hijacked_large_e-bill.html

The attack, first reported by *The Register* began in the early morning hours of 2 Dec 2008, when CheckFree's home page and the customer login page were redirected to a server in the Ukraine. CheckFree spokeswoman Melanie Tolley said users who visited the sites during the attack would have been redirected to a blank page that tried to install malware.

Digging Deeper Into the CheckFree Attack

http://voices.washingtonpost.com/securityfix/2008/12/digging_deeper_into_the_checkf.html?nav=rss_blog

The hijacking of the nation's largest e-bill payment system this week offers a glimpse of an attack that experts say is likely to become more common in 2009.

A spokeswoman for Network Solutions, the Herndon, Va., domain registrar that

CheckFree used to register its Web site name, told Security Fix Wednesday that someone had used the correct credentials needed to access and make changes to CheckFree's Web site records.

CheckFree controls between 70 to 80 percent of the U.S. online bill pay market. Still, the phishing angle suggests that the attackers managed to phish not only an employee at CheckFree, but an employee who happened to know the credentials needed to administer the company's site records.

I can think of a couple of ideas that would help avoid disasters like this.

Spreading the word about this particular event is probably the most important. People need to understand why they are doing all the extra silly work.

I think the registration update procedure for major domains should require more than a simple web login. One approach would be a phone call by the registrar to a number setup out of band. The cost would be minor since the data doesn't change very often.

Of course, people with valuable passwords should take good care of them. Using it on a Windows machine is obviously a high risk. So is using a system you aren't familiar with.

If I was paranoid enough, I'd probably store the password on paper and never store it on a disk. To do something that needs that password I'd boot a system that runs from a CD. If I had to use Windows, I'd use a system that had been freshly installed and was behind a good firewall. A good web proxy and lots of logging might help.

How many other important passwords does a company like CheckFree have?

✶ Software Security Top-10 Surprises

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

Thu, 18 Dec 2008 14:04:03 PST

Gary McGraw <gem@cigital.com> thought RISKS readers might get a kick out of an article just published by Gary, Brian Chess, and Sammy Migues:

<http://www.informit.com/articles/article.aspx?p=1315431>

✶ iPhone thief thwarted by MobileMe sync

<Nick Rothwell <nick@cassiel.com>>

Thu, 18 Dec 2008 16:14:55 +0000

"While at the dry cleaner one day, Rob's iPhone was stolen. He immediately

chalked it up as gone forever, and proceeded to purchase a brand new one that same evening. It was the next day when unfamiliar contacts began to appear on the new phone. The (not-too-bright) thief was unwittingly supplying him with names and phone numbers of his or her closest friends, via the magic of MobileMe synchronization from the stolen phone to the cloud and eventually to his new phone."

<http://www.tuaw.com/2008/12/17/iphone-thief-thwarted-by-mobileme-sync/>

Nick Rothwell / Cassiel.com Limited www.cassiel.com

✂ Risks of data retention

<Mark Armbrust <mark.armbrust@pobox.com>>

Thu, 18 Dec 2008 14:17:58 -0700

I received a phone call yesterday morning from Fed Ex Freight confirming that I had equipment available to unload the 28 foot beam that they were delivering today. My name, my cell phone number, my home address.

Well, I'm happy they called to make sure I can get my load off the flatbed truck that's delivering it, but there's a small problem -- this is not my order. I've never hear of the shipper, some redwood products company in California.

I haven't heard anything more from Fed Ex so I assume they figured out where this beam was supposed to go.

I had some furniture shipped by Fed Ex Freight earlier this year. A one time shipment that was arranged by the furniture vendor with shipping fees paid through the vendor.

I'm assuming that an account was created for the destination address for my shipment, and that account still exists and somebody at Fed Ex mistyped the account number for the actual destination and got my (should have been temporary) account number and the beam made an erroneous 1200 mile trip to Colorado.

Two things are fairly obvious:

- o One-time accounts should be very hard, if not impossible, to reuse. They should also have short purge times.
- o Account numbers should have check codes to preclude typical entry errors like transpositions and off by ones.

I wonder where that beam was supposed to go!

I wonder if I'll get a bill for the shipping!

✂ Password complexity? Not wiith LinkedIn

<Leon Kuunders <leon@kuunders.info>>

Fri, 12 Dec 2008 10:30:59 +0100

The social network website LinkedIn is very well known. It is the place where professionals meet and extend their networks. Just as other social network sites the LinkedIn network offers third parties the ability to add applications to their framework. There are API's for Amazon, Huddle, Google and also one for Slideshare.net. This last website offers you the possibility to publish your presentations online.

When you add the Slideshare API to your LinkedIn profile you are able to connect your Slideshare account to your LinkedIn profile. The way it works: you enter your user-id and password of Slideshare into a box, and presto! your Slideshare profile is linked.

I tried it several times but failed. Somehow the system kept telling me that my user-id and/or password did not match the ones used at Slideshare. First I wondered: is it my username ("leon") which has too few characters? But then it occurred to me: it was the "complexity" of my password that caused the problems. My password (generated with a password generator) was "az<VK/gq#".

Notice the "<" sign?

The risks: a chain is as strong as the weakest link (..edIn).

leon@kuunders.info <http://xri.net/@trusted-id/leon> skype://leonkuunders

Teacher Throws Fit Over Student's Linux CD

<Mike Rechtman <mike@rechtman.com>>

Sat, 13 Dec 2008 15:58:31 +0200

http://austinist.com/2008/12/10/aisd_teacher_throws_fit_over_studen.php

Free? - That's illegal!

A teacher has thrown a student into detention and threatened to call the police for using Linux in her classroom.

The teacher spotted one of her students giving a demonstration of the HeliOS distro to other students. In a somewhat over-the-top reaction, she confiscated the CDs, put the student on detention and whipped off a letter to the HeliOS Project threatening to report it to the police for distributing illegal software.

Home: <http://alpha.mike-r.com/> QOTD: <http://alpha.mike-r.com/php/qotd.php>

FYI - !b404

<Rob Slade <rMslade@shaw.ca>>
Wed, 10 Dec 2008 17:37:33 -0800

An interesting study. As one who has published an infosec dictionary, I've seen, first hand, how fast our technical jargon has changed (and often degraded). The effect of the technology, and the pervasive nature of the changes, is intriguing.

Highlights:

- new communications technology, particularly text messaging abbreviations (textese), creating new terms entering the language
- errors by the technology ("predictive" numeric keypad text interpretation of "book" instead of "cool") creating new slang (book now means cool or good) *
- terms from local technologies (the Oyster card error codes) are entering the language more broadly
- textese messages take longer to read, and generate more errors

<http://news.bbc.co.uk/2/hi/technology/7775013.stm>
<ftp://ftp.royalmail.com/Downloads/public/ctf/po/TechChat-Draft2.pdf>

(Unfortunately, a link to the Australian study seems to be missing.)

Relevance to security? Well, I don't agree with the final statement in the BBC story. Any change to the language that increases the error level in communications has got to be dangerous.

* I've heard my grandkids say this, and wondered where it came from. The technical reasons for this are fascinating in themselves. Predictive typing technology is based on the numeric keypad equivalent of words, and is based on the frequency of word usage in English. "Book" and "cool" are equivalent (2665) on a numeric keypad. In general English, book is going to be the more widely used word, and so the algorithm chooses book first when you type 2665. However, textese is used by teens much more widely than by the rest of the population, and I am morally certain that teen textese uses cool much more frequently than it uses book.

I am also interested in competition in terms of the acronyms. LAMP has been widely used in technical (and particularly online) circles to refer to the use of Linux, Apache, MySQL, and PHP/Python/Perl for the creation of Websites. It is interesting to note a completely different use of LAMP in the financial arena. (We already have a similar confusion of SOA depending upon whether the speaker is from the BS 7799/ISO 27K community [statement of applicability, aka scope] or the ITIL tribe [service oriented architecture].)

rslade@vcn.bc.ca rslade@computercrime.org victoria.tc.ca/techrev/rms.htm
blogs.securiteam.com/index.php/archives/author/p1/

 "Helpful" authentication

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>

Fri, 12 Dec 2008 17:06:08 +0100

I phoned my credit card company.

After giving my name and address, the following conversation took place:

Credit card guy: Please give me your date of birth for authentication.

Me: <my date of birth>

Credit card guy, sounding genuinely surprised: Strange, I have a completely different date. I have <another date>.

Me: That's my wife's date of birth.

(which is true, but he couldn't really know that, my wife hasn't got a card with that company; I could have said that to whatever date he had given me).

This seemed to satisfy him, and we proceeded with the business I called about.

✂ The Perfect Law: Re: Dangerous Precedence Set

<Martin Ward <martin@gkc.org.uk>>

Tue, 9 Dec 2008 11:34:02 +0000

(Re: Federal Criminal Charges for Violation of Commercial Online ToS?)

>From the government's point of view, the "Perfect Law" is one which everyone has broken. With this law, anyone the government does not like (for whatever reason) can be arrested and imprisoned.

>From the citizen's point of view, such a law means the end of the rule of law. You are now living in a tyranny: any criticism of the government could land you in jail with no recourse.

"But," you protest, "I haven't violated the Terms of Service of any web site!" What about that government-run web site which just about everyone in the country is required to sign up for. On page 16 of the voluminous Terms of Service is a poorly-worded note to the effect that anyone who criticises any action of the government is in violation of the Terms of Service of this web site.

martin@gkc.org.uk <http://www.cse.dmu.ac.uk/~mward/>

✂ REVIEW: "The Business Privacy Law Handbook", Charles H. Kennedy

<Rob Slade <rMslade@shaw.ca>>

Thu, 18 Dec 2008 12:18:25 -0800

BKBUPRLH.RVW 20081123

"The Business Privacy Law Handbook", Charles H. Kennedy, 2008,
978-1-59693-176-3, U\$109.00

%A Charles H. Kennedy ckennedy@mofo.com

%C 685 Canton St., Norwood, MA 02062

%D 2008

%G 978-1-59693-176-3 1-59693-176-0

%I Artech House/Horizon

%O U\$109.00 617-769-9750 800-225-9977 artech@artech-house.com

%O <http://www.amazon.com/exec/obidos/ASIN/1596931760/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/1596931760/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/1596931760/robsladesin03-20>

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

%P 312 p.

%T "The Business Privacy Law Handbook"

The preface states that this is a survey of business privacy law in the United States, and the changes that field is undergoing, intended for business managers and those advising them. The introduction is rather interesting: on the one hand, it lays out a five-step process to guide the task of ensuring compliance with privacy regulations, and on the other, it points out how complex this undertaking is, in the labyrinthine legal environment of the US.

Part one addresses issues of information relating to consumers and customers. Chapter one deals with information collected on the Internet and through Websites. As the US has no general national standards in this regard, most of the discussion deals with the design of corporate privacy policies for Websites. There is also an examination of the Children's Online Privacy Protection Act (COPPA). Various US and state laws with implications for general information security and protection are noted in chapter two, which also has a brief section on information risk identification. Legislation relating to companies in the financial industry are reviewed in chapter three. Chapter four notes the provisions of the Electronic Communications Privacy Act, the Stored Communications Act, and special provisions for communications carriers. The implications of HIPAA (the Health Insurance Portability and Accountability Act) for the health industry are outlined in chapter five, which also notes some related state laws. Although ostensibly about the European Union privacy directives, the rather terse material in chapter six is more about the Safe Harbor framework of the US Department of Commerce.

Part two looks at job applicants and employees. Chapter seven is a brief review of the hiring process, and it is interesting to note that the common opposition (by employers) to providing detailed references has little objective basis. The examination of internal investigations, as discussed in chapter eight, is limited, and repeats content from chapter seven. Chapter nine's deliberation on surveillance is primarily concerned with tapping of phone and email conversations.

Part three turns to communications with customers and consumers, with three successive chapters on marketing types of intercourse; telemarketing (in chapter ten), fax advertising (eleven), and spam (twelve). Chapter thirteen, on the monitoring of customer communications, is a mere three paragraphs in total length, and is a reiteration of some of the content of chapter nine.

Appendices list state privacy and data security laws.

It is unfortunate that the title does not make clear the US-centric nature of the material, but it is reasonable for a legal text to concentrate on one jurisdiction. Despite occasional shortcomings in specific areas, this text does provide a detailed, up-to-date and quite comprehensive overview of the convoluted mess of American privacy law.

copyright Robert M. Slade, 2008 BKBUPRLH.RVW 20081123
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
victoria.tc.ca/techrev/rms.htm blogs.securiteam.com/index.php/archives/author/p1/



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 49

Tuesday 30 December 2008

Contents

- [Three undersea cables cut](#)
[Dave Burstein via Dave Farber](#)
- [Risks of flawed default behavior for your UAV](#)
[John O Long](#)
- [Risks of excessive State data collection](#)
[Toby Douglass](#)
- [Fun with speed-trap cameras for revenge](#)
[Arthur T.](#)
[David Hollman](#)
[No-Name](#)
- [Trust me, I have a cert!](#)
[David Leshner](#)
- [Massive Embezzlement Case Involving Fry's Electronics](#)
[Lauren Weinstein](#)
- [Fired Fry's executive: 'Caught up in the game'](#)
[Lisa Fernandez and Julia Prodis Sulek via Monty Solomon](#)
- [In Move to Digital TV, Confusion Is in the Air](#)
[Eric A. Taub via Monty Solomon](#)
- [VHS Rides Off Into The Sunset](#)
[Geoff Duncan via Monty Solomon](#)
- [Inauguration Cellular Overloads](#)
[David Leshner](#)
- [Automatic URL recognition](#)
[Bill Hopkins](#)
- [Shooting Yourself in the Foot - on purpose?](#)
[Marc](#)
- [Another method to lose your credit card](#)
[Erich Neuhauser](#)
- [Re: Cute piece of malware engineering](#)
[Paul Robinson](#)
- [Re: Teacher Throws Fit Over Student's Linux CD](#)
[Kelly Bert Manning](#)
- [How to become a digital forensic evidence expert](#)
[Fred Cohen](#)
- [Info on RISKS \(comp.risks\)](#)

✂ Three undersea cables cut (via Dave Farber's IP)

<Dave Burstein <daveb@dslprime.com>>

December 19, 2008 11:27:46 AM EST

Traffic greatly disturbed between Europe and Asia/Near East zone

> From: France Telecom / Press <infos.group@orange-ftgroup.com>

> To: France Telecom / Press <infos.group@orange-ftgroup.com>

> Subject: Three undersea cables cut: traffic greatly disturbed

> between Europe and Asia/Near East zone

> Date: Fri, 19 Dec 2008 17:09:03 +0100 (CET)

http://www.orange.com/en_EN/press/press_releases/cp081219en.html

Paris, 19 Dec 2008

France Telecom Marine cable ship about to depart

France Telecom observed today that 3 major underwater cables were cut: Sea Me We 4 at 7:28am, Sea Me We3 at 7:33am and FLAG at 8:06am. The causes of the cut, which is located in the Mediterranean between Sicily and Tunisia, on sections linking Sicily to Egypt, remain unclear.

Most of the B to B traffic between Europe and Asia is rerouted through the USA. Traffic from Europe to Algeria and Tunisia is not affected, but traffic from Europe to the Near East and Asia is interrupted to a greater or lesser extent (see country list below). Part of the internet traffic towards Reunion is affected as well as 50% towards Jordan. A first appraisal at 7:44 am UTC gave an estimate of the following impact on the voice traffic (in percentage of out-of-service capacity):

- Saudi Arabia: 55%
- Djibouti: 71%
- Egypt: 52%
- United Arab Emirates: 68%
- India: 82%
- Lebanon: 16%
- Malaysia: 42%
- Maldives: 100%
- Pakistan: 51%
- Qatar: 73%
- Syria: 36%
- Taiwan: 39%
- Yemen: 38%
- Zambia: 62%

France Telecom immediately alerted one of the two maintenance boats based in the Mediterranean area, the Raymond Croze. This France Telecom Marine cable ship based at Seyne-sur-Mer has received its mobilization order early this afternoon and will cast off tonight at 3:00 am with 20 kilometers spare cable on board. It should be on location on Monday morning for a relief

mission. Priority will be given to the recovery of the Sea Me We4 cable, then on the Sea Me We3. By December 25th, Sea Me We4 could be operating. By December 31st, the situation should be back to normal.

✂ Risks of flawed default behavior for your UAV

*<John O Long <j1long@us.ibm.com>>
Tue, 30 Dec 2008 14:18:10 -0500*

The Homesick UAV, 29 Dec 2008, <http://www.strategypage.com>:

In 2007, Ireland bought two Israeli Orbiter UAV systems, for \$550,000 each. They had lost two of their six UAVs in Chad, where a battalion of Irish peacekeepers are operating. The second one UAV casualty apparently tried to fly back to Ireland, after it lost its communications link with the operator. The Orbiter is programmed to head back to the operator if it loses its comm link. But this Orbiter apparently still had a GPS location back in Ireland in its memory, and headed there. Since Ireland is 5,000 kilometers from Chad, the Orbiter ran out of juice and landed about 4,800 kilometers short of its goal.

The designers were trying to provide some appropriate default behavior in case the UAV lost contact with its operator. This is good, and may not have been a big deal in Israel, because most of its UAVs are operated near its borders. No one thought about the possibility of using the UAV far outside a country's borders. It should have recorded the original operator's location in order to fly back to that location.

John O Long * Process Architect - IBM Tivoli Unified Process
919-224-1446 t/l 687-1446 * j1long@us.ibm.com

[Erin go blagh? Erin call home. PGN]

✂ Risks of excessive State data collection

*<"Toby Douglass" <trd@45mercystreet.com>>
Tue, 30 Dec 2008 20:39:58 +0100 (CET)*

A British Government report, funded by money taken through tax, argues for speed limiting devices on cars. Argues it will reduce car accidents with injuries by 29%.

<http://news.bbc.co.uk/1/hi/uk/7803997.stm>

First questions; 29% of what? what's the period which is being used to compare against? is it representative? does it just include cars, or lorries? does it include all roads, everywhere, or just (say) cities? what about accidents with fatalities? what about the additional accidents which will happen now, where people previously managed to escape by accelerating

out of danger? how do they figure that accidents would be reduced anyway? I'm kinda wondering if they just took existing car accident statistics (how accurate are they? on what basis are they calculated?), looked at those accidents which happened where speeding was involved, and applied some sort of reducing factor they constructed.

What about accidents which would have happened anyway, even if they cars had been doing the local speed limit? presumably this was accounted for in their reducing factor? if so, by how much? how do you decide what reduction to use?

It works like this; each car has a GPS unit. Each car has a speed-limiting unit, which contains a map of the roads in the UK and their speed limits and since GPS is there, knows where the car is, and prevents the car going faster than the speed limit.

First thoughts; you know as well as I do that unit will record your journeys and that data will be available, by law, to the State, and that your car, sooner or later, will be legally obliged to carry that unit.

All because powers are granted to a State by a democratic process does not mean the State will use them democratically.

What about our right of privacy? of simply being left alone?

Here's another thought; what if there's an emergency and you need to break the local speed limit? will there be an over-ride switch? if so, what's to stop it being permanently turned on? will it have a time-out? what if the time-out is too short or too long? and if your unit notices that you are persistently breaking the local speed limit, what's it going to do? will it report you to the police? will, next time you car is serviced, the record of all your journeys be checked for breaking the speed limit and then you'll be charged?

Fun with speed-trap cameras for revenge

*<"Arthur T." <Risk200812.risk.atsjbt@xoxy.net>>
Tue, 23 Dec 2008 00:11:21 -0500*

According to one news article, students are printing up fake license plates specifically in order to speed past speedcams. The person whose plate was printed then gets a bill for the fine.

There's no reason it wouldn't work, as long as the speedcams don't also get pictures of the driver (as they do in England). However, the one story on it that I saw is not convincing. All of the reports of its occurrences seem to come from one unnamed source. One of the quotes may be correct regardless, though: "It will cause potential problems for the Speed Camera Program in terms of the confidence in it."

Montgomery [Maryland] County Sentinel, 11 Dec 2008

<http://www.thesentinel.com/302730670790449.php>

✶ Fun with speed-trap cameras for revenge

<"David Hollman" <dah8@cornell.edu>>

Tue, 23 Dec 2008 00:41:32 +0000

Students Use Speed Cameras to Frame Innocent Drivers, Prank Teachers

<http://www.dailytech.com/Students+Use+Speed+Cameras+to+Frame+Innocent+Drivers+Prank+Teachers/article13749.htm>

"I've objected to the robotic menaces primarily on the grounds that they were fallible revenue machines for the state rather than legitimate means of protecting life and limb," said Examiner.com's J.D. Tucille. "It never occurred to me that the [speed cameras] were also handy tools for wreaking revenge on enemies and authority figures. That was clearly a lapse of imagination on my part."

Aside from the pranking itself, a secondary effect may be to diminish trust in the legitimacy of valid tickets (particularly since it was reported some perpetrators used similar-looking cars to the victim's). Good quality and access to the data collected would help to address this (e.g., are the photos provided with the ticket? High or low res? Color or B&W? etc...) as better data should make it easier to prove there was fraud. But on whom does the burden of proof lie?

✶ Fun with speed-trap cameras for revenge

<No-Name <labmanager@gmail.com>>

December 20, 2008 2:46:21 PM EST

Maryland Students Use Speed Cameras for Revenge (via Dave Farber's IP)

<http://www.thenewspaper.com/news/26/2632.asp>

Maryland Students Use Speed Cameras for Revenge

Students in Montgomery County, Maryland use fake license plates to send speed camera tickets to enemies.

Maryland plate, photo by Amy the Nurse/FlickrHigh school students in Maryland are using speed cameras as a tool to fine innocent drivers in a game, according to the Montgomery County Sentinel newspaper. Because photo enforcement devices will automatically mail out a ticket to any registered vehicle owner based solely on a photograph of a license plate, any driver could receive a ticket if someone else creates a duplicate of his license plate and drives quickly past a speed camera. The private companies that mail out the tickets often do not bother to verify whether vehicle registration information for the accused vehicle matches the photographed vehicle.

In the UK, this is known as number plate cloning, where thieves will find the license information of a vehicle similar in appearance to the one they wish to drive. They will use that information to purchase a real license plate from a private vendor using the other vehicle's numbers. This allows the "cloned" vehicle to avoid all automated punishment systems. According to the Sentinel, two Rockville, Maryland high schools call their version of cloning the "speed camera pimping game."

A speed camera is located out in front of Wootton High School, providing a convenient location for generating the false tickets. Instead of purchasing license plates, students have ready access to laser printers that can create duplicate license plates using glossy paper using readily available fonts. For example, the state name of "Maryland" appears on plates in a font similar to Garamond Number 5 Swash Italic. Once the camera flashes, the driver can quickly pull over and remove the fake paper plate. The victim will receive a \$40 ticket in the mail weeks later. According to the Sentinel, students at Richard Montgomery High School have also participated, although Montgomery County officials deny having seen any evidence of faked speed camera tickets.

[Source: Local teens claim pranks on county's Speed Cams, *Montgomery County Sentinel* (MD), 11 Dec 2008]

Archives: <https://www.listbox.com/member/archive/247/=now>

✶ Trust me, I have a cert!

<"David Leshner" <wb8foz@panix.com>>
Tue, 30 Dec 2008 14:27:15 -0500 (EST)

<<http://www.win.tue.nl/hashclash/rogue-ca/>>

We have identified a vulnerability in the Internet Public Key Infrastructure (PKI) used to issue digital certificates for secure websites. As a proof of concept we executed a practical attack scenario and successfully created a rogue Certification Authority (CA) certificate trusted by all common web browsers. This certificate allows us to impersonate any website on the Internet, including banking and e-commerce sites secured using the HTTPS protocol.

✶ Massive Embezzlement Case Involving Fry's Electronics

<Lauren Weinstein <lauren@vortex.com>>
Tue, 23 Dec 2008 09:08:22 -0800 (PST)

I dare say that many of us have a love/hate relationship with Fry's Electronics, and their massive, themed stores. There are several of them here in the L.A. area, and my favorite is the SciFi themed (the UFO crashed into the building!) site in Burbank

<http://lauren.vortex.com/archive/000071.html> -- apologies for the horrid cell phone camera photo from more than four years ago). The store out here in the West San Fernando Valley is themed to "Alice in Wonderland" throughout. [Lauren's comment suggests he is a rabbit admirer? PGN]

Fry's has always seemed to have a highly disciplined, very much top-down management style -- to say the least. If you've been there, you know what I mean. Fry's has become the "go to" place for immediate access electronics parts for many years.

Now comes word that the single individual reported to be ultimately responsible for all merchandise stocking at all Fry's has been arrested in a \$65M embezzlement case, complete with gambling debts and jets to Vegas.

<http://www.latimes.com/business/la-fi-frys24-2008dec24,0,7762946.story>

And that's no white rabbit.

lauren@vortex.com +1 (818) 225-2800 lauren@pfir.org <http://lauren.vortex.com>
<http://www.pfir.org/lauren> Network Neutrality Squad - <http://www.nnsquad.org>

[Do you want Fry's with that order instead of Fries? PGN]

✶Fired Fry's executive: 'Caught up in the game' (MercNews)

<Monty Solomon <monty@roscom.com>>
Sun, 28 Dec 2008 23:10:46 -0500

Fired Fry's executive: 'Caught up in the game' in Vegas, Silicon Valley
Lisa Fernandez and Julia Prodis Sulek, *San Jose Mercury News*, 28 Dec 2008

Abbi Vakil was hoping to strike a deal with Fry's Electronics to sell his company's iPhone battery when he first met Omar Siddiqui on the second floor of the company's headquarters on Brokaw Road.

Siddiqui, Fry's vice president of merchandising, wasn't tall, but he looked like he stepped out of the pages of a men's fashion magazine with his sharp tailored suit - the gold chains around his neck notwithstanding. Just as Vakil began his sales pitch, Siddiqui grabbed the \$15 battery and flung it "like a Frisbee" into the credenza.

What happened next gives an indication of just how this high-level executive, the son of a Pakistani diplomat who was crazy about fast cars and blackjack tables, bullied his way over three years into \$65 million in kickbacks from vendors for space on Fry's shelves to try to pay off his gargantuan gambling debts, according to federal authorities. It's an allegation the 42-year-old bachelor now faces in San Jose federal court.

If Vakil's company wanted to do business with Fry's, Siddiqui glowered at him, Vakil would have to pay him \$20,000. "It just didn't make any sense,"

Vakil, now vice president at FastMac.com, told the Mercury News of the 2006 encounter. "How many products would we have to sell to make a profit? We could have been selling horse manure. All he cared about was, 'What's in it for me?' ...

http://www.mercurynews.com/ci_11322297

[Fired? Fried or Fryed! PGN]

✂ In Move to Digital TV, Confusion Is in the Air (Eric A. Taub)

<Monty Solomon <monty@roscom.com>>

Sun, 28 Dec 2008 03:18:18 -0500

Eric A. Taub, *The New York Times*, 22 Dec 2008

The Federal Communications Commission sponsored a Nascar race car as part of its effort to inform Americans that on Feb. 18, television signals transmitted over the air will be transmitted solely in digital format. Old TV sets will no longer work.

It paid \$350,000 to emblazon "The Digital TV Transition" and other phrases on a Ford driven by David Gilliland.

So how's that going? In November, the car crashed during a Nascar race in Phoenix. It was the second crash in as many months.

And how is the digital TV transition going? According to critics, about as well, despite a major marketing campaign that includes nightly ads on TV.

According to surveys conducted by the Consumers Union, a consumer advocacy group that also publishes Consumer Reports magazine, while 90 percent of the nation is aware of the transition, 25 percent mistakenly believe that one must subscribe to cable or satellite after February, and 41 percent think that every TV in a house must have a new converter box, even those that are already connected to cable or satellite. ...

<http://www.nytimes.com/2008/12/22/technology/22digital.html>

✂ VHS Rides Off Into The Sunset (Geoff Duncan)

<Monty Solomon <monty@roscom.com>>

Wed, 24 Dec 2008 17:51:06 -0500

Geoff Duncan, VHS Rides Off Into The Sunset, 23 Dec 2008

<http://news.digitaltrends.com/news-article/18730/vhs-rides-off-into-the-sunset>

The venerable VHS tape is finally vanishing in the rear-view mirror as the last major supplier stop distribution.

VHS tape, the format that for better-and worse-brought video into untold millions of households around the world is finally going the way of the dinosaur -- at least in the United States. After the 2008 holiday season, Distribution Audio Video-the last major distributor of VHS tapes in the United States-is finally calling it quits, and will stop distributing VHS tapes. Although Hollywood hasn't released a movie in VHS format since 2006, a number of bargain retailers were still stocking the format, and it's also lived on in a number of isolated markets like cruise ships, public libraries, military bases, and care facilities.

"It's dead, this is it, this is the last Christmas, without a doubt," said Distribution Video Audio president Ryan J. Kugler, to the L.A. Times. "I was the last one buying VHS and the last one selling it, and I'm done. Anything left in warehouse we'll just give away or throw away."

Consumers have long since indicated their preference for DVD over VHS tapes, and Distribution Audio Video is now in the DVD distribution business -- although it predicts DVDs are also on their way out, to be replaced by Blu-ray.

Nonetheless, the shutdown of the last major VHS distributor in the United States doesn't mean the world has finally embraced digital video. Countless titles and content that have been available on VHS has yet to be released on DVD, whether it be classic films from pre-war Hollywood or simply performances by under-appreciated bands and artists, the amount of material available on DVD has yet to encompass everything that was available on VHS. And, of course, VHS will continue to live for some time in developing markets around the world.

Inauguration Cellular Overloads

*<"David Leshner" <wb8foz@panix.com>>
Fri, 26 Dec 2008 16:33:35 -0500 (EST)*

So with various estimates for the 20 Jan Inauguration turnout running from 1.5 to 5 million people, the cellular industry has been releasing PR about what they are doing to prepare.

The usual approach is to add small portable cell-sites, often "COWs" [Cell On Wheels] with some kind of backhaul to the region's Mobile Telephone Switching Office [MTSO].

They are also pleading with customers to abstain from talking and sending pictures; instead please use SMS/texting. [Texting queues, unlike voice.] And they have more quietly mentioned pecking order control that gives precedence to specific phones, presumably the police chief, various coordinators, etc.

But I have a different concern. Well before the talking stage, each carrier's MTSO must first recognize and register every phone it finds. I

wonder how large the available registration tables are in the various CDMA/GSM/iDen/ MTSS's -- can they even poll and hold all that respond?

Automatic URL recognition

*<"Bill Hopkins" <whopkins@wmi.com>>
Fri, 19 Dec 2008 14:25:58 -0500*

A *Philadelphia Inquirer* article, when rendered for their website, has an interesting artifact of (I suspect) a simple-minded automatic URL recognition algorithm. Is it okay to assume that three consecutive w's won't occur in English, and need not be lexically distinct to start a URL? "Awwwwww," said the RISKS community.

http://www.philly.com/inquirer/weekend/classical_music/20081211_Young_conductor__old_soul__eh_.html

The concert, despite short rehearsal, was fabulous.

[I presume they did not play anything by WacslawWWieniawsky? PGN]

Shooting Yourself in the Foot - on purpose?

*<Marc <Heart.of.Dixie@gmail.com>>
Fri, 19 Dec 2008 12:18:19 -0600*

I'm a Big User of Gmail. I generally don't notice the targeted ads that appear alongside messages, but this one caught my eye:

E-Mail Lists-Free Quotes
Free Quotes from Multiple Brokers Compare & Save - 5000+ names only
[www.\(domain-removed\).com/email_lists](http://www.(domain-removed).com/email_lists)

Is Google trying to use up spare bandwidth & server resources?

Google does have very big feet, though.

Another method to lose your credit card

*<"Erich Neuhauser, ENSOFT GmbH" <E.Neuhauser@ensoft.de>>
Tue, 30 Dec 2008 15:18:18 +0100*

Yesterday, my wife tried to do some transactions on an ATM. Everything looked fine and so she fed her credit card into the appropriate slot. The machine pulled the card inside, the screen turned black and the machine stood still. Very annoyed, she pushed her finger against the dark touchscreen repeatedly. The screen remained dark, but an acoustic signal

told her, that the computer still was alive. As she had some idea about where the Eject-"button" should be on the screen, she repeatedly pushed that position with her finger and after some 10 or 20 tries suddenly here credit card came out of the beast. One more victory of men over machines..

But - what would the system have done, if she had given up after some tries less? Worst: push out the card after a timeout. Best: dump the card to the safe after a timeout. Probably: hold the internal state, waiting for the next visitor (that would find the card slot full and then try - what?).

Handling failures of signaling devices is not new to many technical domains, but in the case of a touchscreen the control device also becomes (nearly) useless and so does the idea of emergency action via the input device. The solution: a good old emergency pushbutton beneath the touchscreen?

Re: Cute piece of malware engineering (Dean, [RISKS-25.48](#))

*<Paul Robinson <paul@paul-robinson.us>>
Wed, 24 Dec 2008 19:30:03 -0800 (PST)*

UPX was a type of (obviously) lossless compression used on executable files, with the idea that on slow media like hard drives, it would be faster to load a program which was compressed, then uncompress it into memory. The UPX header in the front of the executable, I believe, decompresses itself as it's being loaded. It could also be used as a type of anti-reverse-engineering tool, since the actual program would not be on disk, only a compressed version would be, and if the compressed version were encrypted with an internal password (I don't know if UPX did this, but it is possible) then you'd need to use something like the software equivalent of a logic probe to watch where the executable was loaded in order to be able to figure out what it was doing. In the case of a piece of Malware, it would be a great idea because it would make it much, much harder to get a virus signature since you'd have to allow the header to load the program (in order to decompress it) but somehow stop it from fully loading before the payload was executed.

Machines have gotten so much faster that compressing executables to save time loading off of disk is basically a deprecated practice. Also some of the software has gotten smarter, e.g. Borland's compilers would discard code that is never used when its linker built the program, so the executable might not even have extra unused code.

Re: Teacher Throws Fit Over Student's Linux CD (Robinson, [RISKS-25.48](#))

*<bo774@freenet.carleton.ca (Kelly Bert Manning)>
Sun, 28 Dec 2008 23:33:16 -0500 (EST)*

The incident may be exactly as described, but my paranoia level tends to rises when something that seems to perfectly match my sterotypical view of some group or individual crops up. If it sounds too perfect an incident to be true, then perhaps it isn't true and someone is hoping to have fun seeing what reaction they can generate.

I hope that the HeliOS project member who responded to "Karen" checked the e-mail headers and applied other e-mail authentication strategies before responding.

In addition to Joe-job spam, "jokes" mean that even non-bulk e-mail is not always what it purports to be.

This might turn out to be an example of a different sort of computer related risk, assuming that e-mail came from the source shown in the visible From: line and that it was composed by them.

✈ How to become a digital forensic evidence expert

<Fred Cohen <dr.cohen@mac.com>>
Sat, 20 Dec 2008 17:43:19 -0800

California Sciences Institute will be hosting a short course on "How to Become a Digital Forensic Evidence Expert" on Jan 19, 2009 in the Bay Area near San Francisco, CA. There will be a \$40 charge for attendees, and the program will run from 6-9 PM. If you are interested in additional details, please look for them at:

<http://calsci.org/2008/2009-01-HowTo-Become-DFE-Expert.pdf>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 50

Sunday 4 January 2009

Contents

- [Sunrise on the post-leap-second era](#)
[Tony Finch](#)
- [Zounds! Zinger: Zune Zapped Zealously with Zero-tolerance](#)
[PGN](#)
[David Magda](#)
- [Backward Hebrew writing on iPhone calendar](#)
[Steven M. Bellovin](#)
- [We can't stop the train because our GPS is broken](#)
[Hawkins Dale](#)
- [Medical devices lag in iPod age; Patients' safety is at risk](#)
[Carolyn Y. Johnson via Monty Solomon](#)
- [JournalSpace wiped out; no backups](#)
[Lindsay Marshall](#)
- [Some *digital* reception will go black in February!](#)
[Daniel P. B. Smith](#)
- [Digital photo frames: risks of infecting PCs](#)
[Deborah Gage via PGN](#)
- [Risks of Australians shouting at your hard drive?](#)
[Alec Muffett](#)
- [Firewall product uses man-in-the-middle attack to defeat SSL crypto](#)
[Mike Coleman](#)
- [Woman fools Japan's airport security fingerprint system](#)
[PGN](#)
- [The danger of DNA: It isn't foolproof forensics](#)
[Maura Dolan and Jason Felch via Monty Solomon](#)
- [Phishing Scam Spreading on Twitter](#)
[Chris Pirillo via David Farber](#)
- [Domain registrar hacked; numerous repointings...](#)
[Danny Burstein](#)
- [Qwest cuts off Internet subs in NM, including government VoIP](#)
[Lauren Weinstein](#)
- [Computer vs. food and warmth](#)
[jidanni](#)
- [Yahoo tracking where you go - invasion of privacy](#)
[jidanni](#)

- [Intelligent Speed Adaptation](#)
[Martin Ward](#)
 - [Re: License plate camera readers](#)
[Danny Burstein](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Sunrise on the post-leap-second era

<Tony Finch <dot@dotat.at>>
Thu, 1 Jan 2009 08:10 +0001

Just before the start of this year there was a leap second, and I am looking forward to reading the usual collection of stories about the problems it caused.

Over the last several years there has been discussion about abolishing leap seconds, to eliminate the glitches they cause and simplify standard time so that it agrees with the naive model built in to much software and many API and protocol standards. For a recent update on the discussion, see the following slides.

<http://www.navcen.uscg.gov/cgsic/meetings/48thmeeting/Reports/Timing%20Subcommittee/48-LS%2020080916.pdf>

The disadvantage is that atomic time has a different length of day to the Earth, and this difference is increasing more and more rapidly. Some people object strongly to the idea of decoupling civil time from the rotation of the Earth, and the break with historical ways of measuring time that this implies. The problem is how to reconcile the simple uniformity of atomic time with the erratic deceleration of the Earth. I believe that my proposal for a rational replacement for daylight saving time also provides an answer to the leap second question.

<http://catless.ncl.ac.uk/Risks/25.10.html#subj1>

The essence of sunrise time is that we reset our clocks each day (by slightly adjusting their timezone) to a fixed time when the sun rises at a benchmark location. For the UK, the benchmark location would be where the Greenwich meridian crosses the Tropic of Cancer. This simple mechanism makes even more daylight available when people are awake than conventional DST, and eliminates political argument.

If you are setting civil time according to when the sun rises, then it is by definition coupled to the rotation of the Earth, and there can be no accelerating difference between them. This is true even if the underlying time scale does diverge in this way because it uses fixed-length SI seconds. This mechanism even lasts beyond the time when the current leap second rules become unworkable because we need more than 12 each year.

Our systems would only have to know about atomic time and local time, translating between them using the existing time zone mechanism. There would no longer be any need for complicated and unpredictable UTC. Instead we'd gain straight-forward compatibility between the most modern way of

keeping time - the atomic clock - and the most ancient - getting up when the sun rises!

f.anthony.n.finch <dot@dotat.at> <http://dotat.at/>

#Zounds! Zinger: Zune Zapped Zealously with Zero-tolerance

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

Fri, 2 Jan 2009 14:40:27 PST

Starting at midnight on 30 December 2008, the 366th day of the year, Zunes (Microsoft's portable media players) displayed only a frozen start-up screen. [Source: Jenna Wortham, A Year Ticks Over, and Zunes Get Hiccups, *The New York Times*, 1 Jan 2009, National Edition B9; PGN-ed]

The most logical cause of this bug would seem to be a programmer forgetting that not all years have 365 days.

[This risk was also noted by Martyn Thomas, Martin Ward, and Peter Gregory -- who added this comment:

Microsoft is yearning to expand its market space into embedded systems in automobiles, military systems, and other areas. Am I being overly fearful of the consequences of a Microsoft whose products are even more deeply embedded into the machinery of our lives? Today is one of those days when I am distrustful of technology as a path for an easier life. PG
See also the following follow-up item from David Magda. PGN]

This is of course reminiscent of numerous previous leap-year fiascos previously reported in RISKS. For leap-year historians, do a search on "leap" (year and day help narrow it a little). Even apart from the leap-year digital watch problems noted repeatedly over the years by Mark Brader (see [RISKS-25.07](#)), the number of RISKS items is quite large -- particularly in volume 6 (1988), 13 (1992), 17 (1996), 20 (2000), and 25 (2008).

#Zounds! Zinger: Zune Zapped Zealously with Zero-tolerance

<David Magda <dmagda@ee.ryerson.ca>>

Thu, 1 Jan 2009 15:26:18 -0500

On Dec 31, 2008, at 20:36, David Magda wrote:

> People still can't get leap years right even though they've been
> around since Pope Gregory XIII's decree in 1582:

> Q: Why did this occur at precisely 12:01 a.m. on December 31, 2008?

> A: There is a bug in the internal clock driver causing the 30GB device
> to improperly handle the last day of a leap year.

> <http://forums.zune.net/412486/ShowPost.aspx>

The issue is an infinite loop:

```
> while (days > 365) {
>   if (IsLeapYear(year)) {
>     if (days > 366) {
>       days -= 366;
>       year += 1;
>     }
>   } else {
>     days -= 365;
>     year += 1;
>   }
> }
```

> Under normal circumstances, this works just fine. The function keeps
> subtracting either 365 or 366 until it gets down to less than a year's
> worth of days, which it then turns into the month and day of month. Thing
> is, in the case of the last day of a leap year, it keeps going until it
> hits 366. Thanks to the if (days > 366), it stops subtracting anything if
> the loop happens to be on a leap year. But 366 is too large to break out
> of the main loop, meaning that the Zune keeps looping forever and doesn't
> do anything else.

<http://www.zuneboards.com/forums/349447-post1.html>

✶ Backward Hebrew writing on iPhone calendar

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Thu, 1 Jan 2009 12:21:24 -0500

I recently succumbed to the reality distortion field and bought myself an iPhone. To make sure I have Jewish holidays on my calendar, I used a Mac to subscribe to a web-based calendar; this particular one will, on request, include the name of the holiday in Hebrew as well as in English transliteration. The result was amusing: the Hebrew words are written left-to-right, rather than the proper right-to-left. It's a display problem on the iPhone itself; my Mac's iCal program (from which the iPhone got the data) and the open source Sunbird calendar both display the text correctly.

The iPhone's web browser is even more amusing. It displays the text of Hebrew language web pages correctly; however, the characters in the title bar are reversed. Again, Safari on MacOS gets it all right (or, rather, gets it right-to-left).

Ah, well -- at least it's not a 30GB Zune on December 31 of a leap year....
(<http://www.nytimes.com/2009/01/01/technology/personaltech/01zune.html>)

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

We can't stop the train because our GPS is broken

<Hawkins Dale <hawkins@hawkinsdale.com>>

Fri, 02 Jan 2009 10:18:04 -0500

<http://new.dailyexpress.co.uk/posts/view/77987/>

"Passengers on a Southern [England] service from East Croydon were stunned when they were told that their stopping train would skip six stations and go direct to the end of the line in Caterham, Surrey. When they got there the driver said the reason was that the train had lost its satellite link.

Apparently the GPS isn't there to determine where to line up the train with the platform. Instead, it senses which station the train's in, so that it knows not to open doors that may not be lined up with the platform, since some stations have short platforms.

Other methods, such as having the driver look out the window at the sign, have apparently been discarded in favor of these more modern techniques.

There'll always be a Nengland, I guess.

[I cannot res-train myself from chuckling. PGN]

Medical devices lag in iPod age; Patients' safety is at risk

<Monty Solomon <monty@roscom.com>>

Wed, 31 Dec 2008 13:46:47 -0500

[Source: Carolyn Y. Johnson, *The Boston Globe*, 29 Dec 2008]

A 32-year-old woman was on the operating table for routine gall bladder surgery, and doctors needed a quick X-ray. To keep her chest still while the image was shot, her ventilator was switched off. But the anesthesiologist, distracted by another problem, forgot to turn the breathing machine back on. The woman died.

The case is an extreme example of the kind of error that could be prevented if medical devices were designed to talk to each other, says Dr. Julian Goldman, a Massachusetts General Hospital anesthesiologist who has compiled such instances from across the United States to highlight the need for medical device "connectivity." In this case, he says, synchronizing the X-ray machine with the ventilator, so the image was automatically timed to a natural pause in breathing, would have made it unnecessary to turn it off.

As technology moves forward, people expect the electronic devices of everyday life to work together, from cellphones that can call or text-message other phones, to computers that interconnect with a slew of

gadgets. But in the medical world, where the stakes are higher, such flexible interconnection is rare. Each device operates in its own silo.

"It is really unacceptable, and it's one of the reasons we're unable to make dramatic improvements in patient safety," said Goldman, a leader in calling for a new generation of medical devices that talk to each other.

Now the push for greater connectedness in hospital electronics is gaining momentum. The goal is devices that can not only plug into one another, but can also "understand" each other and automatically identify potential life-threatening problems sooner than they would have been caught by busy nurses and doctors.

In October, a task force -- including Partners HealthCare, Mass. General, Johns Hopkins Medicine, Kaiser Permanente, and the Boston-based Center for Integration of Medicine and Innovative Technology -- released sample language that hospitals can incorporate into contracts with vendors of medical devices, requiring that manufacturers create products capable of communicating with other devices using agreed-upon standards. ...

http://www.boston.com/news/science/articles/2008/12/29/medical_devices_lag_in_ipod_age/

✶ JournalSpace wiped out; no backups

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

Sun, 4 Jan 2009 09:37:37 +0000

Blogging service JournalSpace has been completely wiped out after the drives that housed their entire database were overwritten. The problem was that their backups weren't actually backups at all. The servers were set up with a mirrored RAID system so that if the primary drive should fail, the secondary drive would be used to recover the primary. As a result, when the data was overwritten on one drive, the other followed suit and cleared itself. A data recovery team was unable to retrieve the database.

<http://lifehacker.com/5122848/hard-lessons-in-the-importance-of-backups-journalspace-wiped-out>

✶ Some *digital* reception will go black in February!

<"Daniel P. B. Smith" <usenet2006@dpbsmith.com>>

Wed, 31 Dec 2008 23:03:41 -0500

I'm pretty sure I'm right about this, but I haven't succeeded in getting a clear answer from anyone. It isn't discussed in any FAQ I've seen.

On 17Feb 2009, some of the people most surprised by the transition will be those who carefully prepared in advance and are happily watching digital TV over the air with an "HDTV antenna." Because, on February 17th, some of the stations they are watching in _digital_ now will effectively go black.

The reason is that the antennas that have been sold for years as "HDTV antennas" or "digital antennas" are UHF-only antennas. This made sense, because VHF antennas are large, bulky, expensive, and difficult to install, and because currently all digital television frequency assignments are in the UHF band.

The problem is that on 17 Feb 2009, when the transition occurs, some stations will be moving their signals from the UHF band to the VHF band, to take advantage of VHF spectrum that has been freed up by the cessation of analog broadcasting.

For example, according to antennaweb.org, WHDH-DT in Boston, which is currently broadcasting on UHF channel 42, will move to VHF channel 7.

However, you will not find any discussion of this on WHDH's website, which contains the stock DTV advice and says nothing about any special considerations in receiving WHDH-DT. Like other FAQs, it refers vaguely to antennas and does not emphasize any need to be sure that your antenna includes VHF capability if you want to receive all stations after February 17th.

Not very many people will be affected by this problem. Only those who actually prepared!

Another issue is that digital television receivers and converter boxes generally set themselves up automatically when first powered on, scanning through the channels and identifying and marking those where digital signals were found. It is a one-time process and people can forget that it ever took place. I wonder how many DTV receivers will handle the channel reassignments automatically and gracefully? I suspect many people, even if their antennas receive VHF, will simply lose the reassigned channels, perhaps for weeks... until they figure out that they need to initiate a manual rescan and can remember how to do it.

✂ Digital photo frames: risks of infecting PCs

*<"Peter G. Neumann" <neumann@csl.sri.com>>
Fri, 2 Jan 2009 15:02:47 PST*

More than 7 million digital frames were sold in 2008, with expectations that perhaps 10 million more might be sold in 2009. However, the 2008 holiday sales included a Samsung 8-inch frame sold by Amazon.com, a 9-inch Element frame sold by Circuit City and a 1.5-inch Mercury frame sold by Wal-Mart -- all of which were infected with malware. [Source: Deborah Gage, *San Francisco Chronicle*, 2 Jan 2009, C1-C2, in a long article, PGN-ed here]

Those of you with good memories may recall this as another example of an old problem that keeps recurring: similar infections were experienced during the 2007 holiday sales in frames sold by Sam's Club, Best Buy, Target, and Costco, as reported by Deborah Gage, 15 Feb 2008 and noted in [RISKS-25.13](#).

[Thanks to Deborah and the *Chronicle* for the intellectual history as well as the new report.]

Risks of Australians shouting at your hard drive?

<Alec Muffett <Alec.Muffett@Sun.COM>>

Fri, 02 Jan 2009 01:52:51 +0000

ObDisclaimer: I work for Sun, but this is really *neat*: it's a demonstration of what happens when you shout at hard disks / other loud noises, visualised as performance impact -- watch the latency spikes:

<http://uk.youtube.com/watch?v=tDacjrSCeq4>

It makes you think.... maybe "audio tempest" next? A sort of inverse of <http://www.vimeo.com/1109226?pg=embed> ? :-)

Firewall product uses man-in-the-middle attack to defeat SSL crypto

<"Mike Coleman" <tutufan@gmail.com>>

Fri, 2 Jan 2009 21:32:41 -0600

Here's a new wrinkle on man-in-the-middle attacks I'd not seen before. Palo Alto Networks' PA-4000 transparent firewall claims to decrypt SSL traffic passing through it, so that organizations can apply tracking and blocking to HTTPS traffic. As explained in the review (link), users' browsers are configured to trust a new root CA that the PA-4000 itself has the private key for. It then interposes itself into HTTPS requests (and other SSL requests?) by automatically generating a masquerading certificate for the site the user is trying to connect to, decrypting the traffic so that it can be scanned in plaintext on the PA-4000, and finally re-encrypting the traffic with a second HTTPS connection to the true site.

I invite my fellow RISKS readers to contemplate the technical, legal, business, and ethical implications of this approach.

<http://www.informationweek.com/news/hardware/reviews/showArticle.jhtml?articleID=206904763>

Woman fools Japan's airport security fingerprint system

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

Fri, 2 Jan 2009 20:27:02 PST

[Source: 2 Jan 2009, PGN-ed; thanks to Keith Schwalm]

<http://www.smh.com.au/travel/woman-fools-japans-airport-security-fingerprint-system-20090102-78rv.html>

A South Korean woman barred from entering Japan last year has reportedly

passed through its immigration screening system by using tape on her fingers to fool a fingerprint reading machine. She told investigators that she placed special tapes on her fingers to pass through a fingerprint reader. (She had been deported in July 2007 for illegally staying in Japan after she worked as a bar hostess in Nagano. She was not allowed to re-enter Japan for five years after deportation but the Tokyo immigration bureau found her in August 2008 again in Nagano.)

The biometric system was installed in 30 airports in 2007 to improve security and prevent terrorists from entering into Japan. Japan spent more than Y4 billion (\$A64 million) to install the system, which reads the index fingerprints of visitors and instantly cross-checks them with a database of international fugitives and foreigners with deportation records.

#The danger of DNA: It isn't foolproof forensics (Dolan/Felch)

*<Monty Solomon <monty@roscom.com>>
Thu, 1 Jan 2009 19:16:40 -0500*

[Source: Maura Dolan and Jason Felch, *Los Angeles Times*, 1 Jan 2009]

In 2004, a New Jersey prosecutor announced that DNA had solved the mystery of who killed Jane Durrue, an eighth-grader who was raped, beaten, and strangled 36 years earlier.

"Through DNA, we put a face to the killer of Jane Durrue, and that face belongs to Jerry Bellamy," prosecutor John Kaye said.

The killer, however, turned out to be someone else.

Two years after Bellamy's arrest, investigators discovered that evidence from the murder scene had been contaminated by DNA from Bellamy, whose genetic sample was being tested at the same lab in an unrelated case. He was freed. Another man ultimately was arrested.

DNA has proved itself by far the most effective and reliable forensic science. Over the past two decades, it has solved crimes once thought unsolvable, brought elusive murderers and rapists to justice years after their misdeeds, and exonerated innocent people. In courtrooms and in the popular imagination, it often is seen as unassailable.

But as the United States rushes to take advantage of DNA's powers, it is becoming clear that genetic sleuthing has significant limitations:

Although best known for clearing the wrongfully convicted, DNA evidence has linked innocent people to crimes. In the lab, it can be contaminated or mislabeled; samples can be switched. In the courtroom, its significance has been overstated by lawyers or misunderstood by jurors.

The rush to collect DNA and build databases has in some cases overwhelmed the ability of investigators to process the evidence and follow up on

promising leads. Some crime labs have huge backlogs of untested evidence, including thousands of rape evidence kits. In some cases, criminals who might have been caught have offended again. ...

http://www.boston.com/news/nation/articles/2009/01/01/the_danger_of_dna_it_isnt_foolproof_forensics/

Phishing Scam Spreading on Twitter

<David Farber <dave@farber.net>>

Sun, 4 Jan 2009 09:35:25 -0500

[From Dave Farber's IP distribution]

[Chris Pirillo suggests that you really shouldn't click on the Twitter phishing URL he exhibits. You certainly don't want to sass pirillo [!], because he does show you what would happen. PGN]

<http://chris.pirillo.com/2009/01/03/phishing-scam-spreading-on-twitter/>

Domain registrar hacked; numerous repointings...

<danny burstein <dannyb@panix.com>>

Sat, 3 Jan 2009 00:41:54 -0500 (EST)

[This incident is related to the ongoing hostilities in the Mideast. I'm posting it here for the technical and security info value. Please keep this neighborhood in mind if following up.]

Niv Lillian, Israeli domain registration server hacked, *Israel News*, 2 Jan 2009, from: ynetnews.com (an Israeli based web source)

An Islamic group based on Morocco hacked into DomainTheNet's registration system server on Friday, effectively "highjacking" various prominent domain names, the likes of ynetnews.com and Bank Discount, and rerouting users to a page featuring anti-Israel messages. ... Appearing as a defacement attempt at first, the attack soon turned out to be more sophisticated: The hackers were able to obtain a password which granted them access to the server which updates and "translates" the websites' IP addresses into a Domain Name Service; and change the IP's numeral values, effectively rerouting users away from the original websites. ... The site formed by the group featured graphic images of dead bodies and abused Iraqi prisoners. ...

<http://www.ynetnews.com/articles/0,7340,L-3649281,00.html>

Qwest cuts off Internet subs in NM, including government VoIP

<Lauren Weinstein <lauren@vortex.com>>

Sat, 3 Jan 2009 18:11:17 -0800 (PST)

Apparently as a result of a billing dispute and related lawsuit, Qwest reportedly cut off Internet connectivity to ISP SkyWi in New Mexico, suddenly leaving some 13000 Internet subscribers and 5400 SkyWi VoIP phone subscribers without service. Some reports indicate that those VoIP subscribers suddenly without working phones included NM public safety entities.

The NM Public Regulation Commission has now stepped in and ordered Qwest to restore service, but the process has been taking some time.

Regardless of who is actually at fault in the billing matter, the behavior of both companies in this situation appears to have been anything but stellar, and again points to the need for a more proactive regulatory approach to Internet access service provisioning.

<http://tinyurl.com/qwest-cutoff>

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org/lauren>
Blog: <http://lauren.vortex.com> Network Neutrality Squad <http://www.nnsquad.org>

✶ Computer vs. food and warmth

<jidanni@jidanni.org>

Sat, 03 Jan 2009 04:11:48 +0800

In order to use the computer, I cannot use the frying pan nor electric blanket. Their cheap circuits cause the computer's uninterruptible power supply to emit an awful whine:

http://groups.google.com/groups/search?as_umsgid=87d4f8ow30.fsf%40jidanni.org

[A fine example of the EXCLUSIVE OR operation. I hope you don't keep the awful w(h)ine in the refrigerator. PGN]

✶ Yahoo tracking where you go - invasion of privacy

<jidanni@jidanni.org>

Sat, 03 Jan 2009 05:20:22 +0800

<http://permalink.gmane.org/gmane.recreation.radio.hardware.icomr5/150>

✶ Intelligent Speed Adaptation (Re: Douglass, [RISKS-25.49](#))

<Martin Ward <martin@gkc.org.uk>>

Wed, 31 Dec 2008 14:41:06 +0000

Re: Risks of excessive State data collection (Douglass, [RISKS-25.49](#))

Answers to many of the questions posed by Toby can be found in the original research paper:

<http://eprints.whiterose.ac.uk/archive/00002008/>

The UK has reduced road deaths from 8,000 per year in 1964 to just over 3,000 per year in 2005:

<http://www.statistics.gov.uk/CCI/nugget.asp?ID=1208&Pos=&ColRank=1&Rank=374>

Most of the reduction is due to "low tech" methods: repainting roads to create space between traffic lanes, speed bumps and other traffic calming methods in built up areas, more junctions controlled by lights, and so on. But the paper above makes a strong case for the "high tech" option.

The savings may be overestimated: but every 1% reduction in fatal accidents would mean 30 lives saved each year. When 35 people were killed in the Clapham Junction rail crash, it was in the news for weeks and there was a public Inquiry which led to major changes in the operation of the railways. The inquiry recommended the introduction of an Automatic Train Protection System, at a cost of over Â£1 billion. Nobody pointed out that in the week of the crash, about 100 people died on the roads. And another 100 in the next week, and another 100 the week after... In the time between the crash and the publication of the report, nine months later, over 100 times as many people had died on the roads, as had died in the crash.

martin@gkc.org.uk <http://www.cse.dmu.ac.uk/~mward/>

Re: License plate camera readers (Re: Arthur T., [RISKS-25.49](#))

*<danny burstein <dannyb@panix.com>>
Tue, 30 Dec 2008 17:31:42 -0500 (EST)*

> Fun with speed-trap cameras for revenge

There's actually a very good reason why this won't work, at least in regards to making people pay up for the bad tickets.

In fact, I've received one myself, which I got dismissed.

The key point is that the digital image is NOT a perfectly cropped photograph of "just" the license plate. Rather, the picture (and often it's a sequence of them) includes a hefty portion of the rear of the car, and generally the sides and top as well.

In my own case the interpreter of the original photograph, whether human or computer recognition, misread a "0" (the number zero) as an "8", and I received a ticket in the mail.

I simply wrote back pointing out that the photo showed the license plate attached to the rear end of a BMW, and that my car was most certainly not from that line.

The ticket was promptly dismissed.

Annoying? Mildly. But far from critical.

Now finding the "real speeder" is left as an exercise to the student...



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 51

Friday 16 January 2009

Contents

- [Software glitch causes incorrect medication dosages](#)
[Jeremy Epstein](#)
 - [Police avoid arrests due to time-consuming QPRIME computer system](#)
[Steven J Klein](#)
 - [Maryland Police surveillance](#)
[Lisa Rein and Josh White](#)
 - [Army subcontractor sends 7,000 misaddressed letters: 'computer glitch'](#)
[Rob McCool](#)
 - [Risks in Hating Web Video](#)
[Lauren Weinstein](#)
 - ["Spy pens" and the future of private speech](#)
[Jerry Leichter](#)
 - [Risk of Car Sharing: Getting Pinned with Someone Else's Ticket](#)
[Kent Borg](#)
 - [Taiwan Immigration Computer down for the Count](#)
[jidanni](#)
 - [Tony Hoare: "Null References: The Billion Dollar Mistake"](#)
[Olivier Dagenais](#)
 - [Facebook hacked and no avenue for redress](#)
[Mark Neely](#)
 - [How to NOT perform customer service and updates](#)
[Gene Spafford](#)
 - [Risks of digital signatures](#)
[Ron Garret](#)
 - [Update: N.J. officials order paper trail upgrades to voting machines](#)
[Danny Burstein](#)
 - [Teenagers' Internet Socializing Not a Bad Thing](#)
[Monty Solomon](#)
 - [SecAppDev 2009](#)
[Johan Peeters](#)
 - [REVIEW: "Intellectual Property and Open Source", Van Lindberg](#)
[Rob Slade](#)
 - [Info on RISKS \(\[comp.risks\]\(#\)\)](#)
-

Software glitch causes incorrect medication dosages

<Jeremy Epstein <jeremy.j.epstein@gmail.com>>

Fri, 16 Jan 2009 11:51:46 -0500

``Patients at VA health centers were given incorrect doses of drugs, had needed treatments delayed and may have been exposed to other medical errors due to the glitches that showed faulty displays of their electronic health records, according to internal documents obtained by The Associated Press under the Freedom of Information Act. The VA's recent glitches involved medical data -- vital signs, lab results, active meds -- that sometimes popped up under another patient's name on the computer screen. Records also failed to clearly display a doctor's stop order for a treatment, leading to reported cases of unnecessary doses of intravenous drugs such as blood-thinning heparin. According to interviews and the VA's internal memos, the glitches began after the VA distributed its annual software upgrade last August [2008].''

By early October, hospitals began reporting the troubling problems: When doctors pulled up electronic records of different patients within 10 minutes of each other to offer treatment advice, the medical information of the first patient sometimes displayed under the second person's name. In some records, a doctor's stop order for intravenous injections also failed to clearly display."

<http://www.msnbc.msn.com/id/28655104/>

No explanation of what caused the software problem, which was reportedly fixed in December.

[Also noted by Danny Burstein, who added that this was not disclosed to patients by the VA. PGN]

Police avoid arrests due to time-consuming QPRIME computer system

<Steven J Klein <steveklein@mac.com>>

Sun, 04 Jan 2009 20:05:49 -0500

Excerpt:

FRUSTRATED Queensland police are turning a blind eye to crime to avoid time-consuming data entry on the force's new \$100 million computer system.

Queensland Police Union vice-president Ian Leavers said the system turned jobs that usually took an hour into several hours of angst.

He said police were growing reluctant to make arrests following the latest phased roll-out of QPRIME, or Queensland Police Records Information Management Exchange.

"They are reluctant to make arrests and they're showing a lot more discretion in the arrests they make because QPRIME is so convoluted to navigate," Mr Leavers said. He said minor street offences, some traffic offences and minor property matters were going unchallenged, but not serious offences.

<http://www.news.com.au/couriermail/story/0,23739,24723327-952,00.html>

Steven J Klein, Your Mac & PC Expert, Phone: (248) YOUR-MAC or (248) 968-7622

[p prime and q prime are of course the basis for public-key crypto.
QPRIME by itself sounds like public-free flip-tow. PGN]

✶ Maryland Police surveillance (Lisa Rein and Josh White)

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

Thu, 8 Jan 2009 15:12:07 PST

Lisa Rein and Josh White, More Groups Than Thought Monitored in Police Spying, *The Washington Post*, 4 Jan 2009

http://www.washingtonpost.com/wp-dyn/content/article/2009/01/03/AR2009010301993_pf.html

The Maryland State Police surveillance of advocacy groups was far more extensive than previously acknowledged, with records showing that troopers monitored - and labeled as terrorists - activists devoted to such wide-ranging causes as promoting human rights and establishing bike lanes. Intelligence officers created a voluminous file on Norfolk-based People for the Ethical Treatment of Animals, calling the group a "security threat" because of concerns that members would disrupt the circus. Angry consumers fighting a 72 percent electricity rate increase in 2006 were targeted. The DC Anti-War Network, which opposes the Iraq war, was designated a white supremacist group, without explanation. [...]

✶ Army subcontractor sends 7,000 misaddressed letters: 'computer glitch'

<Rob McCool <robm@robm.com>>

Wed, 7 Jan 2009 15:19:09 -0800 (PST)

<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2009/01/07/national/w123829S48.DTL&tsp=1>

The US Army said today that 7,000 family members of soldiers killed in recent wars were sent letters addressing them as "John Doe". The U.S. Army Human Resources Command's Casualty and Mortuary Affairs Center in Alexandria, Va. issued a formal apology for what they described as a contractor's error. The contractor had used a placeholder greeting of "Dear John Doe" in the letter, which was to have been automatically replaced by the specific names of and addresses of the survivors but somehow wasn't.

Army Chief of Staff Gen. George W. Casey, Jr. is said to be sending a personal letter to the families who received the improperly addressed

letters.

✂ Risks in Hating Web Video

<Lauren Weinstein <lauren@vortex.com>>

Fri, 16 Jan 2009 09:29:06 -0800

Greetings. Since I occasionally post audio (and more recently video) commentaries and other features on the Web, and have been doing so for a number of years, I've been becoming increasingly concerned about the phenomenon of what I might call "audio and video media haters" in the Internet environment. I'm beginning to see some significant related risks.

Without fail, after each of my posting announcements of an audio or video presentation, I get e-mail from people that amount to variations on:

"I refuse to watch video [listen to audio] on the Net. Please make a text-only version of all your materials available."

Such messages have been particularly notable for this week's "Stimulus or Ripoff" - "Network Neutrality in 30 Seconds - Part 3" video segment (<http://lauren.vortex.com/archive/000494.html>), which I announced a couple of days ago.

The reactions to the announcement of this particular video are a perfect example of my concern. Without the accompanying video track, and especially its animations, the entire humor of the piece, and even the key punch line itself, would be completely lost. The short narration script alone might be interesting to Net Neutrality intelligentsia, but the piece is designed to try reach a much broader audience, and the visuals are key to driving home the concepts (to those who have seen the video, no pun is intended by the term "driving" in this case!)

There are of course legitimate accessibility concerns with all media. Unfortunately, I have not found available captioning tools, for example, to be entirely practical at this stage. In some of my very early audio efforts, I did make scripts available, and then ran into a wall trying to note tone of voice (sarcasm, etc.) in a way that would make sense. Without such notations, I found that some readers were misunderstanding the intent of the pieces. And while it's certainly possible to write commentary without tone of voice sarcasm, it can be quite constraining in an audio presentation.

As the powerful capabilities of video to entertain, inform, explain, and convince -- video is increasingly a sort of default "coin of the realm" in many ways on the Internet -- it seems likely that the sorts of issues and concerns described above will be exacerbated.

I don't claim to possess any magic wand solutions to this, though I have some relevant ideas. But I do believe we'd be very foolish to declare such matters as insignificant or unworthy of study.

The ways in which people react to new forms of media have always been important, sometimes in political contexts that have affected untold millions of lives over the centuries. Video on the Web will not be an exception.

Lauren Weinstein lauren@vortex.com +1 (818) 225-2800 <http://www.pfir.org/lauren>
Network Neutrality Squad <http://www.nnsquad.org> Blog: <http://lauren.vortex.com>
PRIVACY Forum - <http://www.vortex.com>

"Spy pens" and the future of private speech

<Jerry Leichter <leichter@lrw.com>>

Sat, 10 Jan 2009 06:45:46 -0500

The decreasing size of electronics has made all kinds of devices from fantasy practical. Look around at audio and video recorders that fit in pens, packs of gum, etc.:

http://gadget.brando.com.hk/prod_list.php?dept_id=001&cat_id=024

Now, that stuff is specialized and hardly mass market. One can even imagine attempts to outlaw it. But there's a really neat gadget, the Pulse Smartpen by Livescribe - <http://www.livescribe.com/> - that *is* mass market. This is a pen with 2 or 4GB of memory, a microphone, an optical scanner at the pen tip, and a small LCD display. You write on special paper - you can print your own - and it records "digital ink" of what you wrote and time-sync's it with the recording. Later, you can review what you wrote and listen to what was being said at the same time. Sold today as a device for note-taking - but Livescribe was apparently started by a bunch of ex-Apple guys, and they are thinking big. There's an SDK so you can use the thing as a "pen computing environment". For example, they include a calculator: Write down an arithmetic problem and the answer appears on the LCD.

Anyway ... besides the intended uses, with this kind of thing in millions of pockets - you should expect that anything you say will be recorded. Not all bad, of course - we'll certainly have some more cops caught lying on the stand about their interrogation techniques, as has happened of late with cell phones. But the overall effects on our ideas of privacy are hard to predict. People treated mail and chat and such as equivalents of speech - transitory and private. Reality - and the courts - have shown us that these are permanent, searchable records. Actual speech is about to cross over into the same territory.

Welcome to the Panopticon.

Risk of Car Sharing: Getting Pinned with Someone Else's Ticket

<Kent Borg <kentborg@borg.org>>

Fri, 09 Jan 2009 11:24:05 -0500

Last year I signed up for Zipcar, a car sharing service that operates in the Boston area (among other cities). It seemed good to support such an enterprise--and it might come in handy. OK, so one day my car is in the shop and I need to get to work. I rent a Zipcar for the day, drive to work, park, work my day, return the car to its packing place, walk home. Cool.

A month later I get an e-mail from Zipcar telling me I am being charged for my parking ticket. Charged for the fine, plus an extra \$20 for handling.

What ticket!? I don't remember getting a ticket. I check the address of the violation. Nope, I never went to that Cambridge neighborhood.

I don't know where the error occurred. Did the Cambridge police get the plate number wrong? Did they get the date wrong? Did Zipcar match up plate number to the wrong car?

Zipcar uses an RFID/proxcard system to unlock and lock their cars. Somehow they communicate to each car to tell it what proxcard is authorized per their reservation records. They have told me what time I picked up the car--supposedly I picked up the car 4-minutes before the reservation time.

That is odd. I don't claim to always be on time (ask my wife) but I am a bit of a time nerd and always know how late I am, my watch is usually within 10-seconds of the correct time. Even before I had my coffee, I am quite sure I didn't pickup my first Zipcar 4-minutes early, I would have been startled that they let me have the car early. So I don't trust their time stamping.

Getting this cleared up might be difficult.

The risk: By sharing cars, if all the computer and human systems don't work right, we risk also sharing parking tickets (and other liabilities?) that are not shouldered by their rightful violators...

kb, the Kent who is \$60 guilty until he can prove himself innocent.

Taiwan Immigration Computer down for the Count

<jidanni@jidanni.org>

Wed, 07 Jan 2009 02:15:27 +0800

... Legislator Ker said the computer crash lasted far too long and had jeopardized national security as well as the nation's image... National Immigration Agency Chief Hsieh said "faulty hard drives" were responsible ... in the meantime, to prevent criminal suspects from seizing the opportunity to flee Taiwan, his agency had provided a list...

<http://www.taipeitimes.com/News/front/archives/2009/01/07/2003433115>

Fortunately former President Chen "Count the towels" Shuibian is safely behind bars and won't be making a break for it.

[I presume no Count was ennobled thereby. PGN]

✶ Tony Hoare: "Null References: The Billion Dollar Mistake"

<"Olivier Dagenais" <olivier.dagenais@gmail.com>>

Tue, 13 Jan 2009 15:36:04 -0500

RISKS readers may be interested in the following presentation by Tony Hoare [Sir Anthony C. A. R. Hoare] at the upcoming QCon London 2009:

Abstract: I call it my billion-dollar mistake. It was the invention of the null reference in 1965. At that time, I was designing the first comprehensive type system for references in an object oriented language (ALGOL W). My goal was to ensure that all use of references should be absolutely safe, with checking performed automatically by the compiler. But I couldn't resist the temptation to put in a null reference, simply because it was so easy to implement. This has led to innumerable errors, vulnerabilities, and system crashes, which have probably caused a billion dollars of pain and damage in the last forty years. In recent years, a number of program analysers like PREFIX and PREFAST in Microsoft have been used to check references, and give warnings if there is a risk they may be non-null. More recent programming languages like SPEC# have introduced declarations for non-null references. This is the solution, which I rejected in 1965.

<http://qconlondon.com/london-2009/presentation/Null+References:+The+Billion+Dollar+Mistake>

✶ Facebook hacked and no avenue for redress [Via Dave Farber's IP]

<"Mark Neely" <mark.neely@gmail.com>>

January 15, 2009 9:32:17 AM EST

I am writing partly to vent my frustration but mainly in the vain hope someone on the IP list can help me out.

My Facebook account was hacked approximately 40hrs ago. I discovered this when I was called by a concerned friend who wanted to confirm that I was being held at gunpoint in London and desperately needed him to wire me cash (via Western Union) so I could escape the country and return to Australia. Of course, I was not in London, and it was not me he was chatting to on Facebook.

I immediately attempted to log into Facebook, but the password had been changed. So I tried to reset the password, but the e-mail address linked to my Facebook account had also been changed. I could not access my account.

I spent an hour scanning the Facebook site looking for a contact phone number. No such luck. I completed 2 different incident reporting forms, and

received auto-confirmations. I then scanned their T+Cs and Privacy notices and discovered the privacy@facebook.com e-mail address and sent an e-mail to that address.

40 hours later, I have had no response from Facebook, and I have been alerted by friends that the perpetrators are still active on my account, initiating chats with people begging for help and a money transfer. I just alerted several authorities in Australia (though it is now 1.30am in Sydney, so had to use online forms). Unfortunately, the Australian Federal Police (who do have a 24hr hotline) couldn't help me (they referred me to a Scam Watch service!).

So I am asking whether anyone on the IP list has a direct contact with an appropriate stakeholder at Facebook, or some specific advice on who I might contact in the US to get the account suspended and the perpetrators locked out (or, better, traced and apprehended).

Mark Neely, Master Strategist, Infolution Pty Ltd 'Beyond Strategy. Leading Change' e: mpn@infolution.com.au m: +61 (0)412 0417 29 skype: mark.neely
Read my blogs --> www.infolution.com.au

IP Archives: <https://www.listbox.com/member/archive/247/=now>

[A follow-up note in IP from Chris Kelly <ckelly@facebook.com> indicated that Facebook had disabled the account while they are attempting to pinpoint the perpetrators. PGN]

✂ How to NOT perform customer service and updates

<Gene Spafford <spaf@cerias.purdue.edu>>
Sat, 10 Jan 2009 16:45:11 -0500

This both an accounting of experience and a warning away from a vendor.

I recently purchased 2 Samsung Blu-Ray DVD players: a BD-P2500, and a BD-P1500. Both have Internet connections for firmware updates and Blu-Ray Live. The BD-P2500 also supports live streaming of Netflix content.

A couple of days after Christmas, the 2500 froze up. I could not get it to respond to anything, including the factory reset code. I contacted Samsung and was given information to send the player in for service. They've had it for nearly 2 weeks with a status of "waiting for parts." It has now been broken longer than it was working.

The 1500 came up with a message on Thursday that a firmware update was available. So, I initiated the download. It went without error, according to the display. After completion, it too was dead in the water -- no response to anything. So, I called Samsung again. The problem was escalated in customer service. This is what I got told:

1) There was a bad update put on the servers, and many players that got the

- download have frozen up.
- 2) They do not have a fix for it at the current time and do not know when one will be available.
 - 3) I should check their WWW site once a week to see when an update is available. "It should almost certainly be within a month."
 - 4) Even though it is their fault for putting up a bad firmware update, if I am required to send in the player, it is out of warranty for service so it is my own expense.

I wonder how many other people around the world are stuck with non-functional players and a vague answer about the fix? And the best they can do is have me check the WWW site once a week to see when they are ready for me to pay to install a fix to a problem they caused in the first place. What crock!

Needless to say, I will probably not buy another Samsung product. You might want to consider this as a big red flag in your own purchasing decisions -- the risk of bad updates and really bad customer service.

✂ Risks of digital signatures

*<Ron Garret <ron@flownet.com>>
Thu, 15 Jan 2009 11:51:32 -0800*

Last year I started a small investment fund. Earlier today I sent out an e-mail to a mailing list for all the investors reminding everyone to send me their SSN or Tax ID number, which I needed in order to complete the tax filings for the fund. The investors are mostly tech-savvy people who are better educated about computer risks than most, and I am a long-time RISKS reader. So in order to insure that no one thought this was a phishing expedition, I signed the message with my PEM key.

I then went to run some errands. When I returned there was a message in my inbox from one of the investors saying, "Would you please delete the message with my SSN in it from the mailing list archives?" Apparently he saw my digital signature and thought that meant he didn't have to worry about security any more, so he just hit "reply" on his mail client and typed in his SSN -- which was of course sent out to the entire mailing list.

When I went to delete the message in question I found that it had spawned a rather extensive discussion thread about the risks of blindly hitting the "reply" button and what could be done to mitigate them. Every message in the thread contained a copy of the previous message. I did eventually manage to delete them all from the archives, but there are now dozens of copies of this poor man's SSN sitting in various people's mail boxes, e-mail logs, etc. etc. which are of course out of my (and his) control.

✂ Update: N.J. officials order paper trail upgrades to voting machines

<danny burstein <dannyb@panix.com>>

Thu, 8 Jan 2009 21:25:16 -0500 (EST)

A bit late in the game, but a welcome move -- "Electronic voting machines used in 18 New Jersey counties will be refitted with attachments to provide a paper trail that could be used for potential recounts, Secretary of State Nina Mitchell Wells has decided. Wells made her decision Monday, accepting the recommendation of a special voting machine examination committee, and making a change sought by activists who contended that electronic voting machines are vulnerable to hackers. ...

rest:

http://www.nj.com/news/index.ssf/2009/01/nj_officials_order_paper_trail.html

#Teenagers' Internet Socializing Not a Bad Thing

<Monty Solomon <monty@roscom.com>>

Sun, 11 Jan 2009 00:38:11 -0500

[Source: Tamar Lewin, *The New York Times*, 20 Nov 2008]

Good news for worried parents: All those hours their teenagers spend socializing on the Internet are not a bad thing, according to a new study by the MacArthur Foundation.

"It may look as though kids are wasting a lot of time hanging out with new media, whether it's on MySpace or sending instant messages," said Mizuko Ito, lead researcher on the study, "Living and Learning With New Media." "But their participation is giving them the technological skills and literacy they need to succeed in the contemporary world. They're learning how to get along with others, how to manage a public identity, how to create a home page."

The study, conducted from 2005 to last summer, describes new-media usage but does not measure its effects. ...

<http://www.nytimes.com/2008/11/20/us/20internet.html>

#SecAppDev 2009

<"Johan Peeters" <yo@secappdev.org>>

Sun, 4 Jan 2009 14:51:45 +0100

secappdev.org is excited to announce SecAppDev 2009, an intensive one-week course in secure application development. secappdev.org is a non-profit organization dedicated to improving security awareness and skills in the developer community. The course is a joint project with K.U. Leuven and Solvay Brussels School of Economics and Management.

SecAppDev 2009 follows the widely acclaimed courses in 2005, 2006, 2007 and 2008, attended by an international audience from a broad range of industries including financial services, telecom, consumer electronics and media. In order to offer an effective learning environment, we limit the number of participants. This allows for optimal interaction between participants and faculty.

The course is taught by leading experts including

- Dr. Gary McGraw, the Cigital CTO, inspired speaker and prolific author.
- Prof. Dr. Daniel Bernstein whose Internet applications have impeccable security credentials.
- Prof. dr. ir. Bart Preneel who heads COSIC, the renowned crypto lab.
- Ken van Wyk, well-known author and lecturer as well as the moderator of the SC-L.

The course takes place from March 2nd to March 6th in the Groot Begijnhof in Leuven, Belgium, a UNESCO World Heritage site.

Registration is on a first-come, first-served basis. Early Bird registration offers a 25% discount on the course fee and ends on January 15th. Public servants can attend the course at a 50% discount.

[Sorry not to get to this issue of RISKS until the day after the Early-Bird deadline. If you apply after seeing this message here, tell them you saw it in the 16 Jan RISKS, and maybe they can give you a break. Johan, Please give them a break! Dank U wel. PGN]

More information on the web site, <http://secappdev.org>.

Wishing you a safe, happy and secure 2009,

Johan Peeters, Program Director, <http://secappdev.org>

REVIEW: "Intellectual Property and Open Source", Van Lindberg

<Rob Slade <rMslade@shaw.ca>>

Mon, 5 Jan 2009 10:22:01 -0800

BKIPOPSO.RVW 20081128

"Intellectual Property and Open Source", Van Lindberg, 2008,
978-0-596-51796-0, U\$34.99/C\$34.99

%A Van Lindberg

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 2008

%G 978-0-596-51796-0 0-596-51796-3

%I O'Reilly & Associates, Inc.

%O U\$34.99/C\$34.99 800-998-9938 707-829-0515 nuts@ora.com

%O <http://www.amazon.com/exec/obidos/ASIN/0596517963/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0596517963/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/0596517963/robsladesin03-20>
%O Audience i Tech 2 Writing 2 (see revfaq.htm for explanation)
%P 371 p.
%T "Intellectual Property and Open Source"

The preface states that this book provides documentation for the legal system, obviously intending that it be addressed to a technical audience, explaining to them what the legal operations are (as related to intellectual property, or IP).

Chapter one outlines the legal categories of IP (patent, copyright, trademark, and trade secret), as well as reviewing general economic theory, and the philosophy of knowledge as a type of material "good." Patent documents are explained, in chapter two, in terms of file formats. The important concepts of invention (as claim) versus embodiment, conception versus reduction to practice, and first to file as opposed to first to invent are also defined. What is, and isn't, patentable is covered in chapter three. The details, requirements, and limits of copyright are in chapter four. Chapter five points out that trademark has value not only for the company, but also for the customer. The discussion of trade secret, in chapter six, notes the factors involved in the utility of a trade secret. This chapter also examines some issues of open source software for the first time, since the preceding material is fairly generic.

Chapter seven looks at contracts and licences, a number of issues of which are important to open source. Using an interesting (and useful) analogy of the difference between banks and credit unions, chapter eight notes the economic and legal basis for open source software, and why (and where) it works. (The licencing discussion is also extended here.) The factors involved in ownership of intellectual property (whether on the part of the individual, company, or work-for-hire) are examined in chapter nine. Chapter ten notes terms, and provides examples, of open source licences. Some very interesting implications of accepting code patches are noted in chapter eleven. Chapter twelve extends chapter ten's content, specific to the General Public License (GPL). Chapter thirteen briefly looks at the process of reverse engineering, but is primarily concerned with the legality of the operation. The establishment of non-profit organizations, and particularly in relation to the benefit for open source projects, is outlined in chapter fourteen.

Appendices provide various samples of legal documents.

The writing is articulate, and the material reasonably comprehensive. The organization leaves a little bit to be desired. The book is almost two books; one on IP and one on open source; and it's not clear why chapters seven, ten, and twelve are distinct (and separated). However, this is a valuable guide for anyone in the technical world who wishes to know about legal issues of intellectual property, and particularly for anyone in, or contemplating, an open source project.

copyright Robert M. Slade, 2008 BKIPPOSO.RVW 20081128
rslade@vcn.bc.ca <http://victoria.tc.ca/techrev/rms.htm>

http://blog.isc2.org/isc2_blog/slade/index.html

<http://blogs.securiteam.com/index.php/archives/author/p1/>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 52

Thursday 22 January 2009

Contents

- [German Train System Computers Down for Hours](#)
[Debora Weber-Wulff](#)
- [Yet Another Reason Not to use Windows for Medical Devices](#)
[Jeremy Epstein](#)
- [Tricky Windows Worm Wallops Millions](#)
[Brian Krebs via Monty Solomon](#)
- [Electronic Medical Records, Google, and Microsoft](#)
[Lauren Weinstein](#)
- [Cursive, foiled again: What will become of handwriting?](#)
[David Mehegan via Monty Solomon](#)
- [The perils of trusting the UK government to get software right](#)
[Bernard Peek](#)
- [New Web Analytics Service Spies on Web Browsing Activity Without Permission](#)
[Lauren Weinstein](#)
- [Re: "Spy pens" and the future of private speech](#)
[Henry Baker](#)
[Jerry Leichter](#)
- [Re: Tony Hoare: "Null References: The Billion Dollar Mistake"](#)
[Henry Baker](#)
- [Risks of Avis insufficient customer data checking](#)
[Chris Warwick](#)
- [Info on RISKS \(comp.risks\)](#)

German Train System Computers Down for Hours

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>
Sat, 17 Jan 2009 13:05:55 +0100

Another Peter Neumann (!!) reports in the *Berliner Zeitung* 17 Jan 2009:

On January 14, 2009 at 14.03 the plug got pulled on the German national train system's computers - all of them. No ticket machines would work, either the self-service or the counter machines; the Internet pages returned

404s; the boards in the train stations telling you which track to take died; and apparently even some of the operations computers just shut off.

There was a single point of failure - the "uninterruptible" power system (UPS).

The computer center of the Deutsche Bahn in Mahlsdorf (Berlin) was upgrading the UPS. Suddenly there was no electricity flowing through the mains. None. And the entire system fell like a house of cards.

Oh, they had a backup system set up [for lots of money, we suppose, I've seen the computer centers, they look like prisons, windowless monstrosities with high fences topped by razorwire -dww] just down the road in Biesdorf. The speaker won't say exactly what happened, but the cut-over to the backup system did not work.

It took hours to get the system back up and running - apparently every system assumes that every other system is already up and running, and turning them all on at the same time is quite a drain on electricity. The speaker will not go into any more detail on this topic, except to say that the specific nature of the error meant that each system had to be restarted by itself.

Of course, the usual speculation made the rounds - hackers, terrorists, viruses. But again - never make up complicated theories for what can be explained by simple incompetence.

The speaker: We have found the weak point and can guarantee that something like this will never happen again.

comp.risks has a long memory....

Prof.Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Treskowallee 8, 10313 Berlin
<http://www.f4.fhtw-berlin.de/people/weberwu/> +49-30-5019-2320

Yet Another Reason Not to use Windows for Medical Devices

<Jeremy Epstein <jeremy.j.epstein@gmail.com>>

Wed, 21 Jan 2009 09:07:31 -0500

The Register reports that "staff at hospitals across Sheffield are battling a major computer worm outbreak after managers turned off Windows security updates for all 8,000 PCs on the vital network" with "more than 800 computers ... infected with self-replicating Conficker code". And how did this happen? The worm takes advantage of a known problem that is resolved through a Windows patch that wasn't installed because "the decision to disable automatic security updates was taken during Christmas week after PCs in an operating theatre [were] rebooted mid-surgery. Conficker was detected" on 29 Dec 2008.

http://www.theregister.co.uk/2009/01/20/sheffield_conficker/

Or in short:

- Life-critical systems rely on software that has a long history of vulnerabilities.
- To avoid critical interruptions, automatic fix installation is disabled, with no backup process for installing them at non-critical times.
- These systems are interconnected (including to the Internet) for whatever reason.
- There are (apparently) no other protection mechanisms beyond installing fixes.
- Malware leaks in to the network and spreads.
- The interaction of the above leads to really bad results.

And where is the surprise? Even Microsoft's license agreement notes that you shouldn't use their software for life-critical systems (among other things). Perhaps that's just a CYA thing, but one would hope that there's consideration of the risks before ignoring those terms.

[Also noted by Toby Douglass.

Incidentally, Phil Porras (whose Cyber-Threat Analytics project <<http://www.cyber-ta.org>> has been tracking conficker) noted to me that the relevant RPC exploit was patched and distributed by MS's security update service on 23 Oct 2008. PGN]

Tricky Windows Worm Wallops Millions (Brian Krebs)

<Monty Solomon <monty@roscom.com>>
Tue, 20 Jan 2009 22:59:08 -0500

Brian Krebs, *The Washington Post*, 16 Jan 2009

A sneaky computer worm that uses a virtual Swiss army knife of attack techniques has infected millions of Microsoft Windows PCs, and appears to be spreading at a fairly rapid pace, security experts warn.

Also, while infected PCs could be used for a variety of criminal purposes -- from relaying spam to hosting scam Web sites -- there are signs that this whole mess may be an attempt to further spread so-called "scareware," which uses fake security alerts to frighten consumers into purchasing bogus computer security software.

The worm, called "Downandup" and "Conficker" by different anti-virus companies, attacks a security hole in a networking component found in most Windows systems. According to estimates from Finnish anti-virus maker F-Secure Corp., the worm has infected between 2.4 million and 8.9 million computers during the last four days alone.

If accurate, those are fairly staggering numbers for a worm that first surfaced in late November. Microsoft issued an emergency patch to fix the flaw back in October, but many systems likely remain dangerously exposed.

One reason for this is because businesses will generally test patches before

deploying them on internal networks to ensure the updates don't break custom software applications. In the meantime, an infected laptop plugged into a vulnerable corporate network can quickly spread the contagion to all unpatched systems inside that network.

But the worm also has methods for infecting systems that are already patched against the Windows vulnerability. According to an analysis last week by Symantec, the latest versions of Downadup copy themselves to all removable or mapped drives on the host computer or network. This means that if an infected system has a USB stick inserted into it, that USB stick will carry the infection over to the next Windows machine that reads it. That's an old trick, but apparently one that is apparently still very effective. ...

http://voices.washingtonpost.com/securityfix/2009/01/tricky_windows_worm_wallops_mi.html

[Conficker is apparently even more widespread than reported above. PGN]

✂ Electronic Medical Records, Google, and Microsoft

<Lauren Weinstein <lauren@vortex.com>>
Mon, 19 Jan 2009 12:25:51 -0800 (PST)

Lauren Weinstein's Blog Update, 19 Jan 2009

<http://lauren.vortex.com/archive/000497.html>

Greetings. It's well known that a significant portion of the Obama administration's stimulus plans will likely be a major thrust toward electronic medical records. These are touted as reducing errors, creating jobs, and saving money -- though it's arguable if medical consumers are the ones who actually pocket the savings in most cases.

But there are serious concerns about these systems as well -- reminding us that exactly the same sorts of problems that tend to plague our other computer-based ecosystems could now start hitting people's medical records in pretty much the same ways.

The New York Times (19 Jan 2008) had an excellent story about privacy and security issues associated with electronic medical records -- and the medical industry heavyweights who are trying to water down related provisions in associated and upcoming legislation.

<http://www.nytimes.com/2009/01/18/us/politics/18health.html>

A few days ago, AP reported on a range of potentially serious medical errors *created* by the Veterans Administration's new electronic medical records system.

<http://www.tampabay.com/news/military/veterans/article967778.ece>

Both Google and Microsoft have unveiled electronic medical records systems for users, and are actively seeking partnerships with major medical treatment organizations. While they both promise comprehensive privacy and control by users -- in some ways that exceed those mandated by HIPAA privacy

requirements, these systems are explicitly not actually covered by HIPAA -- though my hunch is that this status is likely to change in the near future.

The key concern with such non-HIPAA medical records systems isn't their privacy and security at the moment -- which as I noted appear to be good at present. Rather, an important aspect of HIPAA is that it represents a set of rules that cannot be arbitrarily changed by the organizations involved. Consumers need to know that the "rules of the game" when it comes to their medical records will not be subject to unilateral alterations on the basis of business conditions or management changes, outside the realm of legislated national rules.

My belief is that electronic medical records in general, and the services like those from Google and MS in particular, have the potential for significant benefits. I also believe that a massive rush into any of these environments could end up creating a whole new range of problems that could waste money, risk privacy, and in the worst case even cost lives.

I trust that Congress will move with deliberate speed, but not be pressured, in the area of electronic medical health records implementation, and that they will put patients' rights to privacy, accuracy, security, control, and choice at the top of agenda. A stampede to electronic medical records without due consideration and care would be a very dangerous prescription indeed.

#Cursive, foiled again: What will become of handwriting? (David Mehegan)

<Monty Solomon <monty@roscom.com>>

Tue, 20 Jan 2009 22:33:03 -0500

[Source: David Mehegan, *The Boston Globe*, 19 Jan 2009]

Cursive, foiled again:

We e-mail, we text, we Twitter - what will become of handwriting?

"The moving finger writes," says the famous Rubaiyat of Omar Khayyam, "and, having writ, moves on." Nowadays, the finger more likely is hammering away on a computer keyboard, texting on a cellphone, or Twittering on a BlackBerry.

If you predate the computer age, you might remember a school subject called "penmanship," which trained your cursive handwriting, usually by the Palmer Method. The penmanship teacher would come by once a week to rate your work, and if your handwriting was bad, you'd hear about it. It's still taught, to be sure, but it's no longer emphasized. "There's been a decline in attention to all kinds of basic skills," said Louise Spear-Swerling, coordinator of the graduate program in learning disabilities at Southern Connecticut State University. "With handwriting, people think it's just not that important."

Some people are concerned, though, and one is Kitty Burns Florey, whose book "Script and Scribble: The Rise and Fall of Handwriting" comes out Friday -

John Hancock's birthday and National Handwriting Day. Florey, author of nine novels and a book about sentence diagramming, became interested in the subject after reading that computer keyboarding has displaced handwriting in schools. ...

http://www.boston.com/ae/books/articles/2009/01/19/cursive_foiled_again/

✶ The perils of trusting the UK government to get software right

<Bernard Peek <bap@shrdlu.co.uk>>

Tue, 6 Jan 2009 21:35:16 +0000

In the UK there is a Government Gateway web site used to access a number of government services. One of the better hidden services is that it is possible to register a claim for unemployment benefit. Like many of the UK's IT staff I now have need of the service.

Everything starts off reasonably well. Access to the site requires an ID that is delivered to users by post, together with a password users can choose for themselves. So far so good.

Registering a claim for "Jobseekers' Allowance" takes the user through a questionnaire that parallels the one that most people deal with via a telephone interview. At the end of the process the user is given a final chance to review the data and finally confirm that they wish to submit a claim.

At this point the user is presented with a pop-up confirmation that the claim has been submitted. The interesting thing is that the claim has not been submitted at that point and still has a status of "not yet submitted." The next stage should presumably be that the claim is actioned, but this part of the code silently fails. The claim will stay in limbo. Unless the user has some reason to return to the system and log in again they have no reason to suspect that their data has been dropped on the floor. If they do log in again they will see the "not yet submitted" status and can complete the submission again, getting a new pop-up saying that the claim has been submitted. Which submission will again be silently dropped on the floor and the "not yet submitted" flag will remain unchanged.

I'm sure that there must be a lesson to be learned from this, probably several. I hope that one of the lessons which will be learned is that when you FUBAR a user's data, don't do it to a RISKS subscriber.

Bernard Peek, London, UK. DBA, Manager, Trainer & Author.

✶ New Web Analytics Service Spies on Web Browsing Activity Without Permission

<Lauren Weinstein <lauren@vortex.com>>

Thu, 22 Jan 2009 09:14:48 -0800

New Web Analytics Service Spies on Web Browsing Activity Without Permission

<http://lauren.vortex.com/archive/000498.html>

Greetings. In the business of "Web Analytics" -- collecting, analyzing, and reporting of Web usage data -- various firms are continuously pushing the envelope.

Such data is in many ways the bread and butter of the free Web services that we've come to expect, since it is in key respects a crucial element of the ad-supported Web services ecosystem. However, the temptation to push analytics technology too far always exists.

A firm that appears to have succumbed to that temptation came to my attention today. "Tealium Social Media," a service of Tealium (<http://www.tealium.com>) in San Diego, California, is a commercial analytics service that uses JavaScript tricks to inspect -- without the knowledge or permission of Web users -- specific URLs in their current browser histories.

The service attempts to provide a finer grain of usage information than is typically available through analytical techniques, by querying users' browsers for the presence of particular URLs. While this does not permit the reading out of complete browser URL histories, it does permit the service to ask the potentially highly privacy-invasive question: "Has this user been to a particular URL recently?"

Obviously, by sending a variety of such queries (all of which are essentially invisible to the user), a fascinating portrait of users' activities could be generated. Visited this CNN story? This government Web page? This porn image? This medical information page? Well, you get the idea.

While the JavaScript functionalities that enable this intrusion have been known for quite some time in hacking and other technical circles, this appears to possibly be among the first commercial applications of this technique.

I had a cordial chat early this afternoon with Olivier Silvestre, one of Tealium's partners, and a later e-mail exchange with Ali Behnam, another partner.

They both emphasized a number of points that will sound all too familiar, and I'm afraid far from convincing. They noted that they do not collect PII ("personally-identifiable information"), don't accumulate user-linked data, and only query browser histories for specific ("social media") related links. It was also mentioned that they have obfuscated their JavaScript to try prevent their clients from altering the code, have a customer use policy that prohibits their clients from attempting such alterations, have put in place a privacy policy ... and so on.

Opt-out is apparently possible via a cookie -- but of course you have to know what's going on before you'd ever think to set an opt-out cookie! They hope to move to non-cookie opt-out techniques, and

claimed in answer to my query that they'd really prefer to be opt-in, but realize that getting people to opt-in to such a service could be, shall we say, impractical.

If so much of this sounds like *deja vu*, it's because we've heard virtually all of it before. In many ways it's quite similar to arguments made by Phorm and NebuAd, which were roundly criticized as self-serving and inadequate.

The fundamental question is an obvious one -- "Unless we're asked for our permissions in advance, what the hell business is it -- of anyone by ourselves -- what is or is not in our browser histories?"

Arguments about not collecting PII, only looking for particular URLs, and all the rest, necessarily fall flat. Inspecting browser URL histories in such a manner -- without affirmative opt-in permission -- clearly crosses the line from acceptable analytics to an unacceptable intrusion into private activities.

If a burglar argued that the only reason they conducted break-ins was to check to see if you had purchased particular products, would such reasoning be likely to prevail in court? I'm not a lawyer, so I won't attempt here to present a legal analysis of the Tealium technique -- though I'd certainly be interested to hear opinions about this.

But again, the guys at Tealium were friendly and open in our contacts, and made no attempt to evade my questions. Clearly we're dealing in this case with a very different view of what privacy is, and what is acceptable behavior on the Web.

My hope is that Tealium will reconsider their use of this methodology, and I urge that all browsers vulnerable to such manipulations be altered to prevent their use.

In the meantime, there are some ways to protect yourself from this technology, though none are particularly pretty. You can make a practice of clearing your browser history frequently, or not keeping a history at all, but these are both inconvenient. You can turn off JavaScript, but this will completely break a vast number of sites and is generally not very practical these days.

[Update (1/22/09): Several people have suggested the Firefox "NoScript" plugin as a method for finer-grained control over JavaScript. This is certainly available, though it is not necessarily clear which sites to script block, or what the side-effects of selectively blocking JavaScript will be in any given case. But as a practical matter, most people can't run NoScript since they don't use Firefox, and most people who run Firefox tend not to use plugins. The only ad hoc "solution" available to pretty much everyone with a Web browser is to turn off JavaScript completely, with the serious downside already noted. More to the point, blocking such activities at the PC is essentially a diversion from the larger issues surrounding the Tealium service, such as should their technique be permitted at all and is it legal in all jurisdictions? It is unrealistic to expect everyone to

fiddle around with their browser configurations to try protect against these sorts of intrusive activities.]

Or you might contact Tealium and let them know if you do (or don't) approve of their practices in these regards.

As far as I'm concerned, my browser history is mine, nobody else's. Period. Full stop. End of discussion.

+1(818)225-2800 <http://www.pfir.org/lauren> <http://lauren.vortex.com>
<http://www.pfir.org> Network Neutrality Squad - <http://www.nnsquad.org>

Re: "Spy pens" and the future of private speech (Leichter, [RISKS-25.51](#))

<Henry Baker <hbaker1@pipeline.com>>
Sat, 17 Jan 2009 09:20:07 -0800

At the Consumer Electronics Show (CES) this year, a number of booth personnel were wearing cameras on their chests that recorded video & audio of every person they talked to the entire day. The cameras had enough quality to pick up the names on the badges of the people they talked with. According to one gentleman, the camera allowed him to focus on talking with the person and not wasting time getting his/her badge information.

These cameras are not expensive -- one of the booths I stopped at was actually selling them. I expect them to start showing up at all kinds of business meetings.

The future you project is already here.

Re: "Spy pens" and the future of private speech (Baker, [RISKS-25.52](#))

<Jerry Leichter <leichter@lrw.com>>
Sun, 18 Jan 2009 06:33:47 -0500

> The future you project is already here.

That being the case ... I'll add my social predictions. :-)

Prosecutors today complain of the "CSI effect": On the CSI series of TV shows, every week, crimes are solved by introducing all kinds of detailed, highly specific, scientific evidence. Juries assume that that's the way things work in the real world, and convincing them without it has gotten harder - an attitude the defense bar encourages, of course. But the reality of scientific evidence doesn't approach the fantasy.

In a world of ubiquitous recording, anything that **wasn't** recorded will seem, at the least, less reliable - and eventually even suspicious. "If you had nothing to hide, why didn't you make a recording of what you were

doing?" The common law has traditionally accepted oral contracts - special cases, going back the the oddly- named Statue of Frauds, excepted - in recognition of the inconvenience of memorializing on paper the huge number of dealings in which we are involved on a daily basis, especially in business. The "he said/she said" evidentiary arguments that inevitably follow are just something that we have to accept to keep commerce flowing. In a world where every conversation is trivially recorded - will we continue to do that? -- Jerry

✂ Re: Tony Hoare: "Null References: The Billion Dollar Mistake"

<Henry Baker <hbaker1@pipeline.com>>

Sat, 17 Jan 2009 09:43:31 -0800

Billion Dollar Mistake? (Dagenais, [RISKS-25.51](#))

I'd be willing to bet that the actual number is far, far higher, especially when adjusted for inflation.

But I applaud Tony for his apology. I haven't yet heard an apology from Fortran/C/C++/etc. creators over their inability to police array bounds. A good fraction of the ACM Fellows (perhaps the ACM itself?) need to provide mea culpas over this issue.

To a first approximation, the lack of array bounds checking created the virus/worm industry, and we are still paying handsomely for this.

Madoff was a rank amateur by comparison. Computer "scientists" have been producing insecure code like this since before NASDAQ was started.

✂ Risks of Avis insufficient customer data checking

<Chris Warwick <chris.warwick@shaw.ca>>

Mon, 19 Jan 2009 21:46:11 -0700

[Re: Risks of data retention 25.48 (Armburst [RISKS-25.48](#))]

I'm not sure I agree the assertion that one-time accounts should never be re-used. I can see a significant benefit of storing and keeping current such information as a way to reduce errors from having to enter the information each time.

I think the problem comes from the resulting system, and ensuring that the re-used information is correct and correctly used. Also, if a failure occurs, then the system (human and automated) needs to be able to determine where the error occurred, so it can be corrected.

I have a related story:

Avis, and other car rental companies, have a service where information (driver's license number, billing info, etc.) is pre-entered into their reservation/billing system, under a Wizard Number. The benefit, to me, is that the time needed to rent a car is significantly reduced.

I checked my account last summer and found that someone had made a reservation in my name.

I called Avis and was told that they thought that operator error had resulted in my Wizard Number being used as part of someone else's reservation.

Issues:

- The system should have done some checking to ensure the correct Wizard Number was being used. Canadian banks love asking silly questions to confirm identity, why not this system?

- The system didn't seem to have any way to determine who had made the reservation, and inform them that correction was needed. Was the reservation made through an agent? Was it associated with an airline reservation?

I canceled the reservation, and suggested Avis send a note to the place the car was to be picked up, so they would know what happened when this person arrived (and hopefully keep a car available for him).

Somewhat later copy of receipt from this person's rental turned up on my Avis account.

So, logically, he must have arrived at the rental office, with a printed copy of the reservation. Rather than checking why the reservation was canceled, the rental office must have simply reconstituted the reservation under my Wizard Number.

Issues:

- Something should have detected a fault. A detailed check of this person's information against what was in stored under my Wizard Number should have detected something.

- The system has stored the record of the rental, complete with parts of his credit card number, under my Wizard Number.

I called Avis, and their response was that since the rental hadn't been charged to me (the renter had provided a credit card) nothing was wrong.

So, I called the rental office. The person I talked to told me they remembered the rental, and that the Wizard Number had come up when they swiped his credit card <!. Further discussion revealed that the name on the credit card was the same as mine, and that the driver's license was issued from the same province as where I live.

Issues:

- The linking of his information to my Wizard Number seems like a serious system fault, so I am curious about Avis's response.

- In cases where the information between two customers has some overlap the system (human and automated) needs to do extra special checking. In this case there is a strong possibility that I could have been billed, without any way to determine who had actually rented the car.

I guess the risk is all Avis (since the stamps on my passport prove it wasn't me who rented the car), but in these days of identity theft, I would hope our automated systems are being developed to reduce the IT reservation under my Wizard Number.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 53

Saturday 31 January 2009

Contents

- [England's NHS loses patient data: bad news, good news, bad news](#)
[Steven J Klein](#)
- [Michigan man freezes to death after electric company cuts power](#)
[Mark E. Smith](#)
- [Worm Infects Millions of Computers Worldwide](#)
[John Markoff via PGN](#)
- [Trojan virus spreads to as many as 20,000 Macs](#)
[Boy Genius via Dave Farber](#)
- [Fannie Mae insider attack](#)
[Kevin Poulsen via Jeremy Epstein](#)
- [NSW, Australia Govt Jobs website hacked; authorities in denial](#)
[Andrew Jones](#)
- [MP3 player contained US military secrets](#)
[Danny Burstein](#)
- [Digital road sign in Austin, TX was altered to read, "Zombies Ahead."](#)
[David Hollman](#)
- [Friends, Until I Delete You](#)
[Douglas Quenqua via Monty Solomon](#)
- [Political risks of poorly configured email advocacy](#)
[Rich Mintz](#)
- [Canadian do-not-call list becomes valuable telemarketing database](#)
[Olivier Dagenais](#)
- [Staff Finds White House in the Technological Dark Ages](#)
[Anne E. Kornblut via Monty Solomon](#)
- [Amex goes phishing](#)
[James J. O'Donnell](#)
- [American Express Kept a *Very* Watchful Eye on Charges](#)
[Ron Lieber via Monty Solomon](#)
- [Statue of Frauds \[sic\]](#)
[Martyn Thomas](#)
- [Re: Yet Another Reason Not to use Windows for Medical Devices](#)
[Bernard Peek](#)
- [Re: Tony Hoare: "Null References"](#)
[Michael Albaugh](#)
[Jurek Kirakowski](#)

[Ray Blaak](#)

[Martin Torzewski](#)

[Richard O'Keefe](#)

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

England's NHS loses patient data: bad news, good news, bad news

Steven J Klein <steveklein@mac.com>

Sun, 25 Jan 2009 03:33:10 -0500

Bad news: A National Health Service employee lost a flash drive containing personal information of up to 6,360 patients.

Good news: The data on the flash drive was encrypted.

Bad news: The password was written on a sticky-note attached to the drive.

Paraphrased from the *Lancashire Evening Post*

<http://www.lep.co.uk/news/Apology-after-prisoners39-health-info.4862265.jp>

Steven J Klein, Your Mac & PC Expert, Phone: (248) YOUR-MAC or (248) 968-7622

Michigan man freezes to death after electric company cuts power

"Mark E. Smith" <mymark@gmail.com>

Tue, 27 Jan 2009 04:06:40 -0800

In this case the risk appears to be the assumption that anyone who wishes to pay their electric bill can do so easily. The 93-year-old WWII veteran may not have had a checking account, a computer, or online bill paying, and the weather was too severe for him to leave home to pay his electric bill in person. After his death, a large amount of cash was found clipped to his utility bill on his kitchen table.

Worm Infects Millions of Computers Worldwide (John Markoff)

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

Fri, 23 Jan 2009 11:26:18 PST

[Source: John Markoff, *The New York Times*, 23 Jan 2009]

<http://www.nytimes.com/2009/01/23/technology/internet/23worm.html>

A new digital plague has hit the Internet, infecting millions of personal and business computers in what seems to be the first step of a multistage attack. The world's leading computer security experts do not yet know who programmed the infection, or what the next stage will be.

In recent weeks a worm, a malicious software program, has swept through corporate, educational and public computer networks around the world. Known as Conficker or Downadup/Downandup, it is spread by a recently discovered Microsoft Windows vulnerability, by guessing network passwords and by hand-carried consumer gadgets like USB keys.

Experts say it is the worst infection since the Slammer worm exploded through the Internet in January 2003, and it may have infected as many as nine million personal computers around the world. [...]

✶ Trojan virus spreads to as many as 20,000 Macs: Boy Genius Report

*David Farber <dave@farber.net>
Sun, 25 Jan 2009 12:52:32 -0500*

via false ilife leak

<http://www.boygeniusreport.com/2009/01/23/trojan-virus-spreads-to-as-many-as-20000-macs/>

✶ Fannie Mae insider attack

*Jeremy Epstein <jeremy.epstein@sri.com>
Fri, 30 Jan 2009 08:42:17 -0500*

Threat Level, By Kevin Poulsen, Wired.com, 29 Jan 2009
<http://blog.wired.com/27bstroke6/2009/01/fannie.html>

A logic bomb allegedly planted by a former engineer at mortgage finance company Fannie Mae last fall would have decimated all 4,000 servers at the company, causing millions of dollars in damage and shutting down Fannie Mae for a least a week, prosecutors say.

Unix engineer Rajendrasinh Babubha Makwana, 35, was indicted on 27 Jan 2009 in federal court in Maryland on a single count of computer sabotage for allegedly writing and planting the malicious code on Oct. 24, the day he was fired from his job. The malware had been set to detonate at 9:00 a.m. on Jan. 31, but was instead discovered by another engineer five days after it was planted, according to court records.

Makwana, an Indian national, was an employee of technology consulting firm OmniTech, but he worked full time on-site at Fannie Mae's massive data center in Urbana, Maryland, for three years.

On the afternoon of 24 Oct 2008, he was told he was being fired because of a scripting error he'd made earlier in the month, but he was allowed to work through the end of the day, according to an FBI affidavit (.pdf) in the case. "Despite Makwana's termination, Makwana's computer access was not immediately terminated," wrote FBI agent Jessica Nye.

Five days later, another Unix engineer at the data center discovered the malicious code hidden inside a legitimate script that ran automatically every morning at 9:00 a.m. Had it not been found, the FBI says the code would have executed a series of other scripts designed to block the company's monitoring system, disable access to the server on which it was running, then systematically wipe out all 4,000 Fannie Mae servers, overwriting all their data with zeroes. [...]

✂ NSW, Australia Govt Jobs website hacked; authorities in denial

*Andrew Jones <andrew2004sydney@yahoo.com>
Mon, 26 Jan 2009 16:28:14 -0800 (PST)*

Spammers hack into Government jobs website

<http://www.smh.com.au/news/technology/security/id-theft-alert-as-job-site-hacked/2009/01/26/1232818299147.html>

"The NSW Government website used to advertise public service jobs has been hacked into and the perpetrators have spammed the Government's database of job seekers with phony vacancies in an effort to steal personal data and possibly to spread viruses." [...]

"However, Turner said the blame did not lie solely with the Government as 'any computer system can be hacked ... even American defence force computers'." [...]

" 'The Department of Commerce is currently looking into the matter and has alerted the relevant authorities,' the spokeswoman said."

✂ MP3 player contained US military secrets

*danny burstein <dannyb@panix.com>
Fri, 30 Jan 2009 00:18:08 -0500 (EST)*

Kerri Ritchie, 28 Jan 2009

When a New Zealand man spotted a portable MP3 player for \$US9 in an American op-shop, he thought he'd landed a real bargain. But Chris Ogle got far more than he bargained for.

Instead of storing songs, the MP3 player contained secrets; 60 highly sensitive US military files. ... When he got back to New Zealand, he tried to download some songs onto his computer and says he got the shock of his life - 60 US military files labeled top secret popped up on his screen. ...

Kerri Ritchie: The files contained the social security numbers, home addresses, even mobile phone numbers of American soldiers based in Afghanistan and Iraq.

rest:

<http://www.abc.net.au/pm/content/2008/s2476665.htm>

[Also noted by Gene Wirchenko,

<http://arstechnica.com/security/news/2009/01/man-buys-used-ipod-gets-60-pages-of-sensitive-military-data.ars>

PGN]

✂ Digital road sign in Austin, TX was altered to read, "Zombies Ahead."

David Hollman <dah8@cornell.edu>

Thu, 29 Jan 2009 15:23:13 +0000

Excerpts from <http://www.foxnews.com/story/0,2933,484326,00.html> :

Transportation officials in Texas are scrambling to prevent hackers from changing messages on digital road signs after one sign in Austin was altered to read, "Zombies Ahead."*

...The sign was reverted back to its original message within hours... the signs are tamper-resistant and equipped with external locks.

According to the blog i-hacked.com, some commercial road signs, including those manufactured by IMAGO's ADDCO division, can be easily altered because their instrument panels are frequently left unlocked and their default passwords are not changed.

"Programming is as simple as scrolling down the menu selection," i-hacked.com reports. "Type whatever you want to display -- In all likelihood, the crew will not have changed [the password]."

[Also noted by Geoffrey Brent:

http://www.woostercollective.com/2009/01/hacking_the_grid_in_austin_zombies_ahead.html

PGN]

✂

Monty Solomon <monty@roscom.com>

Fri, 30 Jan 2009 23:59:50 -0500

Subject: Friends, Until I Delete You

Douglas Quenqua, *The New York Times*, 29 Jan 2009

A person could go mad trying to pinpoint the moment he lost a friend. So seldom does that friend make his feelings clear by sending out an e-mail alert.

It's not just a fact of life, but also a policy on Facebook. While many trivial actions do prompt Facebook to post an alert to all your friends -

adding a photo, changing your relationship status, using Fandango to buy tickets to "Paul Blart: Mall Cop" - striking someone off your list simply is not one of them.

It is this policy that Burger King ran afoul of this month with its "Whopper Sacrifice" campaign, which offered a free hamburger to anyone who severed the sacred bonds with 10 of the friends they had accumulated on Facebook. Facebook suspended the program because Burger King was sending notifications to the castoffs letting them know they'd been dropped for a sandwich (or, more accurately, a tenth of a sandwich).

The campaign, which boasted of ending 234,000 friendships, is history now - Burger King chose to end it rather than tweak it to fit Facebook's policy - but the same can hardly be said of the emerging anxiety it tapped. As social networking becomes ubiquitous, people with an otherwise steady grip on social etiquette find themselves flummoxed by questions about "unfriending" people: how to do it, when to do it and how to get away with it quietly. ...

<http://www.nytimes.com/2009/01/29/fashion/29facebook.html>

✂ Political risks of poorly configured email advocacy

Rich Mintz <richmintz@richmintz.com>

Sat, 31 Jan 2009 10:59:04 -0500

In the UK last week, Greenpeace asked its supporters to email their MP on the issue of runway expansion at Heathrow. Apparently, the email system in question was set up to send the supporter's email to their own MP -- and to copy the email to all the other targeted MPs on the system. As a result, 57 MPs each got thousands of emails in three or four hours. Hilarity ensued.

What makes this interesting: the 57 targeted MPs are all *supporters* of Greenpeace's position, who were being asked in the emails to hold firm in their support.

<http://business.timesonline.co.uk/tol/business/columnists/article5600838.ece>

<http://www.mattwardman.com/blog/2009/01/27/david-taylor-mp-raises-greenpeace-heathrow-automated-mass-email-campaign-in-parliament/>

✂ Canadian do-not-call list becomes valuable telemarketing database

Olivier Dagenais <olivier.dagenais@gmail.com>

Sat, 24 Jan 2009 10:22:15 -0500

The Consumers' Association of Canada says it has been inundated with complaints from people who have been called by scam artists after placing their telephone numbers on the registry, which went into effect last September.

The do-not-call list was created to prevent telemarketers from contacting

people who do not want to be pestered with uninvited sales pitches. For companies to find out who they are not permitted to call, the Canadian Radio-television and Telecommunications Commission sells the list online for a fee.

"You can buy any list you want of people who subscribe to the do-not-call registry online. The whole of Toronto costs you 50 bucks for 600,000 names," Bruce Cran, president of the CAC, said in a telephone interview yesterday.

"That's just perfect for any telemarketer, because these are good names which they would otherwise have to pay money for to verify. In addition to that, there's no index list of cell phone numbers that you can get. However, people were encouraged to put their cell phone numbers on there as well."

Source: Fraudsters abusing do-not-call list, *The Globe and Mail*, 23 Jan 2009

<http://www.theglobeandmail.com/servlet/story/RTGAM.20090123.wdonotcall23/BNStory/National/home>

The article makes it sound like names are also included in the lists, but the DNCL website seems to indicate otherwise (unless, of course, reverse-lookup is used with other public listings):

http://www.crtc.gc.ca/ENG/INFO_SHT/t1028.htm

★ Staff Finds White House in the Technological Dark Ages

Monty Solomon <monty@roscom.com>

Thu, 22 Jan 2009 22:24:40 -0500

[Source: Anne E. Kornblut, *The Washington Post*, 22 Jan 2009, A01]

If the Obama campaign represented a sleek, new iPhone kind of future, the first day of the Obama administration looked more like the rotary-dial past. Two years after launching the most technologically savvy presidential campaign in history, Obama officials ran smack into the constraints of the federal bureaucracy yesterday, encountering a jumble of disconnected phone lines, old computer software, and security regulations forbidding outside e-mail accounts.

What does that mean in 21st-century terms? No Facebook to communicate with supporters. No outside e-mail log-ins. No instant messaging. Hard adjustments for a staff that helped sweep Obama to power through, among other things, relentless online social networking. "It is kind of like going from an Xbox to an Atari," Obama spokesman Bill Burton said of his new digs.

In many ways, the move into the White House resembled a first day at school [...]. There were plenty of first-day glitches, too, as calls to many lines in the West Wing were met with a busy signal all morning and those to the main White House switchboard were greeted by a recording, redirecting callers to the presidential Web site. A number of reporters were also shut out of the White House because of lost security clearance lists. [...]

<http://www.washingtonpost.com/wp-dyn/content/article/2009/01/21/AR2009012104249.html>

Amex goes phishing

"James J. O'Donnell" <provost@georgetown.edu>

January 22, 2009 5:36:54 PM EST

[From Dave Farber's IP]

Got messages on various accounts over the weekend from American Express to tell cardholders that their 2008 year-end statement is online. Just click on this address, it said, giving an address. If you mouse-overed the address, a different address appeared in the status bar, and if you clicked on the address, you went to a third uniquely different address. I did so, on a machine that could be cleaned if it were compromised, twice. What I found when I got there is that after you clicked on the nonconforming link, you went to a page that asked you to input credit card information: either your existing login/password for the amex site *or*, if you didn't have login/pwd yet, to input your actual credit card information including card number, expiry date, and 4-digit "security code".

Now I believe that the message was in fact legit: came from Amex and led you to a site that was what it said it was. What gobsmailed me was that Amex was using classic phishing technique to get you to their site, and asked you once there to engage in *exactly* the behavior that we tell everybody not to behave in.

So what happened? Today we got two messages that obviously responded to the incomplete logins yesterday -- alerts to tell us that there was a problem with that account due to multiple attempted logins and asking us to login to the site to check and confirm information there. The "security messages" took exactly the same form: please click on this inconsistent URL and when you get to the page referenced, go ahead and input confidential information.

I phoned Amex and nobody on their standard phone lines understood the issue, but they got me eventually to corporate in NYC and I spoke to someone in "investigations" who got what I was saying instantly and I could hear him shaking his head. He said he'd get on it.

Archives: <https://www.listbox.com/member/archive/247/=now>

American Express Kept a *Very* Watchful Eye on Charges (Ron Lieber)

Monty Solomon <monty@roscom.com>

Sat, 31 Jan 2009 00:11:59 -0500

YOUR MONEY

Ron Lieber, American Express Kept a (Very) Watchful Eye on Charges,

The New York Times, 31 Jan 2009

You probably know that credit card companies have been scrutinizing every charge on your account in recent years, searching for purchases that thieves may have made. Turns out, though, that some of the companies have been suspicious of your own spending, too.

In recent months, American Express has gone far beyond simply checking your credit score and making sure you pay on time. The company has been looking at home prices in your area, the type of mortgage lender you're using and whether small-business card customers work in an industry under siege. It has also been looking at how you spend your money, searching for patterns or similarities to other customers who have trouble paying their bills.

In some instances, if it didn't like what it was seeing, the company has cut customer credit lines. It laid out this logic in letters that infuriated many of the cardholders who received them. "Other customers who have used their card at establishments where you recently shopped," one of those letters said, "have a poor repayment history with American Express."

It sure sounded as if American Express had developed a blacklist of merchants patronized by troubled cardholders. But late this week, American Express told me that wasn't the case. The company said it had also decided to stop using what it has called "spending patterns" as a criteria in its credit line reductions. ...

<http://www.nytimes.com/2009/01/31/your-money/credit-and-debit-cards/31money.html>

✶ Statute of Frauds [sic] (Re: Leichter, [RISKS-25.52](#))

*Martyn Thomas <drmartynthomas@googlemail.com>
Sat, 24 Jan 2009 13:46:04 +0000*

"The common law has traditionally accepted oral contracts - special cases, going back the the oddly-named Statute of Frauds, ..."

What an excellent idea! Where is it? What does it look like?

There has been a long-running debate on what should occupy the vacant fourth plinth in London's Trafalgar Square.

[Woops! Your immoderate moderator's spelling checker had no trouble with that one, cast in concrete or frozen in stone. PGN]

✶ Re: Yet Another Reason Not to use Windows for Medical Devices

*Bernard Peek <bap@shrdlu.com>
Fri, 23 Jan 2009 13:28:58 +0000*

(Epstein, [RISKS-25.52](#))

It seems that a reality check is required here. In simple terms we have to realise that there is no perfect solution to the problem of installing software patches, there are only choices between different risks.

If we choose to install every patch immediately it is released we face the risk that a patch may conflict with existing software or hardware and bring systems to a halt.

If we choose to delay installation, even by a day, we risk attacks from people who have reverse-engineered malware from the patches.

Given that there is no win/win solution it appears to me that we either have to accept that our systems will occasionally fail or decide that using MS Windows for critical systems is tantamount to professional negligence.

Bernard Peek, London, UK. DBA, Manager, Trainer & Author

[This is an old issue for RISKS readers. However, it continues to be a serious issue. PGN]

Re: Tony Hoare: "Null References" (Baker, [RISKS-25.52](#))

*Michael Albaugh <m.e.albaugh@gmail.com>
Thu, 22 Jan 2009 13:43:51 -0800*

... or Gresham's law?

While it is a widely held belief, it is not a fact that C is "unable" to police array bounds. I cannot speak for Fortran or C++, but the C89 standard, at least, sufficiently circumscribes the definitions of pointers and the operations that may be reliably performed on them to `_allow_` bounds-checking. A decent optimizing compiler could even "hoist" much of the checking out of loops etc.

The issue is that much (most) software "written in C" is in fact "written in a language corresponding to the mental model formed by firing random snippets from Byte through the compiler one happened to have handy". A big part of that mental model is "A pointer is nothing more than a machine address, which is nothing more than an index into an undifferentiated sea of octets". Wrong in so many ways!

There have been a few attempts at promoting C compilers that correctly compile correct programs, and diagnose issues with incorrect ones. These have been doomed by the overwhelming mass of incorrect programs.

When the (time effective) solution to the problem of error messages is to buy instead a compiler which does not emit them, the situation snowballs.

"We have met the enemy, and he is us" (Walt Kelly)

> To a first approximation, the lack of array bounds checking created the
> virus/worm industry, and we are still paying handsomely for this.

Actually, I disagree. A lack of clear separation of code and data, and a cavalier attitude toward "least privilege" has more to do with this, IMHO.

✉ Re: Tony Hoare: "Null References" (Baker, [RISKS-25.52](#))

*"Kirakowski, Jurek" <jzk@ucc.ie>
Fri, 23 Jan 2009 10:20:53 -0000*

> "I haven't yet heard an apology from Fortran/C/C++/etc. creators over
their inability to police array bounds."

I suppose it would be going a bit too far to request a similar apology from writers of macro assemblers and autocoders? I'm presuming Henry has his tongue as firmly in his cheek as I do. The real risk has been that the art of computer programming is badly taught, and that the cherished ideal for many programmers is to not have to write a line of code ever again after some point in their lives.

There IS a market for idiot-proof programming environments. But there is also a market for precision tools like C.

✉ Re: Tony Hoare: "Null References" (Baker, [RISKS-25.52](#))

*Ray Blaak <rblaa@telus.net>
Sun, 25 Jan 2009 13:14:43 -0800*

I don't think Tony Hoare should be apologizing for inventing null pointers. For any language with reference semantics, trying to program without being able to express a "reference to nothing" would be quite difficult.

I am sure Tony Hoare could do it, but most programmers are not comfortable with the more formal languages that this would require. They think better in terms of simple assignments to state, pointer references, etc.

For array bounds checking on the other hand, there is no excuse.

Henry Baker <hbaker1@pipeline.com> writes:

> Madoff was a rank amateur by comparison. Computer "scientists" have been
> producing insecure code like this since before NASDAQ was started.

Well, at least with the compsci folks, they were unintentional early mistakes, compounded by generations of programmers enthusiastically repeating them. You use C yourself? Then you are just as culpable.

Madoff on the other hand, was intentionally stealing from people for years.

Re: Tony Hoare: "Null References" (Baker, [RISKS-25.52](#))

<Martin.Torzewski@blueyonder.co.uk>
Mon, 26 Jan 2009 12:38:53 -0000 (GMT)

Fortran (at least until 77) WAS amenable to the hardware policed, and hardware speed, storage area bound checking implemented by e.g. ICL's VME architecture. (As were, to my knowledge, all extant languages of the time.) Less efficient bound checking was also implementable in software.

C was not, and had to have that mandatory checking suppressed (by allocating a vast uniform area of store for the entire "C supporting" environment) in order to run.

It's possible (and if so, unfortunate) that subsequent Fortrans have jettisoned their sound industrial-strength approach to storage management, reducing their engineering quality to that of C.

Re: Tony Hoare: "Null References" (Baker, [RISKS-25.52](#))

"Richard O'Keefe" <ok@cs.otago.ac.nz>
Fri, 30 Jan 2009 19:12:17 +1300

Fortran's creators, at least, have nothing to apologise for: Fortran DOES allow array bounds to be checked and the Burroughs Fortran compiler DID check them. IBM's xlf compiler has a -C (-qcheck) option which makes the compiler check bounds. Sun's f95 compiler also has a -C option doing the same thing. Both GNU Fortran compilers (g77 and gfortran) have a -fbounds-check option.

I agree that the compiler writers who do not make this the default have much to answer for, but the Fortran standardisers are under no obligation to apologise for a non-existent inability.

It's interesting that Dijkstra waxed enthusiastic about Hoare's records, uses null extensively. If Dijkstra didn't see a problem, I don't think Hoare need blame himself overmuch.

<http://www.cs.utexas.edu/users/EWD/transcriptions/EWD01xx/EWD132.html>

Indeed, he may be claiming too much credit/blame for the idea. PL/I (designed in 1964) had null pointers (and null offsets). I don't know when it got them. Lisp had NIL well before that, so null pointers were an obvious invention. AED-0 started in 1961, and 'Its compact syntax was the first language to directly support "n-component elements" of Plex programming (now called "pointers", "records", and "fields".' Douglas Ross's classic "The AED-1 Free Storage Package" (CACM, Aug 1967) starts 'The use of multiword "n-component elements" for the representation and manipulation of complex problem models in programming systems was first proposed by the author in 1960'. I can't tell from that paper whether AED

had null data pointers, but the paper certainly uses null function pointers, represented as 0. The earlier paper he mentioned was "A generalized technique for symbol manipulation and numerical calculation", CACM March 1961, which is the earliest reference I know to general linked webs of records. The idea was so new at the time that holding a machine address in a register was called "reversed use of index registers"! (For which 0 would have been possible.)

Perhaps some Risks reader knows something about the history of AED and whether AED typed pointers allowed null references or not.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 54

Wednesday 4 February 2009

Contents

- [Automated BART trains crash during manual operation of one of them](#)
[Rob McCool](#)
 - [Earthquake Alert System Failed To Work Properly](#)
[Max Power](#)
 - ['Foul play' suspected in Tucson Super Bowl porn feed](#)
[Brian J. Pedersen via Monty Solomon](#)
 - [Perils of html e-mail](#)
[Charles Wood](#)
 - [Votes lost in Finnish e-voting](#)
[Antti Vaha-Sipila](#)
 - [Fannie Mae Logic Bomb](#)
[Jim Schindler](#)
 - ["This site may harm your computer" on every search result](#)
[Maxim Weinstein via Monty Solomon](#)
 - [Google Account Takeover, Mark Ghosh](#)
[jidanni](#)
 - [Local Police Want Right to Jam Wireless Signals](#)
[Spencer S. Hsu via Monty Solomon](#)
 - [911 service not prepared for new generation of pranksters](#)
[David Chartier via Monty Solomon](#)
 - [Re: Digital road sign in Austin, TX was altered ...](#)
[Mark Feit](#)
 - [Re: MP3 player contained US military secrets](#)
[Geoff Kuening](#)
 - [Re: American Express Kept a *Very* Watchful Eye on Charges](#)
[David Alexander](#)
 - [Re: Statue of Frauds](#)
[Mark Jackson](#)
 - [Re: Tony Hoare: "Null References"](#)
[Dimitri Maziuk](#)
[Tony Finch](#)
[Jay Carlson](#)
 - [Info on RISKS \(\[comp.risks\]\(#\)\)](#)
-

✂ Automated BART trains crash during manual operation of one of them

Rob McCool <robm@robm.com>

Wed, 4 Feb 2009 08:53:19 -0800 (PST)

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/02/04/BAUI15N63L.DTL&type=newsbayarea>

Two BART subway trains crashed yesterday on a Y junction in Oakland. The automation in the BART system made this crash a surprise for some, and the newspaper article specifically says that one of the trains was under manual operation at the time of the collision. Many will likely conclude that the cause of the crash was operator error, which is certainly a possibility.

But a common risk of automated systems is the problem of what happens when they fail, and infrequently used manual protocols must come into effect. Complacency is always a risk with automation. It will be interesting if the details of this crash are found and are released.

✂ Earthquake Alert System Failed To Work Properly

Max Power <dist23@juno.com>

Sun, 1 Feb 2009 17:13:53 -0800

[See note at end on request from Max for help requested on a paper on Hyperinflation impact on electronic commerce. PGN]

The risk is that older computer and networking systems can be overloaded when not updated regularly. Yes, there are risks in upgrading too -- so the success or failure here is in the backup systems.

Max Power, CEO

Power Broadcasting

<http://HireMe.geek.nz>

Wellington / Adelaide / Vancouver / Seattle

When an earthquake larger than magnitude 3.0 strikes the Northwest, an automated system is supposed to page University of Washington seismologists and notify emergency managers.

But that's not what happened with Friday morning's magnitude 4.5 jolt. The **Seattle Times** reported that because computers were apparently overloaded with data from an expanded network of seismic instruments, the scientists were awakened instead by predawn calls from journalists. "The system has worked flawlessly for 10 years," said Steve Malone, emeritus professor and former director of the Pacific Northwest Seismic Network. "This time, nothing went off."

The quake didn't cause any damage, though it woke people across the region and the shaking was felt from the Olympic Peninsula to Seattle. The glitch in the UW's routine also had no serious fallout, thanks to functioning

systems in other states.

An automatic warning from the U.S. Geological Survey in California arrived at Washington's Emergency Management Division headquarters within seconds of the 5:25 a.m. quake. Notification from Alaska's Tsunami Warning Center followed minutes later.

"That's the value of redundancy," said EMD spokesman Mark Clemens.

It took Malone and other UW scientists about 15 minutes to check seismic data and compute the earthquake's size and epicenter -- about 14 miles northwest of Seattle near Kingston, Kitsap County.

<http://www.kirotv.com/news/18612303/detail.html>

==> ALSO: Research assistance needed on
Hyperinflation impact on electronic commerce

I would like to do a fully detailed research paper [on Hyperinflation vs Electronic Commerce] that can be distributed on the web via my website - so if you have any practical suggestions on how to expand this paper do so.

THERE IS NO WIKIPEDIA PAGE ON THIS TOPIC, as there is little if any official research.

Hopefully, I will be able in future to submit the core conclusions to RISKS -- to the amusement or horror of this strategically important part of the IT SECTOR.

[DRAFT deleted by PGN]

'Foul play' suspected in Tucson Super Bowl porn feed

Monty Solomon <monty@roscom.com>

Mon, 2 Feb 2009 20:27:14 -0500

Brian J. Pedersen, *Arizona Daily Star*, 2 Feb 2009

The pornographic content that interrupted thousands of local Comcast subscribers' Super Bowl broadcast was the result of an "isolated malicious act," a company spokeswoman said Monday.

But company officials have yet to determine how that act was committed, spokeswoman Kelle Maslyn said, though any sort of equipment malfunction has been ruled out.

"We did an extensive preliminary check on our technical systems, and everything appeared to be working properly when the incident occurred," Maslyn said.

Meanwhile, the U.S. Attorney's office in Phoenix said it is looking into the interruption, which lasted about 30 seconds, and featured full male nudity.

"We take this matter seriously," spokesman Wyn Hornbuckle said. "We're working with appropriate agencies to review the incident."

One of those agencies, the Federal Communications Commission, was not aware of any formal complaints made regarding the porn clip, FCC media relations director David Fiske said Monday afternoon.

It is still unclear how many viewers saw the clip, from a porn movie being shown on Shorteez, an adult cable channel offered by Comcast on a pay-per-view basis.

Only Comcast subscribers who received a standard definition signal could see the clip, while those who watched the game on high-definition televisions were not affected, Maslyn said.

Comcast is Southern Arizona's second-largest cable subscriber, with more than 80,000 customers in unincorporated Pima County, Marana and Oro Valley. ...

<http://www.azstarnet.com/sn/hourlyupdate/278448.php>

✶ Perils of html e-mail

*Charles Wood <j.charles.wood@gmail.com>
Sun, 1 Feb 2009 12:41:44 +0900*

We just cut and paste from the e-mail to the program we use for printing the edible images, we are usually in such a hurry that we really don't have time to check. and if we do the customers yell at us for bothering them.

Result

<http://cdnll-7.liveleak.com/s/14/media14/2009/Jan/31/LiveLeak-dot-com-e9f763bb9c03-cake.jpg?h=fc165d4705b83d83ab53fb1bfbd44c49&e=1234064051&rs=150>

or

*<http://tinyurl.com/as7ree>

ASCII art anyone?

✶ Votes lost in Finnish e-voting (Antti Vaha-Sipila)

*"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 2 Feb 2009 15:50:01 PST*

Kirjoittaja: Antti Vaha-Sipila, Lokakuu 28, 2008 - 19:12.
Electronic Frontier Finland ry

<http://www.effi.org/blog/2008-10-28-finnish-evoting-votes-lost.html>

[29th Oct 2008 Updated the e-voting interface link to point to the English version]

[29th Oct 2008 Edited to add a report of touchscreen issues]

A fully electronic voting system was piloted in the Finnish municipal elections on the 26th of October, 2008.

Electronic Frontier Finland (EFFI) had criticised the pilot program for years, recently releasing a report on its deficiencies
<<http://www.effi.org/blog/2008-09-01-evoting-report-in-english.html>>.

Today, the Ministry of Justice revealed
<<http://www.om.fi/Etusivu/Ajankohtaista/Uutiset/1224166604122>> that due to a usability issue, voting was prematurely aborted for 232 voters. The pilot system was in use in three municipalities; this amounts to about 2 per cent of the electoral roll. Seats in the municipal assemblies are often determined by margins of only a couple of votes.

It seems that the system required the voter to insert a smart card to identify the voter, type in their selected candidate number, then press "ok", check the candidate details on the screen, and then press "ok" again. Some voters did not press "ok" for the second time, but instead removed their smart card from the voting terminal prematurely, causing their ballots not to be cast.

This usability issue was exacerbated by Ministry of Justice instructions, which specifically said
<http://www.vaalit.fi/sahkoinenaanestaminen/aanestyksen_kulku.html> that in order to cancel the voting process, the user should click on "cancel" and after that, remove the smart card. Thus, some voters did not realise that their vote had not been registered.

[Added 29th Oct:] There has now been at least one report
<<http://www.hs.fi/keskustelu/Brax%3A+Vaalitulosta+ei+voi+perua+hukka%E4%E4nien+takia/thread.jspa?threadID=148607&tstart=0&sourceStart=40&start=60>>
of touchscreen issues. A voter had repeatedly tried to click on "ok", but either due to system lag or touchscreen sensitivity problems, it took "minutes" to get the button press registered. If hit by this type of problem, the voters may well have thought that the ballot casting process had completed.

EFFI argues that the election should be re-run in the affected municipalities, and has issued a press release
<<http://www.effi.org/julkaisut/tiedotteet/lehdistotiedote-2008-10-28.html>>
(in Finnish) arguing for the legal basis of a re-election. According to Finnish election law, this would require a decision from the Administrative Court.

A Flash demo of the e-voting user interface is available
<<http://www.vaalit.fi/sahkoinenaanestaminen/en/esitys/index.html>> on the Ministry of Justice elections portal.

Fannie Mae Logic Bomb

Jim Schindler <jimschin@gmail.com>

Sat, 31 Jan 2009 23:13:36 -0800

(Just imagine the 'excitement'!)

Fannie Mae Logic Bomb Would Have Caused Weeklong Shutdown

Kevin Poulsen <kevin_poulsen@wired.com>

29 Jan 2009

<http://blog.wired.com/27bstroke6/2009/01/fannie.html>

<http://blog.wired.com/27bstroke6/threats/index.html>

A logic bomb allegedly planted by a former engineer at mortgage finance company Fannie Mae last fall would have decimated all 4,000 servers at the company, causing millions of dollars in damage and shutting down Fannie Mae for a least a week, prosecutors say.

Unix engineer Rajendrasinh Babubha Makwana, 35, was

indicted<http://blog.wired.com/27bstroke6/files/fannie_indictment.pdf>

Tuesday in federal court in Maryland on a single count of computer sabotage for allegedly writing and planting the malicious code on Oct. 24, the day he was fired from his job. The malware had been set to detonate at 9:00 a.m. on Jan. 31, but was instead discovered by another engineer five days after it was planted, according to court records.

Makwana, an Indian national, was a consultant who worked full time on-site at Fannie Mae's massive data center in Urbana, Maryland, for three years.

On the afternoon of Oct. 24, he was told he was being fired because of a scripting error he'd made earlier in the month, but he was allowed to work through the end of the day, according to an FBI affidavit<http://blog.wired.com/27bstroke6/files/fannie_complaint.pdf>(.pdf) in the case. "Despite Makwana's termination, Makwana's computer access was not immediately terminated," wrote FBI agent Jessica Nye.

Five days later, another Unix engineer at the data center discovered the malicious code hidden inside a legitimate script that ran automatically every morning at 9:00 a.m. Had it not been found, the FBI says the code would have executed a series of other scripts designed to block the company's monitoring system, disable access to the server on which it was running, then systematically wipe out all 4,000 Fannie Mae servers, overwriting all their data with zeroes.

"This would also destroy the backup software of the servers making the restoration of data more difficult because new operating systems would have to be installed on all servers before any restoration could begin," wrote Nye.

As a final measure, the logic bomb would have powered off the servers.

The trigger code was hidden at the end of the legitimate program, separated by a page of blank lines. Logs showed that Makwana had logged onto the server on which the logic bomb was created in his final hours on the job.

Makwana is free on a \$100,000 signature bond. His lawyer didn't immediately return a phone call Thursday.

(Updated January 30, 2009 | 3:00:00 PM to correct Makwana's employment information)

"This site may harm your computer" on every search result

Monty Solomon <monty@roscom.com>

Sat, 31 Jan 2009 19:42:13 -0500

If you did a Google search between 6:30 a.m. PST and 7:25 a.m. PST this morning, you likely saw that the message "This site may harm your computer" accompanied each and every search result. This was clearly an error, and we are very sorry for the inconvenience caused to our users.

What happened? Very simply, human error. Google flags search results with the message "This site may harm your computer" if the site is known to install malicious software in the background or otherwise surreptitiously. We do this to protect our users against visiting sites that could harm their computers. ...

<http://googleblog.blogspot.com/2009/01/this-site-may-harm-your-computer-on.html>

Google glitch causes confusion

Maxim Weinstein, 31 Jan 2009

This morning, an apparent glitch at Google caused nearly every [update 11:44 am] search listing to carry the "Warning! This site may harm your computer" message. Users who attempted to click through the results saw the "interstitial" warning page that mentions the possibility of badware and refers people to StopBadware.org for more information. This led to a denial of service of our website, as millions of Google users attempted to visit our site for more information. We are working now to bring the site back up. We are also awaiting word from Google about what happened to cause the false warnings. ...

<http://blog.stopbadware.org/2009/01/31/google-glitch-causes-confusion>

Google Account Takeover, Mark Ghosh

<jidanni@jidanni.org>

Mon, 02 Feb 2009 06:50:44 +0800

What if you woke up tomorrow and your Gmail, Orkut, Docs, Reader, Google Checkout account was gone?

<http://ma.tt/2009/01/google-account-takeover/>

[Check out this one. Mark Ghosh, Et Tu Google? Then Fail, Net Safety.

Mark is the "owner" of the Orkut community.

Apologies to those of you who complain when I occasionally run items that are URLs only. In this one, Mark speaks for himself. PGN]

Local Police Want Right to Jam Wireless Signals

Monty Solomon <monty@roscom.com>

Sun, 1 Feb 2009 14:14:37 -0500

Spencer S. Hsu, *The Washington Post* 1 Feb 2009

As President Obama's motorcade rolled down Pennsylvania Avenue on Inauguration Day, federal authorities deployed a closely held law enforcement tool: equipment that can jam cellphones and other wireless devices to foil remote-controlled bombs, sources said.

It is an increasingly common technology, with federal agencies expanding its use as state and local agencies are pushing for permission to do the same. Police and others say it could stop terrorists from coordinating during an attack, prevent suspects from erasing evidence on wireless devices, simplify arrests and keep inmates from using contraband phones.

But jamming remains strictly illegal for state and local agencies. Federal officials barely acknowledge that they use it inside the United States, and the few federal agencies that can jam signals usually must seek a legal waiver first.

The quest to expand the technology has invigorated a debate about how widely jamming should be allowed and whether its value as a common crime-fighting strategy outweighs its downsides, including restricting the constant access to the airwaves that Americans have come to expect. ...

<http://www.washingtonpost.com/wp-dyn/content/article/2009/01/31/AR2009013101548.html>

911 service not prepared for new generation of pranksters

Monty Solomon <monty@roscom.com>

Wed, 4 Feb 2009 00:36:38 -0500

(David Chartier)

Prank callers are using VoIP and caller ID spoofing services to pull expensive wool over the eyes of 911 call centers. Solutions are available to bring these centers into the 21st century, but even the cheapest ones are priced outside the realm of the aging service.

David Chartier, arstechnica, 2 Feb 2009

The Internet and the hooligans who exploit it have evolved over the past few years, but sadly, America's 911 service hasn't kept up. Pranksters are wreaking havoc on the service and on call center budgets by placing fake calls through a flaw in the way the aging emergency phone system handles VoIP networks.

After paying a small fee to one of the readily available caller ID spoofing services available on the Web, a prank caller with a grudge or a serious psychological problem can call 911 and tell the operator just about any story he or she wants. Since the 911 system wasn't built with VoIP in mind, these calls appear to originate from anywhere, and said hooligans take full advantage of the opportunity. The practice has been dubbed "swatting," typically because the spoofed emergency stories that these troubled individuals make up are horrible enough to send police and even SWAT teams to unsuspecting victims on the other side of town or the continent.

The AP reports one recent incident that occurred in 2007, when 18-year-old Randal Ellis in Mukilteo, WA falsified his location and called a 911 support center in Orange County, CA. For 27 minutes, Ellis spun a story about drugs and murder that sent the Orange County Sherriff's department SWAT team to the house of Doug and Stacey Bates. Ellis told the operator that he was high and had just shot his sister, and after police stormed the house, Doug and Stacey were handcuffed.

This was just one of the 185 calls Ellis made to 911 call centers around the US, according to Yahoo Tech, and the Bates family was picked at random. After being caught, the teen pleaded to five felony counts that include computer access and fraud, as well as false imprisonment by violence, and was sentenced to serve three years in prison. Another major case involved eight people who arranged over 300 swatting calls, while another in 2006 involved a teen in Dallas, TX who made up a story about killing family members and threatening hostages with an AK-47. ...

<http://arstechnica.com/telecom/news/2009/02/911-service-not-prepared-for-new-generation-of-pranksters.ars>

Re: Digital road sign in Austin, TX was altered ...

*Mark Feit <mfeit@notonthe.net>
Sun, 1 Feb 2009 06:16:06 -0500*

In [RISKS-25.53](#), David Hollman <dah8@cornell.edu> writes:

- > [Signs] manufactured by IMAGO's ADDCO division can be easily
- > altered because their instrument panels are frequently left
- > unlocked and their default passwords are not changed.

Even more worthy of mention here is the fact that ADDCO's signs allow themselves to be reset to their from-the-factory state, complete with

default password, using what is now a well-known password:

<http://www.i-hacked.com/content/view/274/1>

| **** HACKER TIPS****

| Should it will ask you for a password.

| Try "DOTS", the default | password.

|

| In all likelihood, the crew will not have changed it. However if they

| did, never fear. Hold "Control" and "Shift" and while holding, enter

| "DIPY". This will reset the sign and reset the password to "DOTS" in the

| process. You're in!

Re: MP3 player contained US military secrets

Geoff Kuenning <geoff@cs.hmc.edu>

Sat, 31 Jan 2009 22:54:41 -0800

> 60 US military files labeled top secret popped up on his screen. ...

> Kerri Ritchie: The files contained the social security numbers, home

> addresses, even mobile phone numbers of American soldiers based in

> Afghanistan and Iraq.

Although I'm disturbed by the several levels of carelessness needed to allow this to happen, I think I'm even more disturbed by the idea that the names and personal information of soldiers is "top secret".

Confidential, definitely. Maybe even "secret", since some of those people are high-ranking officers and I can imagine movie-plot scenarios involving their home addresses. But "top secret" on the level of attack plans and nuclear technology? I think not.

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

Re: American Express Kept a *Very* Watchful Eye on Charges

David Alexander <dave_ale@online.rednet.co.uk>

Sun, 01 Feb 2009 08:57:30 +0000

Ron Lieber's submission about surveillance of account activity reminded me of an incident some years ago when I applied for a mortgage through my bank.

I completed the forms with the help of my Bank Manager for a mortgage through their partner (UK) Building Society. The application charges would be debited from my bank account. Two days later I received a call from the Fraud detection department of the bank - Did I owe "XYZ loans" (name obscured to protect those involved) £900, which they were trying to take by direct debit ?

"No" said I.

"That will be fraud then, we'll stop the payment, cancel the card and send you a new one" they replied.

'Thank you my bank's fraud team, job well done' I thought.

The very next morning I received a letter from the Building Society in question with all the relevant mortgage paperwork. One of those papers informed me that the mortgage application fee of £900 was being requested from my bank. Yes, that's right, the mortgage fee request from the Building Society to the Bank had been detected by the bank as fraudulent and denied.

Adrenaline kicks in, as it tends to do at moment like that, 'Gosh' (or words to that effect) I thought, 'there goes my mortgage'. Fortunately logic kicked in about 2 minutes later, together with my knowledge of Behavioral Analysis and the Merchant Account payment systems for credit/debit cards (my wife runs an e-commerce business and I set one up for her, together with the encrypted links to the Payment Service Providers).

I could see what must have happened, the Building Society was using a Merchant Account name for the debit card transaction that bore no resemblance to their actual name. The fraud system had no knowledge of it and wondered why I was getting a request from a loan company when I had a five figure positive balance in my account. What got me is that it's a major Bank and Building Society. I couldn't have been the first to be processed through a new system could I ? One where the new Merchant Account details had not been entered into the Fraud System as a 'trusted' account ? Did they set up a different one for each kind of mortgage to make the accounting simpler ?

By good fortune I know the CTO of the Bank in question and rang him up. I explained what had happened and my theory. He rang back later, I was right on the money - or not in this case. It was exactly as I had supposed. I was one of more than 240 people to whom this had happened in the last 48 hours, but no-one in the Bank had realised the reason why.

The good thing was that, for identifying their problem, the Bank waived my application fee and the mortgage was approved.

The risks - that not everyone knows the CTO of their bank personally, that mortgages get declined and there is an adverse impact on one's credit rating, that you don't get that dream house...you get the idea.

David Alexander, Towcester, Northamptonshire, England
Founder member, European Top Methanol Racers Association www.etmra.com

Re: Statue of Frauds (Thomas, [RISKS-25.53](#))

Mark Jackson <mjackson@alumni.caltech.edu>

Tue, 03 Feb 2009 16:47:34 -0500

Martyn Thomas wrote:

- > "The common law has traditionally accepted oral contracts - special cases,
- > going back the the oddly-named Statue of Frauds, ..."
- >
- > What an excellent idea! Where is it? What does it look like?

In Paris - across from the Musée de la Contrefaçon, of course:

http://www.placesinfrance.com/counterfeit_museum_paris.html

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

Re: Tony Hoare: "Null References" (Blaak, [RISKS-25.53](#))

Dimitri Maziuk <dmaziuk@bmr.b.wisc.edu>

Sat, 31 Jan 2009 19:35:38 -0600

- > For any language with reference semantics, trying to program without being
- > able to express a "reference to nothing" would be quite difficult.

I expect about as difficult as dealing with integers without int NaN.

Let's see -- just off the top of my head. If a function returning a pointer had no way to return an unambiguous error value, we'd have to have a global errno that nobody bothers checking and (except when it's or) application-specific error semantics. Some functions would return a reference to a zero value, others would return reference to zero to indicate success. Some would return 0xdeadbeef, others: negative one, or 9999.999. Hopefully it is all correctly documented and everybody gets the memo when things change in the next release.

Then we'll try to work around that mess by returning the actual value as a var parameter and using return value as an error code. In which case everyone will start ignoring the return value, just as they were ignoring the errno before.

There'd also be a bit of a problem fetching values from sources that understand nulls: we'd have to define a second function in our API and then everyone will forget to call wasNull() after each and every get().

In other words, it'd be situation normal.

[Presumed reference to SNAFU. PGN]

Re: Tony Hoare: "Null References" (Blaak, [RISKS-25.53](#))

Tony Finch <dot@dotat.at>

Sun, 1 Feb 2009 23:17:13 +0000

Perhaps Prof. Hoare is apologising because he knew a better way but took the short cut instead. The better way is to make nullability distinct from referencing, as in ML's option type or Haskell's Maybe type. A halfway house is to distinguish nullable and non-nullable references, which is getting closer to mainstream via things like Java @NonNull type annotations.

f.anthony.n.finch <dot@dotat.at> <http://dotat.at/>

✂ Tony Hoare: "Null References: The Billion Dollar Mistake"

Jay Carlson <nop@nop.com>

Tue, 3 Feb 2009 01:23:31 -0500

IMO the real blindspot is in how we think of aggregate textual types. Clearly, it is a type error, detected at compile-time to add an integer to a Date and expect an integer. My compiler hates me when I say things like what. But it is perfectly happy to take a string representing a Date and then concatenate a string representing hours past that date. And in fact, it's pretty happy for me to just glue some random HTML sludge string onto a nice valid Date.

Spackman pointed out that flat text is just **never** what we want. But as long as (char *) is the (void *) of throwing random crap together without reference to eventual contract I see no motivation not to view the world as a vast ocean of Unicode codepoints and then go sailing those Seven Seas.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 55

Tuesday 10 February 2009

Contents

- [RFID Passports cloned wholesale](#)
[Dan Goodin](#)
 - [Windshields and Windows combine to provide malware vector](#)
[Mark Brader](#)
 - [FAA Notifies Employees of Personal Identity Breach](#)
[Danny Burstein](#)
 - [390,000 to access child database](#)
[Amos Shapir](#)
 - [Confidential LAPD misconduct files mistakenly posted on Internet](#)
[Danny Burstein](#)
 - [Risks of computer-gibberish names on forms](#)
[Joseph A. Dellinger](#)
 - [Mathematics and screening](#)
[Jerry Leichter](#)
 - [The privacy vs. health tradeoff](#)
[Jeremy Epstein](#)
 - [Variant of Mac Trojan Horse iServices Found in Pirated Adobe C54](#)
[Monty Solomon](#)
 - [Re: Fannie Mae logic bomb](#)
[Wendell Cochran](#)
 - [Re: Tony Hoare: "Null References"](#)
[Rob Diamond](#)
[Robert P Schaefer](#)
 - [Re: Flat text is *never* what we want](#)
[Tony Finch](#)
 - [No wikipedia page](#)
[Olivier MJ Crepin-Leblond](#)
 - [What if you can't pull the plug?](#)
[Rex Sanders](#)
 - [Security Psychology](#)
[Gadi Evron](#)
 - [Call for contributions: New Security Paradigms Workshop: NSPW](#)
[Konstantin /Kosta/ Beznosov](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ RFID Passports cloned wholesale (Dan Goodin)

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

Fri, 6 Feb 2009 12:52:59 PST

Using inexpensive off-the-shelf components (a Motorola RFID reader and antenna, and a PC) bought mostly on eBay and a self-developed Windows app, Chris Paget ("an information security expert") built a mobile platform in his spare time that can clone large numbers of the unique RFID tag electronic identifiers used in U.S. passport cards and next generation drivers licenses. While driving around San Francisco for 20 minutes, he was able to harvest two passport tags without knowledge of their owners from up to 30 feet away. Demo and software at Shmoocon. (Paget says with some modifications, the range could be extended to more than a mile.) [Source: Dan Goodin, *The Register,* 4 Feb 2009; PGN-ed, noted by Ashish Gehani]

<http://www.securityfocus.com/news/11544>

[URL fixed in archive. PGN]

See [RISKS-25.08](#) and [25.42](#) for other recent items on RFID cloning.

✂ Windshields and Windows combine to provide malware vector

Mark Brader

Mon, 9 Feb 2009 02:42:50 -0500 (EST)

Fake parking tickets were placed on car windshields in several parking lots in Grand Forks, North Dakota. They showed a URL to check for further information, but the site required a download... and you can guess the rest.

<http://isc.sans.org/diary.html?storyid=5797>

<http://www.grandforksherald.com/articles/index.cfm?id=105232§ion=news>

Mark Brader, Toronto, msb@vex.net

[I swiped the subject line pun from someone on the Internet.]

✂ FAA Notifies Employees of Personal Identity Breach

danny burstein <dannyb@panix.com>

Tue, 10 Feb 2009 03:26:06 -0500 (EST)

(from the FAA [Federal Aviation Administration] website)

Washington - The FAA today notified employees that an agency computer was illegally accessed and employee personal identity information was stolen electronically. All affected employees will receive individual letters to notify them about the breach. ... Two of the 48 files on the breached computer server contained personal information about more than 45,000 FAA

employees and retirees who were on the FAA's rolls as of the first week of February 2006.

The server that was accessed was not connected to the operation of the air traffic control system or any other FAA operational system, and the FAA has no indication those systems have been compromised in any way.

http://www.faa.gov/news/press_releases/news_story.cfm?newsId=10394

[Also noted by Dres Zellweger. PGN]

390,000 to access child database

Amos Shapir <amos083@hotmail.com>

Tue, 27 Jan 2009 17:40:05 +0200

"A child protection database containing the contact details for all under 18-year-olds in England will be accessible to 390,000 staff, say ministers."

Opponents had already described the proposed project as "another expensive data disaster waiting to happen".

Full story at:

http://news.bbc.co.uk/2/hi/uk_news/education/7850871.stm

<http://www.microsoft.com/windows/windowslive/events.aspx>

Confidential LAPD misconduct files mistakenly posted on Internet

danny burstein <dannyb@panix.com>

Sat, 7 Feb 2009 18:18:00 -0500 (EST)

per the *LA Times*:

"The Los Angeles Police Commission violated its own strict privacy policy -- and perhaps state law -- on Friday, releasing a confidential report on the Internet that contained the names of hundreds of officers accused of racial profiling and other misconduct. ... "The commission and department staff had reviewed a paper copy of the report that did not contain the confidential information and assumed the electronic version would be the same, Tefank said."

rest:

<http://www.latimes.com/news/local/la-me-lapd7-2009feb07,0,3336411.story>

- aside from the "oops" issue, the article also discusses the politics and other reasons why this info should, or shouldn't, be public in the first place.

✂ Risks of computer-gibberish names on forms

"Joseph A. Dellinger" <geojoe@freeusp.org>

Thu, 5 Feb 2009 01:39:16 -0600

My company provides me with a cell phone to use for business purposes. I only use it when traveling, so it sometimes goes 2 months at a time without being turned on. The bill arrives monthly and has various gibberish entries on it. For example, the entry "Mobile Messeng:31000#2109" has been there on my statement every month, starting with the very first bill, at a cost of \$10 per month. I assumed that was AT+T's charge for enabling international text messaging. I didn't pick and choose the features that came with the phone... I got what the company chose for me.

Comparing cell phone bills with a cubicle neighbor today it turned out that only SOME people have that on their bill. So I called AT+T to ask what that was. Turns out \$10 is the charge for the "service" of receiving a "trivia alert" spam text message once a month. The AT+T customer-service agent told me that of course since I am receiving this extremely valuable service, it could only be because I requested it.

When I turn on that phone at the start of a new trip I generally find I have half a dozen or so spam text messages to wade through. And, indeed, one of those was always a trivia question with an invitation to reply to find out the answer. As I worked through the spam erasing it, mildly annoyed at the hassle, I at least got to feel a slight twinge of smugness. Hah! Do you actually think I'm idiot enough to fall for wheezes such as a request to call a toll number in the Caribbean for an "important message"?

Hah indeed: the joke's on me. Merely by cloaking their theft in computerese gibberish they got right past my defenses. And by the simple expedient of inserting the fictitious charge by computer, "so it must be right", they got right through AT+T's. A quick check on the internet revealed hundreds of similar stories. I wonder how many people at my company are victimized and still don't know it. I'd guess at a minimum several thousands. I turned the case over to corporate security for further investigation.

✂ Mathematics and screening

Jerry Leichter <leichter@lrw.com>

Thu, 5 Feb 2009 16:36:45 -0500

Not a computer-related risk as such, but an area many participants here will find of interest:

<http://www.pnas.org/content/early/2009/02/02/0813202106>

The paper "Strong profiling is not mathematically optimal for discovering rare malfeasors" looks at the question of how to best screen a population for "terrorists". Suppose you have a profile of likely terrorists, but that profile is just probabilistic, subject to both false positives and false

negatives. Should you use the profile to select people to be screened? (Of course, there are all kinds of social and political questions here - this is just about the mathematical question.)

You'd think the answer is "yes", and in fact it is - but there's a subtle problem. "Strong screening" - the obvious approach, where you select someone for detailed screening with a probability at least as high as your a priori estimate that they are actually a threat - means that you spend many of your resources repeatedly screening the same innocent people. In fact, the end result is shown to be no better than a simple random screening process. (This is in a memory-less situation, where you don't change your estimate as a result of the screen - essentially what TSA does today.)

Interestingly, the optimal strategy in this situation can be calculated. It turns out that you want to choose people for detailed screening proportionally to the *square root* of your a priori estimate of how likely they are to be a threat.

This result was apparently derived earlier in a much different setting (having to do with Monte Carlo methods for protein folding) but, according to the current author, is not widely known. There are certainly other settings - various computer security mechanisms; possibly testing and bug finding strategies - where this would apply.

#The privacy vs. health tradeoff

*Jeremy Epstein <jeremy.j.epstein@gmail.com>
Thu, 5 Feb 2009 10:52:01 -0500*

Some grocery stores are using the data gathered from their "loyalty cards" [cards that tell the store who you are and what you buy] to notify customers who bought products that have been recalled due to the widening peanut contamination affair. At least one consumer group (Center for Science in the Public Interest) is urging stores to use their data this way.

<http://www.msnbc.msn.com/id/28802536/>

<http://cspinet.org/new/200902031.html>

<http://www.ocregister.com/articles/recalled-peanut-consumers-2289676-butter-loyalty>

(and many others)

How do customers feel about their purchasing information being used in this way? I suspect most people are positive about it - but I wonder whether it would be viewed quite so positively if the product in question were, say condoms. "Honey, I got a call from the grocery store that the condoms have been recalled - who are you using condoms with?"

I checked the privacy policy for one of the major grocery stores in my area (Giant Food - http://giantfood.com/savings/card/privacy_policy.htm), I think this usage would fall within their privacy policy, since it explicitly allows for sending direct mail and similar communications based on purchases. I suspect other privacy policies are similar. So it would seem

to be within their rights to contact customers about purchases they've made, whether peanut butter or condoms. But regardless of policy, how would customers feel about it?

Variant of Mac Trojan Horse iServices Found in Pirated Adobe CS4

Monty Solomon <monty@roscom.com>

Thu, 29 Jan 2009 01:37:04 -0500

INTEGO SECURITY ALERT - January 26, 2009

New Variant of Mac Trojan Horse iServices Found in Pirated Adobe Photoshop CS4

Exploit: OSX.Trojan.iServices.B Trojan Horse

Discovered: January 25, 2009

Risk: Serious

Description: Intego has discovered a new variant of the iServices Trojan horse that the company discovered on January 22, 2009. This new Trojan horse, OSX.Trojan.iServices.B, like the previous version, is found in pirated software distributed via BitTorrent trackers and other sites containing links to pirated software. OSX.Trojan.iServices.B Trojan horse is found bundled with copies of Adobe Photoshop CS4 for Mac. The actual Photoshop installer is clean, but the Trojan horse is found in a crack application that serializes the program. ...

<http://www.intego.com/news/ism0902.asp>

Re: Fannie Mae logic bomb

Wendell Cochran <atrypa@eskimo.com>

Thu, 5 Feb 2009 09:15:42 -0800

> On the afternoon of Oct. 24, he was told he was being fired because
> of a scripting error . . .

Fired -- for a scripting error?

The FBI's affidavit in support of the criminal complaint adds little:

'MAKWANA erroneously created a computer script that changed the settings on the Unix servers without the proper authority of his supervisor ...'

Where were controls?

Other holes in the story abound. Fallout from the logic bomb may have obscured Risks in management.

Re: Tony Hoare: "Null References"

Rob Diamond <robd at langdale dotty com dotty au>

Fri, 06 Feb 2009 19:03:33 +1100

"I haven't yet heard an apology from Fortran/C/C++/etc. creators over their inability to police array bounds"

I think, rather, that it is Mr Baker who owes Ken Thompson and Denis Ritchie (the inventors of the C language) an apology. Complaining about the lack of array bounds checking to the inventors of C is like complaining to Henry Ford about not fitting ABS brakes to the Model T.

Thompson and Ritchie developed C so that they could write the very early versions of the Unix system (circa 1970) in a language that was "higher-level" than assembler. In those days memory was at an absolute premium since it was very expensive. I Googled for some prices, and found that Bell Labs paid \$65,000 for the PDP-11 on which Unix was developed, while an extra 4k bytes of core memory cost \$4,000. Doesn't sound like a lot of money *now*, but when I graduated as an electrical engineer in 1972 my starting salary was a bit over Aus \$4,000 a year, so a year's salary for 4k bytes of memory seems expensive to me ! At that time array bounds checking would have been one of the last things on the C developers' minds - just getting an operating system going that was small enough to leave room for useful programs to run was an amazing achievement.

I do think that it's a pity that in the more than four decades since it's invention the C language standard hasn't been modified to mandate array bounds checking - after all what's a bit more software bloat on top of the gigantic software bloat we have now ? But NoBody *did* modify it, and now we are stuck with the consequences. If only we could track down that elusive Mr NoBody - he's got a lot to answer for !

Re: Tony Hoare: "Null References"

*"Schaefer, Robert P \{(US SSA)\}" <robert.p.schaefer@baesystems.com>
Thu, 5 Feb 2009 12:57:03 -0500*

The current set of replies to Tony Hoare: "Null References" remind me a little bit of Godel, a little bit of Flatland, and a little bit of Alice in Wonderland.

You can't prove that a system is both correct and complete without going outside that system. In this instance, you have data, and then you have meta-data, where meta-data is reasoning about data. Any time you use data as meta-data within a system you introduce the risk of confusion between the two realms, but how can you ever use meta-data if not as data in another context? Similarly how can you relate meta-data in one context to data in another without having a back-reference (more meta-data) from that data in one context to a reasoning about that data (meta-data) in another?

If you live in Godel's version of Flatland, as we appear to do, the correct and complete relationship between the data and meta-data contexts is

mathematically/logically/physically impossible. And yet we can and do imagine this to be mathematically/logically/physically possible, and when we fail in our attempt, apologize for not living up to impossible ideals. One may as well apologize for being human and be done with it.

"There's no use trying," she said; "one can't believe impossible things."
"I daresay you haven't had much practice," said the Queen. "When I was younger, I always did it for half an hour a day. Why, sometimes I've believed as many as six impossible things before breakfast." - Alice in Wonderland.

Re: flat text is **never what we want (Carlson, [RISKS-25.54](#))**

Tony Finch <dot@dotat.at>
Thu, 5 Feb 2009 14:43:44 +0000

Was: Tony Hoare: "Null References"

There are plenty of well-known consequences of the problem Jay identifies: SQL injection, cross-site scripting, etc. I don't know of many coherent practical solutions, so I'd be interested in any pointers from RISKS readers.

One of the best is Mike Samuel's proposal for secure string interpolation in Javascript, linked below. A more heavy-weight approach is to represent everything as a parse tree, so incoming data is necessarily checked for well-formedness as it is parsed, and outgoing data is correctly quoted by the pretty-printer.

<http://google-caja.googlecode.com/svn/changes/mikesamuel/string-interpolation-29-Jan-2008/trunk/src/js/com/google/caja/interp/index.html>

f.anthony.n.finch <dot@dotat.at> <http://dotat.at/>

No wikipedia page

"Olivier MJ Crepin-Leblond" <ocl@gih.com>
Thu, 5 Feb 2009 11:06:21 +0100

(was Re: Earthquake Alert System Failed To Work Properly, Power, [RISKS-25.54](#))

> THERE IS NO WIKIPEDIA PAGE ON THIS TOPIC, as there is little if any
> official research.

I am alarmed by such a statement. It reminds me of an increasing trend by today's researchers to say that "if you can't find it in Google, it doesn't exist".

Unless we make sure that this does not become the norm, complete sections of

knowledge are likely to "disappear" because they are published in formats which have not been ported online. Rather than expanding knowledge, we are currently risking shrinking it.

Olivier MJ Crépin-Leblond, PhD <http://www.gih.com/ocl.html>

✂ What if you can't pull the plug?

Rex Sanders <rsanders@usgs.gov>

Wed, 28 Jan 2009 11:25:02 -0800

Last night I literally awoke from a nightmare about my iPhone getting hacked, spewing spam and doing other nasty things. The nightmare was that I had no way to shut it off, and no way to disconnect it from the Internet.

I've stopped many misbehaving computing devices from causing more damage by "pushing the big red button" or "pulling the plug" (power or network cables). This was a simple, direct, easy-to-do-when-panicked scheme to stop further damage. Examples include printers spewing paper, runaway tape drives, and hacked servers. I've had to unplug power *and* remove batteries from laptops, PDAs, and smart phones.

Recently released devices like the Apple iPhone, MacBook Air, and MacBook Pro, have these features in common:

- Software-controlled power switches
- Long-life batteries that can't be removed
- Continuous wireless Internet access via WiFi or mobile phone networks

I'm not picking on Apple, their devices are just high profile examples of a growing trend.

These devices might have some magic combination of button pushes to turn the device off. I would not be able to recall these rarely used incantations during an emergency, and they might not work if the software is badly compromised or hung in tight loops.

I don't normally carry around Faraday cages to cut off wireless Internet access, which would solve only one class of problems.

I could smash them to smithereens, but that gets expensive.

I love the convenience, long battery life, and ubiquitous Internet access of these devices.

But we have a new risk from not having a positive, easy to find method of keeping these devices from doing more damage when all else fails.

✂ Security Psychology

Gadi Evron <ge@linuxbox.org>
Sat, 24 Jan 2009 22:57:17 -0600 (CST)

I just came across a post telling of the Security and Human Behavior workshop (or conference).

<http://www.crypto.com/blog/shb08/>

Other posts about it:

<http://www.lightbluetouchpaper.org/2008/06/30/security-psychology/>

http://www.schneier.com/blog/archives/2008/06/security_and_hu.html

As some of you may be aware, I've been researching this subject for about two years now, and I am very excited that a conference has now happened! It means I did not waste the last two years of my life after all! :)

This is very exciting, and I am very thankful to these guys for making it happen.

Here's a post I wrote about something similar, although syndicated from early on with an ancient post, in my exploration of the subject matter:

<http://gadievron.blogspot.com/2008/09/im-interested-but-in-you.html>

I hope that more researchers will start looking into this subject, which as of the last six months I've been calling Humexp.

I am currently engaged in research looking into the Estonian cyber war from a social psychology perspective, which turned out to be quite interesting. More on that when I can share, though.

✶ Call for contributions: New Security Paradigms Workshop (NSPW)

"Konstantin (Kosta) Beznosov" <beznosov@ece.ubc.ca>
Fri, 06 Feb 2009 18:18:37 -0800

2009 New Security Paradigms Workshop
The Queen's College, University of Oxford, UK
September 8-11, 2009

Read the full call at <http://www.nspw.org/current/cfp.shtml>
The submission deadline: April 17, 2009, 23:59 (UTC -12, or Y time).

The New Security Paradigms Workshop (NSPW) is seeking papers that address the current limitations of information security. Today's security risks are diverse and plentiful--botnets, database breaches, phishing attacks, distributed denial-of-service attacks--and yet present tools for combatting them are insufficient. To address these limitations, NSPW welcomes unconventional, promising approaches to important security problems and innovative critiques of current security practice.

We are particularly interested in perspectives from outside computer

security, both from other areas of computer science (such as operating systems, human-computer interaction, databases, programming languages, algorithms) and other sciences that study adversarial relationships such as biology and economics. We discourage papers that offer incremental improvements to security and mature work that is appropriate for standard information security venues.

To facilitate research interactions, NSPW features informal paper presentations, extended discussions in small and large groups, shared activities, and group meals, all in attractive surroundings. By encouraging researchers to think "outside the box" and giving them an opportunity to communicate with open-minded peers, NSPW seeks to foster paradigm shifts in the field of information security.

Kosta Beznosov, NSPW Publicity Chair, Assistant Professor,
Laboratory for Education and Research in Secure Systems Engineering
Electrical and Computer Engineering, University of British Columbia
<http://lersse.ece.ubc.ca> <http://www.ece.ubc.ca/~beznosov/>
4047-2332 Main Mall, Vancouver, BC, Canada V6T 1Z4 Phone: +1 604 822 9181



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 56

Thursday 19 February 2009

Contents

- [Train brake failure; broken valve](#)
[David Leshar](#)
- [Collision - UK and French Nuclear subs](#)
[Charles Wood](#)
- [Control-Alt-Eject? French Navy grounded...](#)
[David Leshar](#)
- [GCTIP: New Forums for Internet Transparency, Performance, ISP Issues](#)
[Lauren Weinstein](#)
- [The mystery of 'Ireland's worst driver': an HR/training problem](#)
[Max Power](#)
- [Hiding in plain sight](#)
[Jeremy Epstein](#)
- [Stolen military laptop risks](#)
[Atom Smasher](#)
- [Risks of reading RISKS](#)
[Bruce Horrocks](#)
- [When a bit of knowledge is a dangerous thing](#)
[Jeremy Epstein](#)
- ["It leaked into the kiosks and fried our computers"](#)
[Monty Solomon](#)
- [Facebook Forever](#)
[John Kolesar](#)
- [Opening event goes with a bang](#)
[David Alexander](#)
- [Re: Hoare on Null References](#)
[Peter Bernard Ladkin](#)
[CBFalconer](#)
[William Bader](#)
[Dan Franklin](#)
- [Info on RISKS \(comp.risks\)](#)

✶ Train brake failure; broken valve

"David Leshar" <wb8foz@panix.com>

Fri, 13 Feb 2009 00:11:14 -0500 (EST)

<http://www.raib.gov.uk/publications/bulletins/bulletins_2009/bulletin_03_2009.cfm>

During a switching movement at a siding, a locomotive's automatic brake valve handle suddenly has no effect. Engineer applied independent brakes, but they can't stop the train due to its weight.

[Broken valve roll pin]

Paul Hirose <jvcmz89uwf@earthlink.net>:

Releasing the deadman pedal was no help because the brake system was designed to ignore it if the locomotive brake cylinders had at least 30 PSI. There was no other means in the cab to exhaust the train line.

Risks? First, not having a second, independent emergency valve. Second, the override on the deadman almost lead to dead men.....

MetaRISK? How long have we been making trains with Westinghouse air brakes, and we still have not found all possible critical failures?

How will we ever do so for complex systems?

[Attribution to Paul Hirose added in archive copy. PGN]

Collision - UK and French Nuclear subs

Charles Wood <j.charles.wood@gmail.com>

Tue, 17 Feb 2009 19:03:05 +0900

The report is at http://news.bbc.co.uk/2/hi/uk_news/7892294.stm

Quote *"*A Royal Navy nuclear submarine was involved in a collision with a French nuclear sub in the middle of the Atlantic, the MoD has confirmed.*"*

What is interesting is the potential causes of this incident.

The British published point of view is that it is a random accident caused by two extremely stealthy submarines accidentally colliding.

May I suggest two alternative hypotheses?

First: The collision was a result of one of the submarines stalking the other, and as an unexpected outcome, colliding with the target?

Second: Perhaps current submarine navigation systems constrain the vessels to travel at specific, and integral, depths and tracks?

The second hypothesis has an all too real correspondent in the present air

navigation systems. The precision of current air navigation systems means that aircraft fly within metres of expected altitude and track. The result of such precision is an increased risk of collision in case of accidental assignment to conflicting air routes. A case in point is the collision on September 26, 2006 over Brazil.

<http://www.washingtonpost.com/wp-dyn/content/article/2006/12/08/AR2006120800835.html>

#Control-Alt-Eject? French Navy grounded...

"David Leshner" <wb8foz@panix5>

Sat, 7 Feb 2009 23:31:49 -0500 (EST)

[Source: UPI, 7 Feb 2009]

A computer virus infected French military databases and grounded some navy fighter jets for two days last month, a navy spokesman says. Naval spokesman Jerome Erulin said the recent computer security breach was limited but prevented the aircraft from downloading flight plans, The Daily Telegraph reported Saturday. "It affected exchanges of information but no information was lost. It was a security problem we had already simulated," Erulin said. "We cut the communication links that could have transmitted the virus and 99 percent of the network is safe."

The database infection by "Conficker," a malicious software virus publicly reported by Microsoft last October, likely was the result of negligence, naval officials said. *The Telegraph* said, according to a report by French newspaper *Liberation*, the infection involved France's Villacoublay air base and the 8th Transmissions Regiment and left fighter jets grounded for two days starting Jan. 15.

[Also noted by Mark J Bennisson on Dave Farber's IP list, with the article by Kim Willsher in Paris. PGN]

<http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html>

#GCTIP: New Forums for Internet Transparency, Performance, ISP Issues

Lauren Weinstein <lauren@vortex.com>

Mon, 16 Feb 2009 16:21:12 -0800

Announcing GCTIP - New Forums for Internet Transparency,
Performance, and ISP Issues

<http://lauren.vortex.com/archive/000506.html>

Greetings. I'm pleased to announce the availability of a new venue for discussion, reporting, analysis, information sharing, queries, and consumer assistance regarding Internet performance, transparency, and measurement, plus a wide range of topics associated with consumers and their interactions with Internet Service Providers (ISPs).

Called GCTIP Forums:

<http://forums.gctip.org>

this project -- The "Global Coalition for Transparent Internet Performance" -- is the outgrowth of a network measurement workshop meeting sponsored by Vint Cerf and Google at their headquarters in June, 2008 for a number of academic network measurement researchers and other related parties. This is the same meeting that formed the genesis of the open platform M-Lab ("Measurement Lab") project that was recently announced (<http://www.measurementlab.net>).

GCTIP was the original name for the mailing list that I maintained for that Google meeting and subsequent discussions (full disclosure: I helped to organize the agenda for the meeting and also attended).

Unless we know what the performance of the Internet for any given users really is -- true bandwidth performance, traffic management, port blocking, server prohibitions, Terms of Service concerns, and a wide range of other parameters, it's impossible for anyone who uses Internet services to really know if they're getting what they're paying for, if their data is being handled appropriately in terms of privacy and security, and all manner of other crucial related issues.

While transparency and related concerns do have impacts on "network neutrality" issues, neither GCTIP nor GCTIP Forums are oriented toward network neutrality discussions.

The purpose of GCTIP Forums is to provide a free discussion environment to act as a clearinghouse for all stakeholders (technical, consumers, ISPs, government-related, etc.) to interact on the range of "network transparency" and associated topics. The focus is on collecting, analyzing, and disseminating reports relating to Internet measurement/test data -- plus associated concerns, discussions, etc., in manners that are most useful to the network community at large. There are many groups working in the network measurement area, but surprisingly little data sharing, coordination, or ongoing reporting in a form that is useful to most ordinary Internet consumers or other interested observers.

An area of particular concern is helping to assure that measurement tests and perceived consumer problems with their ISPs aren't misinterpreted by users resulting in unfair or simply wrong accusations against those ISPs. I feel strongly that consumers need a place to go with these sorts of issues where the broader community and experts can help interpret what's really going on. Guilty firms should be exposed, but the innocent must not be inappropriately branded.

All current GCTIP Forums topics can be viewed without signing up on the system. Simple registration is required to post new discussion threads and replies, but no non-administrative topics are currently pre-moderated (any reported materials confirmed to be inappropriate will be deleted promptly).

GCTIP Forums exist to enable the exchange of relevant ideas, queries, data, and other information for anyone concerned about the Internet worldwide.

The Forums are seeded with five top-level discussion topics to get things rolling, but suggestions for additional categories are welcome. New threads (e.g. discussions of particular measurement tools, measurement results, specific ISP issues and concerns, etc.) can be created by registered users, starting right now.

Please note that I am running GCTIP on my own dime at this point. At such a time as any outside support funding becomes available for the project (which would be very much appreciated!) it will be publicly announced of course.

Spread the word! This is your chance to help yourself and everyone else better understand what the Internet is **really** doing, and by extension, where it is going tomorrow.

Thanks very much. Be seeing you ... at: <http://forums.gctip.org> ...

Lauren Weinstein <lauren@vortex.com> Tel: +1 (818) 225-2800
<http://www.pfir.org/lauren> Lauren's Blog: <http://lauren.vortex.com>
Co-Founder, PFIR - People For Internet Responsibility - <http://www.pfir.org>
Co-Founder, NNSquad - Network Neutrality Squad - <http://www.nnsquad.org>
Founder, PRIVACY Forum - <http://www.vortex.com>

#The mystery of 'Ireland's worst driver': an HR/training problem

*Max Power <dist23@juno.com>
Thu, 19 Feb 2009 14:39:37 -0800*

This seems to me that this is an HR and training problem. True -- it involves a computer database -- but the database is not at fault. As a preventative measure you would probably want to have "Driver's Licence" in as many different languages in said same offence database, but tagged to indicate as such just in case some untrained person makes a mistake.

Ultimately, in Greater Europe (from Vladivostok to Iceland to Saint Helena) the traffic-oriented part of the police forces must be trained in knowing all the variants of driver's permits in their region.

Countries that need to check their own national driving offence databases for this problem: Southern Hemisphere: Australia, NZ & Fiji.
North America: US, Canada & Mexico.

Max Power <http://HireMe.geek.nz/>

The mystery of Ireland's worst driver

Details of how police in the Irish Republic finally caught up with the country's most reckless driver have emerged, the Irish Times reports.

He had been wanted from counties Cork to Cavan after racking up scores of speeding tickets and parking fines.

However, each time the serial offender was stopped he managed to evade justice by giving a different address.

But then his cover was blown.

It was discovered that the man every member of the Irish police's rank and file had been looking for - a Mr Prawo Jazdy - wasn't exactly the sort of prized villain whose apprehension leads to an officer winning an award.

In fact he wasn't even human.

"Prawo Jazdy is actually the Polish for driving licence and not the first and surname on the licence," read a letter from June 2007 from an officer working within the Garda's traffic division. "Having noticed this, I decided to check and see how many times officers have made this mistake. "It is quite embarrassing to see that the system has created Prawo Jazdy as a person with over 50 identities." The officer added that the "mistake" needed to be rectified immediately and asked that a memo be circulated throughout the force.

In a bid to avoid similar mistakes being made in future relevant guidelines were also amended. And if nothing else is learnt from this driving-related debacle, Irish police officers should now know at least two words of Polish. As for the seemingly elusive Mr Prawo Jazdy, he has presumably become a cult hero among Ireland's largest immigrant population.

http://news.bbc.co.uk/go/pr/fr/-/1/hi/northern_ireland/7899171.stm

[Also noted by several others. PGN]

Hiding in plain sight

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Thu, 19 Feb 2009 12:05:44 -0500

I recently started working on a project that has a * in the middle of its name - think of GM's On*Star as an example. Google (and other search engines I tried, including Microsoft Live, Yahoo!, and Lycos) all treat the * as a wildcard, and don't allow wildcard escaping.

Now On*Star isn't hard to find with Google, because the words "on" and "star" rarely appear together except in this context. But if you take two other words that frequently occur together, put a * between them, and then try to find references to that unique term, you won't get very far. For example, stimulus*package would not be a good name, nor would high*tech.

It's not clear to me whether the people who started this project knew that their project name would make it effectively impossible to find the project and either did that intentionally or didn't care, or whether it's a happenstance that is now a problem. But in any case, it's a way to hide in plain sight - any websites they have can be indexed by robots, but won't be found by searchers.

The risk is the interaction between name selection and search engine operation. If someone deliberately picks a name this way, and then the search engines change their behavior, the value (anonymity) instantly disappears. The classic security problem of a distributed system with uncoordinated security policies....

✂ Stolen military laptop risks

Atom Smasher <atom@smasher.org>

Fri, 13 Feb 2009 10:58:34 +1300 (NZDT)

The US Struggle to Keep the Taliban From Stealing What's Inside This Box

<http://www.truthout.org/021209A>

<http://www.globalpost.com/dispatch/pakistan/090211/exclusive-the-wrong-hands>

It's one thing when banks and universities screw up by not encrypting their hard drives, but an unencrypted drive in a military laptop ostensibly filled with sensitive information in a war-zone has to win first place in the f**k-up olympics.

"A good price means \$800, he says. This would be a steep price in the secondhand market for a regular Intel Pentium M laptop manufactured in 2004. But this is not ordinary equipment... The computer also contained dozens of manuals on how to operate, assemble and trouble shoot U.S. Army equipment - everything from "space heaters" to "up-armored humvees." Some of the manuals contain restricted information and warn that "distribution is limited to U.S. government agencies," with instructions to "destroy by any methods that must prevent disclosure of contents or reconstruction of the document." But the machine - and all the information inside - was available for a price in the open market in Peshawar. And it makes an attractive investment for anyone who has in their possession any form of serious U.S. military hardware."

Read the article for more alarming info about the sensitive info on this laptop. OTOH, maybe it's a honey-laptop? filled with tracking software and misinformation... but i doubt it.

<http://atom.smasher.org/>

✂ Risks of reading RISKS

Bruce Horrocks <bruce@scorecrow.com>

Mon, 16 Feb 2009 23:14:25 +0000

Re: 390,000 to access child database ([RISKS-25.55](#))

One of the risks of reading RISKS is that one may be tempted to believe that articles described as "Full story at:" do actually contain the full story.

For example, hands up how many of you read "390,000 to access child database ... of all under 18 year-olds in England" and assumed that this means all 390k have full access to the whole database?

[Whoops! That's 390,000 pounds. See jidanni's comment in [RISKS-25.57](#). PGN]

It would help if those submitting risks items actually state what they think the risk is, so that their concerns can be allayed should they be misplaced.

✂ When a bit of knowledge is a dangerous thing

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Fri, 13 Feb 2009 13:34:22 -0500

As has been widely reported (but for whatever reason not in RISKS that I can find), the ability to find MD5 collisions has been used to create counterfeit intermediate certificates, thus putting users at risk of trusting incorrect sites. More detail at <http://www.win.tue.nl/hashclash/rogue-ca/> and hundreds of news reports, such as Markoff's blog (*The NY Times) at <http://bits.blogs.nytimes.com/2008/12/30/outdated-security-software-threatens-web-commerce/?pagemode=print>

I got an e-mail recently from a colleague who is not a security specialist, but is a specialist in designing power plants. He read the news coverage, interpreted it as "SSL is no longer secure", and decided to roll his own security protocol for use in a new power plant where he's designing the control systems. My reaction, of course, was "NO! don't do that", but I wonder how many other people out there have drawn the same conclusion, and don't have a security expert to turn to for advice.

The risk? In finding security problems, we need to carefully communicate not only the problem, but also what people should do in response, lest the cure be worse than the disease. I think the researchers did a good job of that -- explaining that use of SHA-1 hashes in certificates are much better than MD5, and eventually moving to SHA-2 or something else in the certificates is the long term solution -- but that level of detail got lost in much of the popular reporting.

✂ "It leaked into the kiosks and fried our computers"

Monty Solomon <monty@roscom.com>

Wed, 11 Feb 2009 01:57:23 -0500

Virgin America spiffs up at Logan [Excerpt]

http://www.boston.com/business/articles/2009/02/10/virgin_america_spiffs_up_at_logan/

Of course, the fancy digs could come with unintended consequences: A few months ago at the San Francisco airport, a passenger using the check-in kiosk watered the fake orchids atop the kiosk table with leftover soda.

"It leaked into the kiosks and fried our computers," Pawlowski said.

So Virgin has designed its Boston kiosk tables with smaller computer processors and interior pathways to funnel fluids away from the electronics. "I'm not going to say it can't happen again, but I'm hoping it doesn't."

Facebook Forever

*"John Kolesar" <john@kolesar.net>
Tue, 17 Feb 2009 08:23:46 -0500*

This article showed up on Fox News. While Fox News is noted for being somewhat a sensational tabloid I thought this was interesting.

<http://www.foxnews.com/story/0,2933,494064,00.html>

I am not a facebook fan or user but does the average "Joe" know what he is allowing them to do? Should we care?

<http://www.facebook.com/terms.php>

Licenses

You are solely responsible for the User Content that you Post on or through the Facebook Service. You hereby grant Facebook an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to (a) use, copy, publish, stream, store, retain, publicly perform or display, transmit, scan, reformat, modify, edit, frame, translate, excerpt, adapt, create derivative works and distribute (through multiple tiers), any User Content you (i) Post on or in connection with the Facebook Service or the promotion thereof subject only to your privacy settings <<http://www.facebook.com/privacy/>> or (ii) enable a user to Post, including by offering a Share Link on your website and (b) to use your name, likeness and image for any purpose, including commercial or advertising, each of (a) and (b) on or in connection with the Facebook Service or the promotion thereof. You represent and warrant that you have all rights and permissions to grant the foregoing licenses.

John Kolesar, 440-871-7965 W, 248-760-4040 M, john@kolesar.net

Opening event goes with a bang

*David Alexander <dave_ale@online.rednet.co.uk>
Wed, 11 Feb 2009 23:17:19 +0000*

This isn't strictly a technology risk, but it's too good to ignore.
The UK *Daily Telegraph*, 11 Feb 2009:

"China 'sorry' for towering inferno"

China central television, the official broadcasting mouthpiece of the Communist party, has apologised for burning down its new headquarters building with an illegal fireworks display. One fireman died and six were injured in the blaze on Monday night. The 30-story building, which was designed by Rem Koolhaas, a leading Dutch architect, and engineered by the British firm ARUP, was burnt out.

Beware the risks and impacts of your opening ceremony

David Alexander, Towcester, Northamptonshire, England

Re: Hoare on Null References (Schaefer, [RISKS-25.55](#))

*"Prof. Dr. Peter Bernard Ladkin" <ladkin@rvs.uni-bielefeld.de>
Wed, 11 Feb 2009 07:47:57 +0100*

Rpbert Schaeffer's assertions in [Risks-25.55](#) concerning what I take to be Goedel's Theorem are misleading. And I am not persuaded by a corrected version of his argument, either.

Schaeffer asserts: "You can't prove that a system is both correct and complete without going outside that system." So, to begin with, let's get a more accurate expression of what Schaeffer might want to say. He doesn't explain what "correct" means in his statement. Let me assume he means "consistent" in its classical sense.

First, given a theory L in first-order logic, you can, contrary to Schaeffer, indeed prove in L that L is both consistent and complete, provided that L has the resources to express those statements, if L is inconsistent. Indeed, you can prove anything in L that L can express.

Second, a partial reverse: given a theory L in first-order logic that contains Peano arithmetic (indeed, it doesn't need to be full Peano arithmetic - an substantial fragment will suffice), one can prove completeness of L in L only if L is inconsistent.

The conditions that Schaeffer missed was that L must be a consistent classical first-order theory containing an appropriately substantial fragment of Peano arithmetic. Then you can say that L cannot prove its own completeness.

Now, consider these conditions one by one. One may think that inconsistent theories are not useful. One may also think that all useful theories must be formulated in, or contain, classical first-order logic. One may also think that all useful theories contain Peano arithmetic. All these conditions may be questioned when dealing with computer systems of any sort, as follows.

The people who study and develop paraconsistent logics would disagree that inconsistent theories are not useful. Paraconsistent logics are classically

inconsistent. There are obvious ways to weaken first-order logics to allow some statements of the form (A & not-A) to be proved, but not all. And even if one retains classical inference, if one uses L for reasoning (rather than for illustrating purely mathematical points) then for practical purposes one might only be interested in things one can deduce in L through proofs of bounded length (there is a limit to what we can achieve in the life of the universe), say length B. If the shortest proof of a statement of the form (A and not-A) is longer than B, then for one's purposes the inconsistency of L might not be relevant.

Finally, it is questionable that Goedel's theorem could apply here at all. I don't know any computer languages or compilers, and certainly no physical machines, that implement Peano arithmetic, or indeed a sufficiently substantial fragment. All computer arithmetic I know is finite, and I confidently expect it to stay that way.

Peter Bernard Ladkin, Causalis Limited and the University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

✉ Re: Tony Hoare: "Null References" (Diamond, [RISKS-25.55](#))

CBFalconer <cbfalconer@yahoo.com>

Thu, 12 Feb 2009 02:24:16 -0500

There was an even earlier language, Pascal, that provided all that security, and more. It had simultaneous advantages and disadvantages over C:

Pascal was complete. You didn't need a large standard library. It was defined. This was both an advantage and a disadvantage, since you could immediately write your software, but the language couldn't evolve as easily as could C.

The act of having run-time checks, and many compile-time checks, allowed the checking code to be fairly trivial. Good systems could expect about a 5% effect. In comparison equivalent C checking was (and is) virtually impossible, or requires exorbitant run-time support. The same things that create C advantages (e.g. string storage that can be a great variable) cause horrible checking problems.

Pascal had an approved ISO standard about 10 years before C.

Pascal suffered greatly from the Borland disease. Borland implemented a form of Pascal that did not meet the standards, and still doesn't. That meant that programmers never learned the appropriate ways to write code, especially interactive code.

Pascal had the great advantage of defined i/o systems (files, etc.) which were extremely flexible. However the limitations of some of the standard procedures affected things. For example, there was no way to programatically control the error response on a "read(integer);" call.

Chuck F (cbfalconer at mainline dot net) <<http://cbfalconer.home.att.net>>

Re: Tony Hoare: "Null References" (Baker, [RISKS-25.52](#))

William Bader <williambader@hotmail.com>

Fri, 13 Feb 2009 20:49:52 -0500

Array bounds checking (and pointer checking) is possible in C.

<http://gcc.gnu.org/extensions.html>

<http://sourceforge.net/projects/boundschecking/>

<http://williambader.com/bounds/example.html>

<http://freshmeat.net/projects/valgrind/>

Re: Tony Hoare: "Null References" (Diamond, [RISKS-25.55](#))

Dan Franklin <dfranklin@dan-franklin.com>

Sun, 15 Feb 2009 00:35:24 -0500

The inventors of the C language did not merely omit array bounds checking from C; they encouraged C programmers to omit manual bounds checking as well. This is what really bothers me. Consider:

1. Early C programming books suggested the idiom

```
while (*p++ = *q++);
```

to copy a string from one area to another. No bounds checking was ever suggested.

2. The C library contained several functions that ignored array bounds, including the infamous "gets" function, which read an input line into a buffer - and took no length parameter for the buffer. It was impossible to use gets safely; no matter what buffer you provide, there was a potential input line long enough to cause a buffer overflow.

3. When you pass an array as a parameter, its size is lost to the called function. As with Fortran, if you care about buffer size, you must pass it as an additional parameter - a sizable (so to speak) nuisance.

Omitting array bounds checking may have made sense at the time given the available hardware and compiler technology. But there was no need to create "gets" without a size parameter, or to avoid passing array sizes by default. (Cases where it would have been too inefficient to push the array size parameter onto the stack could have been handled by distinguishing between arrays and pointers.)



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 57

Friday 20 February 2009

Contents

- [Taiwan immigration computer down again](#)
[jidanni](#)
- [Wikipedia prankster dupes German media](#)
[Allen Hainer](#)
- [The Trouble with Trusting Trend Micro](#)
[Kevin Way](#)
- [ESTA visa waiver online doesn't provide existing waiver ref number](#)
[George Michaelson](#)
- [Stove's Bad Crash Handling](#)
[Gene Wirchenko](#)
- [Dates of birth are not unique identifiers](#)
[Steven J Klein](#)
- [Re: Train brake failure; broken valve](#)
[Matt Roberds](#)
- [Re: Collision - UK and French Nuclear subs](#)
[Richard I. Cook](#)
[Geoffrey Brent](#)
- [Re: What if you can't pull the plug?](#)
[Michael Loftis](#)
[David Leshner](#)
- [Re: Windshields and Windows combine to provide malware vector](#)
[Tom Perrine](#)
- [Re: Godel and correctness](#)
[Martyn Thomas](#)
- [Re: Tony Hoare: "Null References"](#)
[Dimitri Maziuk](#)
[King Ables](#)
- [Re: The mystery of 'Ireland's worst driver'](#)
[David Cantrell](#)
- [Re: Opening event goes with a bang](#)
[Mark Brader](#)
- [Re: Risks of reading RISKS](#)
[jidanni](#)
[Martyn Thomas](#)
[Scott Miller](#)

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

#Taiwan immigration computer down again

<jidanni@jidanni.org>

Sun, 15 Feb 2009 14:28:20 +0800

I swear I'm not making this up just trying to give itty bitty countries who can't fend for themselves a bad name, see:
<http://www.taipeitimes.com/News/taiwan/archives/2009/02/14/2003436061>

IMMIGRATION: Airport system crashes again

The immigration computer system at Taiwan Taoyuan International Airport experienced another breakdown yesterday morning, lasting 20 minutes. Added to the two more serious breakdowns suffered last month, yesterday's incident marked the third system breakdown this year. National Immigration Agency Deputy Director-General Huang Pi-hsia said that yesterday's incident happened because of a system database capacity shortage when the agency was converting files in the database. No flight delays were caused as a result of the incident and no one banned from leaving or entering the country passed immigration during the 20-minute stoppage.

(Including Ex-President Chen "Count TheTowels" Shuibian, still safely in the slammer.)

#Wikipedia prankster dupes German media

Allen Hainer <risks@hain-veilchen.de>

Thu, 12 Feb 2009 16:51:58 +0100

"An article meant to poke fun at the lengthy royal name of new Economy Minister Karl-Theodor zu Guttenberg turned out to be a joke on daily *Das Bild* and other German publications who revealed their reliance on Internet encyclopedia Wikipedia when they published his name incorrectly this week."
<http://www.thelocal.de/society/20090212-17397.html>

#The Trouble with Trusting Trend Micro

Kevin Way <kevin@insidesystems.net>

Thu, 12 Feb 2009 10:26:24 -0500

Many of us use blacklists such as those provided by Trend Micro's MAPS program as part of an anti-spam solution. However, by doing so we're adding significant risk due to ineffective (or absurd) administrative procedures on the part of the list provider.

For example, a datacenter I use has IP space incorrectly listed on Trend Micro's MAPS DUL. When they attempted to have the static space removed (15 blocks totaling 159,744 IPs), Trend Micro responded that they would not remove the IPs from their blacklist unless the rDNS for every IP in the space was modified to include the word 'static'.

Trend Micro was unwilling to offer any alternative way to correct the DUL, and indicated that since the center hadn't changed rDNS on all of the IPs that their space would remain listed, incorrectly, on the DUL.

The damage done by such mistakes is then magnified by the common anti-spam practices of either silently dropping the mail, or delivering the mail to a "Junk Mail" folder which often remains unchecked. In both cases, the sender is unaware that a problem has occurred, and that an alternate means of communication must be established.

The experience made me wonder how many blacklist consumers really understand and recognize the amount of risk they're accepting, when they trust a third-party blacklist so thoroughly that they will silently squelch communications according to that list.

✂ ESTA visa waiver online doesn't provide existing waiver ref number

*George Michaelson <ggm@apnic.net>
Thu, 19 Feb 2009 15:39:58 +1000*

The US Government instituted an online mandatory visa waiver process for travelers. The visa waiver consists of a 16 character alphanumeric string. If you visit the URL: <https://esta.cbp.dhs.gov/esta/esta.html> you can either apply for a new waiver, or re-update an existing one.

If you HAVE one, you cannot use the new application side: it terminates 5 screens in. This is not made plain to you until you have completed the entire I94w equivalent "no I am not a former nazi" declaration (cute, that they removed the "nor am I a member of the communist international")

If you HAVE one, but don't know the number, then the site cannot send you your number, not tells you your number. Therefore, unless you record your number offline, you are locked out.

Sure, there are risks of telling people their number. But one presumes that the system at least understands people might have forgotten a 16 digit magic number.

72-hour deadline. You have to do it, or you risk being offloaded by the airline. Nice!

✂ Stove's Bad Crash Handling

Gene Wirchenko <genew@ocis.net>

Sun, 15 Feb 2009 13:40:56 -0800

Following is a post from alt.folklore.computers about a stove's software crashing. The risk is what happens: it turns everything on at lowest setting.

Date: Sun, 15 Feb 2009 18:20:55 +0100

From: Morten Reistad <first@last.name>

Subject: Re: I need magic incantation for a power conditioner

In article <proto-9E06BD.11220115022009@news.panix.com>,

Walter Bushell <proto@panix.com> wrote:

>In article <v318ng.lht.ln@eden.reistad.name>,

> Morten Reistad <first@last.name> wrote:

>

>> In article <19tep4l1vgahtate1dofomm0aks3u0ai4d@4ax.com>,

>> krw <krw@att.bizzzzzzzzzz> wrote:

>> >On Sat, 14 Feb 2009 07:39:23 -0500, jmfahciv <jmfahciv@aol> wrote:

>> >

>> >>Charles Richmond wrote:

>> >>> jmfahciv wrote:

>> >>>> sidd wrote:

>>

>> >>>>

>> >>>> I was thinking of the field. The way I stopped the modems

>> >>>> from getting busted was to ban the cleaning lady from the

>> >>>> the terminal room.

>> >>>>

>> >>>

>> >>> Aside: Did you leave your stove that interfered with you

>> >>> AM radio... when you moved to your new house???

>> >>>

>> >>>You betcherass I did. It is Mass. law that a stove be

>> >>>left on the premises.

>> >

>> >Ok, gotta ask... Does the new stove kill the radio like the old?

>> >

>> >... or as completely as congress is about to?

>>

>> Or does the new stove have software crashes, like I discovered

>> ours has.

>>

>> "Sorry Dear, dinner is late, had to reboot the stove."

>>

>> -- mrr

>

>Now that is just wrong, putting Microsoft in critical life support

>equipment. It says in the contract that it is not to be used in mission

>critical equipment.

I have no reason to believe there is Micro\$oft in\$ide; the whole controller box with 8-character display is around 5x5xsub 1 cm, 2x2x1/3rd inches. It

has three cable attachments plus power; one to the touch panel, one to a series of BIG regulators, and one to a front panel.

It went "Error 32" (ISTR) blinking, while all active positions went on, but on the lowest possible setting. (A fencepost error in the error handling code?) This means it turns ON the stove, but at a very low setting, on crash. Sheesh.

It then just said "beep" when trying to manipulate something.

We had to drop the fuse for around 5 seconds before it restarted, beeped loudly, said "Error 32" again, then a couple of other diags, including a hex value, and then went back to being happy again. -- mrr

Dates of birth are not unique identifiers

Steven J Klein <steven@klein.us>

Wed, 11 Feb 2009 02:13:23 -0500

USAA is a membership-based financial services company; existing members like myself can create memberships for family members -- even minor children.

Recently I used their web site to try and create memberships for my kids. It worked for my son, and the first of my three TRIPLET daughters. (Some of you have already guessed where this is going.)

But after putting in all the info for my 2nd daughter (name, social security number, date of birth, and other data), I got an error message saying "We have canceled your request. To add this person, please call ..."

As their customer service rep later explained to me, there was some concern that careless users might accidentally try to add the same child more than once. To overcome this, their programmers decided to use the birth-date as a unique identifier.

But it's not unique for twins, triplets, etc. It's also possible (though less likely) for two step-siblings in a "blended family" to have the same date of birth.

Why not use the social security number, which is guaranteed to be unique? I don't know, and neither did the person who answered my call.

[* It is probably illegal, unethical, and subject to misuse. PGN]

(It is interesting to note that 2 of my triplets received sequential social security numbers, but the 3rd differs by 1,930.)

Steven J Klein, CompTIA A+ Certified, Apple Certified, Your Mac & PC Expert
Phone: (248) YOUR-MAC or (248) 968-7622

Re: Train brake failure; broken valve (Lesher, [RISKS-25.56](#))

Matt Roberds <mroberds@att.net>

Fri, 20 Feb 2009 15:12:41 +0000

In [RISKS-25.56](#), David Lesher commented on a report of a rail accident in the UK. Following the release of that report, there was also a bit of discussion in news:misc.transport.rail.americas . (Part of the summary posted to RISKS appears to be from the first post in that thread.) There was also a discussion a few weeks earlier in news:uk.railway . Links:

http://groups.google.com/group/misc.transport.rail.americas/browse_thread/thread/2e15e2405ed0114a

http://groups.google.com/group/uk.railway/browse_thread/thread/48705d7fd6838040

The discussion shows that the risks of not having an independent emergency valve have been known for some time; one poster cited a steam locomotive built in 1913 that had two such valves, presumably as standard equipment. There was speculation that the accident locomotive probably had an independent emergency valve from the factory, but that it was later removed. (This is likely a well-known story on RISKS: your computer (locomotive) can have as much buggy hardware as you want if it's just sitting in the corner (running around the quarry) by itself. Once you plug it into the network, though, you can cause problems for everybody.)

A couple of posters also echoed the statement in the accident report that if the train driver had _released_ the locomotive brakes, the dead-man system would have started operating again, and would have applied the train brakes, probably stopping the train. As noted briefly in the report, this is a training issue. As Stephen Furley put it, "When you're running downhill, with a heavy stone train behind you and the train brakes have failed, it's not exactly obvious that the best thing to do is to release the only functioning brake that you do have, even if that's not managing to stop the train." (Two more well-known stories: training and user interfaces.)

Anyway, I think that the problem here wasn't so much that a new critical failure mode was discovered, but that part of the system that was designed to cope with a known failure mode was disabled. (Another well-known story.)

Re: Collision - UK and French Nuclear subs (Wood, [RISKS-25.56](#))

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

Thu, 19 Feb 2009 20:11:31 -0600

Charles Wood hypothesized the collision was the result of...

(1) ...one of the submarines stalking the other, and as an unexpected outcome, colliding with the target?

or

(2) ...current submarine navigation systems constrain the vessels to travel

at specific, and integral, depths and tracks?

(1) is extremely unlikely. The vessels are strategic nuclear submarines (missile launch platforms) and unsuited to pursuit and shadowing. This function is provided by 'attack' submarines which are smaller, more agile, and armed differently. (BTW, the number of attack submarines in the U.S. fleet is maintained at number sufficient to have at least one follow each Soviet sub as it leaves harbor and this has been the practice for a very long time.)

(2) is probably closer to the mark, although the reasons are different. The ballistic and accuracy characteristics of each country's sea-launched ICBMs are quite similar because of the physics of flight. The targeting of these missiles is also likely to be similar because potential targets are all in the few nuclear-armed and potentially hostile countries. Given the ocean characteristics which effect the 'hiding' of strategic submarines and the interior location of their major targets (mostly Russian missile silos, etc.), the number of cruise routes that allow a strategic sub to carry out its mission is actually rather limited. Remember that the entire purpose of strategic nuclear submarines is deterrence and for deterrence to be credible it has to be continuously present -- that is, unlike other weapons systems, strategic nuclear submarines must always be prepared to launch their missiles against their targets. This is a rather severe requirement that makes the useful ocean relatively small. For this reason, it is not at all unlikely that two strategic subs would collide.

BTW, all of this info is publicly available...you just need to know where to look.

✉ Re: Submarine collisions (Wood, [RISKS-25.56](#))

*Geoffrey Brent <gpbrent@optusnet.com.au>
Sat, 21 Feb 2009 02:37:36 +1100*

Charles Wood suggests that integral depth settings might be a cause of the recent submarine collision (perhaps this problem could be avoided if the British agreed to use imperial units and the French metric?)

Another consideration is that while there are about a billion cubic kilometers of water in the Earth's oceans, some of them are much more attractive than others for submarine commanders - seafloor topography and gradients in water temperature or salinity can have a lot of influence on stealth. Increasing precision in measuring these things might also have something to do with why the French and British commanders ended up hiding on top of one another.

✉ Re: What if you can't pull the plug?

Michael Loftis <mloftis@wgops.com>

Tue, 10 Feb 2009 21:57:07 -0700

One thing about all the current apple devices is that the power button (or a combination of buttons on the iPods) have a supervisory power circuit system that can, and will, disconnect the main software controlled power supply when held down. The macbook air, new macbook pro, and even all the old macbook pro's are no different. The power management subsystem cooperates with the software in the OS, but is itself a separate, and very simple, embedded device. So if you hold the power button down, even if there's no OS going, it'll go off. But it will take ~10 seconds.

This is in fact a very common behavior (and architecture) for many battery operated devices.

For the iPod there's a set of supervisory circuits that allow you to cause the power to be turned off/on, and for the reset line to be triggered on the CPU.

I've not used an iPhone, but I think it does have a power button. Apple's engineers however, are usually a little more thorough with details than some other companies, so I can't say that this holds true for all hardware manufacturers, but it does for most.

Re: What if you can't pull the plug? ([RISKS-25.55](#))

"David Lesh" <wb8foz@panix.com>
Wed, 11 Feb 2009 01:03:16 -0500 (EST)

- > Software-controlled power switches
- > Long-life batteries that can't be removed
- > Continuous wireless Internet access via WiFi or mobile phone networks

I agree with the risk, but have a suggestion.

Place in plastic bag.
Wrap with foil.
Insert in freezer.

Not only is it as good a RF cage as your house likely has; the reduced temp will sap the battery's enthusiasm...

Alternately, you can buy RF-proof zipper bags, but they are rather costly.

Of course, if the FBI is tracking you/listening via same; you'll soon get a visit... {The OTHER RISK of never-off devices...}

Re: Windshields and Windows combine to provide malware vector

Tom Perrine <tperrine@scea.com>

Wed, 11 Feb 2009 12:23:42 -0800

([RISKS-25.55](#))

This may just be my former "cold war" past rising up after all these years, but Grand Forks is an interesting place to see this happen (first).

Grand Forks is the home of a US Air Force base for aerial refueling and airlift. The refueling and airlift commands have information about the missions of all the groups that they support, and are a prime source of military planning and readiness data.

The malware had 3 components: 1) join to botnet, 2) steal passwords, and 3) buy fake A/V software.

Items 1 and 2 would be great vectors to get "on base", if a home or laptop computer of a military member became infected.

But, it's probably just someone trying to make a buck on the fake A/V.

Re: Godel and correctness (Was: Tony Hoare ...)

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

Wed, 18 Feb 2009 10:51:30 +0000

In the context of Schaefer's posting, I assume

- * Correct = self-consistent = code implements the specification.
- * Complete = "The specification doesn't omit anything I consider important".

The issue of whether the specification actually describes the system that, with hindsight, you would wish you had specified is also helped by formal specification (because you get faced by a lot of questions that force you to think hard about the properties you want your system to have and the consequences of those properties). But no formal system can guarantee 20/20 hindsight.

Martyn Thomas CBE FREng <http://www.thomas-associates.co.uk>

Re: Tony Hoare: "Null References" (Franklin, [RISKS-25.56](#))

Dimitri Maziuk <dmaziuk@bmrw.wisc.edu>

Fri, 20 Feb 2009 09:48:32 -0600

Sometimes I think the problem with C is that they're teaching it backwards. What they should teach is "here's how you create a memory area, here's how you use pointers to fill it with values of the same type. Here's how you can emulate multi-dimensional arrays, and here's how you emulate one-dimensional array of printable bytes that you can use as a close enough approximation of a string."

Once they're certain the students got it, then they could say "oh, and by the way, for our convenience we've created this square bracket notation and this nifty zero-byte hack. Keep in mind they're just handy shortcuts, there are no strings. Nor arrays."

There are languages that have built-in string data type and no buffer overflow in gets. There are languages with array data type that knows its own size, has bounds checking and often lets you indexed elements from e.g. -3 to 5. C just isn't one of them. All it is is glorified assembler and all it really has is what the computer has: integers and floats. With some integers getting special treatment because they represent memory addresses.

Re: Tony Hoare: "Null References" (Franklin, [RISKS-25.56](#))

*King Ables <king.ables@alumni.utexas.net>
Fri, 20 Feb 2009 06:13:25 -0600*

> The inventors of the C language did not merely omit array bounds checking
> from C; they encouraged C programmers to omit manual bounds checking as
> well. This is what really bothers me.

I think one has to be older than "a certain age" to understand the mindset.

This was a time when many people wrote in assembly language. For many writing in "high-level languages," that language was FORTRAN (and the 1966 standard, at that). What you wanted from a high-level language was data structure and functional convenience without losing any of the direct access to any location in memory that you were accustomed to in assembly code (this is why peek() and poke() stayed around so long in early PC languages, they were useful). I'm the programmer, I'll keep track of what I'm doing and where I'm putting things, thank you.

When you had a buffer overflow, it was because your own code did something you didn't intend, and the only result was your program crashed. Your only incentive to fix your bug was to prevent the crash. Buffer overflows with a specific and malicious intent were unknown. There was no Internet. Nobody in another country was pushing data into your program, nor could you conceive of any such an eventuality. Heck, you were happy when the operator mounted the right tape with the right input file on it.

I'm not defending it, clearly, with the benefit of hindsight, it was the wrong choice. But it wasn't such a bad choice at the time. There were good reasons for doing it that way. Try telling a caveman that one day he'll leave his cave and build a house out of wood and then that fire he just invented will be dangerous so he'd better go invent the fire extinguisher right now. His biggest problem today is keeping the fire going, why would he ever want to put it out? He has no context in which to see your issue.

Assigning blame for the current state of things when we have much more information than those to whom we may try to assign that blame is unfair.

We're all making choices today that people 20 or 50 years from now will look back and wonder "what were those idiots thinking?"

The mystery of 'Ireland's worst driver' (Power, [RISKS-25.56](#))

David Cantrell <d.cantrell@outcometechnologies.com>

Fri, 20 Feb 2009 15:23:15 +0000

"Max Power" wrote:

> Ultimately, in Greater Europe (from Vladivostok to Iceland to Saint Helena)
> the traffic-oriented part of the police forces must be trained in knowing
> all the variants of driver's permits in their region.

Within the EU, the layout of drivers' licences is standardised. So even if you don't know the Polish or Finnish or German or whatever for "name" and "surname" you can still tell which fields they are.

Here are licences from Germany, the UK, and Poland:

http://www.bundesdruckerei.de/pics/produkte/fuehrerschein/fuehrerschein_front_internet.jpg

<http://www.day-tripper.net/xzi/xphotodriving-licence.jpg>

http://www.eng.pwpw.pl/rep/f39/r48/min_prawo_jazdy.jpg

Fields 1 and 2 are surname and forename.

There are, of course, still some people driving around with old pre-standardisation licences, and I don't know how far along the road to standardisation Ireland is, but Irish police should already be familiar with the layout, as it's already commonly used elsewhere.

David Cantrell, Outcome Technologies Ltd, BUPA House, 15-19 Bloomsbury Way, London WC1A 2BA ENGLAND Registered in England, No: 3829851

Re: Opening event goes with a bang (Alexander, [RISKS-25.56](#))

Mark Brader

Thu, 19 Feb 2009 22:58:10 -0500 (EST)

Well, it's not the first time a ceremonial opening has turned lethal. Look up how William Huskisson died in 1830; there must have been others. Destroying the building as well is a nice touch, though.

Mark Brader, Toronto msb@vex.net

Re: Risks of reading RISKS (Horrocks, [RISKS-25.56](#))

<jidanni@jidanni.org>

Fri, 20 Feb 2009 10:44:34 +0800

BH> For example, hands up how many of you read "390,000 to access child
BH> database ... of all under 18 year-olds in England" and assumed that
BH> this means all 390k have full access to the whole database?

Ah, [It will cost one] 390,000 [British pounds] to access the child database...
wherein the "pounds" symbol is not ASCII and went bye-bye... :-)

[Noted in the archive copy of 25.56 as well. PGN]

✂ Re: Risks of reading Risks (Horrocks, [RISKS-25.56](#))

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

Fri, 20 Feb 2009 10:26:05 +0000

Most RISKS readers understand that the risks from improper access to data
involve the nature of the data, who has access to it, and what they can do
with it.

For example, if access to the child database were limited to those in the
geographic area where the child data subject lived, it would greatly reduce
the number of people who had access to any particular child's data, without
significantly reducing the risk to children from the data being abused - as
most abuses would involve people who know or have access to the child, and
most of these will be in that geographic area.

Martyn Thomas CBE FREng <http://www.thomas-associates.co.uk>

✂ Re: Risks of reading RISKS (Horrocks, [RISKS-25.56](#))

Scott Miller <SMiller@unimin.com>

Fri, 20 Feb 2009 09:10:44 -0500

It might also be helpful if those who appear to be claiming that a
submission is inaccurate, incomplete, or misleading would supply some
specific information regarding the perceived deficiencies. Otherwise a RISK
exists of evoking an analogy involving cooking vessels. Is Mr. Horrocks
stating that the 390,000 did *not* have full read access to the entire
database? In that case, what are some examples of the limitations? If that
access was limited, did the limitations meaningfully restrict access to all
government employees who might be careless enough to leave it laying about
unprotected on a laptop or portable media (of course this would be
unprecedented in the UK)? Was it restricted to all (hypothetical)
government-employed pedophiles in such a way as to protect the vital
information of the children from would-be predators? The only statement
regarding access that I find in the article cited by A. Shapir is from

Minister Morgan, "For someone fleeing domestic violence for example it is important we make sure the ContactPoint directory can shield in some way." Coming from someone who should be thoroughly familiar with whatever confidentiality measures are planned, had I the welfare of such a child entrusted to me, I would find that example of vague bureaucrat-speak more distressing than reassuring. As a long-time RISKS reader, I am convinced that the choice made to submit the incident with only those facts that were available was consistent with established RISKS practice, and the correct decision. Some risks are adequately and succinctly self-defining by description, and I believe this is an example. I'm also pretty certain that my comment clearly indicated my additional perceived risk (albeit somewhat sarcastically): assuming that government regulations, employees, and systems exist solely to serve the public interest and typically succeed in that endeavor.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 58

Sunday 22 February 2009

Contents

- [Buffer overflows in SHA-3 submissions](#)
[Joy Marie Forsythe](#)
- [Re: Train brake failure - broken valve](#)
[Al Stangenberger](#)
- [Due Diligence or is that "Don't..."? Citibank fraud](#)
[David Leshner](#)
- [Digital Archivists, Now in Demand](#)
[Conrad De Aenlle](#) via [Monty Solomon](#)
- [Re: Wikipedia prankster dupes German media](#)
[Debora Weber-Wulff](#)
- [Re: Control-Alt-Eject? French Navy grounded](#)
[CBFalconer](#)
- [Capital One Phishing Warning is dangerous](#)
[Marc Auslander](#)
- [Re: The mystery of 'Ireland's worst driver'](#)
[Bernard Lyons](#)
- [Re: Hiding in plain sight](#)
[Phil Smith III](#)
- [Bounds checking in C](#)
[Andrew Koenig](#)
- [The risks of Silver Bullets](#)
[Michael Smith](#)
- [Re: Tony Hoare: "Null References"](#)
[Steven M. Bellovin](#)
[Dimitri Maziuk](#)
[Randy Saunders](#)
- [Related to blacklists for antispam](#)
[De Vries Duane](#)
- [Re: Dates of birth are not unique identifiers](#)
[David E. Ross](#)
- [Re: USAA Web site follies](#)
[Jonathan Kamens](#)
- [Alert TA09-051A -- Adobe Acrobat and Reader Vulnerability](#)
[US-CERT](#) via [Monty Solomon](#)
- [Info on RISKS \(comp.risks\)](#)

Buffer overflows in SHA-3 submissions

Joy Marie Forsythe <jforsythe@fortify.com>

Sat, 21 Feb 2009 11:19:27 -0800

NIST is currently holding a competition to choose a design for the SHA-3 algorithm. The reference implementations of a few of the contestants have bugs in them that could cause crashes, performance problems, or security problems if they are used in their current state. Based on our bug reports, some of those bugs have already been fixed.

Two of the projects (Blender and MD6) contained buffer overflows. The rest of the issues found were out-of-bounds reads, memory leaks and null dereferences. The code was good overall, but it's important to get these implementations right. They end up being the basis for future implementations, or used as is, and can be a factor in the outcome of the SHA-3 competition.

More details about the issues:

<http://blog.fortify.com/blog/fortify/2009/02/20/SHA-3-Round-1>

Joy Marie Forsythe, Security Researcher, Fortify Software 1-650-358-5621
jforsythe@fortify.com

Re: Train brake failure - broken valve (Leshner, [RISKS-25.56](#))

Al Stangenberger <forags@nature.berkeley.edu>

Fri, 20 Feb 2009 12:19:44 -0800

The lack of an emergency brake exhaust valve in a locomotive must be a British peculiarity. Every American locomotive built within the past century has an emergency dump valve in the locomotive cab (and these are the Westinghouse brake design). When locomotives had firemen, the valve was located by the fireman's seat in case the engineer was incapacitated.

Also, every American railroad passenger car has an emergency dump valve (aka the conductor's valve). In older cars this valve was connected to a cord which ran above the windows for the full length of the car. Modern cars eliminated the emergency cord, and now the handle for the conductor's valve is often found near the vestibule at the end of the car. It is often not very obvious, but the crew knows where it is.

AL Stangenberger, Western Railway Museum

[Added: Fri, 20 Feb 2009 19:43:15 -0800]

I learned a lot more about railroad locomotive emergency brake valve requirements.

Emergency brake valves are now only required by U.S. Federal law (49 CFR Ch. II, sec. 229.47) if the locomotive cab is designed for occupancy by more than one person. The requirement is actually for the valve to be accessible to a member of the crew other than the engineer.

In the British case in RISKS, the US-built locomotive was designed for only one person in the cab, so the emergency brake pipe valve was not required. Possibly this policy should be reconsidered.

In any case, though, it is not the case that nobody ever thought about having emergency valves in Westinghouse-design air brake systems.

✂ Due Diligence or is that "Don't..."? Citibank fraud

*"David Leshar" <wb8foz@panix.com>
Sat, 21 Feb 2009 15:10:59 -0500 (EST)*

<http://www.nytimes.com/2009/02/21/nyregion/21scam.html?emc=3Deta1>

"A Nigerian citizen duped Citibank into wiring \$27 million to accounts that he and others controlled, prosecutors said." Citibank accepted a package changing contact data for the National Bank of Ethiopia; and only months later noticed it came not from Ethiopia but Lagos, Nigeria. When they finally started looking into it; they also found the new contact numbers were cell phones in Nigeria, UK and South Africa.

I'm reminded of the ex-President who'd never seen a grocery store scanner. An enormous international bank has never connected Nigeria and identity fraud?

The Risk? Reliance on easily forged documents with no verification.

Sometimes, a fraud too simple to ever work, shall...

✂ Digital Archivists, Now in Demand (Conrad De Aenlle)

*Monty Solomon <monty@roscom.com>
Sat, 21 Feb 2009 15:53:29 -0500*

Conrad De Aenlle, Fresh Starts: Digital Archivists, Now in Demand, *The New York Times*, 8 Feb 2009

When the world entered the digital age, a great majority of human historical records did not immediately make the trip.

Literature, film, scientific journals, newspapers, court records, corporate documents and other material, accumulated over centuries, needed to be adapted for computer databases. Once there, it had to be arranged - along with newer, born-digital material - in a way that would let people find what

they needed and keep finding it well into the future.

The people entrusted to find a place for this wealth of information are known as digital asset managers, or sometimes as digital archivists and digital preservation officers. Whatever they are called, demand for them is expanding.

One of them is Jacob Nadal, the preservation officer at the University of California, Los Angeles. He does not use the "digital" modifier because his duties include safeguarding analog materials in U.C.L.A.'s collection, not just preparing them to cross the digital divide.

"I don't think there's any day where I would say I'm the digital guy," he said. But he concedes that he's not really an analog, ink-on-paper guy, either, and that is increasingly the case in his field. These days, he noted, "if you want to work in a library, you have to deal in electronic resources."

Mr. Nadal and 10 or so colleagues at U.C.L.A. devote much of their effort to organizing and protecting material in digital form. Their duties include licensing and buying digital content from vendors, assigning identification markers called meta-tags so that material can be found easily, researching copyright matters and ensuring that files remain intact whenever new iterations of relevant software or hardware come along. ...

<http://www.nytimes.com/2009/02/08/jobs/08starts.html>

Re: Wikipedia prankster dupes German media (RISKS-25.57)

*Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>
Sat, 21 Feb 2009 14:00:06 +0100*

Actually, the prank goes deeper.

An anonymous IP (shorthand for non-registered editors on the Wikipedia), 78.34.237.194, a broadband user from Cologne, added the additional given name "Wilhelm" on 8 Feb 2009 at 9.40 pm for the newly designated German Minister of Commerce [1]. As a true blue-blood, he has more than the average number of them.

On 9 Feb at 12.23 pm the administrator Arudaki complained that there was no source for this name, and removed all of the additional given names [2]. But by then the damage had been done, and the newspapers who had done a quick Wikipedia "fact"-check were already online and included the name "Wilhelm".

A rage ensued, as people "fixed" the Wilhelm back in, quoting the now online sources that had used the faked Wikipedia entry. As is usual in a vandalism war, the page was removed from editing mode until people could cool down and get out a copy of the German peerage book [3] and discover that there was no "Wilhelm" listed there. The page is back being editable (and of course the pranksters keep putting in new names such as "Marcus", but they get quickly reverted (and the prankster given an hour in the corner, unable to edit).

Anonymous then bragged about his or her heroic feat in [4], and it became clear that the German media relies heavily on the Wikipedia, without citation, of course. And this is not just the more yellow press, many newspapers printed the name.

The risks? Don't rely on Wikipedia information for current events. And find a second, preferably offline, source for your information if you are doing serious journalism. Especially if you are doing print.

[1]

http://de.wikipedia.org/w/index.php?title=3DKarl-Theodor_zu_Guttenberg&oldid=3D56419545

[2]

http://de.wikipedia.org/w/index.php?title=3DKarl-Theodor_zu_Guttenberg&oldid=3D56439344

[3]

Genealogischen Handbuch des in Bayern immatrikulierten Adels, Band 17.

Neustadt, Aisch, 1988

[4]

<http://www.bildblog.de/5695/wie-ich-freiherr-von-guttenberg-zu-wilhelm-machte/>

with picture document of the Bild front page

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Internationale Medieninformatik (from 1.4.2009 HTW Berlin), Treskowallee 8, 10313 Berlin +49-30-5019-2320 weberwu@(f)htw-berlin.de [http://www.f4.f\)htw-berlin.de/people/weberwu/](http://www.f4.f)htw-berlin.de/people/weberwu/)

✂ Re: Control-Alt-Eject? French Navy grounded (Leshner, [RISKS-25.56](#))

CBFalconer <cbfalconer@yahoo.com>

Fri, 20 Feb 2009 23:26:21 -0500

... From this I conclude that France is using Windows in its military. I thought nobody other than the US (and possibly the UK) were so foolish.

<http://cbfalconer.home.att.net>

✂ Capital One Phishing Warning is dangerous

"Marc Auslander" <marcausl@gmail.com>

Sat, 21 Feb 2009 16:00:53 -0500

I got an e-mail alert from Capital One that a new message was in my account. The message was a boilerplate warning that a phishing attack on Capital One was in progress. Unfortunately, the email alert was sent by a third party which Capital One uses for this purpose. Capital One does not have an SPF record for the sender, but is using SPF. GMAIL correctly marks this as a phishing letter and throws it into SPAM. If you try to read it you get the big bright GMAIL phishing warning!

So I try to tell Capital One they have a problem. Their response is advice

on how to turn the warning off! So much for their anti-phishing campaign.

Re: The mystery of 'Ireland's worst driver' (Cantrell, [RISKS-25.57](#))

Bernard Lyons <bernard.lyons@mac.com>

Sat, 21 Feb 2009 00:25:16 +0000

Ireland doesn't yet have credit-card style licenses (they've been coming Real Soon Now for several years), but we've had the tri-fold licenses with standardised numbered fields for well over a decade. Mine is one.

It defies belief that any Garda doesn't know how to figure out a driving license - no matter what it looks like - or establish someone's name from other documentation. Their internal performance rating depends on it, amongst other things.

Further, Polish people have been working in Ireland since at least the late 1970's to my personal knowledge. They just didn't suddenly appear from nowhere. So 50 members of An Garda Siochana making the same mistake stretches credulity.

It's far more likely to be a problem with their PULSE system, perhaps to do with data entry. It's known to be inflexible, and there were several expensive investigations into poor design and cost overruns before it went live.

Something about this story doesn't add up.

Re: Hiding in plain sight

"Phil Smith III" <lists@akphs.com>

Sat, 21 Feb 2009 09:38:59 -0500

Jeremy Epstein <jeremy.j.epstein@gmail.com> wrote about a product with an asterisk in the middle between two common words, making it almost impossible to find using search engines.

IBM has done something similar: the hardware line once known as AS/400, then iSeries, then System i, is now known simply as "i", making it beyond impossible to find. I can't imagine what their marketroids were thinking.

Bounds checking in C

"Andrew Koenig" <ark@acm.org>

Sat, 21 Feb 2009 12:36:14 -0500

There have been a number of claims in RISKS recently that bounds checking is impossible in C. These claims are false. In fact, there was a software product (Centerline) available for a number of years that checked bounds in C programs at run time.

However, out-of-bounds array references are far from the only run-time transgressions in C programs that are both common and difficult to check. Another such is referring to memory after it has been freed.

Such problems are exacerbated by the fact that at one time (before approximately 1980), freeing memory was guaranteed not to affect its contents--it was not until the next time you tried to allocate memory that any values would be changed. This phenomenon led to code such as this:

```
struct node *p = listhead;
while (p) {
    free(p);
    p = p->next;
}
```

Even worse, the original definition of `realloc` *required* the memory being reallocated to be freed first; if you tried to call `realloc` with memory that had not been freed, it would *always* allocate new space and copy the contents of the old memory block into the new space, relying on you to free the old block in the fullness of time.

Thus the original definition of `malloc` and `free` encouraged, and sometimes required, programmers to use pointers to unallocated memory. This requirement made checking for legitimacy very difficult indeed.

The definition of `free` and `realloc` were eventually changed to say that `free` was permitted to destroy the contents of the memory being freed, and that `realloc` could (and should) accept the address of a block that was already allocated, and would free the block after copying its contents elsewhere. That change at least made it plausible to check the legitimacy of pointers.

✂ The risks of Silver Bullets (was Tony Hoare: "Null References")

*Michael Smith <emmenjay@zip.com.au>
Sun, 22 Feb 2009 18:34:29 +1100*

Ah! If only we had the right programming language, then we could write robust software.

I have heard that refrain since the early eighties as I developed software in FORTRAN, BASIC, COBOL, C, C++ Pascal, Prolog and various assemblers, 4GLs, 5GLs and more. It remains, as it has always been, garbage.

You can write robust code in almost any language and can write garbage just as easily.

We have known for many years how to write robust software. We do not do so for one reason: cost. We can write junk software much more cheaply than the good stuff and nobody wants to pay the extra cost.

1. We skimp on training our programmers and architects. Maybe you can teach yourself <\$PROGRAMMING_LANGUAGE> in 30 days (or whatever) but it takes many years to learn quality software engineering.
2. We rush through the specification phase. Stakeholders are too busy to give time to nailing down requirements. Sometimes we skip this stage altogether.
3. We skimp on the design phase. Frequently we just start coding with no thought of a proper architecture. Even when we do a design phase it is with mobile requirements and a short deadline.
4. We skimp on testing. We don't have adequate test specs. We don't have well trained testers. And the pressure to ship, so that we can book some revenue, is overwhelming.

We chose not to produce quality software because all those things cost money and we'd rather make do with the cheap alternative.

If we produced a word processor with almost zero bugs, an intuitive user interface and excellent performance, but it cost \$50,000 per copy, we would not have a top seller.

Though if every company summed all the cost of crashed and buggy software, bad products and training to manage poor interfaces, I wonder if it is still a bargain.

Michael J Smith <emmenjay@zip.com.au>

Re: Tony Hoare: "Null References" (Franklin, [RISKS-25.56](#))

*"Steven M. Bellovin" <smb@cs.columbia.edu>
Sat, 21 Feb 2009 14:29:35 -0500*

If we're going to take Hoare's name in vain, let me point people to his Turing Award lecture from 1980:

The first principle was security: ... A consequence of this principle is that every occurrence of every subscript of every subscripted variable was on every occasion checked at run time against both the upper and the lower declared bounds of the array. ... I note with fear and horror that even in 1980, language designers and users have not learned this lesson. In any respectable branch of engineering, failure to observe such elementary precautions would have long been against the law.

And novelty? Circa 1966, I knew a magic incantation (in Fortran II, using some platform-specific subroutines) to interfere with the ability to do a

soft reboot. (The machine in question was an SDS 920; as I recall, it didn't even have any disk drives.)

Re: Tony Hoare: "Null References" (Ables, [RISKS-25.57](#))

*Dimitri Maziuk <dmaziuk@bmrwisc.edu>
Sat, 21 Feb 2009 13:01:01 -0600*

In this particular case I have to disagree: I believe with C it's not so much "hysterical raisins" as "nails and screwdrivers".

What gets lost in advocacy hype is that creators of a programming language usually have a specific set of problems (real, perceived, transient or fundamental) in mind and are thinking of ways to solve them. The programmers get to choose what language to write in and it's their job to understand available tools and choose the right one for the task at hand. For some definition of "right".

C was created to write portable operating systems in, not end-user applications. "Portable" is the big plus when you consider potential customers and all the different computing platforms they may have been using. The lack of proper high-level facilities is a minus, but what choice do we have -- the language that has `std::string` and `std::vector`? Up until recently those weren't portable, and judging from past experience there's a good chance they'll revert to that state again when the next version of C++ standard comes out.

Of course nowadays 99.9% of the target user base is using an x86-based platform with mice and graphical user interfaces, so one would expect the focus to shift to the tool that built-in GUI and runs on all x86 computers: Java virtual machine. Which has a whole lot of its own shortcomings and I'm sure 20 years down the track we'll read all about them in RISKS.

Re: Tony Hoare: "Null References" (Ables, [RISKS-25.57](#))

*Randy Saunders <R.Saunders@ieee.org>
Sat, 21 Feb 2009 16:19:45 -0500*

Not everyone in the "olden days" was as trusting as King Ables in [RISKS-25-57](#). In the 1970's the Multics implementors at MIT and Honeywell were developing a time-sharing system. The language was PL/1, though that's a minor difference. Pointers that pointed to segments had bounds, and you got a hardware exception if you violated them. In PL/1 this was reflected as part of a higher level construct called the refer extent of a structure.

The problem programmers happened alone the scene later on, with microprocessors and "personal" computers. The professional computer scientist was displaced by hordes of self-taught C coders.

I hope to live to see today's programming paradigms replaced, I'm on my third round of "what where those idiots thinking?"

Randy Saunders, JHU Applied Physics Lab +1.240.228.3861 R.Saunders@IEEE.org

✉ Related to blacklists for antispam

De Vries Duane <duanedv@earthlink.net>

Sun, 22 Feb 2009 12:10:25 -0500

This may be pure coincidence but it struck me as very odd. I use Earthlink as my E-mail provider. I have the 'spam' setting set to put all suspicious things into a 'spam folder' which I look at every few days (as opposed to them automatically being deleted). During the U.S. presidential campaign, I would frequently find E-mail from 'Democratic' candidates AND conservation groups in this folder. Not once did I find any E-mail from Republican candidates in this folder. I flagged the Democrat and conservation E-mails as 'not spam' which supposedly sent copies to Earthlink to figure out why they were improperly marked as spam. However, this kept up until AFTER the election was over. Then all my mail was delivered correctly. I'm not accusing Earthlink of anything duplicitous but I did find it curious.

Duane De Vries, Retired, ex-computer geek, practicing curmudgeon

✉ Re: Dates of birth are not unique identifiers

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

Sun, 22 Feb 2009 11:08:09 -0800

> Steven J Klein asked, "Why not use the social security number, which is guaranteed to be unique?"

In California, Civil Code Section 1798.85 generally prohibits the use of Social Security numbers as identifiers, especially for Internet services. This law is the result of numerous instances where Social Security numbers were not adequately protected from improper disclosure, resulting in identity theft. Of course, this law cannot be enforced against services based outside of California.

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

✉ Re: USAA Web site follies (Klein, [RISKS-25.57](#))

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

Sat, 21 Feb 2009 18:47:57 -0500

Preventing siblings with the same birthdate from being entered via the Web site seems like a reasonable precaution, especially given that there is an easy fallback, i.e., calling and giving the information over the phone. On the other hand, I acknowledge that I might see it differently if I had been thus inconvenienced.

Steven Klein's story about his problem with the USAA Web site brings to mind a problem I had with the site last week which might be of interest to RISKS readers.

I was entering the information on the Web site for myself and my wife, when I found listed in my wife's profile a "parent" whose name most certainly was not the name of one of my wife's parents. I sent USAA a message about this through their Web site, and they confirmed that the "parent" had been added to my wife's profile in error and they had removed it (I was not able to remove it myself through the Web site).

I don't know what precautions USAA has in place to prevent such "errors" (e.g., do their member numbers have a checksum digit to detect mistyping?), but something definitely seems wrong with the fact that someone was able to attach a complete stranger to my wife's record in their database.

Re: The Trouble with Trusting Trend Micro ([RISKS-25.57](#))

*"Jonathan Kamens" <jik@kamens.brookline.ma.us>
Sat, 21 Feb 2009 18:39:18 -0500*

Kevin Way's description of the absurd hoops demanded by Trend Micro before removing static IP ranges from their DNS blocklists reminded me of an incident which occurred during the 2008 U.S. Presidential Campaign.

I was an active volunteer for one of the candidates and thus regularly received bulk emailings and email list messages from his campaign. At some point during the campaign, the flow of email petered out to nothing. Eventually I realized that this was because one of the blocklists my mail server was configured to use, NJABL, had the candidate's mail servers listed as spam sources.

Only registered users of the candidate's site and donors to his campaign were added to his mailing lists, and every single message sent by the candidate had a working unsubscribe link at the bottom of it, so the candidate could not reasonably be categorized as a spammer. I contacted both the maintainers of NJABL and the webmasters of the candidate's site, pointing out that the site was listed in the blocklist and suggesting that perhaps one or more people who opposed the candidate had falsely reported his site as a spam source as a political dirty trick.

I received no response from either NJABL or the webmasters, and after waiting in vain for several days for the problem to be fixed, I threw up my hands and removed NJABL from the set of blocklists my server was using. I'm now using only the Spamhaus ZEN blocklist, which apparently has somewhat

more rigorous procedures than NJABL.

The implications of being able to use DNS blocklists as weapons in political campaigns are quite frightening.

#Alert TA09-051A -- Adobe Acrobat and Reader Vulnerability

Monty Solomon <monty@roscom.com>

Fri, 20 Feb 2009 21:56:43 -0500

National Cyber Alert System
Technical Cyber Security Alert TA09-051A
[PGN-excerpted: Please see the cited item in case of updates.]

Adobe Acrobat and Reader Vulnerability

Original release date: February 20, 2009

Last revised: --

Source: US-CERT

Systems Affected

- * Adobe Reader version 9 and earlier
- * Adobe Acrobat (Professional, 3D, and Standard) version 9 and earlier

Overview

Adobe has released Security Bulletin APSB09-01, which describes a vulnerability that affects Adobe Reader and Acrobat. This vulnerability could allow a remote attacker to execute arbitrary code.

I. Description

Adobe Security Bulletin APSB09-01 describes a memory-corruption vulnerability that affects Adobe Reader and Acrobat. Further details are available in Vulnerability Note VU#905281. An attacker could exploit these vulnerabilities by convincing a user to load a specially crafted Adobe Portable Document Format (PDF) file. Acrobat integrates with popular web browsers, and visiting a website is usually sufficient to cause Acrobat to load PDF content.

II. Impact

An attacker may be able to execute arbitrary code.

III. Solution

Disable JavaScript in Adobe Reader and Acrobat [...]
Prevent Internet Explorer from automatically opening PDF documents [...]

IV. References

* Adobe Security Bulletin apsa09-01 -
<<http://www.adobe.com/support/security/advisories/apsa09-01.html>>

* Securing Your Web Browser -
<http://www.us-cert.gov/reading_room/securing_browser/>

* Vulnerability Note VU#905281 -
<<http://www.kb.cert.org/vuls/id/905281>>

The most recent version of this document can be found at:

<<http://www.us-cert.gov/cas/techalerts/TA09-051A.html>>

Feedback can be directed to US-CERT Technical Staff. Please send email to <cert@cert.org> with "TA09-051A Feedback VU#905281" in the subject.

For instructions on subscribing to or unsubscribing from this mailing list, visit <<http://www.us-cert.gov/cas/signup.html>>.

Produced 2009 by US-CERT, a government organization.

Terms of use:

<<http://www.us-cert.gov/legal.html>>

Revision History

February 20, 2009: Initial release



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 59

Sunday 1 March 2009

Contents

- [Iridium and Cosmos satellites collide](#)
[Ken Knowlton](#)
- [When your files are online and you aren't](#)
[Hiawatha Bray](#) via [Monty Solomon](#)
- [Man charged \\$81 billion for a fuel fill-up](#)
[Peter Gregory](#)
- [Computer "Glitch" Results in \\$31 billion Error](#)
[Malcolm Pack](#)
- [Best Buy swindled for \\$31 million by chip supplier](#)
[Jim Haynes](#)
- [Google Gaffe: Gmail Outage Shows Pitfalls of Online Services](#)
[Jonathan B Spira](#)
- [Power outage disables power failure alarm](#)
[Jim Haynes](#)
- [UK building society online account open to DOS attack](#)
[Andy Repton](#)
- [Wikileaks cracks key NATO document on Afghan war](#)
[Jeff Nye](#)
- [Re: Hiding in plain sight](#)
[Al Macintyre](#)
[Mark Feit](#)
[Phil Smith III](#)
[Steve Lamont](#)
[Marcos H. Woehrmann](#)
- [Urban legends in RISKS](#)
[David Guaspari](#)
- [Info on RISKS \(comp.risks\)](#)

✶ Iridium and Cosmos satellites collide

<KCKnowlton@aol.com>

Sun, 22 Feb 2009 20:31:24 EST

Reported in **The Week** magazine 27 Feb 2009 and its website: Two satellites have collided in orbit, destroying both, creating two large clouds of debris: an old Russian Cosmos satellite and an Iridium satellite (one of a fleet of communication satellites launched by Motorola in the late 90s and early 2000s). Nicholas Johnson of NASA said "This is the first time we've ever had two intact spacecraft accidentally run into each other."

http://www.theweek.com/article/index/93177/Iridiums_satellite_collision

When your files are online and you aren't (Hiawatha Bray)

Monty Solomon <monty@roscom.com>

Fri, 20 Feb 2009 11:12:02 -0500

Hiawatha Bray, When your files are online and you aren't, **The Boston Globe**, 19 Feb 2009

Funny thing about cloud computing - it's useless at 35,000 feet.

In cloud computing, you rely on applications running on the Internet instead of on your personal machine. So rather than write a file in Microsoft Corp.'s Word or Excel, you might use Google Docs. This online suite from Google Inc. features word processor and spreadsheet programs and stores your documents in the Internet cloud.

But online documents aren't much use when you're disconnected from the Internet - like when you're flying. Airline companies are beginning to deploy on-board Wi-Fi service, but it'll be a couple of years before it is generally available. And even on the ground, you can't always find an Internet connection.

With earthbound copies of critical files, you can work on them as needed and upload any changes to the Net, first chance you get. And if you work on multiple computers, you can share updated files with all your other machines.

If you're a Google Docs user, get a copy of Gears. This free program, available at gears.google.com, lets you download your Google-generated documents onto your computer. Work with them even when you're offline, and when you log in again, Gears uploads your modified documents to the Google Docs Internet server, so your up-to-date document is available on any Internet-connected machine.

Gears isn't just for Google Docs fans; it works with other cloud computing services, including Zoho, a rival online document editing service, and Google's Gmail messaging service. You can plow through your e-mail on the plane, write up replies, then transmit them once you're back online.

But Gears has its limitations. For instance, you can edit your existing Google Docs when offline, but you can't create new ones. Besides, Gears gives you no easy way to share multimedia files, like video, audio, and digital photographs. ...

http://www.boston.com/business/technology/articles/2009/02/19/when_your_files_are_online_and_you_arent/

Man charged \$81 billion for a fuel fill-up

Peter Gregory <petergregory@yahoo.com>

Fri, 27 Feb 2009 12:20:25 -0800 (PST)

Washington State resident Juan Zamora filled his Camaro at a local Conoco station using his PayPal debit card just as he does every week. The pump registered \$26, but his account was debited \$81,400,836,908 instead. The cause of the error has not yet been identified.

http://seattletimes.nwsourc.com/html/localnews/2008790918_webbigbill27.html

Peter Gregory, CISA, CISSP, DRCE | Security and Risk Manager
petergregory@yahoo.com | www.peterhgregory.com | Biometrics For Dummies

Computer "Glitch" Results in \$31 billion Error

Malcolm Pack <risks.2009.02.25@potnoodle.net>

Wed, 25 Feb 2009 10:40:59 +0000

<http://news.bbc.co.uk/1/hi/business/7909627.stm>

UBS in \$31bn bond order mistake

A Japanese unit of Swiss banking group UBS has mistakenly placed an order for 3 trillion yen (\$31bn) of bonds.

UBS Securities Japan said the error was caused by a glitch in its computer system, and that it had asked the Tokyo Stock Exchange to cancel the order.

According to reports, this request has now been granted by the stock exchange."

[...]

This is not the first time that a UBS unit has given the Tokyo Stock Exchange an incorrect order.

In 2001, a UBS business mistakenly issued an order to sell shares in Japanese advertising firm Dentsu. USB subsequently had to buy more stock in Dentsu in order to honour the order.

This and a number of incidents by other firms saw the Tokyo Stock Exchange introduce new rules in 2007 that allow the cancellation of large-scale erroneous orders.

Increasingly we see new mitigations being put into place for bad outcomes from risks that ought, by right, to be mitigated at source. A little sense-checking on such trades - don't sell more than you own (or significantly more, if automated short trading is to be allowed), don't spend more than a billion Yen in a single automated transaction, that kind of thing - should not be beyond the wit of the programmers, nor the wit of the bank's risk managers.

✂ Best Buy swindled for \$31 million by chip supplier

*Jim Haynes <jhhaynes@earthlink.net>
Tue, 24 Feb 2009 11:19:10 -0600 (CST)*

Deerfield couple swindled \$31 million from Best Buy, federal court documents say; \$2.75 million used to buy the land and build their house were 'the proceeds of fraud'

Jeff Long, Chicago Tribune, 24 Feb 2009

<http://www.chicagotribune.com/business/chi-best-buy-fraudfeb24,0,6558363.story>

✂ Google Gaffe: Gmail Outage Shows Pitfalls of Online Services

*"Jonathan B Spira" <jspira@basex.com>
February 26, 2009 3:51:52 PM EST*

[From Dave Farber's IP list]

I didn't realize the number of Gmail users was so large until the outage.

"Google's Gmail system was down for 2.5 hours earlier this week, the sixth such outage in the past eight months. It isn't unusual that an e-mail system crashes, but most such occurrences are limited to one organization. When Gmail, a service Google touts to businesses as more reliable and easier to use than Microsoft Exchange and Lotus Notes/Domino, goes down, it makes headlines - as well it should. " ...

Just imagine if all of the phone lines to your office failed - not today but ten years ago, when the telephone was the most important means of communication (along with fax, I should add). That's what Gmail's users were facing on Monday. The silence was deafening..."

<http://www.basexblog.com/2009/02/26/google-gaffe-gmail-outage-shows-pitfalls-of-online-services/>

Jonathan B. Spira, CEO and Chief Analyst, Basex, Inc. 8 www.basex.com

✂ Power outage disables power failure alarm

*Jim Haynes <jhhaynes@earthlink.net>
Tue, 24 Feb 2009 11:05:24 -0600 (CST)*

An item in Santa Cruz Sentinel for 24 Feb 2009 tells of a power outage affecting pumps that provide water to a storage tank, causing the tank to run dry. "Power also was cut to the communication lines designed to alert the district to a problem."

UK building society online account open to DOS attack

*Andy Repton <risks@pteron.org>
Tue, 24 Feb 2009 15:04:16 +0000*

Recently, I needed to access my online account with the Nationwide building society. I'd recorded my secret number in an encrypted store, but had mistyped one digit. After three attempts to log in to my account I received the message that my account was now locked and I should re-register and wait for up to 5 days for the new details to appear through the post.

I called the internet helpline and they confirmed that there is nothing they can do, the system forces the lockout and indeed I had to re-register. I pointed out the potential denial of service aspects of this approach but the only response was "Why would anyone do that?"

Wikileaks cracks key NATO document on Afghan war

*Jeff Nye <jpn213@gmail.com>
Fri, 27 Feb 2009 11:24:08 -0500*

The best encryption in the world won't help you if your passphrase sucks.
Jeff

- ----- Forwarded message -----

From: Wikileaks Press Office <press-office@wikileaks.org>
Date: Fri, Feb 27, 2009 at 08:11
Subject: [WIKILEAKS] Wikileaks cracks key NATO document on Afghan war
To: wl-press@lists.riseup.net

WIKILEAKS EDITORIAL
Fri Feb 27 13:10:25 GMT 2009

"Wikileaks cracks key NATO document on Afghan war"

Wikileaks has cracked the encryption a key NATO document relating to the war in Afghanistan. The document, titled "NATO in Afghanistan: Master Narrative", details the key facts and themes NATO representatives are to give--and to avoid giving--to the world press.

Among the revelations, which we encourage the public to review in detail, is Jordan's presence as secret member of the US lead occupation force.

The encrypted document, from October, and believed still to be current, can be found on the Pentagon Central Command website "oneteam.centcom.mil":

<http://oneteam.centcom.mil/isc/Shared%20Documents/NATO%20Master%20Narrative.doc>

The password is "progress", which perhaps reflects the Pentagon's desire to stay on-message, even to itself.

Jordan is a US backed middle eastern monarchy, and historically the CIA's closest partner in its extraordinary renditions program. In Jordan, "the practice of torture is routine", according to a January 2007 report by UN special investigator for torture, Manfred Nowak.

NATO spokespersons are instructed conceal the country's involvement in the ISAF coalition. Publicly, Jordan withdrew in 2001. It does not appear on the current (Feb 13, 2009) NATO list of ISAF member states:

http://www.nato.int/isaf/docu/epub/pdf/isaf_placemat.pdf

Some other sensitive instructions on what not to say are:

* Any decision on the end date/end state will be taken by the respective national and/or Alliance political committee. Under no circumstances should the mission end-date be a topic for speculation in public by any NATO/ISAF spokespeople.

* The term "compensation" is inappropriate and should not be used because it brings with it legal implications that do not apply.

* Any talk of stationing or deploying Russian military assets in Afghanistan is out of the question and has never been the subject of any considerations.

Only if pressed: ISAF forces are frequently fired at from inside Pakistan, very close to the border. In some cases defensive fire is required, against specific threats. Wherever possible, such fire is pre-coordinated with the Pakistani military.

Altogether four classified or restricted NATO documents of interest on the Pentagon site were discovered to share the 'progress' password. Wikileaks has decrypted the documents and released them in full:

* http://wikileaks.org/wiki/NATO_Media_Operations_Centre:_NATO_in_Afghanistan:_Master_Narrative%2C_6_Oct_2008

* http://wikileaks.org/wiki/ISAF_Afghanistan_Theatre_Strategic_Communications_Strategy%2C_25_Oct_2008

* http://wikileaks.org/wiki/NATO-ISAF_Afghanistan_Strategic_Communications_External_Linkages%2C_20_Oct_2008

* <http://wikileaks.org/wiki/NATO->

[ISAF_Strategic_Communications_Ends%2C_Ways_and_Means%2C_slide%2C_20_Oct_2008](http://wikileaks.org/wiki/ISAF_Strategic_Communications_Ends%2C_Ways_and_Means%2C_slide%2C_20_Oct_2008)

Re: Hiding in plain sight (PHSIII, [RISKS-25.57](#))

Al Macintyre <macwheel99@wowway.com>

Sun, 22 Feb 2009 23:02:00 -0600

IBM does the same thing with all of its specialized kinds of computer lines ... business, scientific, mainframe, servers. There is a move afoot to merge IBM "i" business line with the "p" scientific, so soon there will be a few less types of IBM systems.

Supposedly if you know about IBM's fantastic systems, you don't need to use a search engine to find out about them. But the reality is that there's lots of non-IBM companies serving the IBM market place, and it can be hard to locate them when IBM changes its product naming so often, into generic words and letters.

There are conspiracy theorists that speculate IBM is killing off a line of computers deliberately. They are high performance, unhackable, have never been hit by malware, upwardly compatible, incompatible with Microsoft, so they don't have to be replaced as often. IBM would sell a lot more computers if they broke down as often as the competition.

On the 400, now i5/OS, an asterisk is pervasive. names starting with asterisk are like keywords, functions, types of objects names ending with asterisk are wild cards

Re: Hiding in plain sight (PHSIII, [RISKS-25.57](#))

Mark Feit <mfeit@notonthe.net>
Mon, 23 Feb 2009 05:45:37 -0500

> I can't imagine what their marketroids were thinking.

Me either, but "IBM i" and "System i" (without the quotes) return the right page as the first hit when put into Google.

I can only imagine how difficult it must be for British secret agents to find Q when they need new gadgets. :-)

Re: Hiding in plain sight ([RISKS-25.58](#))

"Phil Smith III" <lists@akphs.com>
Mon, 23 Feb 2009 08:14:04 -0500

Re: Al Macintyre:

Mmm, no, they haven't done the same with the other lines. There are four IBM hardware lines:
System p -- Power (AIX machines)
System x -- x86 (Intel)
System z -- mainframes

i -- which do indeed use Power hardware, same as System p. That's the convergence, and I've seen the speculation that IBM is trying to kill i5/OS.

(I write about this stuff for trade rags, and I also just checked <http://www-03.ibm.com/systems/i/>, <http://www-03.ibm.com/systems/p/>, <http://www-03.ibm.com/systems/x/>, and <http://www-03.ibm.com/systems/z/>.)

They are inconsistent, though: the i page just calls it "i", System p and System x use those names, and the mainframe page says "Mainframe" and then mentions both "System z" and "IBM z Can Do IT". But the mainframe is the world I mostly live in, and I've been assured by Poughkeepsie that "System z" is the real name; the latter usage is just shorthand.

Or perhaps I misunderstood what you were saying?

P.S. Mark Feit noted that "... 'IBM I' and 'System I' (without the quotes) return the right page as the first hit when put into Google."

Interesting (and an improvement over a few months ago). I wonder if that took search engine placement work, or if Google is just smarter? Of course, in any OTHER case (such as searching in a document), the "i" nomenclature is still impossible to find.

✉ Re: Hiding in plain sight (PHSIII, [RISKS-25.58](#))

*Steve Lamont <spl@ncmir.ucsd.edu>
Wed, 25 Feb 2009 17:13:43 -0800*

IBM i. Easy to find.

Typing "IBM i" into the search field in Google gives as the first hit <http://www.ibm.com/systems/i/>

✉ Re: Hiding in plain sight (PHSIII, [RISKS-25.58](#))

*""Marcos H. Woehrmann" <marcosw@gmail.com>
Mon, 23 Feb 2009 10:05:01 -0800*

The original name of Archy was "The Human Environment" which was officially shortened to "THE". Needless to say it wasn't searchable either. Though it appears it now would be; searching for "THE" on Google brings up theonion.com as the top hit. However, Yahoo! might be the winner in this odd contest, it brings up a the band "The The" as the second result, just after "The N Network" (which is a website for teens and has nothing to do with the pejorative term for persons of African descent).

✉ Urban legends in RISKS

David Guaspari <davidg@atc-nycorp.com>

Mon, 23 Feb 2009 11:14:00 -0500

A recent RISKS posting referred (in a throwaway aside) to "the ex-President who'd never seen a grocery store scanner." As this newsgroup is populated by rational people glad to have even trivial errors corrected, I'll note out that the story of Bush 41's supposed amazement at seeing a scanner has been pretty thoroughly debunked. Snopes has a detailed discussion:

<http://www.snopes.com/history/american/bushscan.asp>

David Guaspari, ATC-NY, 33 Thornwood Drive, Suite 500, Ithaca NY 14850
(607) 266-7114 davidg@atc-nycorp.com

[Also noted by Brent Krupp. PGN]



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 60

Friday 6 March 2009

Contents

- [Health-care: The Computer Will See You Now](#)
[Anne Armstrong-Cohen](#) via PGN
- [Turkish Airline disaster and the Altimeter](#)
[Turgut Kalfaoglu](#)
- [Britain's Chinook helicopters unusable for years due to software](#)
[Mark Brader](#)
- [Conviction in attempted 229 million GBP theft](#)
[Mark Brader](#)
- [Altimeter and autopilot possible cause of plane crash near Schiphol](#)
[Ben Blout](#)
- [Normal Accidents and Black Swans](#)
[Jerry Leichter](#)
- [Building-Security-In Maturity Model: BSIMM](#)
[Gary McGraw](#)
- [An insider attack... in the police](#)
[Jeremy Epstein](#)
- [Diebold delete button for erasing audit logs](#)
[Kim Zetter](#) via PGN
- [Re-examining assumptions](#)
[Jerry Leichter](#)
- [Credit card #s plucked out of air at FL Best Buy](#)
[David Ian Hopper](#) via Dave Farber
- [Worldpay ATM system breached](#)
[Neil Youngman](#)
- [Re: Iridium and Cosmos satellites collide](#)
[Ivan Jager](#)
- [Risk Contained In RISKS Posting?](#)
[David E. Price](#)
- [Re: Wikileaks cracks key NATO document on Afghan war](#)
[Charles Wood](#)
- [Re: Google Gaffe: Gmail Outage ...](#)
[Alain Picard](#)
- [Verizon curiosity](#)
[Peter Zilahy Ingerman](#)
- [Info on RISKS \(comp.risks\)](#)

✂ Health-care: The Computer Will See You Now (Anne Armstrong-Cohen)

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

Fri, 6 Mar 2009 12:59:32 PST

In considering one of our classic double-edged RISKS swords, Anne Armstrong-Cohen in today's issue of **The New York Times** discusses the risks of doctors having **less** involvement with patients as a consequence of the push to develop paperless health-care that is heavily dependent on online facilities. Yes, electronic medical records (EMRs) can avoid illegible handwriting and enable doctors to share patients' records more easily. "In short, the computer depersonalizes medicine. It ignores nuances that we do not measure but [that] clearly influence care. ... A box clicked unintentionally is as detrimental as an order written illegibly -- maybe worse because it looks official. ... So before we embrace the inevitable, there should be more discussion and study of electronic records, or at a minimum acknowledgment of the down side. A hybrid may be the answer -- perhaps electronic records should be kept only on tablet computers, allowing the provider to write or draw, and face the patient. The personal relationships we build in primary care must remain a priority, because they are integral to improved health outcomes. Let us not forget this as we put keyboards and screens within the intimate walls of our medical homes."

As always, human intelligence is critical. So are well-designed and easily usable human interfaces that allow human intelligence to prevail -- especially in the presence of erroneous online information!

✂ Turkish Airline disaster and the Altimeter

turgut kalfaoglu <turgut@kalfaoglu.com>

Thu, 05 Mar 2009 09:58:44 +0200

As you probably know, a Boeing 737-800 with 127 passengers and seven crew crashed near Schiphol airport in the Netherlands, killing nine and injuring many others. The details are starting to emerge that the left altimeter was faulty, and that from 2000 feet, it notified the autopilot that they were suddenly at -8 feet. Autopilot immediately cut the power to the engines, stalling it in mid air. Due to the weather, the pilots had to rely on their instruments and could not see what was wrong until the stall indicators came on.

What I would like to know is that how software testing is done at Boeing. I fail to see how the software would not spot a problem and carry out the landing:

- 1) If the two altimeters are reading very different readings,
- 2) If one of the altimeters switches from reading 2000 feet to -8 feet instantly,
- 3) If one of the altimeters reads a negative number?

If the software had warned them, I'm sure these pilots would not have died, along with several passengers.

[Somewhat similar comment from Ben Blout. Also, there has been extensive discussion on this topic around the Net. Having two of anything always suggests the problem of what to do what they disagree. (Les Lamport's paper on Buridan's Ass comes to mind [[RISKS-10.44](#)].) That problem suggests that having THREE might be a better strategy, and seeking consensus. But sanity checking is also a good idea, and trusting absurd readings is not wise. Perhaps the biggest problem is again that autopilots and people are not infallible, but the lack of synergy between the two can be even more debilitating. PGN]

Britain's Chinook helicopters unusable for years due to software

Mark Brader

Thu, 5 Mar 2009 18:55:40 -0500 (EST)

http://news.bbc.co.uk/2/hi/uk_news/7923341.stm

It says here that in 1995 the Royal Air Force ordered Mark 3 Chinook helicopters "with a modified cockpit computer system in order to reduce costs. But the aircraft have never been able to fly..." and the plan now is to downgrade them to Mark 2 models for use next year.

Mark Brader, Toronto, msb@vex.net

Conviction in attempted 229 million GBP theft

Mark Brader

Thu, 5 Mar 2009 19:08:54 -0500 (EST)

This case was briefly noted by Tom Van Vleck in [Risks-23.81](#) in 2005. In that year, British police made a number of arrests in the case of a plan to steal huge sums of money from accounts at the British office of the Sumitomo Mitsui bank by transferring it into their accounts in various countries. Their basic trick was to plant keylogger software on the bank's computers, exposing login names and passwords to them.

The Hollywood-like plan failed only because they got the details wrong as they attempted the invalid transfers totaling 229,000,000 pounds sterling.

The case is in the news again now because the ringleader has now been convicted.

http://news.bbc.co.uk/2/hi/uk_news/7909595.stm
http://news.bbc.co.uk/2/hi/uk_news/7926294.stm

Mark Brader, Toronto, msb@vex.net

✂ Altimeter and autopilot possible cause of plane crash near Schiphol

Ben Blout <bdbnew@MIT.EDU>

Wed, 4 Mar 2009 12:08:45 -0500 (EST)

I read an interesting article from the BBC, headlined "Altimeter 'had role' in air crash". In reporting a news conference conducted by Dutch Safety Board chairman Pieter van Vollenhoven, the article reads in part:

...the plane had been at an altitude of 595m (1950ft) when making its landing approach to Schiphol airport. But the altimeter recorded an altitude of around ground level. The plane was on autopilot and its systems believed the plane was already touching down, he said.

The automatic throttle controlling the two engines was closed and they powered down. This led to the plane losing speed, and stalling.

I am surprised that an autopilot would throttle back engines based on only one instrument, the altimeter. I would have assumed additional criteria would need to be met - perhaps having weight on the landing gear.

The article raises other interested points, and can be found here:

<http://news.bbc.co.uk/2/hi/europe/7923782.stm>

✂ Normal Accidents and Black Swans

Jerry Leichter <leichter@lrw.com>

Wed, 4 Mar 2009 12:03:14 -0500

We've often discussed Perrow's "Normal Accidents" on this list. Fundamentally, Perrow characterizes systems along two axes: Degree of coupling and complexity or linearity vs. nonlinearity of interactions. Systems in the fourth quadrant - high coupling, nonlinear - are inherently prone to disasters.

In his article at:

http://www.edge.org/3rd_culture/taleb08/taleb08_index.html

Nassim Nicholas Taleb has a different but related analysis. (He concentrates on failures in the financial markets, but the lessons are much broader.) The dimensions Taleb identifies are nature of the probability distribution (thin-tailed versus heavy or unknown tails) and complexity of the cost, particularly the sensitivity of the cost of finding yourself in a particular state for small variations in that state. Taleb's 4th quadrant is characterized by systems in which rare events dominate the total cost. In these systems, statistical methods fail: We don't actually know the probability distributions; we can only estimate them from events. But getting estimates of rare events requires huge numbers of observations.

Because most of the cost is in rare events, which never make it into our observations, any estimate we make of expected costs is meaningless.

The connection to Perrow's work is through the complexity of cost axis. Both of Perrow's characterizations of his fourth quadrant go directly to this complexity. Along the other axis, Perrow is specifically talking about rare, outlier accidents - not the small, common, and understood problems that systems are designed to handle, and do handle for years at a time with no problems. In eliminating those, he gets exactly to the rare but costly events.

Taleb has a book out - The Black Swan - which I haven't read - but intend to after reading this article. -- Jerry

#Building-Security-In Maturity Model: BSIMM

*Gary McGraw <gem@cigital.com>
Thu, 5 Mar 2009 06:17:51 -0500*

the BSIMM model went live today ahead of schedule <http://bsi-mm.com>. and the *WSJ* broke the story: <http://blogs.wsj.com/digits/2009/03/04/new-effort-hopes-to-improve-software-security/>

The first phase in our endeavor to bring some science to software security is at a close. Our science-y approach started with some anthropology several months ago. We asked nine firms to tell us about their software security group (SSG), its inception, its activities, and the success it has achieved. The result is the Building Security In Maturity Model authored by Gary McGraw, Brian Chess (Fortify), and Sammy Migues, which is out for public use at <http://bsi-mm.com>.

Please take a look at BSIMM. If you run or are active in a software security group, look at it like a yardstick. Consider the activities listed versus what your organization is doing.

We want to emphasize that we could not have done this without active participation by the nine firms we interviewed. The data in BSIMM is their data. Data from the interviews we conducted were used to build the model from scratch. The examples included with the activities are real examples. After building BSIMM, we scored each organization using it. The individual scorecards, although unreleasable, are fascinating. They provide a unique glimpse into how local culture, perhaps as much or more than business imperatives, drive the approach to software security. Suffice it to say, for now, that the carrot is once again shown to be mightier than the stick.

As a final note, BSIMM is a data-driven model. The model will improve when more real-world data are added.

sammy, gem and brian

✂ An insider attack... in the police

<Jeremy Epstein>

Fri, 06 Mar 2009 08:34:39 -0500

Even police forces aren't immune from insider attacks that compromise personnel information.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9129023>

Jaikumar Vijayan, *Computerworld*, 5 Mar 2009

In a demonstration of how no organization is immune from insider threats, the New York City Police Pension Fund (PPF) office is notifying about 80,000 current and former NYPD officers of the potential compromise of their personal information after a civilian employee recently stole storage media containing the data.

A sample alert posted on the pension fund site identified the individual as an employee of the PPF and said he was arrested Feb. 27 after a security breach at one of the pension fund's disaster recovery sites.

At the time of the arrest, the individual was discovered to be in possession of "certain business records" containing data about retired and active members of the NYPD. The compromised data included Social Security numbers, names, addresses and bank account information, the statement said.

"Even though the property was recovered, we cannot assure you that the information was not compromised," the statement said regarding why it was sending out the notifications. [...]

Jeremy Epstein, Senior Computer Scientist, SRI International
1100 Wilson Blvd, Suite 2800, Arlington VA 22209 703-247-8708

✂ Diebold delete button for erasing audit logs (Kim Zetter)

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

Wed, 4 Mar 2009 11:03:24 PST

Kim Zetter, Diebold Voting System Has 'Delete' Button for Erasing Audit Logs
Wired News, 3 Mar 2009

An investigation by California's secretary of state into why a product made by e-voting system vendor Premier Election Solutions (formerly Diebold Election Systems) lost about 200 ballots in Humboldt County during the U.S. presidential election revealed the presence of a "clear" button in some versions of the machine's Global Election Management System (GEMS) software that allows someone to permanently erase audit logs from the system. The

secretary of state's report says the logs "contain--or should contain--records that would be essential to reconstruct operator actions during the vote tallying process." The proximity of the clear button to the "print" and "save as" buttons raises the risk of the logs being erased accidentally, and the system provides no warning to operators of the danger of clicking on the button. Premier/Diebold retained the button despite an apparent warning from a system developer, and though the button was removed from subsequent iterations of the software, the version with the button is still used in three California counties and other U.S. states. The report says that under the voting system standards "each of the errors and deficiencies in the GEMS version 1.18.19 software...standing alone would warrant a finding by an Independent Testing Authority (ITA) of 'Total Failure' (indicated by a score of 1.0) had the flaw been detected." The California report's findings bring up issues about the auditing logs on voting systems made by other vendors, and about what course of action states that use the Premier system will follow now that they are aware that their voting software fails to produce a sufficient audit trail to guarantee the integrity of an election.

<http://blog.wired.com/27bstroke6/2009/03/ca-report-finds.html>

Re-examining assumptions

*Jerry Leichter <leichter@lrw.com>
Mon, 2 Mar 2009 18:47:06 -0500*

A recent paper submitted to Usenix HotSec:

"Do Strong Web Passwords Accomplish Anything?" -

http://www.usenix.org/events/hotsec07/tech/full_papers/florencio/florencio.pdf

re-opens points that "we all know the answers to". In this case, the question is just how strong a password has to be. It's accepted wisdom that passwords must be taken from large character sets and be long. However, the attacks that led to these conclusion were off line: That is, the attacker could try passwords at any speed for as long as he wanted (for example, by stealing the file of hashed passwords and then generating passwords and computing their hashes). However, this is not a realistic attack against web-based systems. An on-line guessing attack can be detected and blocked easily.

In fact, the most dangerous attacks - phishing, keylogging -- are no less effective against strong passwords than against weak ones. There is an attack (bulk guessing against all accounts) that can be useful against weak passwords, but the authors show that there are alternative defenses that are probably much better from a UI point of view than requiring stronger passwords.

It's all too easy to remember the results of papers without remembering the assumptions that went into them. In a field such as computer science where order-of-magnitude changes in parameters critical to results are common over fairly short periods of time, this is a dangerous way to work!

Credit card #s plucked out of air at FL Best Buy

David Ian Hopper <imhopper@gmail.com>

March 2, 2009 9:09:03 AM EST

[From Dave Farber's IP]

Clever. Try walking into your local Best Buy with an iPhone, and see what networks you can hop on...

<http://www.bestbuy.com/store/550/>

- - - - -

The following advisory applies to customers who shopped at the Best Buy located at 1880 Palm Beach Lakes Blvd in West Palm Beach, FL in November and December 2008.

An employee at Best Buy's 1880 Palm Beach Lakes Blvd in West Palm Beach, FL allegedly stole credit card information during November and December 2008 using an unauthorized personal device. Best Buy learned of the theft on Jan. 5, 2009. With the cooperation and assistance of store management, the employee was identified and taken into federal custody by the Secret Service on Jan. 7, 2009. That person is no longer employed by Best Buy.

Although none of Best Buy's electronic systems were compromised by this former employee's actions, Best Buy believes that approximately 4,000 people could have been affected by this law enforcement authorities and all relevant payment card brands have been notified of the incident and Best Buy is fully cooperating with all investigations.

In addition, Best Buy is sending letters to customers who may have been affected by this fraudulent activity, notifying them of the situation and encouraging them to review their account statements and monitor their credit reports. ...

Archives: <https://www.listbox.com/member/archive/247/=now>

Worldpay ATM system breached

Neil Youngman <n.s.youngman@btinternet.com>

Mon, 2 Mar 2009 08:15:22 +0000

This security breach at Worldpay appears to have 2 unique features. First, the crackers had sufficient access to raise the limits on payment cards and second, the cracked cards were used in a coordinates attack by footsoldiers in 49 different cities worldwide.

http://www.bankinfosecurity.com/articles.php?art_id=1197

<http://www.bizjournals.com/atlanta/stories/2008/12/22/daily24.html>

<http://www.itpro.co.uk/609793/royal-bank-of-scotland-s-worldpay-hit-by-atm-scam>

Re: Iridium and Cosmos satellites collide (Knowlton, [RISKS-25.59](#))

Ivan Jager <aij+@mrph.org>

Thu, 5 Mar 2009 15:15:09 -0500

I found this article gives quite a bit of insight into how the satellites could have crashed: <http://www.thespacereview.com/article/1314/1>

Basically, the US military keeps their high accuracy tracking data secret, and the low accuracy data they publish didn't even make Iridium 33 and Cosmos 2251 look like a likely collision. Of course, even the high accuracy data only gives a probability, and the military doesn't have enough resources (mostly constrained by trained personnel) to analyze all possible collisions. Even if they did, it seems Iridium didn't even have a plan in place for dealing with likely collisions. Or perhaps they were more like, "Lalala, we're going to pretend that can't happen because we can't afford to deal with it." And of course there's the Russians, who left a derelict satellite where it would intersect many other orbits, and launched both satellites which collided. Basically, everyone involved is to blame to some extent.

I guess sometimes it is cheaper to take risks and let everyone else deal with the consequences.

Risk Contained In RISKS Posting?

"David E. Price, SRO, CHMM" <price16@lnl.gov>

Thu, 5 Mar 2009 09:37:16 -0800

Be careful which active links you click, even in RISKS postings.

The recent posting about the Wikileaks cracking of encryption of documents found on a U.S. Pentagon server <Wikileaks cracks key NATO document on Afghan war> highlights a risk in quoting URLs without adding precautionary statements.

The original posting contained a statement saying "Altogether four classified or restricted NATO documents of interest on the Pentagon site were discovered to share the 'progress' password. Wikileaks has decrypted the documents and released them in full:" followed by URLs to pages which I assume lead to downloadable documents.

I assume this statement means that at least one the linked documents was/is classified, but it may indicate only a suggestive teaser. (No, I didn't follow the links...)

Anyone who works in a classified environment and downloads one of the purported classified documents could have contaminated their unclassified computer system (and associated proxy servers and spam scanning servers, etc.) with classified information.

This would result in a large isolation and cleanup effort, requiring at least the local sub-net to be taken offline for some time.

David E. Price SRO, CHMM, Senior Consequence Analyst for Special Projects, Global Security, Lawrence Livermore National Laboratory, P. O. Box 808 L-073 Livermore, CA USA 94551

[The burden of the typical unclassified RISKS reader is not on the reader. The burden on a classified reader reading something classified from a supposedly unclassified system is clearly not on The Risks Forum. There is also a fundamental gap -- the folks who worry about multilevel security (for confidentiality and nonleakage) should also be worried about some form of multilevel integrity (as in the lack of dependence on less trustworthy people, programs, software, hardware, systems, networks, and so on, especially in the presence of malware, phishing, ... PGN]

Re: Wikileaks cracks key NATO document on Afghan war

Charles Wood <j.charles.wood@gmail.com>

Tue, 3 Mar 2009 18:42:03 +0900

(Nye, [RISKS-25.59](#))

I just wonder if this is NATO experimenting with viral marketing?

When you read the documents, you see a press group that has developed the current text of 'the message' including all the good things they want to say about themselves. It is basically propaganda for the troops and for release to interested journalists. They include a small bit about what they don't really like to discuss, but for which a standard and reasonable answer is supplied.

When you look at it, there is nothing in these documents that you wouldn't get doled out continuously at innumerable press briefings and troop briefings. Nothing secret, nothing key, nothing new - rather boring press conference material really.

What is new and unique (I think - though perhaps earlier examples exist?) is that the documents have been trivially located and cracked and the entire message passed to every interested reader on the Internet.

Far more people than ever was likely now know exactly the official NATO position and thoughts.

You don't suppose someone in NATO marketing had a bright idea do you?

I have a theory that in this life, 99% of bad stuff is caused by stupidity

and 1% by malevolence. In this case I'm prepared to even the odds quite a lot.

Re: Google Gaffe: Gmail Outage ... (Spira, [RISKS-25.59](#))

*Alain Picard <Dr.Alain.Picard@gmail.com>
Mon, 02 Mar 2009 20:41:35 +1100*

Except, of course, that e-mail is a store and forward medium, and for me a 2.5hr delay on e-mail is perfectly acceptable. Perhaps the risk is in people using a technology for purposes for which it is not intended? (in this case, as a substitute for instant messaging.)

Gmail didn't lose any mail. For me, having a hosted e-mail system where my mail doesn't get lost and is easily searchable certainly seems worth a 2.5hr inconvenience every few months. It certainly seems better performance than every other in-house system I've used.

Now, once someone hacks and takes over your GMAIL credentials, getting your account back.... now that's a risky proposition! :-)

#

*"Peter Zilahy Ingerman, PhD" <pzi@ingerman.org>
Tue, 03 Mar 2009 15:36:40 -0500*

Subject: Verizon curiosity

>Date: Tue, 03 Mar 2009 14:05:18 -0600 (CST)
> From: Verizon Online, High Speed Internet Customer Care Team
> <verizon.update.2@verizon.net>
> Subject: Important information about your High Speed Internet Service

Dear Verizon High Speed Internet Customer,

On MARCH 17TH, 2009, Verizon will be performing network maintenance that will temporarily interrupt your Verizon High Speed Internet service for approximately one hour between the hours of 11:00 pm and 8:00 am local time. If the lights on your modem are blinking after 8:00 am local time on November 21st, please power cycle your modem. To power cycle your modem, please do the following:

- Use the power switch on the back of the modem to turn off the power
- Wait 60 seconds
- Turn the modem back on.
- Wait 45 seconds to allow the modem to synchronize to the server, and then
- try reconnecting to the Internet.

Note: If your modem doesn't have an on/off switch, unplug the modem from its power source instead of turning the modem off.

We apologize for any inconvenience this may cause and appreciate your cooperation.

Thank you for choosing Verizon Online as your High Speed Internet service provider.

Verizon Online Customer Care Team

[They probably also did this LAST November 20, and just changed THAT date to March 17, but forgot to change the November 21 date. PGN]

[Yup ... exactly what happened, I think. I remember a similar message a few months ago. But I thought that Risks might enjoy it. I've stirred them up for an explanation, and will let you know. PZI]



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 61

Sunday 29 March 2009

Contents

- [DNA contamination led to serial-killer illusion](#)
[Mark Brader](#)
 - [Announcing your crime in a chat room may interfere with it](#)
[Mark Brader](#)
 - [You have won \\$\[2^32-1\]/100, no wait, we mean nothing](#)
[Mark Brader](#)
 - [Student dead 2 months, told to improve attendance](#)
[Mark Brader](#)
 - [Phantom Serial Killer](#)
[Dave Mulkey](#)
 - [E-voting In Ireland](#)
[PGN](#)
 - [Fairfax County Virginia voting glitches](#)
[Jeremy Epstein](#)
 - [Arose by any other name: was Diebold](#)
[PGN](#)
 - ["Security by obscurity Considered Harmful" -- especially for voting](#)
[John Sebes](#)
 - [Malware installed at manufacturer on Diebold ATMs](#)
[Toby Douglass](#)
 - [Driver Says GPS Unit Led Him to Edge of Cliff](#)
[Richard Grady](#)
 - [The Information Security Debt Clock](#)
[Gunnar Peterson](#)
 - [Google translations used for phishing attacks against ISPs](#)
[Gadi Evron](#)
 - [Economics of Finding and Fixing Vulnerabilities in Distributed Systems](#)
[Gunnar Peterson](#)
 - [ZOL downtime and emergency maintenance](#)
[Andrew Yeomans](#)
 - [We seem to be going over the top on "risks", forgetting about some realities](#)
[Fred Cohen](#)
 - [Info on RISKS \(\[comp.risks\]\(#\)\)](#)
-

#DNA contamination led to serial-killer illusion

Mark Brader

Fri, 27 Mar 2009 22:25:57 -0400 (EDT)

When police in Germany, Austria, and France were able to DNA-match evidence from six homicides (including the killing of policewoman Michele Kiesewetter in the town of Heilbronn) and dozens of other crimes, they naturally concluded that a multiple murderer was at work -- one who acquired the nickname "The Phantom of Heilbronn".

But then one of the matches, which seemed unlikely, was retested... and the second time it came back negative.

Now it seems that in fact the only connection between the crimes is that when collecting DNA from the evidence, cotton swabs from the same manufacturer (Greiner Bio-One) were used. Unused swabs were tested and a few were found to have the same woman's DNA on them; she worked at the company that did the packaging. Greiner says that they were only supposed to be sterile swabs for medical use, and were not guaranteed to be free of DNA.

Of course, if this happened in a work of fiction, it'd turn out that the woman actually had committed one of the early crimes and then taken advantage of her job to deliberately contaminate the swabs in order to divert suspicion. But be that as it may, the consequences for law enforcement are not going to be pleasant.

See:

<http://news.bbc.co.uk/2/hi/europe/7966641.stm>

<http://www.dw-world.de/dw/article/0,,4129872,00.html>

<http://www.time.com/time/world/article/0,8599,1888126,00.html>

http://www.google.com/hostednews/ap/article/ALeqM5iEPt22F_xcWatGRrX5ludZOsm5AD976HRM00

#Announcing your crime in a chat room may interfere with it

Mark Brader

Sat, 21 Mar 2009 00:56:53 -0400 (EDT)

When J.P. Neufeld, an Internet chat-room moderator in Montreal, saw someone posting an announcement that he was shortly going to set fire to a school in Norfolk, England, he took it seriously, first communicating with the poster and then phoning the Norfolk police. They acted quickly and in less than an hour a 16-year-old was arrested near the school while carrying matches and "what is believed to be a flammable liquid".

<http://www.cbc.ca/world/story/2009/03/20/concordia-student-forum-norfolk.html>

http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20090320/school_threat_090320/20090320?hub=TopStories

<http://www.eveningnews24.co.uk/content/news/story.aspx?itemid=NOED19%20Mar%202009%2008:52:47:223>

#You have won $\$(2^{32}-1)/100$, no wait, we mean nothing

Mark Brader

Thu, 19 Mar 2009 19:11:47 -0400 (EDT)

It was reported recently that at an Ontario casino in December, a slot machine flashed its lights and displayed a message to the effect that "You have won \$42.9 million" (Canadian, about \$34 million US). The gambler, Paul Kusznirowicz, had 5 minutes to be ecstatic before being told the machine had malfunctioned and he hadn't won anything. (They did give him some dinner coupons.) In fact, according to the Ontario Lottery and Gaming Corp., its highest possible payout was \$9,025 (Canadian). This amount was not marked on the machine, but there was a notice that nothing was payable in case of malfunction. Kusznirowicz is suing, so there probably won't be any further details unless the case makes it to court.

In a followup story today, Ryerson University computer professor Sophie Quigley suggests that the number -1, as a 32-bit 2's complement signed integer, was interpreted as an unsigned integer in cents: \$42,949,672.95. "A casting error", as she put it. (Not necessarily in the strict C sense.)

Incidentally, the Toronto Star ran the followup next to a story about Marie Douglas-David, who is involved in a divorce case and allegedly claims that "she cannot live on \$43 million" (US). The paper put the two pieces side by side under a common headline: "Two very different \$43 million questions".

<http://www.cbc.ca/consumer/story/2009/03/17/slot.html>

<http://www.thestar.com/News/Ontario/article/604035>

[2nd URL corrected in archive copy. Item also noted by David Magda. PGN]

#Student dead 2 months, told to improve attendance

Mark Brader

Wed, 25 Mar 2009 21:15:51 -0400 (EDT)

Macclesfield High School (near Manchester, England), threatened to ban Megan Gillan from their prom if her attendance did not improve. This was unlikely to happen, as Megan had died two months before. The girl's parents, still very much grieving, were "floored".

Megan had been removed from the school's "main database", but was still listed "in a different part of the computer system" that allows letters to be sent to parents of former students.

See: <http://news.bbc.co.uk/1/hi/england/manchester/7963081.stm>

Or if that URL isn't long enough, try:

<http://www.telegraph.co.uk/education/educationnews/5049001/School-apologises-after-letter-warns-parents-over->

dead-schoolgirls-attendance.html

✂ Phantom Serial Killer

"Mulkey, Dave" <Dave_Mulkey@fis.edu>

Sun, 29 Mar 2009 14:24:16 +0200

Amusingly, German police have been searching in vain for a phantom serial killer, apparently responsible for 40 murders. Unfortunately, they were led astray by DNA "evidence" that resulted from using contaminated cotton swabs to collect DNA evidence. They had all been packed by an employee who refused to wear rubber gloves, so here DNA appeared to be scattered all over the country at various crime scenes. Police used the swabs against written advice in the accompanying product instructions that said the swabs were unsuitable for forensic use. Fortunately nobody was injured or arrested as a result. Here is an article from *Time* with the details:

<http://www.time.com/time/world/article/0,8599,1888126,00.html>

If your German is good, you can read this:

http://www.focus.de/politik/weitere-meldungen/phantom-von-heilbronn-des-raetsels-loesung-war-das-wattestaebchen-aid_384841.html

✂ E-voting In Ireland

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

Tue, 17 Mar 2009 13:14:23 PDT

The [Irish] government finds itself in a deep hole because of the purchase and storage of thousands of electronic voting machines. It should stop digging. What had seemed like a good idea, way back in 1999, has turned out to be an unmitigated disaster. The initial waste of public money on the purchase of this dangerously insecure system has been compounded by the establishment of long-term leases of up to 30 years for the storage of machines in controlled environments.

John Gormley is the fourth minister for the environment to have responsibility for the mess. And because there is no question of the machines being used in the forthcoming local and European elections, or thereafter, he should call a halt to the madness. An estimated 52 million euros was spent on voting machines by Noel Dempsey and by his successor, Martin Cullen, in spite of the objections and concerns of the opposition parties. And when a special Commission on Electronic Voting found it was easy to bypass the proposed security system in 2004, the machines were put into storage at an annual cost of about 700,000 euros.

This public waste must end at a time when everybody is being asked to tighten their belts. The cost of storing these machines will amount to 3.5

million euros by the end of this year. And because contracts ranging from 20 to 30 years were entered into on behalf of the State, penalties are likely to be imposed for an early buy-out. The Government should not continue to engage in what is a face-saving exercise.

Ireland is the only country in Europe that holds out a vague prospect of using this technology. Last year, the Dutch government decided to abandon the system because of its inherent vulnerability. Last week, the supreme court in Germany ruled that the Nedep system -- which we also purchased -- breached its electoral laws. It found that the control measures required would not be achieved by a print-out of votes. The ability to recheck votes was more important than early election results. It was not saying a final No to electronic voting, just that the current generation of voting machines was unsatisfactory.

Ten years ago, the replacement of pencils and ballot papers by machines was seen as a badge of modernity. But technology was not sufficiently advanced to guarantee security of the new system. In spite of that, Fianna Fáil ministers ignored the views of computer experts and ploughed ahead. Now that the Netherlands and Germany have abandoned the project on security grounds, the Government should bow to the inevitable. [*The Irish Times*, 29 Mar 2009] <http://www.irishtimes.com/newspaper/opinion/2009/0317/1224242944297.html>

✂ Fairfax County Virginia voting glitches

*Jeremy Epstein <jeremy.j.epstein@gmail.com>
Thu, 12 Mar 2009 13:59:54 -0400*

A special election in Fairfax County Virginia had some voting machine problems. A very close race had one DRE (out of about 50 in use) that printed suspicious results. Coverage at <http://www.washingtonpost.com/wp-dyn/content/article/2009/03/11/AR2009031101675.html> and <http://www.washingtonpost.com/wp-dyn/content/article/2009/03/10/AR2009031002068.html>

I spent the day after the election observing the canvass process at the invitation of the Democratic candidate (but the campaign did not supply me with any information, nor did they pay me). Details of my findings are at <http://abgordia.blogspot.com>. While a winner was eventually declared, there are two unexplained problems: in one, the "zero tape" printed before the polls opened (which is supposed to show that there are no votes recorded) showed that the total votes was 0, of which 3 were for the Republican, 2 for the Democrat, 1 for the independent, and 1 write-in. Or mathematically, $3+2+1+1 = 0$. No one (other than me!) seemed all that concerned that this shows something was *clearly* wrong, because they were able to get the machine to print the (purported) ballots, and count those by hand....

The risks? When the machine can print something that looks reasonable, the people making the decisions are willing to overlook clear problems (as in the math error). Instead of treating the math error as an indication that there's a deeper problem, they wrote it off as an unexplained glitch - "my

car didn't start the first time I turned the key, but it started fine the second time, so I guess there's no problem". That may be true, or it may be the starter getting ready to fail.

✂ Arose by any other name: was Diebold

*"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 18 Mar 2009 9:10:09 PDT*

Premier Election Solutions (formerly Diebold Election Systems) admitted in a California hearing on 17 Mar 2009 that the audit logs in its tabulation software do not record significant events that occur on the system during an election, such as the deletion of votes. The company acknowledged that the problem exists with every version of its tabulation software. [Source: Kim Zetter, Wired.com]

<http://blog.wired.com/27bstroke6/2009/03/diebold-admits.html>

[See also Shannon McElyea in Dave Farber's IP, citing Diebold Admits Audit Logs in ALL Versions of Their Software Fail to Record Ballot Deletions, <http://www.bradblog.com/?p=6995>]

✂ "Security by obscurity Considered Harmful" -- especially for voting

*"E. John Sebes" <jsebes@osdv.org>
Wed, 25 Mar 2009 21:17:04 -0700*

No "Security By Obscurity" for Voting, Please
John Sebes' blog, 25 Mar 2009, <http://osdv.org/blog>

I have to confess to being appalled by the number of times recently that I have heard people talk about potential benefits of "security by obscurity" for voting systems. It's one of those bad old ideas that just won't die: if you hide the inner workings (source code) of a complex device (a voting system), that makes it harder for an adversary to break (hack, steal elections). With regard to voting systems, of course, the issue gets all muddled up with vendors' fears of compelled source code disclosure, but setting that aside, the proposition is simply this: a voting system is "more secure" (whatever that means) if the source code is not public. Or as one election official said to me recently, "We've been schooled to think that making the code public would give up the keys to the system" (my paraphrase) and ensure that a voting system could be hacked to steal elections (my inference).

Wow. It's quite the fallacy, but staying power of the "Security by Obscurity" idea is impressive; despite being completely discredited among digital security professionals, the idea just won't stay dead. But please, don't take my word for it. Despite a couple decades in the security biz, I'm also an open source advocate. Instead, take a look at what security experts (the real ones, not the folks that call themselves "security experts") have

to say about it. You can find several good thought pieces on the blog <<http://www.schneier.com/blog>> of applied cryptographer and author Bruce Schneier. You can find a range of pieces on the topic in the Risks Forum <<http://www.risks.org>> and <<http://www.csl.sri.com/users/neumann/#3>>. For brief and general summary of the topic (including open source), PGN's IEEE <<http://www.ieee.org>> Science and Policy piece "Robust Nonproprietary Software" <<http://www.csl.sri.com/neumann/ieee00.pdf>> provides a pithy and balanced viewpoint. For an entertaining bit of myth-debunking, try "Security by Insecurity" <<http://www.csl.sri.com/users/neumann/insiderisks.html#161>>. And for specificity to voting, try Peter's testimony <<http://www.csl.sri.com/neumann/calsen06.pdf>> to the State of California invited by CA's Secretary of State, Debra Bowen <<http://www.sos.ca.gov/admin/bio.htm>>. [TNX! PGN]

But I can't resist a couple closing thoughts. First is my little theory that closed systems are actually easier to crack. Consider the Windows OS, unsurpassed for widespread adoption, proprietary software, and history of security vulnerabilities. I am not MS-bashing here! My point is that where there is an attractive target (and Windows is #1), the bad guys have all the needed grist for the mill, without the source code!. They have the running software itself; they have some information about the software's interfaces; and they have many years of experience to guide efforts to find weak points. They have a cookbook! They don't need an electron microscope to examine the atoms and reverse engineer the target. In fact, if the source code were available, then it might actually be more work to wade through it to find security vulnerabilities.

Lastly, I want to get back to election technology generally, and voting systems in specific. I do not believe that current voting systems benefit from security by obscurity. I also do not believe that disclosure of the source code would be beneficial. Independent reviewers have found many reasons for security concerns, and the vendors underline those concerns by fear-mongering around the issue of security vs. openness. Where vendors admit security problems, and yet do not display willingness to fix known problems, disclosure doesn't help because new knowledge about problems and fixes is irrelevant if the fixes don't get done. But just as disclosure wouldn't help, it also would not hurt - despite the fear mongering. Plenty enough is already known about vulnerabilities of these systems, and the bad guys have plenty of info - including the ability to buy voting machines on E-bay and reverse engineer to heart's content.

So basically, disclosure of current systems is a matter of indifference to me in terms of security benefit or detriment - there is neither. But it really bothers me when people are misled into thinking that secret computing equals secure computing. It's not so, and especially not for election technology, which should be open and transparent, not for security, but for trust and public confidence in the results -- that is, the selection of those public servants who govern our public life.

The recent New York Times editorial "Still Broken" is well worth the read, especially for its significant focus on dysfunction.

Malware installed at manufacturer on Diebold ATMs

*"Toby Douglass" <trd@45mercystreet.com>
Wed, 18 Mar 2009 22:56:36 +0100 (CET)*

http://www.goodgearguide.com.au/article/295924/criminals_sneak_card-sniffing_software_diebold_atms

Diebold has some of its ATMs fabricated in Russia.

A break-in occurred. These ATMs run Windows. Malware, which captures card details, was installed. Pretty sophisticated stuff, too.

Sophos report they believe the code has been in circulation (whatever that means) since November 2008.

The fix was apparently released Jan 2009.

I'm starting to think cash-from-a-bank may make a comeback.

[Here's an excerpt from another report on this subject: "Security firm Sophos reported this week that it received three samples of a trojan that was customized to run on Diebold-manufactured cash machines in Russia, said Graham Cluley, Sophos' senior security consultant. The malware was able to read card numbers and PINs -- then when the attacker returned to the ATM, he inserted a specially crafted card that told the machine to issue him a receipt containing the stolen information." PGN]

<http://www.scmagazineus.com/ATM-malware-appears-Diebold-issues-security-update/article/129059/>

Driver Says GPS Unit Led Him to Edge of Cliff

*Richard Grady <richard@richbonnie.com>
Thu, 26 Mar 2009 00:28:27 -0700*

A British driver blamed his GPS navigation unit for leaving his car teetering on the edge of a 100-foot cliff in Doncaster, South Yorkshire, after following its instructions. (He was stopped by running into a wire fence.)

<http://www.foxnews.com/story/0,2933,510495,00.html>

The Information Security Debt Clock

*"Gunnar Peterson" <gunnar@visi.com>
Tue, 24 Mar 2009 19:24:19 +0000*

If you want to architect Web security like it's 1995, then the Information Security Debt Clock is for you. The Information Security Debt Clock tracks the time since the Web security architecture based on Network Firewalls and SSL was first deployed:

http://1raindrop.typepad.com/1_raindrop/2009/03/information-security-debt-clock.html

According to c2com, Technical Debt occurs when "During the planning or execution of a software project, decisions are made to defer necessary work...The list can grow quite long, with some items surviving across multiple development cycles."

As of right now its been approximately 4,863 days since SSL 1.0 was added into Netscape in Dec. 1995.

Google translations used for phishing attacks against ISPs

Gadi Evron <ge@linuxbox.org>

Wed, 25 Mar 2009 13:46:01 +0100

In this e-mail message I'd like to discuss two subjects:

- a. Phishing against ISPs.
- b. Phishing in different languages against ISPs as soon as Google adds a new translation module.

In the past few weeks there has been an increasing number of phishing attacks against clients of Israeli ISPs. I've only seen a few of these, but the local ISPs confirm it's happening across the board.

In all these cases, the phishing e-mail is in Hebrew.

While we have seen ISP phishing and Hebrew phishing before, these attacks started when Google added translation into Hebrew.

Is this a trend? Have other countries (or populations) been targeted when Google added a translation module for more languages?

Notes:

- a. Some Israeli ISPs e-mailed their clients warning against such attacks. Saying they'd never ask for their password, etc.
 - b. While I was certainly heavily involved with phishing originally and even started the first coordination group to deal with the issue, I am somewhat removed from it now, dealing more with phishing/banking Trojan horses.
Can anyone educate me as to how often ISPs get phished, if at all?
 - c. If you get phished, what strategies if any have you taken to prevent the attacks/respond to them/educate your clients? What worked?
 - d. I wonder if these translation misuses could eventually translate into some intelligence we will see in Google security reports, such as on malware.
-

#Economics of Finding and Fixing Vulnerabilities in Distributed Systems

"Gunnar Peterson" <gunnar@visi.com>

Tue, 24 Mar 2009 19:26:29 +0000

The Economics of Finding and Fixing Vulnerabilities in Distributed Systems

Quality of Protection Keynote, Alexandria, VA, October 27. 2008

By Gunnar Peterson

Like many people in this industry, my focus on security was fundamentally altered by Dan Geer's speech "Risk Management is Where the Money Is"[1], there are not many people who can call a ten year shot in the technology business, but Dan Geer did. The talk revolutionized the security industry. Since that speech, the security market, the vendors, consultants, and everyone else has realized that security is really about risk management.

Of course, saying that you are managing risk and actually managing risk are two different things. Warren Buffett started off his 2007 shareholder letter [2] talking about financial institutions' ability to deal with the subprime mess in the housing market saying, "You don't know who is swimming naked until the tide goes out." In our world, we don't know whose systems are running naked, with no controls, until they are attacked. Of course, by then it is too late."

Full talk: http://1raindrop.typepad.com/1_raindrop/2008/11/the-economics-of-finding-and-fixing-vulnerabilities-in-distributed-systems-.html

[This item apparently fell through the RISKS crack last year. Don't forget to include "notsp" in your would-be postings. I'm filtering over a thousand spams a day, and still having to cull through 95% spam after that. The subject line is very important. PGN]

#ZOL downtime and emergency maintenance

Andrew Yeomans <ajv@yeomans.org.uk>

Wed, 25 Mar 2009 21:37:26 +0000

Zimbabwe Internet has been having downtime problems recently, and sent their customers the attached disarming honest e-mail.

(I saw this through a friend of a friend; Mark Taylor has also posted it on <http://marktaylor.blogspot.com/2009/03/only-in-zimbabwe.html>)

Subject: ZOL downtime and emergency maintenance

Dear (name removed)

This is a brief update of our considerable downtime today (Monday 16 March) from about 2pm to 5:30pm. We are also announcing emergency maintenance that

will take us offline from approximately 8pm to 10pm tomorrow (Tuesday 17th March).

Unfortunately every backup system including generators, UPS and routers were totally flummoxed by 2 painters painting the building where our satellite dish is housed. Being diligent men, they decided to remove a junction box to paint behind it. Unluckily that box belongs to Telecontract and houses a fiber optic cable joint connecting to ZOL. This took down not only ZOL, but many ISP connections on the same fiber.

We are operating on a temporary solution now, but to fully repair this damage Telecontract have advised us that they will have to redo the entire joint. This will take approximately 2 hours, and will be done at 8pm on Tuesday 17th March.

We apologize for any inconvenience caused. Sometimes human brilliance just shines through regardless of the best laid plans!

Best Regards, *The ZOL Crew*

***We seem to be going over the top on "risks", forgetting about**

Fred Cohen <fc@all.net>

Sun, 8 Mar 2009 09:04:42 -0700

some realities ([RISKS-25.60](#))

In the latest RISKS digest, I detected several problems with the comments. I thought I would bring them in as a risk of people who talk about risks not being thorough in their exploration of the issues.

> Subject: Health-care: The Computer Will See You Now (Anne Armstrong-Cohen)
> ... So before we embrace the inevitable, there should be more discussion
> and study of electronic records, or at a minimum acknowledgment of the
> down side.

This is no different from paper records - except that the stored and displayed answers can be definitive. The problem comes when the computer records are altered without the informed consent of the doctor who made them.

> A hybrid may be the answer -- perhaps electronic records should be kept
> only on tablet computers, allowing the provider to write or draw, and face
> the patient.

With current technologies, this would be worse than either of the current approaches. Tablets today miss lots of the entries put into them and store dotted lines, misinterpret characters, and so forth - so they will produce more errors with less definitive information on what really happened.

> The personal relationships we build in primary care must remain a
> priority, because they are integral to improved health outcomes. Let us

> not forget this as we put keyboards and screens within the intimate walls
> of our medical homes."

The notion that the computer is somehow less personal than the piece of paper or that the doctor cannot still be a human being because they use a computer seems to me to be flawed.

> Subject: Turkish Airline disaster and the Altimeter
> I fail to see how the software would not spot a problem and carry
> out the landing:
>
> 1) If the two altimeters are reading very different readings,
> 2) If one of the altimeters switches from reading 2000 feet to -8
> feet instantly,
> 3) If one of the altimeters reads a negative number?

Great! So what is the list of ALL of the checks that should be done, how do we generate that list, how long is it, and how do we implement ALL of the possible check processes with adequate reliability and proper failsafes when we can't figure out how to do it for the simple things? Then apply this recursively and tell me all the ways in which just these 3 checks could possibly go wrong, and all the checks we need to check them...

By the way, negative altitude is possible - fly into Death Valley some day.

We seem to have forgotten the "simplicity principle" in security - perhaps because it was removed from the GASSP when the GAISP was put in its place? Perhaps not. But as a rule of thumb, the more checks we put in, the more potential failure modes there are.

> Subject: Normal Accidents and Black Swans

Indeed - Risks readers may also be interested in:

<http://all.net/Analyst/2009-04.pdf>

"Risk management: There are no black swans"

Fred Cohen & Associates tel/fax: 925-454-0171 <http://all.net/>

572 Leona Drive Livermore, CA 94550



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 62

Wednesday 1 April 2009

Contents

- [GPS Outages Feared](#)
[Mike Tashker](#)
- [Conficker](#)
[Ned Potter via PGN](#)
- [A Peering risk](#)
[Chris Leeson](#)
- [Google Calendar as a single point of failure?](#)
[Jeremy Epstein](#)
- [Safety and man/machine interactions: Traffic crossings](#)
[Jerry Leichter](#)
- [The Chinese iTunes Gift Voucher Trick](#)
[Monty Solomon](#)
- [The Police don't send chain letters](#)
[Richard O'Keefe](#)
- [UK considering generalised use of deep packet inspection](#)
[Toby Douglass](#)
- [Software Related Accident: Pipe-Laying Equipment](#)
[David Smith](#)
- [Spam as an indicator of network health](#)
[jidanni](#)
- [When Clouds go Bad: Losing Data in MobileMe](#)
[Nick Rothwell](#)
- [Only allow 1, 2, and 100 year domain name registration](#)
[jidanni](#)
- [Re: ESTA visa waiver online](#)
[Chris J Brady](#)
- [Info on RISKS \(comp.risks\)](#)

✂ GPS Outages Feared

Mike Tashker <tashkerm@transdecsys.com>

Wed, 1 Apr 2009 11:59:21 -0700

In a press conference today (1 April 2009), a spokesman for the U.S. Air Force GPS Wing has confirmed fears that a worldwide outage of GPS service is likely. The current system may reach peak capacity before the launch of the next-generation Global Positioning System Space Segment satellites, known as GPS Block III, in 2014.

"The huge proliferation of civilian hand-held, cellphone, and vehicle-based GPS equipment has taxed available bandwidth on the existing satellite constellation beyond our expectations," said Major Stan Ford Parkinson. "We expect that the transceivers in the Block III satellites will handle the load through 2040. But there's a likelihood of a gap -- a rolling worldwide GPS 'brown-out' -- between now and the first launches."

The Air Force is planning a competitive procurement to study the potentially catastrophic effects on transportation and other industries that could occur as early as 2011. This appears to be a good use of stimulus funds, especially if it stimulates some more far-sighted thinking.

Mike Tashker

Conficker

*"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 26 Mar 2009 9:18:20 PDT*

Ned Potter, Conficker Computer Worm Threatens Chaos
Or Is It Just an April Fool's Joke? Security Groups Unite to Stop It
ABC News <<http://abcnews.go.com>>, 25 Mar 2009
<http://abcnews.go.com/Technology/story?id=7163685&page=1>
[Thanks to Phil Porras for this one. PGN-ed]

Somewhere out there, perhaps in Eastern Europe, perhaps next door to us, a very clever hacker is spreading a sophisticated little computer worm called Conficker <<http://abcnews.go.com/Technology/PCWorld/story?id=6667364>>.

It could make an electronic mess as it spreads from one computer to another, taking over machines and commanding them to do things their users never intended.

"We've got some bad guys out there who are extremely sophisticated," said Merrick Furst, a professor at Georgia Institute of Technology who also chairs an Internet security firm called Damballa. "There are a huge number of machines that might be able to be controlled by people other than the owners of those machines."

Who is behind this computer attack? And what do they want from us? Are they trying to bring the world's computers to a halt? Or is the whole thing just some elaborate April Fool's joke?

"It's not an April Fools prank," said Phillip Porras, a program director at SRI International, a major technology research firm. "We don't know

much about how Conficker is being used. We are not sure why Conficker was built." [... Long item.]

[Also note these, courtesy of Monty Solomon. PGN]
Technical Cyber Security Alert TA09-088A
<http://www.us-cert.gov/cas/techalerts/TA09-088A.html>

Conficker Worm: Help Protect Windows from Conficker
<http://www.microsoft.com/conficker>

The 7 Most Important Things to Know About Conficker
http://blogs.pcmag.com/securitywatch/2009/03/the_most_important_things_to_k.php

Is 'Conficker' Solved? Researchers Develop Scan Tool
<http://www.pcmag.com/article2/0,2817,2344060,00.asp>

A Peering risk

*"Chris Leeson" <Chris.Leeson@atosorigin.com>
Wed, 11 Mar 2009 10:47:00 -0000*

According to **The Register**, a site called "Person Rating" has been launched. where you can - anonymously - enter a person's name and rate them against a set of criteria.

http://www.theregister.co.uk/2009/03/11/person_rating/

The idea is that - as is supposed to happen with Wikipedia - a large number of contributors will even out any "extremes of opinion". Of course, there are a number of risks that regular readers of the forum will be all too familiar with -- for example,

- * Mistaken identity (only identifying by name?)
- * Malicious updates (Wikipedia already has this problem with pages on politicians)
- * Invasion of Privacy/Libel

El Reg is, of course, rather dismissive of the site:

"The idea is that the crowd will weed out extremes of opinion and the result will be an accurate and impartial description of the person concerned - which is about as likely as Greenpeace developing an independent nuclear deterrent."

"Unlike Wikipedia, PersonRatings is intending to make money through advertising, though it seems more likely the service will quietly disappear when the crowds decide they've got better things to do than rate their friends and colleagues for the benefit of targeted advertisers."

At least the site has some sort of plan for making money. It will need it, if and when the libel cases start appearing.

Google Calendar as a single point of failure?

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Thu, 12 Mar 2009 17:45:44 -0400

I keep most of my scheduled appointments on Google Calendar (although it is a pain since I have to be careful not to put proprietary information in my appointment descriptions). I missed a teleconference today, because Google Calendar said it was at 4pm, and when I showed up no one was there. Going back through my notes I discovered the meeting was supposed to be at 3pm, and I had set it up as a recurring event. I then discovered from reading Google Help forums that there are known problems - when Daylight Savings Time started, recurring events got moved either an hour earlier or an hour later, depending on whether you were the originator of the meeting or an invitee.

There was another symptom I noticed - my meeting was at 3pm (Standard time) which got shifted to 4pm (Savings) time. When I tried to change the time back to 3pm, it had no effect - presumably because it thought the meeting was already scheduled for 3pm (Standard). So to make it show up on my calendar at 3pm (Savings), I had to change the schedule to 2pm (Standard).

Once Google fixes the problem, I have to remember to move the scheduled time back again, so I show up at the right time!

RISK? When there's a shared calendar infrastructure and it's buggy, everyone ends up at the wrong time. Something similar happened last year when the US switched to Savings time earlier than in previous years - Microsoft and other vendors rushed out patches to handle the time change.

[Along many other problems discussed here, this one seems to recur. PGN]

Safety and man/machine interactions: Traffic crossings

Jerry Leichter <leichter@lrw.com>

Thu, 12 Mar 2009 15:35:51 -0400

Interesting article about the way people interact with cars around the world:

A quote: England has been particular aggressive about having all kinds of warning mechanisms for both drivers and pedestrians. "But sometimes drivers become so inured to this street 'furniture' they forget to look for people crossing - they forget what it's there for. And a 1970 study by the Institute of Transportation Engineers Journal looking at San Diego accidents found incidents were twice as likely at 'marked crossings' as unmarked crossings. Why? Pedestrians lose a sense of personal responsibility - they think that because they are at an official crossing, they don't need to look where they are going. And then they step out into oncoming traffic."

http://news.bbc.co.uk/2/hi/uk_news/magazine/7939353.stm

The Chinese iTunes Gift Voucher Trick

Monty Solomon <monty@roscom.com>

Thu, 12 Mar 2009 01:09:34 -0500

While there are some legitimate digital music download sites in China - including 9Sky, Top100 and the recently launched Wawawa - digital music is proving to be a tough sell in the P.R.C, partly because of the market dominance of Baidu's free mp3 search. There are, however, people making decent profit in this as yet unmeasurable market: the hackers of Apple's iTunes store gift vouchers and their local agents.

In China's biggest C2C online shopping site Taobao, \$200USD iTunes gift cards are for sale at 17.9 RMB, roughly \$2.6 USD. ...

<http://outdustry.com/2009/03/10/the-chinese-itunes-gift-voucher-trick/>

The Police don't send chain letters

"Richard O'Keefe" <ok@cs.otago.ac.nz>

Tue, 10 Mar 2009 11:39:47 +1300

The #09/#90 mobile phone warning has recently been making the rounds in New Zealand. Apparently some people don't routinely check Snopes.Com. The Sunday *Star Times* issue 8 March 2009 has an article about it on page A6. The point of interest to RISKS readers is this:

the hoax's credibility was bolstered by the fact that it had been circulated by a police staff member ... and carried her New Zealand Police e-mail signature. ... the staff member had forwarded it ... in a personal capacity.

So someone in the Police fell for it, didn't think to check it, and forwarded it to her friends just like anyone else might, but recipients took it as a police endorsement of the content. The same article quotes a spokesman saying

Also, people should remember New Zealand police don't use chain e-mails as a way of putting forward information. Neither do banks or anybody else for that matter.

UK considering generalised use of deep packet inspection

"Toby Douglass" <trd@45mercystreet.com>

Wed, 18 Mar 2009 23:38:36 +0100 (CET)

<http://news.zdnet.co.uk/security/0,1000000189,39629479,00.htm>

"Under the EU Data Retention Directive, from 15 March 2009, all UK Internet service providers (ISPs) are required to store customer traffic data for a year."

This means that right now, **today**, all ISPs in the UK must now store when and who you sent e-mail to or received e-mail from. The e-mail I sent earlier to a friend about this has been logged; that it came from me and when it was sent. In case he's a terrorist. I mean, he's a sixty-five year old retired patent agent, but you can't be too careful. He **does** have a huge beard. Lots of terrorists have huge beards.

So if you're having an affair, best not to communicate via e-mail, because that evidence may be used against you in court. I wish I was kidding, but this is going to happen now. Divorce will occur, the house will be contested, the man or wife may suspect infidelity and the evidence -- all e-mail, who they were sent to and when -- **is now recorded**. Don't need a telescope to see this one coming.

But what's being discussed now is deep packet inspection, which means actually recording the data content - what you actually wrote in your e-mail, the comment you typed on a web-site, etc. So basically EVERY communication you have on the net is recorded by the Government and stored for however many years it is.

So when you write to your wife about the fantastic sex you had last night, it's recorded. When you e-mail a friend about your private sexual fantasies, it's recorded. When you discuss the abuse you experienced as a child from your parents, it's recorded.

For anti-terrorism purposes.

I mean, there's absolutely no evidence whatsoever that you are, or could ever be, under any circumstances WHATSOEVER, a danger to anyone. If there was enough evidence that you could be convicted in a court of law after due process, you would already be in that court of law. That evidence does not exist.

But every detail, everything you write on-line, would be recorded by the State. Monitored. Read by software operated by a stranger, sometimes read by strangers, apparently to see if they can find people writing things which give them away as terrorists.

On a related note, the "e-borders" scheme has started rolling out in the UK.

<http://www.telegraph.co.uk/news/uknews/4987415/All-travel-plans-to-be-tracked-by-Government.html>

Every single person entering or leaving the UK must provide their travel plans. Where they're going, how long for, what for, who with, etc. Recorded, with complete unoriginality, in a huge database for however many years. I haven't read about the judicial violence to be used in the event of non-compliance; presumably you will not be allowed to enter the country.

I'm wondering what will happen if you are **inside** and you want to get **out?** will you be refused exit from the country? or will you be fined? if you keep refusing, what happens then? thousands of pounds worth of fines?

Coverage is expected to be about 60% by the end of this year.

The Government uses judicial violence (fines, prison sentences) to compel obedience to their demands. I am **forced** to have my private affairs violated. On what basis is this done? the only ethical justification can be self-defence, of oneself or on behalf of others. There is no such justification for there is no reason whatsoever to think me a danger to anyone.

To be sure, it may be there a very, very, **very** few (a couple of thousand, out of 61,000,000 people) who are a danger but it cannot be known who they are; but there is a certain level of risk which cannot practically be reduced whilst retaining liberty and freedom.

It is possible to reduce that risk if you eliminate liberty and freedom. Watching everyone, all of the time, reduces that risk and eliminates liberty and freedom.

Historically, we have had a police force and an intelligence service to deal with these problems and have chosen to retain liberty and freedom.

Spending 1,200 million pounds to compel all 61 million people to expose their private affairs and have those affairs permanently stored in a database is both profoundly unfree and also profoundly inefficient. That money would achieve far better results going into the police and intelligence services.

I have to say, I am throughly miserable and depressed by all of this. I have all the material needs and comforts in the world; and I am deeply unhappy. The Government, in my view, has missed the point of existence.

As an aside, I left the UK (for Amsterdam) nine months ago. I will not be returning while these monstrous schemes exist.

Software Related Accident: Pipe-Laying Equipment

*"David Smith" <d.smith@fnc.co.uk>
Mon, 16 Mar 2009 09:19:39 +0000*

IMCA Safety Flash 18/08 December 2008

These flashes summarise key safety matters and incidents, allowing wider dissemination of lessons learnt from them. The information below has been provided in good faith by members and should be reviewed individually by recipients, who will determine its relevance to their own operations.

The effectiveness of the IMCA safety flash system depends on receiving

reports from members in order to pass on information and avoid repeat incidents. Please consider adding the IMCA secretariat (imca@imca-int.com) to your internal distribution list for safety alerts and/or manually submitting information on specific incidents you consider may be relevant. All information will be anonymised or sanitised, as appropriate.

A number of other organisations issue safety flashes and similar documents which may be of interest to IMCA members. Where these are particularly relevant, these may be summarised or highlighted here. Links to known relevant websites are provided at www.imca-int.com/links Additional links should be submitted to webmaster@imca-int.com

Failure of Pipe Handling System Causes Injuries and Fatalities

A member has reported an incident in which the failure of a J-lay pipe-handling system caused two pipes to be dropped, one of which caused injuries to eight people, four of whom died as a result. During pipe-laying operations, a system failure in the hydraulic pipe handling system of the J-lay tower (JLT) caused two quadruple joints being handled at the same time in two different areas of the tower to drop suddenly. Each piece of pipe was 50m long with a diameter of 24* and weighed approximately 20 tons.

Just prior to the incident the pipe-laying operation was stopped. Operators reported a system failure and that the hydraulic power had been lost. Such an occurrence was not particularly unusual and, in line with company procedures, this was investigated immediately. A team of technicians led by the chief electrician tried without success to resolve the problems. After these attempts, a more in-depth analysis was made. It was decided, on the basis of input from the system diagnostics, to perform a memory reset. Following this the system appeared to be running correctly. This was the first time that a full memory reset was requested by the internal diagnostics of the control system during a project operational phase.

Only after all indications that everything was in order and all systems were up and running again was the instruction given to the operator to restart the hydraulic packs. As soon as the hydraulic power packs were started, a loud bang was heard along with the noise of the hydraulic systems. One quadruple joint within the J-lay tower, held by the transfer system, was released and fell about a metre to the upper welding deck. At the same time, the quadruple joint held by the pipe elevator at the top of the J-lay tower was also released from its clamps and the hydraulic safety stop swung away, allowing the pipe to fall the full height of the tower, smashing through the access platform located outside the non-destructive testing/coating station to the lower deck below.

All the people who were injured had been on the access platform which was destroyed. The force of impact caused some of the injured persons to fall down on to the lower deck at the base of the pipe-lay tower and some to be thrown overboard.

Eight persons were injured, two seriously and two slightly. Four of the injured persons died as a result of their injuries.

The primary causes of the incident were found to be:

* Sudden release of the two quadruple joints was caused by a failure in conceptual design of the control system software. The program relevant to the JLT initialising instruction was pre-loaded in the erasable programmable read-only memory (EPROM) of the programmable logic controller (PLC) with the instruction to open all clamps. Members are recommended to investigate the possibility that this could happen to the PLC-based control systems on equipment on their vessels.

* The unnecessary presence and uncontrolled access of working personnel on to the access platform destroyed by the falling pipe exposed personnel to suspended load/dropped object hazard. Following investigation of the incident, a number of corrective actions were put in place by the company:

- The first primary cause was resolved with the removal of the EPROM memories from the system;
- The second primary cause has been addressed by a revision of the vessel and JLT working methodologies; pipe handling activities have been reconsidered through a dropped object philosophy in order to identify mechanical and electrical barriers, additional controls, and new set of operational procedures;

* Electrical controls:

- a number of clamp opening operations were prevented by adding electrical circuit breakers
- all critical sequences will be called by PLC and must be confirmed by operator via electrical push buttons;

* Mechanical controls:

- different systems have been and will be implemented to prevent the vertical pipe drop in any section of the JLT, to restrain lateral pipe movement and fall and to secure the pipe until the internal line up is completed in the upper welding station
- an additional public address system was installed for use during quadruple joint loader lift, and audible and visible alarms for elevator movements
- a safety net was installed underneath the J-Lay tower platforms to guarantee protection against persons falling overboard;

* Procedures were revised in light of the incident, with the following points highlighted:

- all pipe handling activities are to be considered as working under suspended loads
- the immediate area around the JLT is restricted to essential personnel only

- transit and from the JLT to be controlled by dedicated watchmen
- no personnel at all allowed in certain areas during J-lay operation

David H Smith MIET, MBCS, MACMm, Frazer-Nash Consultancy Ltd., Unit 11,
Herrington Barn, Herrington, Dorchester, Dorset DT2 9PU, UK 01305 217910

✂ Spam as an indicator of network health

<jidanni@jidanni.org>

Sun, 08 Mar 2009 19:26:48 +0800

There I was listening to the mosquitoes, when it dawned on me that just like mosquitoes, you just can't stamp out spam e-mail. And just like mosquitoes are a good indicator of environmental health, spam is a good indicator of network health, for the common man.

If there was a Silent Spring spam-wise, you had better check to see if you are really getting all of your legitimate e-mail too!

Likewise, spam phone calls are nature's way of helping you check the circuits.

✂ When Clouds go Bad: Losing Data in MobileMe

Nick Rothwell <nick@cassiel.com>

Sat, 7 Mar 2009 21:29:57 +0000

I've been using Apple's MobileMe synchronised online services for contacts, calendar and file sharing on a number of Macs of varying ages, as well as my iPhone. It works fine under OS X 10.5 (Leopard), but has always seemed a little wobbly under 10.4 (Tiger): contacts occasionally not showing up, bits of the calendar not appearing, to-do items vanishing, that kind of thing. Nothing too worrying, since it's always seemed to be a local display problem under Tiger, and MobileMe's "cloud" has always had a complete set of data.

A couple of days ago, the synchronisation process on an old PowerBook running Tiger went a bit off the rails, and it complained about data clashes, offered options to merge, and so on. I clicked the "overwrite this computer with contents of MobileMe" button, and before I knew it, my entire contact database had been wiped - *poof*. (Well, all except a single contact in Australia.)

In a state of some annoyance, I checked my iPhone. Contact database gone - *poof*.

I checked MobileMe online at www.me.com. Contacts - *poof*.

Well, I will say this for MobileMe: their over-the-air synchronisation does indeed seem to be fast and efficient.

Faced with a Plan A recovery procedure of waiting on hold for a MobileMe Support chat session with Apple (whilst needing to get out to a client site, ideally with a non-empty iPhone), I opted for Plan B: rush upstairs, pull the ethernet cable from the (Leopard) Mac mini, fire up Address Book and export contacts to a file, plug in ethernet, synchronise, re-import contacts, synchronise again.

So, the obvious risks: (i) a rogue client can quickly and efficiently wipe out a dataset in a high-speed, wireless network service, and some devices (like the iPhone) are always linked to it. (ii) A cloud is not a backup. Wipe the data in a cloud, and the wipe will propagate everywhere just like you told it to - there isn't an accessible "previous version" to go back to. See also: "A RAID Device is Not a Backup." (Luckily, I had an inadvertent backup on the Mac mini.)

"But," my inner newbie says, "I'm running the Time Machine backup software on the MacBook Pro. Why don't I just roll back to an earlier Address Book?" Well, despite Apple's claims that Time Machine "backs up everything", it really is just a file backup program, and the contacts and calendar information lives in some invisible database somewhere, out of the backup regime.(*)

So, risk (iii): assuming that a backup program will work on important data which is not obviously file-based.

(*) While I think about it, this might also be due to the fact that I run Apple's FileVault encryption on my home directory, and Time Machine has trouble with this as well: FileVault maps a directory structure to a sparse disk image, so Time Machine can only back up the image when I log out (infrequently), and can only roll back the entire image, not its contents. So, risk (iv): assuming that a transparent piece of technology (on-the-fly encryption) is also transparent to the other tools that you rely on.

Nick Rothwell / Cassiel.com Limited www.cassiel.com

✶ Only allow 1, 2, and 100 year domain name registration

<jidanni@jidanni.org>

Sat, 21 Mar 2009 09:13:11 +0800

I purchased a domain name with the longest expiry period available, 10 years. But I am quite sure that at that time I'll be running around like a chicken with its head cut off.

Any longer than two years and if you're like me or Maxwell Smart, you'll say "The old 'Domain Name Expiring Soon' reminder spam e-mail trick? I'm not falling for that again! Ha, and here's another, purporting to be sent from

my very own cron job. Meet the Delete key!"

Any longer than five years and well, the guy who sold you the domain had better still be in the phone book, because I can't navigate the renewal interface or find the contact form.

Any longer than ten years well he and his company had better be in good health because I forgot the password.

Any longer and ... pass the Geritol.

Sure, transfers among users or registration companies would be fine. Those are all initiated by people who know what they are doing.

But just as the hardware and software of 10 years ago may likely not be plugged in, don't expect the user to be either.

Thus domain name registration should only be allowed for 1,2 and 100 years. OK, I mean lifetime.

Re: ESTA visa waiver online (Michaelson, [RISKS-25.57](#))

*Chris J Brady <chrisjbrady@yahoo.com>
Sun, 15 Mar 2009 14:26:19 -0700 (PDT)*

There are a few other problems with the ESTA website -- which should have been sorted out well before making the system mandatory prior to travel.

My experiences are that it only takes a few minutes to return an authorisation - BUT that it takes more than a few minutes to enter all of the info required. AND the system doesn't seem to remember anything.

Recently I obtained authorisation to visit the USA on Visa Waiver to spend my hard earned credit crunch tourist dollars there. At an Internet Cafe I spent an inordinate amount of time entering all of the info. required by ESTA.

However I could not print anything out at the time. So when I visited a friend's house who had a printer I opened up the ESTA record only to find that it had 'forgotten' ALL of my info. and that I had to re-enter it all.

As an airline employee I sometimes have to fly to the USA on 'wait-listed' standby. If I am denied boarding for my listed flight I can list on the next one, but then I have to update my APIS record, and also the ESTA record. The APIS system remembers all my details and it is easy to update them to the new flight. BUT ESTA does not remember anything and I then have to type ALL of the info. back in.

It would also help if all of the scam ESTA websites were closed down - they charge outrageous fees for what is a free service.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 63

Sunday 5 April 2009

Contents

- [ElcomSoft to Recover Passwords with a Tambourine](#)
[Olga Koksharova via Michel Kabay](#)
- [More on Google calendar](#)
[Pat Lincoln and Jeremy Epstein via PGN](#)
- [Woman follows GPS, gets stuck in snowmobile trail](#)
[Monty Solomon](#)
- [A firmware glitch of router software: 32-bit integer handling](#)
[Chiaki Ishikawa](#)
- [No remittance, no ignition: Auto 'electronic repo' in action](#)
[Henry Baker](#)
- [Risks of on-line backups -- is it still safe once there?](#)
[David Leshner](#)
- [Domino's dishes out 11,000 free pizzas by mistake](#)
[Monty Solomon](#)
- [Australian DST in the news](#)
[Tony Finch](#)
- [Medical histories on the Internet](#)
[A Subscriber](#)
- [Playboy TV fined over explicit content](#)
[Max Power](#)
- [Re: E-voting in Ireland](#)
[Robert 'Jamie' Munro](#)
- [Oldest Data Loss Incident Contest](#)
[Monty Solomon](#)
- [2009 IEEE Symposium on Security and Privacy](#)
[David Du](#)
- [Info on RISKS \(comp.risks\)](#)

✉ ElcomSoft to Recover Passwords with a Tambourine (Olga Koksharova)

"Michel Kabay" <mekabay@gmail.com>
Wed, 1 Apr 2009 08:13:44 -0400

Dear Colleagues, This is exciting news for those committed to cultural sensitivity in the pursuit of science and technology. Mich

M. E. Kabay, PhD, CISSP-ISSMP, CTO & Prog Dir, MSc in Info Assurance
School of Graduate Studies, NORWICH UNIVERSITY +1.802.479.7937

-----Original Message-----

From: Olga Koksharova [mailto:o.koksharova@elcomsoft.com]

Sent: Wednesday, April 01, 2009 04:21

Subject: Press Release: ElcomSoft to Recover Passwords with a Tambourine

1 Apr, 2009 -- ElcomSoft Co.Ltd. introduces Password Recovery Tambourine <<http://tambourine.elcomsoft.com>>, a supernatural amulet to recover lost passwords with a 100% guarantee. The new tambourine is produced with genuine deer skin and requires training supervised by a qualified Yakutsk shaman. By offering guaranteed, 100% password recovery rate, ElcomSoft leaves competition behind once and forever.

Why Password Recovery Tambourine

Passwords affect people's lives. Lost and forgotten passwords can cost a life or a job. Striv[ing] to provide a solution to improve peoples' lives, ElcomSoft makes software for helping its customers recover passwords <<http://www.elcomsoft.com/products.html>> they've lost or forgotten. The company's password recovery tools are extremely effective, and literally save lives and jobs every other day. However, not all types of encryption are created equal. Some companies make exceptionally good effort protecting information, and use really secure algorithms from time to time. If a really secure password is used with those algorithms, the protected data is as good as gone.

Background

Universal cryptanalysis methods do exist. Government agencies, intelligence services and, in some countries, even police have successfully used methods such as rubber-hose cryptanalysis <http://en.wikipedia.org/wiki/Rubber_hose_cryptanalysis> for years. Rubber-hose cryptanalysis allows passwords and keys to be discovered in a surprisingly short time. The method is quite computationally inexpensive. However, commercial use of this method is limited due to legal restrictions in most countries. ElcomSoft started a quest to develop a universal cryptanalysis method that is at least as effective as rubber-hose, but comes with no penalty of being inhumane or restricted to exclusive use by government agencies.

Development History

Several unsuccessful attempts were made to design the ultimate password recovery tool. Using a crystal ball seemed like a great idea at first, but was quickly rejected. Rabbit's foot seemed a better idea for some time, but subsequent tests demonstrated that the foot could only solve certain network problems with corporate LANs, and only when used by qualified system administrators. A voodoo doll was a total nightmare, doing anything but recovering passwords.

The first ray of hope shined after one of ElcomSoft's employees was sent to Yakutia, a freezing province in Russia with real bears. He brought a shaman's tambourine that was used regularly by the local tribe's shaman to find missing things. ElcomSoft has conducted a full-scale scientific research of the new tool, spending endless hours chatting with Yakutia locals and shamans who use tambourines more often than we use our toothbrushes. Over than two hundred ritual dances have been performed, and today, ElcomSoft is proud to announce that the ultimate tool to recover lost passwords that cannot be recovered it in a traditional way has emerged.

About Elcomsoft Password Recovery Tambourine

Elcomsoft Password Recovery Tambourine is anything but easy to use. A special supervised training program must be completed, stunts and tricks have to be learned, and spells in Yakutian language must be mastered. The price is barely affordable. A variety of models is available.

Standard model works for most users without special needs. Simple, reliable, not too expensive. Corporate model is based on the standard tambourine, and it can work with hundreds and thousands documents at the time. Special team training is required. Pocket version is easy to take on a trip, but it has some restrictions supporting less exotic formats than its bigger siblings. A comprehensive, 200-page manual is shipped with every tambourine.

To order or get more information on Elcomsoft Password Recovery Tambourine visit <http://tambourine.elcomsoft.com/> <<http://tambourine.elcomsoft.com>>

[Info on ElcomSoft Co Ltd. legitimate, but truncated as inappropriate for RISKS. PGN]

More on Google calendar (Re: Epstein, [RISKS-25.62](#))

*"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 1 Apr 2009 8:20:14 PDT*

> When there's a shared calendar infrastructure and it's buggy, everyone
> ends up at the wrong time.

Patrick Lincoln noted that if *everyone* used Google calendar, everyone else would have been on the telecon at the "wrong" time -- which would have been the right time! So the risk is that not enough people are sharing the same calendar system. He proposed that we lobby for a federal law that requires everyone use Google calendar to avoid this risk.

Jeremy responded to Pat that what may make things a bit easier is that the stimulus package allocated \$3.2B to Google to move the calendar 15 minutes ahead, preserving America's technological lead (by 15 minutes). So those people who don't switch to Google calendar will be perennially 15 minutes late. Since the first 15 minutes of a meeting are frequently wasted with getting everyone into the room, on the phone, etc., this means that

non-Google calendar users will have the advantage of being more efficient, possibly offsetting the job creation value of the stimulus spending. Is that close enough to your proposed federal law?

Pat replied, "That's an excellent first step, but doesn't achieve the entire aim of my proposed law. Also, since the entire Internet and everything it is attached to is going to be destroyed today by Conficker, one other important aspect is a key invention, a survivable carbon-based two-dimensional human-readable storage medium for Google calendar information.

Woman follows GPS, gets stuck in snowmobile trail

*Monty Solomon <monty@roscom.com>
Fri, 3 Apr 2009 01:48:18 -0400*

Woman follows GPS, gets stuck in snowmobile trail, 1 Apr 2009
http://www.boston.com/news/odd/articles/2009/04/01/woman_follows_gps_gets_stuck_in_snowmobile_trail/

Deputy Keith Svoboda said it took a while to find her and much longer to get heavy equipment in to free the vehicle. Deputies dropped her at a motel for the night. Svoboda said the lesson is, "People shouldn't believe everything those things tell you."

[Especially on April Fools' Day! PGN]

A firmware glitch of router software: 32-bit integer handling

*Chiaki Ishikawa <ishikawa@yk.rim.or.jp>
Thu, 02 Apr 2009 23:29:43 +0900*

I am not sure if this is computer risk in the general sense, but I feel we will see more of this type of problems (32-bit signed integer vs unsigned integer) in embedded devices for consumer electronics and elsewhere for some time to come, and so I am reporting it here.

First the public fact.

NEC, a large electronics company, and its subsidiary NEC Access Technica have announced that their line of DSL routers with IP-phone feature which are used by many Japanese ISPs including the giants NTT East and NTT West has a software bug that after a continuous use of 2485 days, the router no longer allows telephone functions. (Internet access is still usable, though.)

The problem can be fixed by firmware upgrade, or for that matter, if power recycling is done, the problem is shifted for another 2485 days into the future.

(Actually, I saw somewhere that NEC and NEC Technica was looking into the

problems reported on different line of routers when they learned of the potential of similar problems. And when they checked the firmware of other products, they found the newly reported problems. I am not sure where I read it. I can't locate it any more. Maybe I read it in the letter which was sent by an ISP to notify the problem urging me to update my firmware of the said affected router.)

The cause of the bug?

The various reports I read didn't mention what are the real cause of the "software" problem, but I guessed that it must be related to the use of 32 bit integer for counting inside the firmware.

To wit, the problem interval in seconds is 214704000 [seconds] (= 2485 [days] * 24 [hours/day] * 3600 [s/h]).

One day shorter T' is 214617600 [seconds] = 2484 [days].

Also, $2^{32} = 4294967296$

$2^{31} = 2147483648$

We can see the following holds:

$$(T' * 10) < 2^{31} < (T * 10) < 2^{32}$$

My conclusion:

A certain integer counter is incremented at 1/10 sec interval within the software using 32 bits data starting from 0 after power-up.

Internally, the firmware code regards this data as "signed" and suddenly somewhere between 2484th and 2485th day, this counter becomes "NEGATIVE" and wreaking havoc within the code, and rendering phone function useless.

Observation:

When I was checking web pages to write this submission, I noticed a bug report that different routers used for IP phones using optical fiber had a similar problem after 249 days. This was found last summer. Obviously 294 days is much shorter than 2485 days and some people suffered from the bug last year. In this case, I think the counter is incremented every 1/100 second. Maybe this discovery led to the massive review of the router firmware.

I noticed that similar problems concerning integer size and its signedness have occurred when

- * file size has begun exceeding 2GB limit (again 31/32 bit boundary),
- * address space has been extended to 64 bits from 32 bits.

I noticed the first file size problems starting around the time Solaris and other Posix-based systems began offering large file size systems. Also, to this day, unmaintained shareware on windows often have problems when we try to handle a large file (2GB) like ISO image on windows. The symptoms are many. But one symptom that suggests the use of signed integer to check for

the remaining file space is messages that say I don't have enough space although I have more than enough (actually larger than 2GB of free space.) I have checked that in many cases, if I create a very large dummy file to shrink the remaining free file space to less than 2GB, then these unmaintained programs proceeded without a hitch or ran into other size-related problems later.

I noticed the second address space problems when linux was ported to x86 architecture with 64bit address space: many device drivers as well as applications began failing. Solaris for x86 also saw many third party drivers facing similar problems when 64 bit address space was supported on x86 architecture. (Solaris for Sparc supported 64 bits address space for many years and I don't remember particular problems.)

We can now add the use of timers/counters to the causes that may trigger careless errors in applications. We have already seen there have been cases where a counter goes over the allocated bits and repeats again from 0, thus causing some software problems in the past: I think the early version of Windows NT had a problem of requiring reboot every 49 days or so for certain applications. (Counters incremented every 1/50 sec?)

As more consumer devices (as well as industry machines) are equipped with 32 bit CPUs, and more programmers who are accustomed to the luxury of 32 bit CPU programming under non-embedded OS have begun to develop software for embedded devices, we may see similar problems in the embedded system space more often. We have seen many already, but I am afraid that this trend will continue.

BTW, routers are complex device and some have linux inside literally. I am surprised somewhat recently to see GNU General Public License repeated verbatim in print inside the manual of my Toshiba Hard Disk recorder. Obviously, certain code used inside is based on GPL'ed code. When I think about the growing pains that drivers and OS itself had to go through when larger file sizes and address space extension were introduced, I have an uncomfortable feeling to trust the complex operations on such products unless software patches are readily available. But how are we supposed to "patch" hard disk recorder software? If power cord is accidentally removed during patching, what happens?! Does hard disk recorder store the "patch" program in a separate place, preferably a ROM or something, so that glitches during patching can not corrupt such software?

Embedded system programming requires certain different mindset, but I am afraid that not many programmers are trained to develop such mindset in the educational system and even in the industry in general. I feel this way because the problems with NT don't seem to have been learned by the would-be developers today.

I am reporting the problem here today so that at least someone can point out that such a problem is a public knowledge for a long time when a similar problem happens again in the future.

⚡ No remittance, no ignition: Auto 'electronic repo' in action

Henry Baker <hbaker1@pipeline.com>

Thu, 02 Apr 2009 09:20:51 -0700

FYI -- Regardless of the date, this technology appears to be genuine. I guess the ultimate use of this technology would be for medical devices like heart pacemakers and defibrillators...

On a Gibbs family trip to Topeka, the littlest passenger wouldn't shut up. 'Beep-beep-beep' recalled Michelle Gibbs, mimicking the palm-sized device installed by her used-car dealer under the dash of the Honda Accord. "Try driving back for two hours with three kids in the car and that sound: Beep-beep-beep. It's very annoying, but for the most part, it's the best thing to happen to us."

The beeping was a reminder that 24 hours remained before a car-loan payment had to be made -- or else the vehicle would fail to start after that, courtesy of 'electronic repossession'. The Gibbises made it home to Blue Springs, punched in a one-time emergency code provided by the dealer to keep the car operable and then drove to the dealership to deliver the delinquent payment. It was the first time in five years they had been late on a payment. [Source: Rick Montgomery, *The Kansas City Star*, posted on 1 Apr 2009, PGN-ed]

<http://www.kansascity.com>

✂ Risks of on-line backups -- is it still safe once there?

"David Leshner" <wb8foz@panix.com>

Tue, 24 Mar 2009 11:13:14 -0400 (EDT)

Besides the issues of security & upload speed, when you use an off-site backup service; you assume that they are smart enough to not lose your data...and don't have problems of their own.

But...

Online backup service provider Carbonite is suing storage vendor Promise Technology, saying repeated failures of Promise gear have caused "significant data loss" at Carbonite.

In the lawsuit, filed 20 Mar 2009 in Suffolk County Superior Court in Boston, Carbonite said it bought more than US\$3-million worth of Promise VTrak Raid products beginning in 2006. In several incidents starting in January 2007, the service provider suffered data loss because the Promise gear failed to support recovery from physical drive errors and array errors. The data losses caused "substantial damage" to Carbonite's business, the company alleged. ... However, in a written statement following news reports on the case, Carbonite elaborated on the failures to say a smaller number of customers actually lost their own data. All customer backups involving the failed equipment were restored immediately and automatically,

the company said.

http://www.pcworld.com/article/161819/backup_provider_carbonite_loses_data_sues_vendor.html?tk=rss_news

(Promises, Promises... or should I say Diamond, not Carbonite, is a bit's best friend?)

✂ Domino's dishes out 11,000 free pizzas by mistake

Monty Solomon <monty@roscow.com>

Fri, 3 Apr 2009 01:54:45 -0400

http://www.boston.com/news/odd/articles/2009/04/02/dominos_dishes_out_11000_free_pizzas_by_mistake/

AP, datelined Cincinnati, 2 Apr 2009

"Bailout" was the magic word as Domino's had to give away thousands of free pizzas because someone stumbled on an online promotion the company scrapped. Domino's Pizza Inc. spokesman Tim McIntyre said Wednesday that the company prepared an Internet coupon for an ad campaign that was considered in December but not approved. He says someone apparently typed "bailout" into a Domino's promo code window and found it was good for a free medium pizza.

Word about the code spread quickly Monday night on the Web and 11,000 free pizzas were delivered before it was deactivated Tuesday morning. Cincinnati-area franchise owner John Glass says his 14 stores gave away more than 600 pies, but that Domino's promised to reimburse him.

[Also noted by Max Power. PGN]

✂ Australian DST in the news

Tony Finch <dot@dotat.at>

Tue, 31 Mar 2009 14:35:37 +0100

<http://www.theage.com.au/articles/2009/03/30/1238261487308.html>

Australia has had quite a lot of DST rule changes in recent years. However this year the clocks are going back according to the same rule as last year (first Sunday in April, except Western Australia changed on the last Sunday in March). Even so, people are still having problems with incorrect automated timezone changes.

The risks here include sophisticated mobile phone software that is difficult to update (I can't update my phone because I don't own a copy of Windows); a complicated service model in which it's unclear who is responsible for DST updates (my phone has an option to get its time from the network, even though it is tied to a network that doesn't provide the service, and its clock is accurate enough that the lack of synchronization isn't clear until there's a DST change), and of course pointless political fiddling with the

DST schedule.

f.anthony.n.finch <dot@dotat.at> <http://dotat.at/>

✂ Medical histories on the Internet

<A Subscriber>

Mon, 30 Mar 2009 14:14:30 +1000

The Australian government is seeking to introduce a blacklist for ISPs to block the inappropriate sites about children before reaching the user. All the usual parallels to Chinese government, etc., and not actually educating the children or stopping the problem.

<http://www.news.com.au/couriermail/story/0,23739,25262805-952,00.html>

Mid-March 2009. In Queensland, Australia, at least 100 patients have their displayed their relevant medical history, current medications, as well as patient's next of kin, on a pathology company's website. They were meant to be made available to treating doctors, but became available to all. The CEO is reportedly to have been very defensive rather than seeking to resolve it and advise the relevant persons. It was also raised that there was no law requiring affected persons to be advised.

<http://www.news.com.au/couriermail/story/0,23739,25253159-3102,00.html>

<http://www.news.com.au/couriermail/story/0,23739,25260243-3102,00.html>

✂ Playboy TV fined over explicit content

Max Power <dist23@juno.com>

Thu, 2 Apr 2009 21:57:41 -0700

A classical encoder-mode Risk:

Essentially what this means is that Adult Channels (and other sensitive content channels) in the UK are obliged to have redundant crypto encoders for the transmission of their content. The crypto itself is not at fault, but the crypto device oversight is. Often these devices are set into "test mode" or the "defeat switch" is on.

If the network used 2nd party encoding (essentially outsourcing beyond the network transmission studio and switch) then the 2nd party may be obliged to pay or split the fine.

British media regulator Ofcom has fined Playboy TV 22,500 pounds (\$32,990) for airing sexually explicit images in breach of broadcasting rules, claiming Playboy One had broadcast unencrypted raunchy, and what the watchdog deemed offensive, material until September 2008. Ofcom had received five complaints relating to seven late night programs broadcast between September and December 2007. ``Depending on the individual breach,

the explicitness, strength and, or, sustained nature of the sexual content and language was unacceptable for broadcast on an unencrypted free-to-air channel." Ofcom said Playboy TV UK/Benelux Ltd had failed to ensure adequate protection for viewers from 'potentially harmful or offensive material'. [Source: Reuters item, 2 Apr 2009; PGN-ed]

<http://www.reuters.com/article/oddlyEnoughNews/idUSTRE5314IR20090402>

Re: E-voting in Ireland ([RISKS-25.62](#))

<Robert 'Jamie' Munro>

Mon, 30 Mar 2009 14:52:01 PDT

"Ten years ago, the replacement of pencils and ballot papers by machines was seen as a badge of modernity. But technology was not sufficiently advanced to guarantee security of the new system."

I disagree with this assertion. I think the technology is /too/ advanced to guarantee security of the system. I'm reminded of Clarke's 3rd law: "Any sufficiently advanced technology is indistinguishable from magic." We cannot have a trusted system of democracy if voting works by magic. Voting needs to work in a way that everyone can fully understand.

Oldest Data Loss Incident Contest

Monty Solomon <monty@roscom.com>

Wed, 1 Apr 2009 21:12:04 -0400

First, a little history about the competition: In 2005, the Open Security Foundation launched the Oldest Vulnerability contest for one of our other projects, the Open Source Vulnerability Database, and from it came vulnerabilities dating back as far as 1965.

The winner, Ryan Russell, found a password file disclosure vulnerability from January of 1965, and helped OSVDB nail down several other old vulnerabilities. That contest resurfaced in our memories recently, and we've decided to do the same thing for DataLossDB.

What is the oldest documented data loss? As far as what is currently in DataLossDB, it is from January 10, 2000 when a hacker claimed to have stolen 300,000 credit card numbers from CD Universe.

We believe there are plenty of data-loss incidents that happened prior to CD Universe. Does anyone have an older incident they can submit to DataLossDB? We want it, and we'll reward you for it!

Find us the oldest documented Data Loss Incident. The oldest three submissions will receive prizes from our wonderful sponsors. In addition, you'll be able to bask in the fame of being the researcher, or Data Loss Archaeologist, who uncovered the oldest documented Data Loss Incident.

Incidents submitted don't have to be older than the CD Universe breach. For instance, the oldest Stolen Computer breach in the database occurred in 2003. So, submit what you find! You might find the oldest stolen laptop breach, or the oldest accidental web exposure breach. ...

http://datalossdb.org/oldest_incidents_contest

[If you are going to submit, you might look though the RISKS archives, beginning in 1976 with the ACM SIGSOFT Software Engineering Notes (SEN), well BEFORE the Risks Forum started. My historical index for SEN and RISKS is online. Although I've been struggling to keep it up to date recently, it is fine for old stuff in pre-RISKS SEN issues -- which Will Tracz now has the old online. PGN]

<http://www.csl.sri.com/neumann/illustrative.html>

#2009 IEEE Symposium on Security and Privacy

"David Du" <du@cs.umn.edu>

Sat, 21 Mar 2009 14:22:35 -0500

This is a reminder that the early registration deadline for the conference is approaching (20 Apr 2009). Some useful information of the conference is listed below. Please visit conference webpage at <http://oakland09.cs.virginia.edu/> if you need more information. Hope to see you in the conference at Oakland, California again from May 17th to 20th.

David Du, General Chair

30th IEEE Symposium on Security & Privacy

The 2009 symposium marks the 30th annual meeting of this flagship conference. Since 1980, the IEEE Symposium on Security and Privacy has been the premier forum for presenting developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field.

The 2009 symposium will be held May 17-20 at the <<http://www.claremontresort.com/>> Claremont Resort in Oakland, California.
<<http://oakland09.cs.virginia.edu/papers.html>> Accepted Papers
<<http://oakland09.cs.virginia.edu/program.html>> Program

Upcoming Deadlines

Travel Grants Deadline: 15 April 2009 [
<<http://oakland09.cs.virginia.edu/grants.html>> Travel Grant Information]

Poster Submission Deadline: 15 April 2009 [
<<http://oakland09.cs.virginia.edu/posters.html>> Call for Posters]

Short Talks Early Deadline: 15 April 2009 [
<<http://oakland09.cs.virginia.edu/shorttalks.html>> Call for Short Talks]

Early Registration Deadline: 20 April 2009 [
<<http://www.regonline.com/Checkin.asp?EventId=707709>> Registration

Information]

Hotel Registration Deadline: 24 April 2009 [

<<http://oakland09.cs.virginia.edu/travel.html>> Hotel Information]

Travel Grants

<<http://oakland09.cs.virginia.edu/grants.html>> Travel Grants information is now posted. Applications are requested by 15 April 2009.

Registration Open

<<http://www.regonline.com/Checkin.asp?EventId=707709>> Registration is now open. The early registration deadline is 20 April 2009.

Call for Short Talks

The <<http://oakland09.cs.virginia.edu/shorttalks.html>> Call for Short Talks is now posted.

Advance Program

<<http://oakland09.cs.virginia.edu/program.html>> Advance Program released.

Workshops and Tutorials

Information on <<http://oakland09.cs.virginia.edu/workshops.html>> Workshops and <<http://oakland09.cs.virginia.edu/tutorials.html>> Tutorials is now available.

Call for Posters

The <<http://oakland09.cs.virginia.edu/posters.html>> Call for Posters is now posted. Poster submissions are due 15 April 2009.

Accepted Papers Posted

<<http://oakland09.cs.virginia.edu/papers.html>> 26 papers have been accepted to the symposium.

[Check it out if you are into research in security and privacy and have never been there before. This is the 30th year at the Claremont, and it is always a worthwhile meeting and certainly a lovely venue overlooking San Francisco. PGN]



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 64

Monday 20 April 2009

Contents

- [Lisa Wangness: Inaccuracies in Google Health records](#)
[Martin Ward](#)
 - [Woman killed by laptop in crash](#)
[Walter Roberson](#)
 - [San Francisco South Bay phone vandalism](#)
[PGN](#)
 - [Vesta tire-pressure warnings](#)
[Click and Clack](#)
 - [Finnish e-voting results annulled; municipalities to hold new elections](#)
[PGN](#)
 - [CIA agent testifies on risks of electronic voting](#)
[PGN](#)
 - [Conficker C Analysis from SRI](#)
[Monty Solomon](#)
 - [Japanese vending machine face recognition accepts 10-yr-old as adult](#)
[Paul Saffo](#)
 - [Pro-regulation viewpoint on cyber vulnerability](#)
[via David Farber](#)
 - ["Nowt for owt" with Amazon](#)
[Chris J Brady](#)
 - [Credit-Card Activation](#)
[Kees Huyser](#)
 - [Bad authentication question](#)
[Erik Mooney](#)
 - [Re: The Security By Obscurity Myth](#)
[Dick Mills](#)
 - [Re: Driver Says GPS Unit Led Him to Edge of Cliff](#)
[jidanni](#)
 - [Re: flat text is *never* what we want](#)
[Tony Finch](#)
 - [Workshop on Service oriented Enterprise Architecture for Enterprise Engineering: EDOC'09](#)
[Selmin Nurcan](#)
 - [Info on RISKS \(\[comp.risks\]\(#\)\)](#)
-

✶ Lisa Wangness: Inaccuracies in Google Health records

Martin Ward <martin@gkc.org.uk>

Fri, 17 Apr 2009 15:27:42 +0100

When Dave deBronkart tried to transfer his medical records from Beth Israel Deaconess Medical Center to Google Health, a new free service that lets patients keep all their health records in one place and easily share them with new doctors, he was stunned at what he found.

Google said his cancer had spread to either his brain or spine -- a frightening diagnosis deBronkart had never gotten from his doctors -- and listed an array of other conditions that he never had, as far as he knew, like chronic lung disease and aortic aneurysm. A warning announced his blood pressure medication required "immediate attention."

It turns out that Google Health uses information from billing records, which can be inaccurate, undated, and was never intended to be used by doctors. Transferring existing paper records could take years and hundreds of millions of dollars. Insurance data, by contrast, is already computerized and far easier and cheaper to download. But it is also prone to inaccuracies, partly because of the clunky diagnostic coding language used for medical billing, or because doctors sometimes label a test with the disease they hope to rule out, medical technology specialists say.

Ironically, Beth Israel has one of the most advanced electronic medical records systems in the country, with clinical records carefully tended by doctors and accessible to patients on a secure website. But Google Health prefers providers send information in coded form to build the list of patient's medical conditions so the program can guide patients to additional information on the Internet about each disease using links. The neatly packaged billing codes are easier to link to than the mix of medical terms and standard language doctors use in their clinical records.

[Source: Lisa Wangness, *The Boston Globe*, 13 Apr 2007]

http://www.boston.com/news/health/articles/2009/04/13/electronic_health_records_raise_doubt/

[I used this case in beginning a keynote talk I gave on identities, trust, and trustworthiness at NIST on 15 Apr 2009 for the IDtrust 2009 conference. It was highly relevant, and came up several times during the talk. My slides are online on my website and on the IDtrust site. PGN]

<http://www.csl.sri.com/neumann/idtrust09+x4.pdf>

[Incidentally, an earlier article by Stephen Smith in *The Boston Globe*, 9 Apr 2009, noted that more than 338 Massachusetts hospital patients "suffered perilous falls, got the wrong medication, or had medical instruments left inside them." On the other hand, almost 2/3 of those involved falls. PGN]

http://www.boston.com/news/local/massachusetts/articles/2009/04/09/hospital_patient_mishaps_top_300/

✶ Woman killed by laptop in crash

Walter Roberson <roberson@hushmail.com>

Thu, 16 Apr 2009 13:11:28 -0500

A Canadian woman driving a small car was involved in a car crash. Investigators found that she likely would have survived if not for her laptop, which had been placed unsecured in the back seat and which flew forward and hit her in the back of the head.

<http://www.cbc.ca/technology/story/2009/04/15/bc-surrey-laptop-crash-kills-woman.html>

[It actually might make some sense for laptops to be in cases and anchored with seatbelts -- particularly the new Mac Airbooks. PGN]

San Francisco South Bay phone vandalism

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

Fri, 10 Apr 2009 12:42:12 PDT

Once again we are reminded of the fragility of our infrastructures -- this time fiber-optic cables and accessible manhole covers. Ten cables were severed at four different locations in the wee hours of the morning of 9 Apr 2009. At least 50,000 landline telephone customers and many others had their service seriously disrupted by fiber-optic cuts that also affected cell-phone service and Internet connectivity in Santa Clara, Santa Cruz, and San Benito counties. It impacted hospitals, businesses, banks, 911 calls to police and fire departments, computerized medical records, ATMs, and ubiquitous use of credit and debit cards. [Source: Long article by Nanette Asimov, Ryan Kim, and Kevin Fagan, *San Francisco Chronicle*, 10 Apr 2009; PGN-ed] With pervasive physical and logical vulnerabilities, sophisticated malware such as Conficker, and `normal accidents', we really need to consider our infrastructures much more holistically.

Vesta tire-pressure warnings

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

Sun, 19 Apr 2009 11:06:45 PDT

Click and Clack (Tom and Ray on NPR's Car Talk) had a caller this morning saying that her Vesta tire-pressure warning system goes off whenever she drove on a particular stretch of highway. After a little grilling, it turns out she was passing the NSA complex at Fort Meade. C&C concluded it had to be Radio Frequency Interference, and wondered whether it affects only Vestas, or perhaps other late-model cars with the newly mandated wireless sensors that might operate on the same frequency. [This was in MD. If it also happens in VA (e.g., near Langley), there might be Vestal Virginians calling in as well. PGN]

✂ Finnish e-voting results annulled; municipalities to hold new elections

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

Fri, 10 Apr 2009 12:42:12 PDT

<http://www.EFFI.org/blog/2009-04-09-EVoting-Supreme-Admin-Court.html>

Electronic Frontier Finland (EFFI), 9 Apr 2009

Kirjoittaja: Antti Vaha-Sipila, Huhtikuu 9, 2009

The Supreme Administrative Court has ruled on the Finnish municipal elections of 28 October 2008, in which an e-voting system was piloted. In its decision, the court sided with the complainants, overturning an earlier decision of Helsinki Administrative Court, and the decisions of the municipal central elections committees to confirm the election results. As a result, the three municipalities that took part in the Finnish e-voting pilot must now hold new elections as soon as possible. As the e-voting pilot has ended and the law authorising e-voting expired in December 2008, the new elections will use a traditional paper ballot system.

The Supreme Administrative Court decision was based on two issues: first, the voting instructions that the voters had received by mail were incorrect, and second, the user interface of the e-voting terminals was deemed to be flawed. The voting process utilised a smart card given to each voter, and upon premature removal of the card, the voting terminals gave no indication that the vote was not cast. As the system did not use a voter-verified paper ballot, voters might have been left with an impression that the vote had in fact been cast.

It is notable that the Court did not address the general lawfulness of e-voting. According to the Finnish law authorising e-voting, electronic ballot boxes would need to be archived until the next election. These electronic ballot boxes contain encrypted information on who voted and how. This poses a risk to voter secrecy. However, the Court refused to rule on whether this is unlawful, or whether the electronic ballot box would need to be destroyed.

In addition, the Court did not address the question whether an e-voting system would need to be more transparent. A significant amount of system design in the Finnish e-voting pilot were declared 'trade secrets', and the system source code is closed. The Court decision still leaves an open question whether paperless, 'black box' e-voting systems could be fielded in the future.

[Many other sources are cited on the EFFI website. PGN]

✂ CIA agent testifies on risks of electronic voting

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

Sat, 11 Apr 2009 16:26:53 PDT

[Thanks to Gene Spafford for spotting this one. PGN]

A CIA agent testified before the Election Assistance Commission. His position (or perhaps the CIA's?): electronic votes are not secure and can be altered -- and are being altered in some locales.

<http://www.mcclatchydc.com/226/story/64711.html>

✶ Conficker C Analysis from SRI

Monty Solomon <monty@roscom.com>

Fri, 10 Apr 2009 22:39:55 -0400

Phillip Porras, Hassen Saidi, and Vinod Yegneswaran,
Technical Report, Addendum
Release Date: 08 March 2009, Last Update: 4 April 2009
Computer Science Laboratory, SRI International, 333 Ravenswood Avenue
Menlo Park CA 94025 USA

This addendum provides an evolving snapshot of our understanding of the latest Conficker variant, referred to as Conficker C. The variant was brought to the attention of the Conficker Working Group when one member reported that a compromised Conficker B honeypot was updated with a new dynamically linked library (DLL). Although a network trace for this infection is not available, we suspect that this DLL may have propagated via Conficker's Internet rendezvous point mechanism (Global Network Impact). The infection was found on the morning of Friday, 6 March 2009 (PST), and it was later reported that other working group members had received other DLL reinfections throughout the same day. Since that point, multiple members have reported upgrades of previously infected machines to this latest variant via HTTP-based Internet rendezvous points. We believe this latest outbreak of Conficker variant C began first spreading at roughly 6 p.m. PST, 4 March 2009 (5 March UTC).

In this addendum report, we summarize the inner workings and practical implications of this latest malicious software application produced by the Conficker developers. In addition to the dual layers of packing and encryption used to protect A and B from reverse engineering, this latest variant also cloaks its newest code segments, along with its latest functionality, under a significant layer of code obfuscation to further hinder binary analysis. Nevertheless, with a careful mixture of static and dynamic analysis, we attempt here to summarize the internal logic of Conficker C. ...

<http://mtc.sri.com/Conficker/addendumC/>

New: Free Detection Utilities

Conficker C P2P Snort Detection Module

<http://mtc.sri.com/Conficker/contrib/plugin.html>

Conficker C Network Scanner

<http://mtc.sri.com/Conficker/contrib/scanner.html>

[Phil Porras and his colleagues have done an amazing job in reverse engineering and analyzing Conficker. See the Malware Threat Center, Cyber Threat Analytics, and BotHunter. PGN]

Japanese vending machine face recognition accepts 10-yr-old as adult

Paul Saffo <paul@saffo.com>

Fri, 17 Apr 2009 12:29:27 -0700

<http://mdn.mainichi.jp/mdnnews/news/20090417p2a00m0na004000c.html>

A 10-year-old boy in Kyoto was able to purchase cigarettes from a vending machine equipped with face identification technology, it has been found.

Kyoto Prefectural Police conducted an experiment with the cooperation of the boy, who had bought cigarettes from a vending machine this February. Neither the Ministry of Finance, which had approved the use of such machines in lieu of those that read Taspo I.C. cards stored with personal identification information, nor the manufacturer of face identification vending machines have heard of other instances in which elementary school children have been misidentified as adults.

According to police, the boy confessed that he had purchased cigarettes from a vending machine when he was questioned by his father about the cigarettes he had in his possession, and the father then contacted the juvenile division of Kyoto police. Early this month, police asked the boy to re-enact what he had done at the vending machine in question. The boy stood on the frame of his bicycle to move closer to the camera installed in the machine, pressed the "confirm" button, and was identified as an adult.

Face identification vending machines determine a person's approximate age from the size of their eyes and mouth and their bone structure. If a buyer is not identified as an adult, they must present a driver's license. Designed to prevent minors from buying cigarettes, 5,200 such vending machines have been in operation across Japan since the system's use was approved in July.

Kyoto police know of at least five instances in which junior high school students were misidentified as adults. "We plan to push the Ministry of Finance and vending machine manufacturers to make efforts to prevent minors from buying cigarettes from vending machines," said police.

"We are currently investigating the cause," said a representative of the vending machine manufacturer. "We are constantly upgrading our software to meet increasingly tough standards. The vending machine in question has also been upgraded." It is unclear, however, whether the boy was able to make purchases after the upgrade.

The legal smoking age in Japan is 20.

✂ Pro-regulation viewpoint on cyber vulnerability

David Farber <dave@farber.net>
Mon, 30 Mar 2009 10:12:42 -0400

[From someone contributing anonymously to Dave Farber's IP]

A paper that speaks to market failure is at:

http://www.csis.org/component/option,com_csis_pubs/task/view/id,5370/type,1/

Given that we know that perimeter defenses are ineffective illusions in cyberspace, to what market should regulation be targeted to have the most desirable impacts? Would it be the market for devices, operating systems, network infrastructure, application software and services, on-line content? All of the above?

"A new Federal approach to cybersecurity will fail if it does not elicit actions that the private sector will not otherwise perform. Government intervention in response to market failure can include regulation (or the threat of regulation) or subsidy. Both have limitations, but both are preferable to inaction. We are at the end of a long era of deregulation, an effort that was initially beneficial but it went too far in the last Administration. Finding a new and more balanced approach will not be easy. The intellectual heritage of deregulation lives in assertions such as any regulation to improve security will hurt innovation. Like all lobbyist mantras, it contains a grain of truth while being fundamentally and dangerously wrong. Innovation is a complex process, and simple statements about cause and effect deserve only skepticism."

Archives: <https://www.listbox.com/member/archive/247/=now>

✂ "Nowt for owt" with Amazon

Chris J Brady <chrisjbrady@yahoo.com>
Sat, 4 Apr 2009 12:17:54 -0700 (PDT)

There is a saying in the North of England of 'nowt for owt' (rhyming with 'out'). That is 'there is nothing for free.' I have just been sucked into an unwanted near 48-pound annual premium membership subscription by Amazon and there is no way to unsubscribe.

I use Amazon.com to purchase various items of interest about four times a year. I'm never in a hurry to receive these.

Just now I attempted to purchase a book and was offered the cheapest deal from Amazon with no packing or postage if I signed up for a 'free' trial of their new premium next day membership. This was easy to do, unsurprisingly. The p&p charges were then zeroed in my basket details - but

then I received a response saying that payment had been declined by VISA. Hmm - payment for a 'free' trial offer - I smelt a rat. It also stated that an email had been sent - which I found was headed: "Payment Declined for Amazon Prime Free Trial Membership." The rat started to smell bad.

I checked my account details and noticed that I had on my account a number of credit cards - all but one - now out-of-date. One of these latter had been used for the 'free' payment - LUCKILY. The email also stated that after the 'free' trial that my card would be charged 47.97 pounds for a one-year full membership!!!!

I searched the web site and could find no information about this premium membership - only that I had inadvertently joined it.

Worryingly I could NOT find any way to unsubscribe.

My only solution to this situation was to delete ALL of my cards' details from my account. And I resolved NEVER to use Amazon again. Their loss.

By this time - and running out of my time at the Internet cafe - I was very angry. The rat stank to high heaven. I trusted Amazon with my VISA card details and they attempted to suck me into an annual - and assumedly ever increasing - membership that I had no need for.

Let others be warned - if you smell a rat with a web site stop and investigate further before submitting credit card details.

✂ Credit-Card Activation

*Kees Huyser <kees.huyser@nikhef.nl>
Mon, 30 Mar 2009 09:12:49 +0200*

Recently, my bank was taken over by another bank. As a consequence of this take-over, I was issued a new credit card. The card needed to be activated by an 'activation code' which was sent in a separate letter a few days after I received the card.

To activate you need to call a toll-free number, enter the number of your credit card, the activation code and your date of birth. I tried to activate twice and both times it failed without telling me the reason for failure. I was advised to call the bank's customer service desk.

This morning I called the service desk and was asked the last eight numbers of the card, my full address (including the post code) and my date of birth. I was then told my date of birth was incorrectly recorded in the system and that this was the reason for activation failure.

The nice lady at the service desk then activated my card without asking for the activation code.

I'm sure you can see the holes in the system here: I can steal a card, phone

the service desk and tell them the date of birth is not what is in their system (the full address and postcode is printed on both letters and thus is also in my possession) and have the card activated.

How can the bank check my DoB over the phone? If they had asked me to give them the activation code at least that would mean I would have to steal two envelopes: the one with the CC and the one with the activation code.

Bad authentication question

*Erik Mooney <erik@dos486.com>
Fri, 17 Apr 2009 19:46:04 -0500*

So here's an entry in the Bad Website Security Question derby:

"What sports team do you most like to see lose?"

This appeared for online banking services for a local northeast US regional bank. If one knows anything about pro sports rivalries in the Northeast, there's maybe two to five potential answers to that question that would cover 90% or more of respondents. (And the bank even sponsors by name a pro sports arena in a northeast city.)

At least it isn't a password-retrieval question. It's an extra factor required for authentication in addition to the regular password. So it can't compromise my account, but the security it provides is quite illusory.

PIN Crackers Nab Holy Grail of Bank Card Security (WiReD)

*David Farber <dave@farber.net>
Thu, 16 Apr 2009 11:16:08 -0400*

Threat Level from Wired.com

<http://blog.wired.com/27bstroke6/2009/04/pins.html>

Hackers have crossed into new frontiers by devising sophisticated ways to steal large amounts of personal identification numbers, or PINs, protecting credit and debit cards, says an investigator. The attacks involve both unencrypted PINs and encrypted PINs that attackers have found a way to crack, according to an investigator behind a new report looking at the data breaches. The attacks, says Bryan Sartin, director of investigative response for Verizon Business, are behind some of the millions of dollars in fraudulent ATM withdrawals that have occurred around the United States. "We're seeing entirely new attacks that a year ago were thought to be only academically possible," says Sartin. Verizon Business released a report Wednesday that examines trends in security breaches. "What we see now is people going right to the source ... and stealing the encrypted PIN blocks and using complex ways to un-encrypt the PIN blocks."

[From Dave Farber's IP distribution. Thanks to Dave for many fascinating items. PGN]

Re: The Security By Obscurity Myth (Sebes, [RISKS-25.62](#))

Dick Mills <dickandlibbymills@gmail.com>

Mon, 30 Mar 2009 18:12:10 -0400

In [RISKS-25.61](#), John Sebes reiterated the expert's condemnation of security by obscurity (SBO). I for one, would certainly not challenge the validity of what Mr. Sebes and others say -- within context. However, I have two social-engineering type speculations as to why the SBO myth won't die.

First and foremost, nearly all governments, businesses, and academic institutions continue to embrace SBO. On the day when the news reports that NSA, IRS and Citibank open source all their software, and universities chip in with their GPA counting software; all to invite scrutiny for vulnerabilities, then I'll start to believe.

Next, as an engineer I'm trained to always check the limiting cases. Suppose all the world's software, or even a substantial fraction of it, was made open source? I can't even guess how many zeroes to put on the number of lines of code in question. 9? 12? 15? Then, the obscurity shoe would shift to the other foot. Benevolent hackers would have their efforts diluted to almost nothing. Only a tiny fraction of the code would benefit from adequate inspection by open source enthusiasts. Malevolent hackers need only find unscrutinized corners of obscure applications to find something to exploit. The average number of pairs of eyes scrutinizing each line of code would be much less than one. It would be disastrous.

Even on a much smaller scale, say the source code of the Windows OS, it seems likely that malevolent hackers inspecting the code would greatly outnumber the benevolent ones; especially, when considering the animosity towards Microsoft exhibited by the open source community. I believe that most of them don't **want** Windows to be secure; nor NSA nor IRS for that matter.

Consider the plight of a manager responsible for the security of any attractive target software, and faced by the prospect of whether to open source the code. The code **might** benefit from the efforts of benevolent hackers, but it would **certainly** suffer from the attentions of malevolent ones.

Within certain context, I can easily accept the arguments against SBO and for open source. The context would be a relatively small block of code (such as a voting machine, an encryption algorithm, or an OS kernel) and an open source community motivated to work, and work hard, on the benevolent side. Outside that context, I'm far from being convinced that SBO is a myth.

Re: Driver Says GPS Unit Led Him to Edge of Cliff

<jidanni@jidanni.org>

Mon, 06 Apr 2009 06:47:26 +0800

The e-maps where I live mark anything long and shiny (creek beds, landslides) as "road", and anything not (roads underneath trees) as "not a road". This combined with no concept of "vertical discontinuity", and any staircase could become the "best road".

At least nobody's managed to drive off the _bottom_ of my cliff (Risks 24.13). I.e., there probably will be slightly less fatalities if the GPS destination is at the top of the cliff instead of the bottom.

Re: flat text is **never what we want (Finch, [RISKS-25.55](#))**

Tony Finch <dot@dotat.at>

Wed, 1 Apr 2009 10:57:14 +0100

A followup to my question in [RISKS-25.55](#) about languages and/or libraries that reduce the problems caused by incorrect / insecure software arising from type mismatches in weakly typed data represented as strings.

Google has recently announced an open-source library that tackles one consequence of this problem: cross-site scripting. It is part of a web page templating system, and it embodies a lot of domain-specific knowledge about the syntax and nesting of the various languages found in web pages.

<http://googleonlinesecurity.blogspot.com/2009/03/reducing-xss-by-way-of-automatic.html>

CfP Workshop on Service oriented Enterprise Architecture for

Selmin Nurcan <nurcan@univ-paris1.fr>

Thu, 09 Apr 2009 19:54:27 +0200

Enterprise Engineering (EDOC'09)

SoEA@EE'09 is organised in conjunction with the 13th International Enterprise Computing Conference (EDOC) on September 1st, 2009, Auckland, New Zealand.

The goal of the SoEA@EE'09 workshop is to clarify the relationship between business process management and service provisioning. The objective is twofold:

- (i) To characterise the strong relationship existing between Business Process Management (BPM) and Service oriented Enterprise Architecture (SoEA)
- (ii) To develop concepts and methods to assist the engineering and the management of Service-Oriented Enterprise Architectures (SoEA) and their support systems.

The Call for Papers can be downloaded from the SoEA@EE'09 Web site :

http://crinfo.univ-paris1.fr/users/nurcan/SoEA@EE_2009/

Selmin Nurcan, SoEA@EE'09 co-organiser

Paper submission: May 31, 2009

[See the website for full details. PGN]



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 65

Wednesday 29 April 2009

Contents

- [New cybersecurity report, National Research Council](#)
[PGN](#)
- [CNN gets it right on swine flu scare](#)
[Jeremy Epstein](#)
- [President Obama says 3% of GDP on R&D](#)
[PGN](#)
- [Computer Spies Breach Fighter-Jet Project](#)
[Danny Burstein](#)
- [Pencils, not pixels: Ireland scuttles electronic voting machines](#)
[Matthew Kruk](#)
- [Russian Voting in Berlin?](#)
[Debora Weber-Wulff](#)
- [Second chance for French Net bill](#)
[Amos Shapir](#)
- [US Senate bills 773 and 776](#)
[Mabry Tyson](#)
- [The Risk of Namespace Collision](#)
[Gene Wirchenko](#)
- [Re: Tire-pressure warnings and RFI](#)
[Philippe Pouliquen](#)
[Bill Hopkins](#)
[John Curran](#)
- [Re: The Security By Obscurity Myth](#)
[Phil Colbourn](#)
[Steven M. Bellovin](#)
[Ted Lemon](#)
[Fred Cohen](#)
- [Firewalls are ineffective?](#)
[Fred Cohen](#)
- [Re: "Nowt for owt" with Amazon](#)
[Julian Bradfield](#)
- [Info on RISKS \(comp.risks\)](#)

✉ **New National Research Council cybersecurity report (Markoff/Shanker)**

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

Wed, 29 Apr 2009 14:25:26 PDT

The United States has no clear military policy about how the nation might respond to a cyberattack on its communications, financial or power networks, a panel of scientists and policy advisers warned Wednesday, and the country needs to clarify both its offensive capabilities and how it would respond to such attacks. The report, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, is based on a three-year study by a panel assembled by the National Academy of Sciences, and is the first major effort to look at the military use of computer technologies as weapons. The potential use of such technologies offensively has been widely discussed in recent years, and disruptions of communications systems and Web sites have become a standard occurrence in both political and military conflicts since 2000. [Source: John Markoff and Thom Shanker, Panel Warns U.S. on Cyberwar Plans, *The New York Times*, 30 Apr 2009 [PGN-ed]

<http://www.nytimes.com/2009/04/30/science/30cyber.html?hp>

[Please browse the entire article, which includes a link to the free Executive Summary of the draft NRC CSTB report, written by an impeccable cast of characters; the 14 authors include Adm. William A. Owens, William O. Studeman, Walter B. Slocombe, Richard Garwin, as well as some very technically savvy folks such as Tom Berson, David Clark, Jerry Saltzer, and Mark Seiden who are well-known to long-time RISKS readers. Ken Dam (co-chair with Owens) was also co-chair with David Clark of the report Computers at Risk: Safe Computing in the Information Age (1990). There's also a long history of reports in between that deserve greater recognition in policy circles, including Trust in Cyberspace (1998) and Toward a Safer and More Secure Cyberspace (2007). (Disclaimer: Although I was a co-author of the 1990 and 2007 studies [a locust who emerges every 17 years?]), the most relevant fact here is that those reports were not read and understood enough by people who really needed to know, and that not much has changed sufficiently in the interim.)

See also a related article earlier this week by David E. Sanger, John Markoff, and Thom Shanker, U.S. Plans Attack and Defense in Cyberspace Warfare, *The NYT*, 28 Apr 2009. PGN]

✂ CNN gets it right on flu scare

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Tue, 28 Apr 2009 21:05:07 -0400

Many of us frequently lambaste the media for their scare tactics. For a change, CNN got it right today, putting the flu scare in proportion.

> Regular flu has killed thousands since January

> There had been no confirmed deaths in the United States related to swine

> flu as of ['until' would now be correct] Tuesday afternoon. But another
> virus had killed thousands of people since January and is expected to
> keep killing hundreds of people every week for the rest of the year.
>
> That one? The regular flu.
>
> [...] But even if there are swine-flu deaths outside Mexico -- and
> medical experts say there very well may be -- the virus would have a long
> way to go to match the roughly 36,000 deaths that seasonal influenza
> causes in the United States each year. [...]

[\[http://www.cnn.com/2009/HEALTH/04/28/regular.flu/index.html\]](http://www.cnn.com/2009/HEALTH/04/28/regular.flu/index.html)

Now if only the media can be convinced to use the same level-headed risk analysis when it comes to technology risks....

✶ President Obama says 3% of GDP on R&D

*"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 27 Apr 2009 11:20:07 PDT*

On 27 Apr 2009, President Barack Obama promised a major investment in research and development for scientific innovation, saying the United States has fallen behind others. At a speech at the annual meeting of the National Academy of Sciences, he said "I believe it is not in our character, American character, to follow -- but to lead. And it is time for us to lead once again. I am here today to set this goal: we will devote more than 3 percent of our GDP to research and development. We will not just meet but we will exceed the level achieved at the height of the space race." [...]

[I hope some of this gets devoted to radically improving our information infrastructures. That's certainly an old running theme in RISKS. PGN]

✶ Computer Spies Breach Fighter-Jet Project

*danny burstein <dannyb@panix.com>
Tue, 21 Apr 2009 02:06:40 -0400 (EDT)*

... and Lockheed claims to be super smart about computers..

Computer spies have broken into the Pentagon's \$300 billion Joint Strike Fighter project -- the Defense Department's costliest weapons program ever -- according to current and former government officials familiar with the attacks. Similar incidents have also breached the Air Force's air-traffic-control system in recent months, these people say. In the case of the fighter-jet program, the intruders were able to copy and siphon off several terabytes of data related to design and electronics systems, officials say, potentially making it easier to defend against the craft.

... The intruders entered through vulnerabilities in the networks of two or

three contractors helping to build the high-tech fighter jet, according to people who have been briefed on the matter. Lockheed Martin is the lead contractor on the program, and Northrop Grumman Corp. and BAE Systems PLC also play major roles in its development. [*Wall Street Journal*, 21 Apr 2009] <http://online.wsj.com/article/SB124027491029837401.html>

#Pencils, not pixels: Ireland scuttles electronic voting machines

"Matthew Kruk" <mkruk@telus.net>

Tue, 28 Apr 2009 01:02:53 -0700

Pencils, not pixels: Ireland scuttles electronic voting machines --
Faced with rising costs and growing fears of hackers, Ireland has decided to join a growing movement in Europe to return to old school voting practices.

For sale: 7,500 electronic voting machines. Never used. Will need retrofit for security. Cost: \$67 million, but all offers considered. Contact Irish government.

Bought in the midst of the booming Celtic Tiger economy, these Dutch-built Nedap Powervote system machines were technologically chic. Piloted in three constituencies during the 2002 general election, they were expected to eliminate lengthy manual counts and parse votes from Ireland's complicated proportional representation system to give instant results. And if Ireland didn't embrace e-voting, warned then Taoiseach Prime Minister Bertie Ahern in 2006, the country would be a laughing stock "with our stupid oul pencils," he said, using an Irish colloquialism for "old." But the stupid oul pencils have had the last laugh. Ireland is now selling its unused machines, which thus far have incurred storage fees of [the equivalent of \$4.6 million]. [Source: Michael Seaver, 26 Apr 2009, *Christian Science Monitor*] <<http://www.csmonitor.com>>

[Also noted by Bernard Lyons. In addition, see
<http://techdirt.com/articles/20090427/0232024663.shtml>

]

#Russian Voting in Berlin?

Debora Weber-Wulff <weberwu@htw-berlin.de>

Wed, 29 Apr 2009 08:43:07 +0200

The city of Berlin held a referendum this past weekend on a complicated question about whether religion can be a substitute for ethics as a compulsory subject in the schools. It was a bitter campaign and the maps showing the precinct's results clearly showed where the Berlin Wall used to be: Western Berlin voted "yes", Eastern Berlin voted "no", and "no" won.

On Monday they had top 10 lists of the precincts that voted one way or the other. I thought that the top "yes" precinct, in trendy Wilmersdorf, did

smell a bit fishy with 99,5 %. But well, okay, that's where all the Germans that emigrated from Russia live, and they are used to voting that way. The party's way or no way.

Today the newspapers report on a "statistical error". The results are counted in the precincts and reported by telephone to the central office. You redial and redial and redial, until some harried person answers, and then you give them your results.

Instead of "415 votes, 225 for yes, 188 for no, 2 invalid", what was recorded in the computer for this precinct was "416 votes, 414 for yes, 1 for no, 1 invalid". And this information is automatically passed on to the next station.

I don't see a statistical error here - I see an input validation problem and antiquated data input methods. And I find it disturbing that the total number of votes is wrong, too.

Perhaps they can switch to text messages for the next election?

Prof. Dr. Debora Weber-Wulff, HTW Berlin, FB 4, Internationale Medieninformatik
10313 Berlin +49-30-5019-2320 <http://www.f4.htw-berlin.de/people/weberwu/>

✂ Second chance for French Net bill

*Amos Shapir <amos083@hotmail.com>
Thu, 30 Apr 2009 00:36:35 +0300*

The BBC site reports: "A controversial French bill which could disconnect people caught downloading music illegally three times returns to parliament on Wednesday for debate." Full story at:
<http://news.bbc.co.uk/2/hi/technology/8024475.stm>

Beside the usual questions and argument about IP vs. human rights, there is also the question of enforcement: How on earth can any legal system (democratic and sane one, anyway) ban a person from access to the net? ISP's deal with Internet accounts, which are not "persons" in the legal sense; I'm not a lawyer, but I cannot think of any legal mechanism which can make a binding and enforcible connection between these terms.

✂ US Senate bills 773 and 776

*Mabry Tyson <Tyson@Al.sri.com>
Mon, 27 Apr 2009 15:37:11 -0700*

Two bills were introduced into the US Senate on 1 Apr 2009 that I believe are intended to guide cybersecurity policy for the US.

* S 773 - A bill to ensure the continued free flow of commerce within the

United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cybersecurity defenses against disruption, and for other purposes.

Full Text: [http://thomas.loc.gov/cgi-bin/query/z?c111:S.773:](http://thomas.loc.gov/cgi-bin/query/z?c111:S.773)
(For more information, search for "S773" in category Bill Number at <http://thomas.loc.gov/>)

* S 778 - A bill to establish, within the Executive Office of the President, the Office of National Cybersecurity Advisor.

Full Text: [http://thomas.loc.gov/cgi-bin/query/z?c111:S.778:](http://thomas.loc.gov/cgi-bin/query/z?c111:S.778)

The status of S773 shows that it was read twice on 1 Apr and referred to the Committee on Commerce, Science, and Transportation. (<http://commerce.senate.gov/public/>) It was the chairman of that committee, Sen. Jay Rockefeller (D-WV) that sponsored the bill.

Considering this was introduced by a Democratic Committee Chairman in a Democratic-controlled Congress with a Democratic President, it seems likely that some version of it will be passed. I urge the RISKS community to take a close look at the bill to see that it achieve the security we require without unduly compromising the privacy we are guaranteed by the Constitution and by Common Law. If changes should be made, it will be easier to get them done sooner rather than later.

Here are a few quick comments on two items that I noticed. By no means have I read it all.

=====
Sec 14(b): The Secretary of Commerce--

(1) shall have access to all relevant data concerning such networks without regard to any provision of law, regulation, rule, or policy restricting such access;

- -----
NOTE: "such networks" here refers to "Federal Government and private sector owned critical infrastructure information systems and networks.". In Sec 23, "Federal Government and United States critical infrastructure information systems and networks" is defined as all Federal Government information systems and networks plus "state, local, and nongovernmental information systems and networks in the United States designated by the President as critical infrastructure information systems and networks"

In other words, it means any networks the government wants it to mean, such as, say, the ISP network serving your home system, or the network at your church. All it takes is the President's designation. The only reason I can think of for the slightly different naming ("private sector" vs "United States") is either sloppiness or removing the restriction that the network is "in the United States" and extending it to "private sector" so it might apply to a US company's network outside the US.

My biggest concern is the "without regard to any provision of law". Does

this mean this law trumps all other laws? Does it mean that the Federal Government claims access to (and jurisdiction over) any network, even if it does not otherwise comes under federal jurisdiction (through Interstate Commerce, etc.).

= =====

SEC. 17. AUTHENTICATION AND CIVIL LIBERTIES REPORT.

Within 1 year after the date of enactment of this Act, the President, or the President's designee, shall review, and report to Congress, on the feasibility of an identity management and authentication program, with the appropriate civil liberties and privacy protections, for government and critical infrastructure information systems and networks.

- -----

This is poorly (or is it expertly?) worded in that is ambiguous what identities are being managed. Individuals (as indicated by the references to civil liberties and privacy) or systems and networks ("identity management...program ... for government... systems and networks")

✶The Risk of Namespace Collision

Gene Wirchenko <genew@ocis.net>

Thu, 23 Apr 2009 08:49:02 -0700

Initials. Make a powerful statement about a company. The suggestion of mystery. Often get pronounced as a word. This should be on anyone's radar.

Canadian tech association offers on-demand video to foster business success
<<http://www.itbusiness.ca/it/client/en/home/News.asp?sub=true&id=52911>>

Paragraph 5: "CATA is tapping the software-as-a-service offering of Calgary-based JITR Inc. Its JET system lets any company or organization deliver live, high-definition video to a large and controlled audience."

Is there anyone else who saw "JITR" and immediately thought "jitter". The whole name could turn into "jittering". Not the best association for on-line video, is it?

✶Re: Tire-pressure warnings and RFI (PGN, [RISKS-25.64](#))

Philippe Pouliquen <philippe@alpha.ece.jhu.edu>

Tue, 21 Apr 2009 08:25:42 -0400 (EDT)

I heard the same episode of car talk and remember the car affected being the Nissan Versa <not Vesta *>. I am fairly confident in my memory because the Versa is a vehicle that my wife and I considered buying a while back, but rejected because when the back seats were folded down, they made a two to three inch step between them and the trunk area (very impractical for loading large objects) that none of the other hatchbacks we looked at had.

[* My Vice is Versa <not Vesta>. I was driving in a noisy environment.
Merci, Philippe, for the correction. PGN]

Re: Tire-pressure warnings and RFI (PGN, [RISKS-25.64](#))

*"Bill Hopkins" <whopkins@wmi.com>
Mon, 20 Apr 2009 18:33:21 -0400*

Listening to Click and Clack's NSA interference hypothesis, I was reminded of an earlier automotive RFI problem.

Our 1968 Volvo used a voltage regulator to supply the temperature and fuel gauges. Approaching a radar cop, the regulator swamped and as the engine overheated, the gas tank filled up (according to the needles). It got one's attention.

A built-in radar detector, disguised as necessary instruments!

Unfortunately, the effect didn't begin until about 30 feet from the radar.

Re: Tire-pressure warnings and RFI (PGN, [RISKS-25.64](#))

*"John Curran" <John.Curran@mms.gov>
Mon, 27 Apr 2009 09:56:54 -0400*

My wife and I flew to Denver last fall and rented a Toyota Camry. We drove all over Wyoming and Montana, and in Yellowstone and Grand Teton NP the tire sensors showed low pressure. When I checked the tires, they were a little low, but not bad. Then the Check Engine light came when we were at Jackson Lodge and I called the Hertz facility at the Denver airport. The manager asked me to take it to the Hertz venue in the Jackson Hole airport. When I explained the issue to the manager there, he told me that telecommunications in the area for Vice President Cheney set off car sensors all the time. He said he could give me a new car, but the warnings would probably come back. I was skeptical about this, but now I wonder if he was right.

John Curran, MMS/OEMM Information Systems Security Officer 703-787-1712

[Shades of Sputnik and later President Reagan's Air Force One affecting garage-door openers ([RISKS-2.37](#)). PGN]

Re: The Security By Obscurity Myth (Mills, [RISKS-25.64](#))

*Phil Colbourn <philcolbourn@gmail.com>
Tue, 21 Apr 2009 22:34:22 +1000*

In [RISKS-25.64](#) Dick Mills suggests that if all closed source software was opened, there would not be enough benevolent hackers to find the bugs before the malevolent hackers do - concluding that it would be disastrous.

I'm not convinced. Much software has been opened sourced to date, including significant code bases of Solaris (~10MLoC), OpenOffice (7.6MLoC) and much of Java (~6.5MLoC) - large code bases that are in significant use in many environments world-wide.

Java is estimated to be installed in 5.4B devices - I imagine that this is a sizable target that malevolent hackers would be working on. But should they find a flaw and exploit it, there will be many companies and individuals looking to close the case quickly.

It is also doubtful that all propriety software would be opened at the same time, allowing more eyes to look through code should they be inclined to do so.

Microsoft software, however, is a special case as Dick indicates.

Similarly, encryption algorithms also suffer from a lack of confidence due to closed designs. An open development process is more likely to find flaws sooner and therefore reduce the risk of insecure data transmission.

Re: The Security By Obscurity Myth (Sebes, [RISKS-25.62](#))

*"Steven M. Bellovin" <smb@cs.columbia.edu>
Mon, 20 Apr 2009 18:04:38 -0400*

Many people who advocate or condemn security through obscurity misunderstand it. The notion goes back to Kerckhoff's 1883 paper on military cryptography. He did not, however, advocate publishing the system. Rather, he wrote "The system must not require secrecy and can be stolen by the enemy without causing trouble" (translation from <http://www.petitcolas.net/fabien/kerckhoffs/>). That is, it should be secure even if compromised.

The real issue is whether one gains more security by publishing (the "many eyes" theory) or by keeping it secret (and thus perhaps increasing the work effort for the attacker). I don't think there's any one answer. In cryptography, I strongly suspect that cryptanalysis is *much* harder without access to the algorithm -- but we also know that it's been done. Source code is probably more secure if published -- but if and only if enough competent good guys are actually motivated to examine it. For voting machines, I think that that's likely the case; for other systems, it's much less clear. (We also know how long some serious security bugs have lurked in open source systems -- <http://www.cert.org/advisories/CA-95.03.telnet.encryption.vulnerability> is my favorite, for many reasons.)

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

Re: The Security By Obscurity Myth (Mills, [RISKS-25.64](#))

Ted Lemon <Ted.Lemon@nominum.com>

Mon, 20 Apr 2009 17:17:01 -0500

In [RISKS-25.64](#), Dick Mills writes that he's not convinced that Security By Obscurity is really a myth. He makes the point that the banks do it, so it must be good. Interestingly, in a previous article in the same digest, we learn that banks have some really serious security problems because their security model for ATM card PINs is much more vulnerable than they'd anticipated. Based on what I've heard of these exploits elsewhere in the press, their security model would have been roundly mocked if it had been public knowledge; in this case, clearly obscurity benefited no-one except the attackers.

Security by obscurity - a myth?

Fred Cohen <fc@all.net>

Wed, 22 Apr 2009 04:52:07 -0700

> From: Dick Mills <dickandlibbymills@gmail.com>...

>

> In [RISKS-25.61](#), John Sebes reiterated the expert's condemnation of
> security by obscurity (SBO). I for one, would certainly not challenge the
> validity of what Mr. Sebes and others say -- within context. ...

I, on the other hand, might...

The notion of security by obscurity as often portrayed as a bad thing, and while I certainly think that covering up weak concepts, designs, implementations, and executions by trying to obscure them is a bad idea, the facts on the ground are that very few programs are properly and formally specified to a level of detail where we can even determine whether or not they meet those specifications at all, much modern programming is evolutionary in nature and hooks into something else that is largely unknown by the programmer, most organizations I have seen are unable or unwilling to put in the resources to do things to a level of surety that would allow full disclosure of everything, and I see no reason that obscurity is any less valid than complexity in terms of defining the security properties of a system.

How many from the RISKS audience would really provide me with all of the information that all of the people in their organization have about everything in the organization along with a mandate to do harm, and expect that I would do no better than I would do if provided with the mandate and none of the information?

Security by obscurity is a fact of risk management, and it is often the only reasonable approach to mitigation of risks.

Fred Cohen & Associates, 572 Leona Drive Livermore, CA 94550
tel/fax: 925-454-0171 <http://all.net/>

✶ Firewalls are ineffective? ([RISKS-25.64](#))

Fred Cohen <fc@all.net>

Wed, 22 Apr 2009 04:42:28 -0700

> Given that we know that perimeter defenses are ineffective illusions in
> cyberspace, ...

Actually, this is just plain untrue. Perimeter defenses are almost all of the defenses we have that actually do work - in that they do things that we can measure and they do them effectively. So this "given" should be taken away.

To be clear, the fact that perimeters are "leaky" by intent, does not mean that they are not effective. To the extent that the writer was deceived about what these defenses do, the cognitive problems with people understanding perimeter defenses should be addresses as well. To aide a bit in this...

Perimeter defenses primarily operate to reduce the quantity and types of event sequences that cross the boundary defined by the perimeter. As an example, process separation is a perimeter defense that puts a perimeter around a process and its resources and limits the ways in which information can cross that perimeter. It works very well in preventing processes from writing all over other processes' memory, but it does not, and is not intended to, prevent the use and abuse of system calls that communicate across the boundary. The perimeter defense associated with identification and authentication is defined by the authorization process. In this case, the perimeter might be, as an example, the division between those input sequences that are allowed to interface with programs other than the login program and other similar service programs and those that cannot. Again, it is effective at what it does, but it does not prevent an individual who takes over the keyboard from an already authorized user from using those interfaces. Perhaps this helps to clarify that perimeters are very often highly effective and reasonably well defined, and that without them we would be in serious trouble.

Fred Cohen & Associates, 572 Leona Drive Livermore, CA 94550
tel/fax: 925-454-0171 <http://all.net/>

[Fred, They may be "almost all of the defenses we have that actually do work", but considering how porous many firewalls are, that is not very much of a consolation. PGN]

Re: "Nowt for owt" with Amazon (Brady, [RISKS-25.64](#))

Julian Bradfield <jcb@inf.ed.ac.uk>

Tue, 21 Apr 2009 08:53:13 +0100

I wonder what planet Chris Brady has been living on for the last few decades? Almost every "free trial offer" you get through the mail or by the Web works by taking payment details, and then charging you at the end of the trial unless you positively decline. Amazon is no different - and Googling for "amazon prime free trial" takes you in a couple of clicks to Amazon's help pages telling you how to decline at the end of your free trial. Most likely this would also appear in an e-mail at the end of the trial, though I don't know whether Amazon is obliged by law to do this. As for the "payment declined", I'd guess this actually just an authorization request to check the card validity.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 66

Sunday 10 May 2009

Contents

- [FAA ATC shutdown](#)
[Linda Gorman](#)
- [Documented risks to FAA computers](#)
[John Sawyer](#)
- [Pipe Leak at NY Indian Point Nuclear Plant Raises Concerns](#)
[Gabe Goldberg](#)
- [Minnesota court says defendants have right to see source code](#)
[Mark Thorson](#)
- [Obama, McCain legal teams promote state-level clean election practices](#)
[David Leshner](#)
- [Richard A. Clarke: Obama's Challenge in Cyberspace](#)
[David Farber](#)
- ['Computer glitch' disrupts Boston city payroll](#)
[Monty Solomon](#)
- [Teenage hiker's calls ignored; no street address](#)
[Rohan Sullivan](#)
- [Hackers Break Into Virginia Health Professions Database, Demand Ransom](#)
[Brian Krebs](#) via [Monty Solomon](#)
- [UCBerkeley health service hacked, with 160,000 at risk of ID theft](#)
[Henry Lee](#) via [Ari Ollikainen](#)
- [How to guarantee bad passwords](#)
[Jeremy Epstein](#)
- [Lexis Nexis does an Oopsis. Data breach...](#)
[Danny Burstein](#)
- ["Server issues" delay Nielsen ratings](#)
[George Mannes](#)
- [Researchers Take Over Dangerous Botnet](#)
[ACM TechNews](#)
- [Materials Database Problem](#)
[Gene Wirchenko](#)
- [Strange cash register arithmetic favors the house](#)
[Bart Thielges](#)
- [Re: Credit card numbers *not* plucked out of the air at FL Best Buy](#)
[Jonathan Kamens](#)
- [Real-Time Networks RTN'09](#)

[ECRTS](#)

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

✂ FAA ATC shutdown

"Linda Gorman" <linda@i2i.org>
Thu, 7 May 2009 09:34:17 -0600

Civilian air-traffic control system computer networks have been penetrated multiple times in recent years, including an attack that partially shut down ATC systems in Alaska. The FAA is expecting to spend about \$20 billion in an upgrade over the next 15 years. [Source: *Wall Street Journal*, 7 May 2009; PGN-ed]

<http://online.wsj.com/article/SB124165272826193727.html>

[RISKS readers will recall that the previous attempted upgrade cost about \$4B before it was scuttled. PGN]

As an economist I'm primarily interested in this case for two reasons: a) whether as a practical and theoretical matter the US government can purchase and maintain modern information systems for specialized civilian applications given that the FAA has been trying and failing to do so for 20 years even as private corporations created for that purpose, entities like Nav Canada and even the US Postal Service, have been more successful, and b) the application that this failure has to the prevailing mythology of how expanding government control over health information storage architecture will improve care and lower costs. To date the myth or electronic systems to the rescue continues to grab people even though almost all of the real world tests of the effects of expanded government control suggest that the most likely result is higher costs and degraded care.

Linda Gorman, Director, Health Care Policy Center, Independence Institute, Golden, Colorado

✂ Documented risks to FAA computers

John Sawyer <jpgsawyer@googlemail.com>
Thu, 7 May 2009 09:35:02 +0100

I thought this would be of interest to RISKS readers.

<http://www.flightglobal.com/articles/2009/05/06/326132/us-air-traffic-exposed-to-serious-harm-from-cyber.html>

Scary stuff if the risks are as serious discussed.

[See also CNET. PGN]

http://news.cnet.com/8301-1009_3-10236028-83.html?tag=newsEditorsPicksArea.0

[The risks are not newly identified. For example, see my Computer Security in Aviation: Vulnerabilities, Threats, and Risks, International

Conference on Aviation Safety and Security in the 21st Century, 13-15 January 1997, for the White House (Gore) Commission on Safety and Security.

<http://www.csl.sri.com/neumann/air.html>

However, perhaps the awareness climate is finally changing. PGN]

✶ Pipe Leak at NY Indian Point Nuclear Plant Raises Concerns

Gabe Goldberg <gabe@gabegold.com>

Fri, 01 May 2009 14:39:32 -0400

Not directly a computer risk but it raises the question of how 100,000 gallons of water could go missing; the leak was only discovered when someone noticed water flowing across the floor. Funny, that's the same technology by which my wife just notices a basement leak in our house. I'm thinking about installing a water detector -- maybe Entergy should also.

- ----

... it has raised concerns about the monitoring of decades-old buried pipes at the nation's nuclear plants, many of which are applying for renewal of their operating licenses. Indian Point 2, whose 40-year operating license expires in 2013, already faces harsh criticism from New York State and county officials who want it shut down.

Representative Edward J. Markey, the Massachusetts Democrat who heads a House subcommittee on energy and the environment, said the leak raised serious questions about Entergy's and the regulatory commission's oversight. "This leak may demonstrate a systemic failure of the licensee and the commission to inspect critical buried pipes in a manner sufficient to guarantee the public health and safety," he wrote to the commission's chairman, Dale Klein, in a letter on Thursday. The letter was also signed by Representative John J. Hall, whose district includes the plant. The congressmen said they were "shocked" that a leak that big could develop without detection and called the system for detecting such problems "profoundly inadequate." [Source: Matthew Wald, *The New York Times*, 2 May 2009; PGN-ed]

<http://www.nytimes.com/2009/05/02/nyregion/02nuke.html?hp>

✶ Minnesota court says defendants have right to see source code

Mark Thorson <eee@sonic.net>

Sun, 03 May 2009 17:55:34 -0700

Drunk driving defendants demand to see source code for testing machines, Minnesota state supreme court rules they have that right, but machine maker refuses citing trade secrecy.

http://www.twincities.com/news/ci_12267906?source=rss

✂ Obama, McCain legal teams promote state-level clean election practices

"David Leshner" <wb8foz@panix.com>

Fri, 8 May 2009 01:06:52 -0400 (EDT)

http://www.rollcall.com/issues/54_125/guest/34584-1.html?type=printer_friendly

Robert F. Bauer and Trevor Potter are attorneys in private practice, specializing in election law. Bauer served as general counsel to the Obama presidential campaign, and Potter was general counsel to the McCain presidential campaign.

Robert F. Bauer and Trevor Potter,
Next Phase of Election Reform: Start With Facts, 5 May 2009

As the general counsel to the Obama and McCain campaigns, we had our disagreements - a fair number of them, as a matter of fact. But we share a deep commitment to fair and well-run elections in which all qualified voters have the opportunity to vote, and all the votes that they cast are accurately counted. Looking back on the 2008 elections, we have no doubt that reforms in the administration of elections in this country are needed if we are to meet these standards. We also believe such reforms can be achieved, with potentially transformative success for the American voter.

It may be news to many readers that reforms are still needed. The media widely reported a smooth election, and in some places, those reports were accurate. The problems - and there were many, scattered across the country - received comparatively little attention because the outcome of the voting was clear.

State voter registration lists suffered from various levels of inaccuracies, there were controversies over registration drives, the lines for early voting almost overwhelmed the system in some states, and absentee ballots often reached voters too late to be cast, especially for armed forces members overseas.

And on Election Day, there were many reports of more long lines, inadequate ballots, malfunctioning machines and voters turned away because of registration issues across the country.

If the election had been close, there would have been legal controversies over counting hundreds of thousands of absentee and provisional ballots in key states.

...

Data provide the reality check that forecloses the most extreme positions. Unfortunately, our state and local governments do not generate, let alone make public, the most basic information on how well the system is working. Many states cannot tell you how many people showed up to vote on Election Day. Other states have no idea how many voters are registered or how voters cast their ballots. What

little data we have suggest that jurisdictions have widely variable numbers of provisional ballots and markedly different ballot discard rates. Even here, however, we lack enough information to figure out why that is so.

It is essential that the data collected is distilled into a usable form. Voters need a readily accessible metric to hold their government accountable for missteps and reward those who perform well.

Policymakers need solid, comparative data to referee the inevitable fights that take place between reformers, parties, candidates and election administrators over whether the system is working. Election administrators need a strategy for sorting through widely varying local practices to identify the best ones.

A critical step toward the production of this data is the Democracy Index, proposed by Heather Gerken of Yale Law School, which would rank states and local election systems based on performance. Such an index would function like a U.S. News and World Report ranking for colleges, pulling together basic information that matters to voters: How long were the lines? How many ballots got discarded? How often did machines break down?

This is the kind of solution that should attract strong bipartisan support. Rather than adopting a top-down, command-and-control approach, it relies on a market-based solution, looking to "sunshine" - the plain light cast by the facts - to motivate responsible officials to do better. Rather than mandate uniform national standards, it takes advantage of local variation to spot and surface good policy.

What's most attractive about a proposal like Gerken's is that it should lay the groundwork for well-reasoned reforms. With better data, we should be able to avoid fruitless discussions about the things that don't matter and focus on the things that do. Reliable performance data, in our view, would make visible the costs associated with our current registration system, potentially moving us toward a system of automatic voter registration by states, which in turn would help eliminate the conflicts over the role of private registration activity.

Reliable performance data would, we also suspect, help advance discussion of the role and rules for early voting and give election administrators the ammunition that they need to fight for the resources that they have so long done without.

Agreement on these issues will not always be easy. But good data offer a shared starting point for discussions about the future path of reform.

When President Barack Obama and Secretary of State Hillary Rodham Clinton were Senators, both proposed bills that would make the Democracy Index a reality. The problems that we saw during the 2008 elections confirm the importance of passing just such a bill and

giving at long last a strong factual foundation to the urgent business of reform - and a strong incentive to elected officials, administrators and parties to get on with the hard work ahead.

2009 c Roll Call Inc. All rights reserved.

Richard A. Clarke: Obama's Challenge in Cyberspace

David Farber <dave@farber.net>

Fri, 8 May 2009 13:59:15 -0400

[From Dave Farber's IP distribution]

http://www.huffingtonpost.com/richard-a-clarke/obamas-challenge-in-cyber_b_199926.html?view=print

In the next few days President Obama will decide whether he will live up to his campaign promises about dealing seriously with the challenge of cyber security by creating a White House office to direct government activity and coordinate with the private sector. None of the options being served up to him will create the stand alone White House office that is needed to provide the leadership on this issue.

The reasons that this decision is important have been spread across the media this last month. Among the facts revealed are that foreign intelligence services have penetrated the control systems of the US electric power grid and have left behind "logic bombs" and "trap doors;" data about America's latest fighter aircraft, the F-35 Lightning II, has been copied off the networks of defense contractors and sent overseas; the Pentagon plans to appoint a new four star general to run a new Cyber Command based on the National Security Agency (NSA); and a National Academy of Sciences blue ribbon panel has urged caution about the US engaging in offensive cyber war.

'Computer glitch' disrupts Boston city payroll

Monty Solomon <monty@roscom.com>

Sat, 2 May 2009 01:25:53 -0400

Boston city employees could not be paid by direct deposit on 1 May 2009, as a result of an unspecified computer problem. The city has 17,000 employees, but it was not clear how many of those were affected. [Source: Andrew Ryan and Michael Levenson, *The Boston Globe*, 1 May 2009: PGN-ed]

http://www.boston.com/news/local/breaking_news/2009/05/computer_glitch.html

Teenage hiker's calls ignored; no street address

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

Fri, 8 May 2009 13:28:42 PDT

Rohan Sullivan, Associated Press, Sydney, Australia, 7 May 2009,
<http://www.miamiherald.com/news/world/AP/story/1037803.html>

Teenage hiker David Ireland used his cell phone to call Australia's equivalent of 911, SEVEN TIMES pleading for rescue after he became lost in tough scrubland and ran out of water in 100-degree (37 C) heat. Each time he got through, he was told he needed to give a street address before an ambulance could be sent. Shortly after the final call, Ireland collapsed and died of thirst. A subsequent inquiry identified deep flaws in the OZ emergency response system -- including an "astonishing lack of empathy" but the operators.

✶ Hackers Break Into Virginia Health Professions Database, Demand Ransom

*Monty Solomon <monty@roscom.com>
Tue, 5 May 2009 23:34:18 -0400*

Brian Krebs, *The Washington Post*, 4 May 2009

Hackers last week broke into a Virginia state Web site used by pharmacists to track prescription drug abuse. They deleted records on more than 8 million patients and replaced the site's homepage with a ransom note demanding \$10 million for the return of the records, according to a posting on Wikileaks.org, an online clearinghouse for leaked documents.

Wikileaks reports that the Web site for the Virginia Prescription Monitoring Program was defaced last week with a message claiming that the database of prescriptions had been bundled into an encrypted, password-protected file. ...

http://voices.washingtonpost.com/securityfix/2009/05/hackers_break_into_virginia_he.html
http://wikileaks.org/wiki/Over_8M_Virginian_patient_records_held_to_ransom_30_Apr_2009

✶ UC Berkeley health service hacked, with 160,000 at risk of ID theft

*Ari Ollikainen <ari@olteco.com>
May 8, 2009 3:24:58 PM EDT*

[From Dave Farber's IP]

[Source: Henry K. Lee, UC hacking leaves 160,000 at risk of ID theft,
San Francisco Chronicle, 8 May 2009; PGN-ed]

Overseas hackers may have stolen confidential information belonging to tens of thousands of students and alumni at UC Berkeley and Mills College after gaining access to computer databases at the Berkeley campus' health services center. The databases contained Social Security numbers, health-insurance

information and non-treatment medical information, such as immunization records and names of some of the doctors that people may have seen and dates of medical visits, said campus spokeswoman Janet Gilmore. The hackers had access to the information for six months before they were discovered. The breach exposed 160,000 people to possible identity theft, Gilmore said. The university is contacting potential victims, who should consider placing a fraud alert on their credit reporting accounts. Among those at risk are 3,400 students at Mills College in Oakland who received, or were eligible to receive, health care at UC Berkeley.

<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/05/08/BAPA17H89B.DTL>

Archives: <https://www.listbox.com/member/archive/247/=now>

✂ How to guarantee bad passwords

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Thu, 30 Apr 2009 14:26:10 -0400

Getting users to choose good passwords and not write them down is always a challenge. It's a tradeoff - if you make the requirements too loose, then an attacker can guess the password. Make it too complex, and users have to write them down. The rules should be proportional to the sensitivity of the data that's accessible - read-only access to a newspaper shouldn't require as strong a password as financial or health information.

In the "too loose" category, the extreme case I've run into was a web site used for storing personnel information - which should have had relatively strong requirements - that required a two character password. No quality restrictions, no frequency of changes, nothing. Bad choice.

Today, I ran into the other end of the spectrum. A site that requires passwords that:

- * have a minimum length of 9 characters
- * must contain two upper and two lower case characters
- * must contain two digits and two special characters
- * must be different from the last 9 passwords you've used
- * must not contain a single quote

But the kicker: passwords may not contain any word of two letters or more. That's apparently determined (as best as I can tell through trial and error) by comparing every substring to a dictionary. So a password like 97to\$%ABC isn't acceptable, because "to" is a word. And 3-5zq?jbeLN isn't valid either, because "be" is a word. Presumably a1b2c3d4e5** would be a valid password, though. (I didn't try that one.) The helpful support person suggested not having any two letters in sequence to avoid tripping over the rule. Human usability, anyone?

Oh, and the password expires every 60 days, so just about when you've come up with something that matches their criteria, it's time to change again.

Now granted this site has some sensitive information, but wouldn't it make

more sense to use certificate-based authentication, which is far harder to attack in a brute force manner than passwords? (Assuming, that is, that you're not using certificates with MD5 signatures.)

I'd bet that 90% of their users have the passwords written down.

Lexis Nexis does an Oopis. Data breach...

danny burstein <dannyb@panix.com>

Fri, 1 May 2009 21:54:19 -0400 (EDT)

LexisNexis Warns 32,000 of Possible Data Breach [WINS radio news]

The LexisNexis online information service is warning 32,000 people their personal information may have been improperly accessed in a credit card fraud scheme that postal officials say bilked hundreds.

New York-based LexisNexis says in a letter mailed Friday that former customers of the service may have viewed information including names, birth dates and Social Security numbers.

rest: <http://www.1010wins.com/32K-May-Be-Victims-of-Breach/4314834>

"Server issues" delay Nielsen ratings

George Mannes <gmannes@gmail.com>

Wed, 6 May 2009 14:21:52 -0400

Brian Stelter, TV Networks Frustrated by Lengthy Ratings Delay,

The New York Times, 6 May 2009

<http://tvdecoder.blogs.nytimes.com/author/brian-stelter/>

<http://tvdecoder.blogs.nytimes.com/2009/05/06/tv-networks-frustrated-by-lengthy-ratings-delay/?ref=business>

ABC is deciding in the next two weeks whether to renew the TV show Castle. But the nation's television networks have not received the ratings for Castle or for any other show since Saturday. Nielsen Media Research, in the midst of a systems breakdown, has failed to deliver ratings for four days in a row, and the networks are increasingly impatient.

Without the overnight ratings that decide the fates of shows, producers and sometimes executives, the networks are flying blind only days before they make pivotal decisions about next season's schedules. Imagine running a movie theater without knowing how many tickets are being sold.

Nielsen attributed the delay to unspecified 'server issues'. The overnight ratings for Sunday, Monday and Tuesday are delayed, as well as the broader TV rankings for last week. ``Since it's necessary to release the data in sequence, we must process Sunday's TV ratings prior to the release of any days this week. We're working around the clock to get the TV ratings back

on schedule."

✦ Researchers Take Over Dangerous Botnet

ACM TechNews <technews@HQ.ACM.ORG>

Fri, 8 May 2009 14:13:03 -0400

Dark Reading (04 May 2009) Higgins, Kelly Jackson, ACM TechNews, 8 May 2009

University of California-Santa Barbara (UCSB) researchers temporarily commandeered an infamous botnet known for stealing financial data and found that the threat it represents is even greater than had been originally assumed. The Torpig/Sinowal/Anserin mini-botnet targets organizations and users to steal bank account information or other sensitive personal data.

It is considered more dangerous than big-name botnets because of its small scale and stealthiness. Torpig uses drive-by download attacks as its initial mode of infection, and upon infection the botnet can unleash crafty phishing attacks that produce bogus but authentic-looking Web pages and forms that trick users into exposing their credentials. The UCSB researchers accumulated approximately 70 GB of data for the 10 days they were in control of Torpig, and in that period the botnet stole banking credentials of 8,310 accounts from more than 400 financial institutions, including PayPal, Capital One, E-Trade, and Chase. Nearly half of the 1,660 stolen debit and credit card accounts the researchers counted belonged to victims in the United States. "The level of sophistication, the amount of data that it is able to steal, and the fact that it has been active for more than three years is truly remarkable," says UCSB researcher Brett Stone-Gross. The researchers' disclosures provoked debate on whether the information they exposed about Torpig, its workings, and its victims could compromise efforts to eventually undo the botnet. "This [research] does create a road map ... for the [botnet] criminals to fix, and not just for others to exploit," says RSA's Sean Brady.

<http://www.darkreading.com/security/client/showArticle.jhtml;jsessionid=OOOXXFK3IM54QSNLPCKHSCJUNN2JVN?articleID=217201422>

✦ Materials Database Problem

Gene Wirchenko <genew@ocis.net>

Wed, 06 May 2009 20:39:32 -0700

[This is a scary excerpt from a recent post in alt.folklore.computers. GW]

Unlike you, I actually still have a job. Guess what I do? I'm a Database Manager. I've had to deal with and fix more f**kups than you've had hot dinners.

For example, a current task is updating the TACO table released by the Illinois Environmental Protection Agency. Standard procedure is to compare the current update to the previous release and check for discrepancies.

Now, it's possible that the CAS number of Tin that was incorrect in the old table (440-31-5 instead of 7440-31-5) was a typo on the part of the person entering the data.

But when I noticed the CAS number of bis(2-chloroisopropyl)ether was 39638-32-9 instead of 108-60-1, that is definitely NOT a typo (unless the person entering the data sneezed at that moment.)

It was clearly a f**kup on the part of the state, obviously caused by the fact that bis(2-chloroisopropyl)ether & 2,2'- dichlorodiisopropylether are both C6 H12 CL2 O.

♣ Strange cash register arithmetic favors the house

*Bart Thielges <Bart.Thielges@synopsys.com>
Wed, 6 May 2009 11:46:47 -0700*

Yesterday I noticed an item on sale for a great price so I picked up four and proceeded to the checkout. When the cashier rung up the items oddly the fourth was charged at the non sale price. We quickly surmised that there was probably a limit of three available at the sale price.

Since I wasn't interested in paying the normal price for the fourth item, I asked to take that one back. Normally this is a quick routine matter. The cashier voids the item by hitting a key on the cash register and then re-scans the item to deduct it from the tab. What happened next was bizarre. Instead of deducting the normal price of \$3.49 that I was charged, it deducted the sale price of \$1.88. Hmmmm.... I was assuming that the register would have used a stack model, removing the last item that had transacted at \$3.49. Maybe the register software was using FIFO instead? Then it got more surreal.

Fortunately no-one was waiting in line so the cashier voided the other 3 items, hoping to clear the FIFO. But all 4 items deducted the sale price of \$1.88 from the total. None of them deducted the normal price of \$3.49. So here we have the strange arithmetic of $A+B+C+D - (A+B+C+D) > 0$. In fact if the cash register software is to be believed $\$0.00 = \1.61 which is the amount remaining on the cash register that I would pay for a null basket.

The only way out was to void the entire transaction (which required the manager to intervene) and start over. So here we have a state machine that enables easy access to an unfavorable state (overpaying for a item) but difficult to transition back out to the favored state (because the manager is required). This creates something of a trap that will result in some customers overpaying. If you make the mistake of bring sale items that exceed the limit (easy to do since the limit was not posted), you will overpay unless you and the cashier take these actions :

1) Notice the overcharge (I would have missed this had the cashier not been

alert)

2) Notice that voiding an item does not remove the overcharge and/or :

3) Call a manager to void the entire transaction

This occurred at a large USA retail chain with thousands of stores and millions of customers. This retailer stands to reap a windfall profit from customers who don't notice that they are being overcharged.

If a similar situation occurred in casino gaming machines you can bet that regulators would become quickly involved.

✂ Re: Credit card numbers *not* plucked out of the air at FL Best Buy

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

Mon, 9 Mar 2009 08:57:21 -0400

(Re: [RISKS 25.60](#))

[Apologies for missing this one earlier. Thanks to JK for poking me. PGN]

It would be good if people would do the research necessary to avoid spreading misinformation.

This theft of credit-card numbers was not accomplished by eavesdropping on WiFi networks, but rather through the use of a skimmer. See, for example, <http://awfulmarketing.com/2009/02/09/credit-card-numbers-stolen-from-best-buy-in-fl/> for additional details.

✂ Real-Time Networks RTN'09

Infos about ECRTS <em-rt-info@wu-wien.ac.at>

Wed, 6 May 2009 11:34:42 +0200

[The paper deadline is 10 May 2009. Strangely, security is not explicitly mentioned in the list of potential topic areas. PGN]

8th International Workshop on Real-Time Networks (RTN'09)

<http://www.hurray.isep.ipp.pt/rtn09>

June 30, 2009, Dublin, Ireland

in conjunction with the

21th Euromicro Intl Conference on Real-Time Systems (ECRTS'09)

<http://ecrts09.dsg.cs.tcd.ie/>

The workshop is seeking original research and position papers dealing with hot topics in real-time networks.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 67

Saturday 16 May 2009

Contents

- [Emirates Tail Strike at Melbourne 20 Mar 2009](#)
[David Landgren](#)
- [Joke foils chess software](#)
[Fred Gilham](#)
- [Canada's tax agency computers pile up](#)
[Ken Knowlton](#)
- [New key-derivation function](#)
[David Magda](#)
- [iCal/iPhone/iPod dislike senior citizens?](#)
[Steven M. Bellovin](#)
- [JHU insider may have breached more than 10,000 patient records](#)
[PGN](#)
- [DC financial-aid agency discloses personal data of 2,400 students](#)
[George Mannes](#)
- [DHS Sensitive But Unclassified sharing platform hacked](#)
[PGN](#)
- [French net piracy bill signed off](#)
[Amos Shapir](#)
- [Kiwibank discovers perils of Google Adwords with 100% Interest campaign](#)
[Max Power](#)
- [Australian emergency services can't break through their own firewall](#)
[Danny Burstein](#)
- [Re: FAA ATC shutdown](#)
[Gene Wirchenko](#)
[Al Macintyre](#)
[Pete Kaiser](#)
[Mike Coleman](#)
[Linda Gorman](#)
- [REVIEW: "Googling Security", Greg Conti](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

✈ **Emirates Tail Strike at Melbourne 20 Mar 2009**

<david.landgren@groupe-bpi.com>

Tue, 12 May 2009 10:47:43 +0200

The Australian Transport Safety Bureau (ATSB) has released its preliminary report regarding the take-off of an Airbus A340-500 flown by Emirates that nearly turned into a disaster.

http://www.atsb.gov.au/publications/investigation_reports/2009/AAIR/pdf/AO2009012_Prelim.pdf
<http://xrl.us/bescyd>

The pilots used a laptop to develop the flight plan which involved a reduced-power take-off. The performance calculation used to determine the power settings required on the engines were based on an incorrect value. The weight of the aircraft was entered as 262 tonnes instead of 362 tonnes. Neither the pilot nor the co-pilot caught the error during cross checks,

The co-pilot attempted to rotate the aircraft to commence the climb, but it failed to respond since the engines were delivering power for a much lighter craft. The pilot selected maximum thrust and the aircraft finally became airborne, but not after having suffered three tail strikes, overrunning the end of the runway and knocking out some ground infrastructure.

They dumped fuel and landed successfully. The airframe suffered damage to structures made from composites and apparently no-one is quite sure how to repair it as this has never occurred before.

RISKS readers will recall a similar incident which did not end so happily. In October 2004, a 747 freighter was launched down a runway with its engine delivering insufficient power, due to errors made in calculating the take-off profile. 250 metres beyond the end of runway it managed to climb into the air, and 100 metres further it struck an earth berm, severing the tail. The craft crashed and all seven crew members were killed.

<http://www.flightglobal.com/articles/2006/07/04/207571/canada-old-data-led-to-october-2004-crash-on-take-off-of-mk-airlines-747.html>
<http://xrl.us/bescyb>

✂ Joke foils chess software

Fred Gilham <gilham@AI.SRI.COM>

Thu, 14 May 2009 07:48:54 -0700

This article tells how the custom of having a celebrity make the first move to open the tournament backfired when he made two consecutive moves with the White pieces as a joke. This caused the software feeding the games to the outside world to freeze up and they were not able to get it working again that day.

<http://reports.chessdom.com/news-2009/mtel-masters-software-r1>

The beginning of the last paragraph was rather amusing: "The technical staff of Mtel Masters proved useless and could not repair the live feed."

✂ Canada's tax agency computers pile up

Ken Knowlton <KCKnowlton@aol.com>

Tue, 12 May 2009 10:36:02 EDT

"Canada's tax agency is stockpiling hundreds of old computers containing sensitive taxpayer data that officials are unable to delete. Police warned federal agencies two years ago that their disk-erasing software was unreliable, but the tax agency failed to buy new software. Since then, tax offices around the country have been storing the old hard drives in locked facilities. Some have resorted to smashing the computers to destroy the data, but police say that technique has mixed results. To properly destroy a drive, they say, it should be run through commercial equipment that slices it into bits no bigger than the width of a pencil." [from **The Week** mag. 8 May 2009, page 8]

✂ New key-derivation function

David Magda <dmagda@ee.ryerson.ca>

Sun, 10 May 2009 21:48:20 -0400

Colin Percival, who happens to be the FreeBSD Security Officer, has created the "scrypt" key-derivation function that he's presenting at BSDCan 2009:

> We estimate that on modern (2009) hardware, if 5 seconds are spent
> computing a derived key, the cost of a hardware brute-force attack against
> scrypt is roughly 4000 times greater than the cost of a similar attack
> against [OpenBSD's] bcrypt (to find the same password), and 20000 times
> greater than a similar attack against PBKDF2.

<http://www.tarsnap.com/scrypt/>

There's a sixteen-page paper that describes the algorithms and logic behind these conclusions.

✂ iCal/iPhone/iPod dislike senior citizens?

"Steven M. Bellovin" <smb@cs.columbia.edu>

Wed, 13 May 2009 14:53:09 -0400

When you view your iCal birthday list on iPhone or iPod, the birthdays of people over 75 disappear. They look like an appointment that has repeated

too many times, because the software cannot handle events that occur more than 75 times. [PGN-ed; MacWorld's Christopher Breen suggests duplicating the entry -- which he notes works just fine unless someone lives over 150.]
http://www.macworld.com/article/140596/2009/05/iphone_repeating_birthdays.html

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

JHU insider may have breached more than 10,000 patient records

*"Peter G. Neumann" <neumann@csl.sri.com>
Fri, 15 May 2009 9:45:13 PDT*

An employee at Johns Hopkins Hospital may have leaked the personal information of more than 10,000 patients in an identity fraud scam. Some 31 individuals with connections to Johns Hopkins have reported identity thefts since 20 Jan 2009. JHU security people have identified a single employee working in patient registration, who is expected to be indicted. Law enforcement agencies suspect the thefts might be part of a fraudulent driver's license scheme discovered in neighboring Virginia. [Source: Tim Wilson, DarkReading, 13 May 2009, PGN-ed; TNX to Jeremy Epstein]
<http://www.darkreading.com/insiderthreat/security/privacy/showArticle.jhtml?articleID=217400831>
<http://www.oag.state.md.us/idtheft/Breach%20Notices/ITU-168293.pdf>

DC financial-aid agency discloses personal data of 2,400 students

*George Mannes <gmannes@gmail.com>
Thu, 14 May 2009 17:03:40 -0400*

Bill Turque, Data About Students Dispersed in Breach
E-Mail Included Personal Information, *The Washington Post*, 23 May 2009
<http://www.washingtonpost.com/wp-dyn/content/article/2009/05/11/AR2009051102299.html>

The D.C. agency that handles college financial aid requests said yesterday that it had accidentally e-mailed personal information from 2,400 student applicants to more than 1,000 of those applicants. The Office of the State Superintendent of Education (OSSE) said it has notified all students of the breach, which occurred when an employee of the agency's Higher Education Financial Services Program inadvertently attached an Excel spreadsheet to an e-mail. The information included student names, e-mail and home addresses, phone and Social Security numbers and dates of birth.

The disclosure involved the "DC OneApp," an online application that allows D.C. students to apply for a series of grant programs. They include DCTAG, which provides awards of up to \$10,000 toward the difference between in-state and out-of-state tuition at public four-year-colleges in the 50 states. The accidental disclosure went to about 1,250 DCTAG applicants.

OSSE never publicly announced the breach, which occurred Wednesday. It did express regret for the incident in an e-mail sent to students and parents

the next day. A parent made the e-mail available to *The Washington Post* over the weekend.

The agency urged all recipients to immediately destroy the spreadsheet attachment. It also offered one-year subscriptions to a credit-monitoring service to help students guard against identity theft or other fraud.

"The OSSE takes very seriously our responsibility to keep personal information private and sincerely apologizes to everyone for any inconveniences," the e-mail said. The agency said it was taking steps to shorten Social Security numbers on any reports or spreadsheets and was reviewing policies and security measures for handling confidential student information.

Parents reacted angrily to word of the breach. Brenda Thomas, whose daughter Leah is a senior at Maret, a private school in Northwest Washington, said she was 'livid'. "We tell her how important it is not to give her Social Security number out, not even to join Facebook, for goodness' sakes." Even more irritating was that she was recently informed by OSSE that Leah, who will attend Stanford University this fall, was ineligible for assistance because the family exceeded income guidelines. "And now this," Thomas said.

🚩 DHS Sensitive But Unclassified sharing platform hacked

*"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 14 May 2009 14:02:55 PDT*

The Homeland Security Information Network (HSIN) platform for sharing sensitive but unclassified data with state and local authorities was hacked recently. The initial penetration in late March was brief and limited, and was followed by a more extensive one in early April, using the HSIN account of a federal employee or contractor. The bulk of the data obtained was federal, but some state information was also accessed, and contained some administrative data (telephone numbers, e-mail addresses, but not SSNs, drivers' licenses, or financial data). [Source: Ben Bain, Homeland Security Information Network suffers intrusions, *Federal Computer Week*, FCW.com, 13 May 2009; PGN-ed; thanks to Jeremy Epstein.]

<http://fcw.com/articles/2009/05/13/web-dhs-hsin-intrusion-hack.aspx>

🚩 French net piracy bill signed off

*Amos Shapir <amos083@hotmail.com>
Wed, 13 May 2009 17:43:29 +0300*

A controversial French bill which will disconnect people caught downloading content illegally three times has been given final approval.

It would be fun (for the non-French, at least) watching them try to enforce it. See for reference "The source of semantic content" in [RISKS-16.87](#) (<http://catless.ncl.ac.uk/Risks/16.87.html#subj3>). The situation is much

more complicated now; with mobile devices which can pick up content from the "data cloud" any time, anywhere, how can they even begin to define legally "downloading content" and "disconnect people"?

Full story at: <http://news.bbc.co.uk/2/hi/technology/8046564.stm>

Kiwibank discovers perils of Google Adwords with 100% Interest campaign

Max Power <dist23@juno.com>

Mon, 11 May 2009 04:00:27 -0700

There are many kinds of risks with targeted keyword marketing on the web. This is merely one example. Univerally keyword based marketing campeigns are not protected for "string" or "checksum" uniqueness. The "Uniqueness" option may emerge during this finance system crisis, but it will not be cheap.

Source: 11 May 2009

<http://www.interest.co.nz/ratesblog/index.php/2009/05/11/kiwibank-discovers-the-perils-of-google-adwords-with-100-interest-campaign/>

Kiwibank has launched a campaign aimed at business customers with the big 4 Australian owned banks that offers `100% interest' in their business. It even has its own website and readers are encouraged to search on "100% Interest" to find out more. The pitch is that Kiwibank is 100% interested in the customer's business. This campaign even has it's own website to inform would-be customers. The trouble with the Google Adwords approach is that it is vulnerable to ambush by a competitor. That is exactly what happened today when Westpac bought the sponsored link for 100% interest. Blogger Dan Roberts from Xebidy Strategic Design also wrote a blog about it to prove a point. Another one here on the need for better bank marketing did the trick too, putting it near the top of the natural search rankings.

Australian emergency services can't break through their own firewall

danny burstein <dannyb@panix.com>

Mon, 11 May 2009 01:26:28 -0400 (EDT)

(Re: [RISKS-25.66](#))

Following the news story about a youth near Sydney, Australia who couldn't get help from emergency services ([RISKS-25.66](#)), the focus in that excerpt was that the emergency dispatch computer system "needed" a street address, and the call receivers were stuck because they wouldn't/couldn't override that requirement. It turns out there's another risk from the story, courtesy of the just completed inquest:

Complicating matters was that when other people in the emergency services systems wanted to listen to the call to try to get a hint as to where he was, it was a lot harder than it should have been:

"Superintendent Patrick Paroz told Penrith Coroner's Court he made two separate requests to the state emergency services for copies of 000 calls made by the Sydney Grammar student. "He did not receive them until almost a day later. ... "A disc containing sound files of the calls had to be driven from the city to Katoomba because computer firewalls in the ambulance service system prevented police receiving them by email."

<http://www.news.com.au/story/0,27574,25396246-421,00.html>

✂ Re: FAA ATC shutdown

Gene Wirchenko <genew@ocis.net>

Mon, 11 May 2009 10:46:59 -0700

700 reasons why air traffic control systems may be hacked: A recent audit in the U.S. has found more than 760 high-risk vulnerabilities in Web applications used to support Air Traffic Control operations. These give attackers a way to gain access not just to underlying Web servers but potentially to other more critical backend systems.

<http://www.itbusiness.ca/it/client/en/home/News.asp?sub=true&id=53123>

✂ Re: FAA ATC shutdown

Al Macintyre <macwheel99@wowway.com>

Sun, 10 May 2009 16:43:23 -0500

Here's the full report

http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/ATC_Web_Report.pdf

It includes identification of which are the 11 ATC sites with ANY kind of protection, so that now terrorists, hackers, and other trouble makers know which are the hundreds of sites without any protection.

It is important for government to be open to the people in identifying problems, but some stuff needs to be kept confidential from potential trouble makers.

✂ Re: FAA ATC shutdown (Gorman, [RISKS-25.66](#))

Pete Kaiser <djc@resiak.org>

Mon, 11 May 2009 09:58:13 +0200

On Government IT competence

Linda Gorman's note is a partisan rant where it suggests that government is uniquely incompetent. That rant doesn't belong in RISKS.

In many years of consulting to government and (often large, sometimes huge international) business, I've seen nothing to suggest that government IT designers and creators are any less able than those in business; indeed, it has often astounded me that some businesses manage to operate at all, considering how grotesquely bad are their IT operations. If there's any difference with government IT in the USA, it may be simply where politics trumps good IT; or, for example, where protected entities like the FBI end up doing their IT work out of the sunlight of dispassionate good judgment (something I've often seen in business); where underfunded entities are asked to perform miracles on inadequate budgets (also often seen in business); or where the rewards to vendors are large and oversight is lacking (amazingly, also found in business). I could provide examples of any of this from businesses whose names everyone knows.

The proper response to these problems, no matter where they occur, is to exercise that dispassionate good judgment and oversight.

Businesses have many ways of concealing their IT incompetence that aren't available to government, especially the option of simple secrecy; and we write our laws to protect (if not always guarantee) their ability to make a profit even when they screw up.

Shall we talk about voting devices? Or perhaps the design and quality problems of certain operating systems used by hundreds of millions of persons daily?

✉ Re: FAA ATC shutdown (Gorman, [RISKS-25.66](#))

*Mike Coleman <tutufan@gmail.com>
Mon, 11 May 2009 11:49:18 -0500*

I nearly fell over in my chair when I read Linda Gorman's comment in RISKS 25.66. I've been reading RISKS for almost 20 years now, and no other submission comes close to being as politically biased and content-free.

Consider just the last sentence: "To date the myth or [sic] electronic systems to the rescue continues to grab people even though almost all of the real world tests of the effects of expanded government control suggest that the most likely result it [sic] higher costs and degraded care."

What myth? As we all know, sometimes electronic systems fail horribly and sometimes they work really well. Is Ms. Gorman seriously suggesting that they be eliminated?

Real world tests of expanded government control? Actually, the real world examples that come to mind--the health care systems of countries like Canada, Sweden, and Denmark--suggest that expanded government control leads to outcomes superior to those reached by private entities.

I smell an axe grinding...

RE: FAA ATC shutdown

"Linda Gorman" <linda@i2i.org>

Mon, 11 May 2009 12:03:33 -0600

Dear Mr. Coleman:

I merely suggest that the involuntary imposition of information systems on people who need or provide health care can lead to excess costs, massive problems with securing private information, and risks to life and limb. Those costs may exceed the benefits. Unfortunately, involuntary imposition is rapidly becoming federal policy in the United States.

Obviously electronic systems work very well in some health care related uses--people in the US would not have CAT scans or MRIs or nationwide Walgreens prescriptions without them. The question is who should decide who must use them, and who chooses the systems to be used, and whether we are safe in assuming that everyone has the same risk reward tradeoff.

As for the comment about grinding political axes, as I am sure you are aware, there is a large literature on comparative health care systems. Recent work does not necessarily support your claim that government run systems provide better results. A few examples of why this is true, and why such comparisons are difficult, are outlined below.

Leaving aside the problems of purchasing power parity and currency translation for non-traded goods, cost comparison is a problem because national accounting systems vary. For example, certain expenditures counted as health expenditures in the US national accounts are not included as health expenditures in Japan's national accounts. The OECD has a decade old program that has been discussing these differences and seeking to harmonize accounting systems. Progress is slow.

Cost comparisons are also hampered by the fact that many national governments impose price controls on health inputs. As a result, recorded payments to providers understate true costs. We can do cost comparisons between private and public systems in the United States, but even those are difficult because Medicare operates under a system of controlled prices, and people can and do switch between the private system, Medicare, and the Veterans Administration, and private systems and Medicaid, in order to optimize their care.

Another problem is that simple definitions differ across countries. Infant mortality rates are an easily understood example of this. For years, the US had been excoriated for having high infant mortality rates. In the 1990s, epidemiologists realized that there were major differences in infant deaths in the first 24 hours across countries. Further research led to the discovery that the mortality differences were created by differences in birth registration--in the US and Canada any birth in which a child showed any signs of life was counted as live. Some European countries would

classify the same very low birth weight babies as dead. Since very low birth weight babies also have the highest mortality risk, excluding them at birth made the European results look better than the US and Canadian rates. OECD comparative health statistics now include a note saying that cross country infant mortality rates are not comparable.

Finally, in order to accept your assertion that "the real world examples that come to mind--the health care systems of countries like Canada, Sweden, and Denmark--suggest that expanded government control leads to outcomes superior to those reached by private entities" one must believe that waiting lists, which exist in virtually all known government run health care systems, do not matter.

Swedish researchers, among others, have done a lot of work showing that they do matter. Waiting lists increase costs by causing enormous productivity losses, and they cause excess mortality as people die waiting for care. This may be part of the reason why the Swedes are now trying to move towards more private provision of health care. In passing, I should note that productivity losses, and losses due to excess mortality, are not included in most health care spending estimates.

I am sorry to have made a statement that you found so upsetting. I hope that these examples show that my comments simply reflect a conclusion that I believe is supported by recent health care research. I suppose that you are correct in saying that my comments are ideological in that in the best case one's ideas are formed by the facts as currently known, and by theory as currently accepted.

Linda Gorman, PhD, Director, Health Care Policy Center
Independence Institute, Golden, Colorado 80401 USA

REVIEW: "Googling Security", Greg Conti

*Rob Slade <rmslade@shaw.ca>
Thu, 14 May 2009 15:05:23 -0800*

BKGGLSEC.RVW 20091020

"Googling Security", Greg Conti, 2009, 978-0-321-51866-8,
U\$49.99/C\$54.99

%A Greg Conti conti@acm.org www.GregConti.com www.rumint.org

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

%D 2009

%G 978-0-321-51866-8 0-321-51866-7

%I Addison-Wesley Publishing Co.

%O U\$49.99/C\$54.99 416-447-5101 800-822-6339 bkexpress@aw.com

%O <http://www.amazon.com/exec/obidos/ASIN/0321518667/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0321518667/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0321518667/robsladesin03-20>

%O Audience i+ Tech 2 Writing 2 (see revfaq.htm for explanation)

%P 332 p.

%T "Googling Security: How Much Does Google Know About You?"

The title is ever so slightly misleading: the subtitle is much clearer. This is not about doing Web searches to find security tools or information, but, rather, the information that Google collects from (and relating to) Internet users in the course of providing its services and tools. The preface states that the intent is to raise awareness of the privacy risks involved in using Google, its utilities and services, and of similar systems and agencies. Conti does not, for the most part, present solutions: some activities admit of no resolution. Google is not being singled out because the author doesn't like the company, but because it is the largest and most pervasive search and information system, with the greatest implications, and because the policies and decisions resulting from discussions of these issues can be applied more generally.

Chapter one is an overview of the online world, and online activity, and the scope and capabilities of Google. There are extensive endnotes supporting the stories and studies cited in the text. The normal information flows involved with computer operations are outlined in chapter two, and Conti points out the potential areas of leakage. Although not named as such, he provides an excellent explanation of the trusted computing base (TCB), as well as reviewing covert channels such as TEMPEST and acoustic surveillance, and Internet entities. Turning more specifically to the structure of requests from browsers, chapter three notes the information that is captured by server logs. The author also notes data provided by users themselves, and that which can be obtained from statistical analysis of a large amount of activity.

Chapter four notes the various search sites and functions, as well as the intelligence that can be inferred about someone, simply by examining the search requests submitted. Communications, mostly Gmail, is the subject of chapter five. Chapter six examines the mapping and related imagery functions, discussing the information disclosed by requests for directions, as well as the occasional invasion of privacy involved in the collection of satellite photographs. (Personally, while I don't use Google Earth, I use Google Maps quite a bit. I was interested to see that my non-standard interaction with the system inadvertently protected against some of the dangers Conti points out. I don't "express interest" by clicking on the "Print" or "Link ..." buttons, but tend to copy the link location URL and use that. Of course, if Google buys up TinyURL I may be in trouble ... :-)

Tracing functions related to the provision of advertising, as well as malicious enterprises associated with commercial proclamations, are noted in chapter seven. Webbot, spider, or crawler operations are detailed in chapter eight. Although Conti did not promise a solution, chapter nine does provide recommendations and resources to raise awareness of the issues, and assist with protecting the reader's privacy. Chapter ten finishes off with a look to the future, and the forces which ensure that whether or not Google survives, the privacy situation online is unlikely to change.

The book is certainly interesting and illuminating. Internet users, for the most part, may have encountered security awareness material that speaks of the dangers of certain types of activities, but not necessarily of how much information they disclose in the course of normal pursuits. While Google is used as a specific example in many parts of this work, the internal

operations of many of the services and utilities are not examined to the internal depth they might have been. A more accurate title might be "Privacy While Surfing."

Which is an important enough topic to read about in any case.

copyright Robert M. Slade, 2009 BKGGLSEC.RVW 20091020

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org

<http://victoria.tc.ca/techrev/rms.htm>

http://blog.isc2.org/isc2_blog/slade/index.html <http://twitter.com/rslade>

<http://blogs.securiteam.com/index.php/archives/author/p1/>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 68

Saturday 23 May 2009

Contents

- [NY voter voted absentee, then died; ballot ruled invalid](#)
[PGN](#)
- [In a Lab, an Ever-Growing Database of DNA Profiles](#)
[David Hollman](#)
- [Computers and Medical Practice: Some actual data](#)
[Jerry Leichter](#)
- [Risks: Hackers 'destroy' flight sim site](#)
[Gabe Goldberg](#)
- [A Lesson in Internet Anatomy: The World's Densest Meet-Me Room](#)
[jidanni](#)
- [Re: "Server issues" delay Nielsen ratings](#)
[Jesse W. Asher](#)
- [Re: Materials Database Problem](#)
[Stuart Levy](#)
- [Re: Australian emergency services](#)
[Bob Frankston](#)
- [How small does the disk chunk have to be?](#)
[Fred Cohen](#)
- [Authentication and Identity theft](#)
[Jay R. Ashworth](#)
- [Re: Tail strikes from improper settings](#)
[Ken Knowlton](#)
- [Re: FAA ATC shutdown](#)
[Stewart Fist](#)
- [Is "security through obscurity" being called for in RISKS?](#)
[Fred Cohen](#)
- [Re: On Government IT competence](#)
[Scott Miller](#)
- [Book Review: The Science of Fear, Daniel Gardner](#)
[Bruce Schneier](#)
- [Info on RISKS \(comp.risks\)](#)

✉ **NY voter voted absentee, then died; ballot ruled invalid**

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

Fri, 22 May 2009 9:27:05 PDT

[Source: Tiebreaking Vote Cast by Dead Man; Runoff Required, AP item, PGN-ed.

Thanks to Joseph Lorenzo Hall for spotting this one.]

<http://www.1010wins.com/Tiebreaking-Vote-Cast-by-Dead-Man--Runoff-Required/4443153>

OGDENSBURG, N.Y. (AP) -- A school board election ended in a tie after an absentee ballot from one candidate's dead brother-in-law was ruled invalid. Vicky Peo and John Wilson each received 388 votes Tuesday for a seat on the Ogdensburg City School Board. The tying tally came after an absentee ballot from Peo's brother-in-law, Franklin "Peanut" Bouchey, was ruled invalid because he died three days before the election. Superintendent Timothy Vernsey said the ruling was based on both education and election law. Vernsey says a special election pitting Wilson against Peo must now be held.

[This is one of those cases that might fall through different cracks in different places. If this voter had opted for in-person early voting, his actual completed ballot was supposedly not attributable to him, and could not have been individually revoked. We know that in-person voting and absentee voting generally have different RISKS. In this case they might also have had different RULINGS -- especially the ambiguity of a one-vote margin under these circumstances might have caused a partisan judge to demand a revote anyway. Besides, dead people have been voting for many years -- unfortunately, it seems to be an old tradition. And in some voting technologies, one-vote margins are statistically a virtual tie anyway. PGN]

✂ In a Lab, an Ever-Growing Database of DNA Profiles

David Hollman <dah8@cornell.edu>

Tue, 12 May 2009 10:59:00 +0100

>From <http://www.nytimes.com/2009/05/12/science/12quan.html>

Interesting article on how the FBI processes thousands of forensic samples into its DNA database. Scant detailed information, but some mention of how the FBI plans to ramping up the quantity and quality of is processing by increasing automation. They claim that this will reduce the error rate, and maybe so (or not), but will the inevitable errors that remain be harder to detect and eliminate? (Is there a nice catchphrase for the effect where information in digital form has more credibility than in other forms?)

Excerpts:

In a Lab, an Ever-Growing Database of DNA Profiles
NY Times

...

The computers contain the National DNA Index System <<http://www.fbi.gov/hq/lab/codis/national.htm>>, a database of 6.7 million genetic profiles, the world's largest repository of forensic DNA information. Under a 2005 federal law, the database will continue to include convicted felons, but it will also add genetic profiles of people who have been arrested but not convicted and of immigrant detainees =97 for an estimated 1.3 million more profiles by 2012. ...

But keeping pace with the expansion of DNA databases is a major challenge for the agency, which has sought ways to speed the processing of DNA evidence. As of 2007, the Justice Department estimated the backlog at 600,000 to 700,000 samples. In 2002, the F.B.I. was processing about 5,000 DNA samples each year. With the help of new robotic systems, analysts with the crime lab plan to process 90,000 samples each month by 2010. ...

In addition to speeding up DNA typing, the robotics will help avoid mistakes. Contamination and mislabeling have been documented in at least five states; the fewer hands needed to process DNA, the better, said Richard A. Guerrieri, chief of the forensic DNA lab. Despite these improvements, F.B.I. officials still expect to struggle to stay abreast of the millions of new DNA samples expected to pour into the lab. Federal officials said that when Congress mandated the database expansion, it did not provide enough money. ...

✂ Computers and Medical Practice: Some actual data

*Jerry Leichter <leichter@lrw.com>
Mon, 18 May 2009 05:28:49 -0400*

The recent arguments about just how much computerization of medical data will help ultimately need to face up to real data. Some such data recently appeared.

[http://www.journalacs.org/article/S1072-7515\(09\)00200-2/abstract](http://www.journalacs.org/article/S1072-7515(09)00200-2/abstract)
(Full article requires membership or payment - I haven't read it.)

Summarizing the abstract: The study looked at the effects of the introduction of a Computerized Physician Order-Entry System (CPOE) on patient safety and on efficiency. "A total of 15 (0.22%) medication errors were discovered in 6,815 surgical procedures performed during the 6 months before CPOE use. After implementation, 10 medication errors were found (5,963 surgical procedures [0.16%]) in the initial 6 months and 13 (0.21%) in the second 6 months (6,106 surgical procedures) (p = NS). Mean total time from placement of order to nurse receipt before implementation was 41.2 minutes per order ... compared with 27 seconds per order using CPOE (p < 0.01)." (The dramatic time decrease was primarily due to the elimination of a transcription step.) There was also a reduction in "ancillary personnel positions".

The study concludes: "Present CPOE technology can allow major efficiency gains, but refinements will be required for improvements in patient safety."

Risks: Hackers 'destroy' flight sim site

Gabe Goldberg <gabe@gabegold.com>

Sun, 17 May 2009 13:20:49 -0400

[More details on the destruction and hackers would be interesting, as would some info on how a site running since 1996 wasn't backed up anywhere but ... on the site itself.]

Hackers 'destroy' flight sim site

Flight simulator site Avsim has been "destroyed" by malicious hackers.

The site, which launched in 1996, covered all aspects of flight simulation, although its main focus was on Microsoft's Flight Simulator.

The attack took down the site's two servers and the owners had not established an external backup system.

<http://news.bbc.co.uk/2/hi/technology/8049780.stm>

A Lesson in Internet Anatomy: The World's Densest Meet-Me Room

<jidanni@jidanni.org>

Sun, 17 May 2009 06:17:59 +0800

In the bowels of the world's most densely populated Meet-Me room -- a room where over 260 ISPs connect their networks to each other -- a phalanx of cabling spills out of its containers and silently pumps the world's information to your computer screen. One tends to think of the Internet as a redundant system of remote carriers peppered throughout the world, but in order for the net to function the carriers have to physically connect somewhere. For the Pacific Rim, the main connection point is the One Wilshire building in downtown Los Angeles.

If this facility went down, most of California and parts of the rest of the world would not be able to connect to the Internet. Tour one of the web's largest nerve centers, hidden in an otherwise nondescript office building.

http://www.wired.com/techbiz/it/multimedia/2008/03/gallery_one_wilshire

<http://en.wikipedia.org/wiki/Meet-me-room>

Re: "Server issues" delay Nielsen ratings (Mannes, [RISKS-25.66](#))

"Jesse W. Asher" <jesse.w.asher@gmail.com>

Sun, 10 May 2009 17:15:18 -0400

While it will certainly be denied, the length of this outage can be directly

attributed to the outsourcing of server administration to an Indian firm Tata Consultancy. Nielsen laid off (or drove off) many of its most important assets and replaced them with Indians brought into this country from India to run these servers. The vast majority of the talent being used is sub par with very little experience in dealing with a complex set of systems such as those used by Nielsen.

See

<http://tvdecoder.blogs.nytimes.com/2009/05/06/tv-networks-frustrated-by-lengthy-ratings-delay/#comments> for more information.

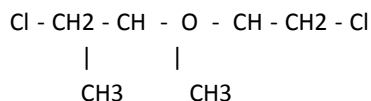
Re: Materials Database Problem (Wirchenko, [RISKS-25.66](#))

Stuart Levy <slevy@ncsa.uiuc.edu>

Wed, 13 May 2009 20:21:40 -0500

[bis(2-chloroisopropyl)ether == 2,2' dichlorodisopropyl ether!]

That looked funny to me. I would have thought that both bis(2-chloroisopropyl)ether and 2,2'-dichlorodisopropyl ether would refer, not just to compounds with the same numbers of atoms, but to the same structure -- they should be chemical synonyms:



And sure enough they are, and the EPA knows it. Googling for each CAS number turned up useful pages, especially this one from US EPA:

<http://www.epa.gov/iris/subst/0407.htm>

Substance Name Bis(2-chloro-1-methylethyl) ether CASRN 108-60-1

At the bottom of the page is the update history for this chemical's record, including these:

06/06/2000 All CASRN changed from 39638-32-9 to 108-60-1

12/03/2002 I.A.6. Screening-Level Literature Review Findings message has been added.

03/15/2004 VIII. Edited synonyms.

11/30/2007 All Chemical name changed from bis(2-chloroisopropyl) ether to bis(2-chloro-1-methylethyl) ether.

So, the 39638-32-9 number is a few years out of date and worth correcting, but it's not the kind of confusion that the matching chemical formulas suggested.

(I may well have other complaints about the IL EPA, but not this one.)

Re: Australian emergency services (Burstein, [RISKS-25.67](#))

"Bob Frankston" <Bob19-0501@bobf.frankston.com>
Sun, 17 May 2009 18:56:53 -0400

... can't break through their own firewall

I do need to preface this with the usual caveat about the risk of taking news stories at face value and setting policy in response to incidents. That said ...

Just curious -- did anyone think of just playing the audio over a standard phone line by holding the phone near a speaker? Did any involved in the inquest think to ask that question?

Perhaps the bigger problem here is the reliance on the artifacts of technology without basic understanding. But then how is it any different from falsely ascribing to broadband the properties that are really due to Internet connectivity (my current sound bite)? In this case the audio was in the computer silo not the telephony silo.

To be fair, the failure to be creative is a general problem -- and one can be taught not to think creatively by punishing exceptions like this one very close to home, in which a cafeteria worker was suspended for offering students an alternative to vegiburgers when their promised grilled cheese sandwiches failed to arrive.
http://www.boston.com/yourtown/news/newton/2009/05/by_calvin_hennick_globe_corres_1.html

Well, I guess if someone thinks about it it could be added to the long list of enumerated exceptions to the long list of rules. After all the term "ambulance chaser" is a reminder of better dead than sued.

How small does the disk chunk have to be?

Fred Cohen <fc@all.net>
Sat, 16 May 2009 16:26:44 -0700

> ...Subject: Canada's tax agency computers pile up
> ...To properly destroy a drive, they say, it should be run through
> commercial equipment that slices it into bits no bigger than the width of
> a pencil." [from *The Week* mag. 8 May 2009, page 8]

RISKS readers will recognize immediately that the size of the chunks, if you are doing it this way, will have to be small enough to make the content on one chunk of no utility. At the density of a HDD, a pencil width holds quite a bit of data. I won't do a calculation for you, but clearly this is not small enough for a disk that holds even 100 gigabyte on 10 sq.in. (10 gigabytes/sq.in.)

Fred Cohen & Associates, 572 Leona Drive Livermore, CA 94550 1-925-454-0171
<http://all.net/> Join <http://tech.groups.yahoo.com/group/FCA-announce/join>

Authentication and Identity theft

"Jay R. Ashworth" <jra@baylink.com>
Tue, 19 May 2009 10:17:54 -0400 (EDT)

In the last several issues of RISKS, there have been a disproportionate number of stories about how the roof was going to fall in because there was a "large data breach including people's (US) Social Security Numbers".

It seems worth taking a look again, explicitly, at why exactly that's a problem... as that's not the underlying cause of the trouble, and no one seems to be working on the thing that *is* the underlying cause, despite over a decade -- at least -- of us flogging it around the barn here in RISKS.

The problem, of course, is one of authentication, on two levels.

The second is easier to solve, but not as applicable to identify theft; the first bears directly on identity theft (more properly, "unauthorized credit reputation injury"), but is much harder to solve.

==

The first and larger problem is one of authenticating that a random person presenting themselves to you is actually the individual -- with a name, address, and possibly SSN -- whom they say they are, and not someone who has stolen that person's credentials.

The other half of that is interlocking credit grantors with credit bureaus so that they all agree they're talking about the same person... without the requirement that the US start issuing national ID cards, which is a major third-rail political issue -- to the point where states were refusing to implement the RealID program for driver license conformation promulgated by the last administration.

The second problem is authenticating already existing customers who wish to make changes to their accounts. This one is far easier to do properly; it entails two major points:

- 1) Using ad-hoc authenticators instead of "things only the customer should know". Once your mother's maiden name or the city in which you were born -- or your Social Security Number (which the government says should not be used as an authenticator for this sort of thing in the first place) "leak", they're useless as authenticators, because they never change.

In fact, Microsoft/Carnegie Mellon research to be released at the IEEE Symposium on Security and Privacy this week shows just how insecure "fixed" challenges (obvious ones like Mother's Maiden Name, chosen by the

business, not the customer) actually are: 1 in 4 chance of guessing by people who know the individual, *1 in 6* by random strangers.

<http://it.slashdot.org/article.pl?sid=09/05/19/0037208>

The only thing valid as an authenticator is a challenge and response *both chosen by the customer* -- at the time of account creation once you've authenticated the customer's ID, or in some secure out of band fashion when a breach may have occurred.

2) Anyone who holds authenticator information in a customer database needs to audit access to it, and do something about the audit data they gather; watching for patterns at the least, and actually checking who had access to it if an adverse report is made -- this is partially to protect from bad actors at the granting company, and partly to make it possible for customers stupid enough to use the same authenticator at multiple suppliers to determine who leaked it if they are stuck with fraudulent transactions.

We all know that people *shouldn't* reuse authenticators, but planning systems around the idea that they won't is ... a poor design choice?

But even this seems too much for most companies: I have seen, in my personal interactions with card companies, utilities, and the like, occasional bursts of "we'll let you specify an authenticator question and answer, if you don't like any of our pre-specified choices" (and you shouldn't), but they're a) few, b) far between, and c) tend to go away again, mostly because they were some smart person's good idea, instead of CIO level fixed company policy, which is apparently what's necessary. In at least one case, I have such an authenticator, but the agents are always bemused to see it, because that option "hasn't been offered for some years, now".

==

That first problem I mentioned, though, is the sticker: how do you authenticate that a person is validly whom they claim to be when, randomly, they walk up to you and ask to open an account -- or worse, call, write, or web into you and ask to start an account.

Lots of companies placed in this position use the knowledge of an SSN -- and let's be clear here; it's not just the contents of the SSN that are the authenticator, *it's the fact that you know it* -- as authentication that you are who you say you are.

[Here comes the money quote :-)]

And the result of that is that they've overloaded the semantics of a SECRET onto a datum that was never meant to be secret -- or, more to the point, to *need* to be secret. In consequence of which, lots of older systems don't treat it that way -- they don't obscure it from view, or audit access to it. And it travels around in cleartext since it is not *only* an authenticator, but *also* an *identifier* -- and this is the root cause of the problem.

It *must* be plaintext to be usable as an identifier... and it *must not* be

plaintext to be useful and safe as an authenticator.

[Does that state it clearly enough?]

At the moment, though, companies don't necessarily have any choice, since there's no other cookie that can be passed from a customer to a credit grantor to a credit reporting agency, and uniformly identify the same person.

==

That's my analysis of the problem, anyway, and since I don't recall seeing anyone really break down, either in the public press or in more technical fora like RISKS, exactly where the failure lies, I have to assume that -- even though I know there are lots of people out there smarter than me -- the problem might well be that the people in position to fix it don't really know why it's a problem, be they systems designers, CIO's or legislators.

Since the problem affects both credit granting vendors *and* credit-reporting agencies on the way to affecting the customers, it's likely they will both have to cooperate to solve it.

One possible solution, as much as I hate granting to CRAs even more power than they already -- some say, unjustly -- possess, is to have the CRAs authenticate creditors directly in some reasonable fashion, and then do a one-time cookie-authentication system for customers to authenticate themselves to new credit-grantors, similar in spirit to the one-time credit card numbers which some banks now issue for on-line purchases.

This will not fix the second, smaller problem -- at least not directly -- but would pretty much wipe out the larger problem or identify theft: if you can't open a new account without tight coupling to the agency which authenticates both you and the seller to one another, then people can't run up bills in your "name", sticking you with both the bill and the reputation problems.

Since this would probably reduce the incidence of credit fraud in general quite markedly, I can't imagine that the credit grantors wouldn't want to participate in such a system.

Even if those commercial parties are on board, though, the problem of making the system design generally palatable to the public who also have to cooperate is a tough one, and one for which I don't have a specific answer yet.

It will be interesting (at least to me :-) to see what opinions others in the RISKS community have to my delineation of the questions, at least.

Jay R. Ashworth, Ashworth & Associates, St Petersburg FL +1 727 647 1274
<http://baylink.pitas.com> <http://photo.imageinc.us> jra@baylink.com

✶ Re: Tail strikes from improper settings (Landgren, [RISKS-15.67](#))

Ken Knowlton <KCKnowlton@aol.com>

Tue, 19 May 2009 17:11:09 EDT

An airplane on a take-off run clearly could perform an automatic sanity check (comparing thrust settings and actual acceleration with gross weight, air speed/temperature/pressure, flap settings ...) and raise an alarm if something's seriously amiss. (It cannot easily automatically know other important things like runway length, aerodynamic effect of ice on wings, obstacles ...). Indeed, the Halifax report does briefly mention that authorities suggest "systems to warn crews of inadequate take-off performance." So what's the problem with the development and installation of such systems? Technical complexity? Expense? Reliability? Training? Longer checklist for pilots? Legal mess with false positives/negatives?

RE: FAA ATC shutdown (Gorman, [RISKS-25.66](#))

Stewart Fist <stewart_fist@optusnet.com.au>

Sun, 17 May 2009 10:45:02 +1000

> ... one must believe that waiting lists, which exist in virtually all known
> government run health care systems, do not matter.

Waiting lists also exist in virtually all known private health care systems. As an long-term ex-private patient, who has now been forced back onto the Australian public health-care system for financial reasons, I've experience the best and worst of both ends of the spectrum.

In my experience, there's very little between them in Australia - both in terms of the quality of the care, the compassion and training of the staff, and in the waiting time for access. I've spent much more time in the waiting rooms of specialist doctors who charge highly for their services, as I do with my local bulk-billed (government paid) local doctor.

It is true that my public-hospital hip replacement waiting time would have been shortened from three months, down to one month -- but since I'd put up with the problem gradually worsening over the previous three years, this was hardly consequential. If it had been heart surgery, there would have been no difference.

However the total cost of the hip replacement to me --- hospital, surgeons, prosthesis, and everything was zero. Loss of productivity for the nation -- also zero. Risk of dying while waiting the extra two months -- not far above zero

I think Ms Gorman needs to get out of Colorado and see how the rest of the world operates before she influences the setting of the state's health-care policy.

Stewart Fist, 70 Middle Harbour Rd, LINDFIELD, NSW 2070 Australia

Is "security through obscurity" being called for in RISKS?

Fred Cohen <fc@all.net>

Sat, 16 May 2009 16:33:48 -0700

Re: FAA ATC shutdown (McIntyre, [RISKS-25.67](#))

> It is important for government to be open to the people in identifying
> problems, but some stuff needs to be kept confidential from potential
> trouble makers.

[Thanks, Fred. I was hoping someone would make that observation! PGN]

Re: On Government IT competence (Kaiser, [RISKS-25.67](#))

Scott Miller <SMiller@unimin.com>

Mon, 18 May 2009 09:21:38 -0400

> Linda Gorman's note is a partisan rant where it suggests that government
> is uniquely incompetent. That rant doesn't belong in RISKS.

In common (US) parlance, "partisan" refers to a bias in favor of one of the two political parties enfranchised by voting regulations: Democrat or Republican. Since both parties routinely promote increased government power as the superior solution to nearly every problem or issue (differences are in the details, and increasingly marginal; e.g - the recent "rescue" of the financial system, begun by a Republican regime, embraced and extended by the Democrat politicians who replaced that regime), I fail to see how Mr. Kaiser's characterization of her post as "partisan" (even if his analysis is accepted at face value) is at all accurate. Further, how is the opinion expressed in Ms. Gorman's post less appropriate to this list than the many others that I have read here on various topics suggesting that government is uniquely competent?

> Shall we talk about voting devices?

Electronic voting systems are IT projects largely contracted by government exclusively to favored private (some would write "mercantilist") contractors (Diebold, Sequoia, etc.) For well over a decade, ATC (tracon & en route alike) systems have been IT projects largely contracted by government exclusively to favored private (some would write "mercantilist") contractors (LockMart, SunHelo<sp?>, etc.) And the point of differentiation was intended to be?

Book Review: The Science of Fear, Daniel Gardner

Bruce Schneier <schneier@SCHNEIER.COM>
Fri, 15 May 2009 02:13:07 -0500

Excerpted from Bruce's CRYPTO-GRAM, May 15, 2009
<crypto-gram-list@schneier.com>

Daniel Gardner's *The Science of Fear* was published last July, but I've only just gotten around to reading it. That was a big mistake. It's a fantastic look at how humans deal with fear: exactly the kind of thing I have been reading and writing about for the past couple of years. It's the book I wanted to write, and it's a great read.

Gardner writes about how the brain processes fear and risk, how it assesses probability and likelihood, and how it makes decisions under uncertainty. The book talks about all the interesting psychological studies -- cognitive psychology, evolutionary psychology, behavioral economics, experimental philosophy -- that illuminate how we think and act regarding fear. The book also talks about how fear is used to influence people, by marketers, by politicians, by the media. And lastly, the book talks about different areas where fear plays a part: health, crime, terrorism.

There have been a lot of books published recently that apply these new paradigms of human psychology to different domains -- to randomness, to traffic, to rationality, to art, to religion, and etc. -- but after you read a few you start seeing the same dozen psychology experiments over and over again. Even I did it, when I wrote about the psychology of security. But Gardner's book is different: he goes further, explains more, demonstrates his point with the more obscure experiments that most authors don't bother seeking out. His writing style is both easy to read and informative, a nice mix of data and anecdote. The flow of the book makes sense. And his analysis is spot-on.

My only problem with the book is that Gardner doesn't use standard names for the various brain heuristics he talks about. Yes, his names are more intuitive and evocative, but they're wrong. If you have already read other books in the field, this is annoying because you have to constantly translate into standard terminology. And if you haven't read anything else in the field, this is a real problem because you'll be needlessly confused when you read about these things in other books and articles.

So here's a handy conversion chart. Print it out and tape it to the inside front cover. Print another copy out and use it as a bookmark.

Rule of Typical Things = representativeness heuristic
Example Rule = availability heuristic
Good-Bad Rule = affect heuristic
Confirmation bias = confirmation bias

That's it. That's the only thing I didn't like about the book. Otherwise, it's perfect. It's the book I wish I had written. Only I don't think I would have done as good a job as Gardner did. *The Science of Fear* should be required reading for...well, for everyone.

The paperback will be published in June.

<http://www.amazon.com/exec/obidos/ASIN/0525950621/counterpane/>

A copy of this essay, with all embedded links, is here:

http://www.schneier.com/blog/archives/2009/04/book_review_the.html



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 69

Sunday 24 May 2009

Contents

- [Another Boston subway crash with cell-phone implications](#)
[PGN](#)
- [HIV patients sue after records left on MBTA](#)
[Elizabeth Cooney](#)
- [NZ bank lends \\$10M instead of \\$10K; couple takes the money and runs](#)
[Ian Wells](#)
- [Re: NY voter voted absentee, then died; ballot ruled invalid](#)
[Paul Wallich](#)
[Harvey Fishman](#)
- [Fragility of telephone system](#)
[Jim Haynes](#)
- [SANS NewsBites gets it very wrong, fails to post a correction](#)
[Jonathan Kamens](#)
- [Re: Nielsen Ratings](#)
[Rupert Moss-Eccardt](#)
- [How to make memorable but secure passwords](#)
[Phil Colbourn](#)
- [Re: A Lesson in Internet Anatomy: The World's Densest Meet-Me Room](#)
[Jidanni](#)
- [Re: FAA ATC shutdown](#)
[Walter Roberson](#)
[Chris Drew](#)
[Gene S. Berkowitz](#)
[Al MacIntyre](#)
[Fred Cohen](#)
- [Re: On Government IT competence](#)
[Pete Kaiser](#)
- [eCrime Researchers Summit CFP](#)
[Monty Solomon](#)
- [Info on RISKS \(comp.risks\)](#)

Another Boston subway crash with cell-phone implications

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

Sat, 23 May 2009 20:52:13 PDT

At 7:18pm on 8 May 2009, one inbound subway train rear-ended another train in the Green Line in the Boston MBTA at 25 mph. The driver of the offending train (24-year-old Aiden or Aidan Quinn [both spellings appear in the same article from the *EDGE*], who reportedly had three auto speeding violations) was allegedly texting his girlfriend at the time. 49 passengers were injured and taken to the hospital, and three cars were crushed. This incident followed another similar case in 2008 in which another driver had allegedly been on her cell phone just before that train collided with the preceding one. [Source: PGN-ed from various news reports. Please browse the Web if want some of the background, which is way beyond the scope of RISKS.]

HIV patients sue after records left on MBTA (Elizabeth Cooney)

Monty Solomon <monty@roscom.com>

Sat, 23 May 2009 23:36:12 -0400

Four HIV-positive patients whose records were left behind on an MBTA train by a Massachusetts General Hospital employee are suing the hospital, contending their privacy was breached. In March 2009, the hospital notified 66 patients who received care at its Infectious Disease Associates outpatient practice that billing records bearing their names, Social Security numbers, doctors, and diagnoses had been lost by a manager who was riding the Red Line. She had brought the paperwork home for the weekend, but left it on the train when she returned to work Monday morning, March 9, according to a hospital security report. [Source: Elizabeth Cooney, HIV patients sue after records lost; Hospital worker left files on MBTA, *The Boston Globe*, 21 May 2009]

http://www.boston.com/news/local/massachusetts/articles/2009/05/21/hiv_patients_sue_after_records_lost/

NZ bank lends \$10M instead of \$10K; couple takes the money and runs

Ian Wells <familywells@gmail.com>

Sat, 23 May 2009 16:40:51 +1200

It is not public yet how this error occurred. Couple is being charged with fraud, who decided to be fugitives when a bank error gave them a \$10,000,000 loan instead of \$6,000,000.

<http://www.stuff.co.nz/national/crime/2428243/Couple-missing-after-10m-bank-bungle>

Ian Wells, Christchurch, New Zealand

Re: NY voter voted absentee, then died; ballot ruled invalid (R-25.68)

*Paul Wallich <pw@panix.com>
Sat, 23 May 2009 21:16:39 -0400*

It gets even more complicated than that. In some jurisdictions, one actually votes during early voting (at a machine or with whatever other tools the site uses), while in others one fills out what is effectively an absentee ballot and hands it to the clerk for storage until election day. (In the latter case, there's a double envelope, with the inner one unmarked and the outer one signed and named, and the name used by the clerk to cross a voter off the main register.) So someone who voted early by machine and then died would have their vote count, whereas someone who voted by the accurately but oddly-named in-person absentee ballot could in principle be culled. Here's a case where reusing existing methods for a new purpose actually improves accuracy compared to inventing new methods.

Re: NY voter voted absentee, then died; ballot ruled invalid ([R-25.68](#))

*Harvey Fishman <fishman@panix.com>
Sat, 23 May 2009 21:06:37 -0400 (EDT)*

> [Source: Tiebreaking Vote Cast by Dead Man; Runoff Required, AP item, PGN-ed.

I do not believe that we have in-person early voting in New York State. Certainly we do not have it in New York City (understandably, as polls are generally in places like schools which are dedicated to other uses except on election days), but I only assume that voting rules are state-wide. [Yes. PGN]

Fragility of telephone system

*Jim Haynes <jhaynes@earthlink.net>
Sat, 23 May 2009 20:52:23 -0500 (CDT)*

It's now been a while since the fiber optic cable cuts in the S.F. Bay Area. I've been waiting for an explanation of why cutting 3 or 4 fiber cables completely killed telephone service in all or part of three counties.

SANS NewsBites gets it very wrong, fails to post a correction

*Jonathan Kamens <jik@kamens.brookline.ma.us>
Sat, 23 May 2009 23:17:45 -0400*

I thought the following might be of interest to RISKS readers, both because I'm sure many of us also read (<http://www.sans.org/newsletters/newsbites/>) SANS NewsBites, and because this deals with misrepresenting computer-related risks in a very real way.

In a recent NewsBites issue (11.39), the following item appeared as the headline story:

>TOP OF THE NEWS

> --One In Five Teenagers Claim to Have Used Hacking Tools

>(15th May 2009)

>A recent survey of 4,000 teenagers between the ages of 15 to 18 years

>of age states that 17% of those surveyed know how to find hacking tools

>online with one third of that group admitting that they have used the

>tools....

In this little blurb, the editors of SANS make two statistical errors, one small and one very, very large.

Here's the actual press release contents: "The survey also revealed that 17 percent of adolescent users claim to have advanced technical knowledge and are able to find hacking tools on the Internet. Of these, 30 percent claim to have used them on at least one occasion."

The minor error is that 30% is less than one third. While a 3.33% difference might seem insignificant, it's little "telephone-game" changes like this that over time result in seriously divergences from reality. Note that one of the articles which SANS cited used the phrase "nearly a third," which is accurate, and SANS apparently saw fit to drop the "nearly."

The second, much more serious error, is that the percentage of teenagers who admitted that they have used the tools is not "one in five," but rather 30% of 17%, which comes out to 5%, or ONE IN TWENTY, a huge difference from what SANS reported.

I emailed the editors of SANS the same day this issue came out, pointed out both errors, and asked them to post a correction. The next issue was published three days later with no correction included. This is rather unfortunate.

I find it just a bit disturbing that none of the editors of NewsBites, supposedly experts in the field, found the "one in five" statistic sufficiently surprising to dig deeper and discover the truth of the matter. I certainly did.

✉ Re: Nielsen Ratings ([RISKS-25.68](#))

Rupert Moss-Eccardt <r.moss-eccardt@computer.org>

Sun, 24 May 2009 08:35:33 +0100

I must say I was surprised to see the assertion that the Nielsen server failures were directly attributable to the outsourcing.

Firstly, I thought this was a moderated list and the assertion is a rather bald one.

Secondly, and this is more of a risk, it appears from this and the comments posted to The New York Times article referenced that the real problem was that Nielsen had a set of systems with no real business continuity. According to former staff, if the comments are to be believed, the systems were fragile enough to be prone to failure if not cared for in special ways that weren't documented fully, or at all.

[Rupert, Many TNX for the comment. PGN]

How to make memorable but secure passwords

phil colbourn <philcolbourn@gmail.com>

Sun, 24 May 2009 20:42:51 +1000

Some people, perhaps most, have a system for making passwords. Some systems involve the use of the same password everywhere - easy to remember but if discovered their online life is easily accessed. Others have different passwords and write them down.

My system is to maintain long, virtually unique passwords which I never need to commit them to paper or electronic note.

My goals are:

- * at least 8 characters
- * the use uppercase, lowercase, digits and symbols/punctuation
- * the discovery of the system should not compromise my passwords
- * no need to record any password
- * be able to quickly work-out my password for any site

The System

- * Make up a memorable code with preferably uppercase, lowercase, numbers and symbols/punctuation.
- * For each site, consistently use some aspect of the site such as 3 or 4 letters/numbers of the site URL - modified in some systematic way - and add it to your memorable code. Add it using any rule you like.

There is a problem with this system: sometimes sites change their name which, for me, has happened once. In this case I have not needed to change my password but since most sites will send your password to you, should you forget, you can easily have your old password recovered and then you can change your password - it doesn't happen often.

Examples

Assume your memorable code is Ab19#z.

Example 1: Use the first, second, second-last and last characters of the site, added in reverse order, first and last capitalized, insert after the

4th character of your memorable code.

So a password for google.com would be Ab19EloG#z.

And for ibm.com it could be Ab19MbbI#z. (You should have some way to handle site names that 'fail' your system or require longer passwords than that of your system).

Example 2: Insert the memorable code into the first and last characters of the site name.

So the password for google.com would be gAb19#ze.

It goes without saying (hopefully) that you should make up your own system and you should probably not use my examples.

Ideas:

- * Consider using the organisation type or country code.
- * Consider using multiple systems. One for important sites and a simpler system for ad-hoc, single-use and other sites not containing personal data
- * Consider a version of the system for your home PC accounts

You should assume that your system could be discoverable, so you need to choose a memorable code that is secure by itself.

If you want to document your system, do so with care. You should not write it down verbatim - try to obscure it ;-)

Re: A Lesson in Internet Anatomy: The World's Densest Meet-Me Room

<jidanni@jidanni.org>

Sun, 24 May 2009 21:17:20 +0800

"without incurring local loop fees" mentioned in <http://en.wikipedia.org/wiki/Meet-me-room> is a factor encouraging putting so many eggs in one basket Re: <http://catless.ncl.ac.uk/Risks/25.68.html#subj5.1>

Re: FAA ATC shutdown (Kaiser, [RISKS-25.67](#))

"Walter Roberson" <roberson@hushmail.com>

Fri, 22 May 2009 14:35:51 -0500

Pete Kaiser, in suggesting reasons why IT might be bad in government, including the possibility of "where underfunded entities are asked to perform miracles on inadequate budgets".

I used to be a systems administrator for a government (outside the USA) in

an underfunded situation. I instrumented and measured and compared published Fortunate 500 surveys: our 2/3-person equivalent networking staff was achieving uptimes slightly better than the average 12-person dedicated network staff reported for the F500 companies -- and was doing so with equipment that was mostly already declared End Of Life by the respective manufacturers.

We worked, underfunded, in government, but we were quite dedicated -- as were the co-workers in other sites that I interacted with.

✂ FAA ATC shutdown & Gov't IT Competence (Kaiser, [RISKS-25.67](#)).

*"Chris Drew" <e767pmk@yehaa.co.uk>
Sat, 23 May 2009 22:37:02 +0100*

> Businesses have many ways of concealing their IT incompetence that aren't
> available to government, especially the option of simple secrecy; and we
> write our laws to protect (if not always guarantee) their ability to make a
> profit even when they screw up.

Yebbut... As I see it from a UK perspective:

- * If a company's IT project is ineffective or costs too much it will damage the company financially and may even put it out of business. In the case of a Government IT project, it can throw taxpayers' money at it until it either works, sort-of, or it is quietly abandoned (or dies of shame).
- * If a company's customers or suppliers feel that the company is storing or using their information improperly, they can take their business elsewhere. Citizens don't have any choice about dealing with and handing data to the Government.
- * If a company's IT project violates laws concerning, say, data protection or security of storage, then the company will likely find itself in big legal trouble. If a Government IT project is illegal..? Well there may be some sound and fury, but that's as far as it goes (e.g. "Private details/UK Government disks" saga, [RISKS-24.92](#) on).

Looks to me like the nature of RISKS of IT projects can vary a lot depending on who is the final customer and who is paying the bill.

✂ Re: FAA ATC shutdown (Gorman, [RISKS-25.66](#))

*"Gene S. Berkowitz" <first.last@verizon.net>
Sun, 24 May 2009 01:30:16 GMT*

"The cheapest and most effective remedy for induced anxiety is to ignore those who profit from it. Easily spotted, they are the ones who continue to repeat what has been soundly discredited in the course of the public debate,

and those who continue to grossly misrepresent the true state of affairs."
Linda Gorman, Independence Institute, Golden, CO, Extremists Create Stress
for Gain, 21 Mar 2000. http://www.i2i.org/main/article.php?article_id=294

Methinks Ms. Gorman should heed her own advice.

✂ Re: FAA ATC shutdown (Cohen, [RISKS-25.68](#))

"Al MacIntyre" <macwheel99@wowway.com>
Sat, 23 May 2009 20:50:25 -0500

Subject: Is "security through obscurity" being called for in RISKS?

> It is important for government to be open to the people in identifying
> problems, but some stuff needs to be kept confidential from potential
> trouble makers.

The IG report included a road map to what security has been installed, what has not been installed, what vulnerabilities exist, at which FAA sites, and what any troublemakers can do right now. If the FAA ever gets caught up implementing standard security advice and patches, the security will be pretty darn good, but based on past track records, that may be a fantasy. The purpose of the inspection was to identify what needed to be fixed, but we know darn well that with government inspections that it can be years between problems identified, and them actually getting fixed.

Before the report, I am sure many troublemakers already knew this stuff.

After the report, an army of me-toos also know. The effect, of the IG report, included magnifying the risk the FAA has put itself into.

It would be like you having a combination lock to your front door, and that combination being blasted on the Internet. Previously, the only people who knew the combination, were you, your family, some friends, some of their friends, some frequent vendors, and whoever has the hidden camera pointed at the touch pad where the secret pin code is keyed in. In your case, changing the password is fast & easy. The FAA does not have the funds, or expertise, to fix their almost total lack of cyber security. We are going to lose some aircraft full of passengers before this gets fixed. Thanks to the IG report, this will happen sooner rather than later.

I think that all *we* the people need to know is that hackers can take over 99% of the Air Traffic Control in America, take down 75% of the public utilities, whatever the figures are, without spelling out step by step how to do it, for the next home grown idiot terrorists who right now can be caught by FBI confidential informant witnesses, but with this kind of report, don't need to use communications tapped by NSA to implement a plot.

✂ Re: FAA ATC shutdown (MacIntyre, [RISKS-25.69](#))

Fred Cohen <fc@all.net>

Sat, 23 May 2009 20:26:55 -0700

I think that security through obscurity is a key component of the overall security plan of any real enterprise. I just get a bit annoyed when people act like it's somehow inappropriate to have/use it. Operations Security is all about deciding when and how to use obscurity, and deception is a part and parcel of any really good overall protection program I have seen.

Fred Cohen & Associates 572 Leona Drive Livermore, CA 94550

<http://all.net/> 1-925-454-0171

Re: On Government IT competence (Miller, [RISKS-25.68](#))

PK <djc@resiak.org>

Sun, 24 May 2009 12:06:02 +0200

Scott Miller's note is a partisan rant which, arguably, belongs in part in RISKS as commentary on what belongs in RISKS. Its partisanship lies where it departs from fact, and from informed technical opinion, to express unsupported political opinion about the motivation of US political parties. (I use "partisan" here not in the narrow context of a particular two American political parties, but in its wide sense.)

Here's a factual question related to RISKS in computing, one I touched in light of my own experience: is government -- not just US government -- worse at computing than private industry? (Not in my experience.) I'd welcome seeing some good data, though it's hard to imagine what it would be in light of the complexity of how large organizations actually operate, and of the large differences among businesses, and agencies of government, and governments, and fields of endeavor.

- > Further, how is the opinion expressed in Ms. Gorman's post less
- > appropriate to this list than the many others that I have read here on
- > various topics suggesting that government is uniquely competent?

Unsupported opinion that government is uniquely [in]competent at technical work is as worthless as any unsupported opinion, and isn't a risk of computing. Let's go elsewhere for our unsupported opinion. I'd prefer it to be omitted from discussion here, or perhaps presented only as speculation when accompanied by facts that relate to risks of computing. Miss Gorman's examples also fail the sniff test, in a partisan way.

- > Electronic voting systems are IT projects largely contracted by
- > government exclusively to favored private (some would write
- > "mercantilist") contractors (Diebold, Sequoia, etc.)

What does "contracted" mean here? I take it as a weasel word. Are current commercial electronic voting products designed and developed under contract to governments with accountability to the contractor? Or are they simply

commercial products developed and sold, in the usual way, to meet a perceived market among public officials ignorant or desperate enough to be induced to buy them? In this venue I believe we know how badly most electronic voting products fail important criteria that representative governments should attend to for voting.

We -- the world, not just the USA -- are only now undertaking serious discussion of what we need for non-paper balloting to be useful and trustworthy.

My final point was, of course, to say that we needn't go far to find atrociously bad software, some of it in very wide use, that was inarguably developed entirely by private industry.

eCrime Researchers Summit CFP

*Monty Solomon <monty@roscom.com>
Sat, 23 May 2009 23:49:55 -0400*

The fourth annual APWG eCrime Researchers Summit will be hosted in Oct 2009, in Tacoma, WA.

Original papers on all aspects of electronic crime are solicited for submission to eCrime '09. Topics of relevance include but are not limited to:

- * Phishing, rogue-AV, pharming, click-fraud, crimeware, extortion and emerging attacks.
- * Technical, legal, political, social and psychological aspects of fraud and fraud prevention.
- * Malware, botnets, ecriminal/phishing gangs and collaboration, or money laundering.
- * Techniques to assess the risks and yields of attacks and the success rates of countermeasures.
- * Delivery techniques, including spam, voice mail and rank manipulation; and countermeasures.
- * Spoofing of different types, and applications to fraud.
- * Techniques to avoid detection, tracking and takedown; and ways to block such techniques.
- * Honeypot design, data mining, and forensic aspects of fraud prevention.
- * Design and evaluation of user interfaces in the context of fraud and network security.
- * Best practices related to digital forensics tools and techniques, investigative procedures, and evidence acquisition, handling and preservation.

<http://www.ecrimeresearch.org/2009/cfp.html>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 70

Monday 1 June 2009

Contents

- [Municipal politician unseated over fake e-mail](#)
[Kelly Bert Manning](#)
- [A new biometrics risk?](#)
[Lee Rudolph](#)
- [No-risk intelligence gathering?](#)
[PGN](#)
- [iDEAL is not so ideal](#)
[Erling Kristiansen](#)
- [Failures of eCommerce are Human not Computers](#)
[Chris J Brady](#)
- [No 911 Service](#)
[Gene Wirchenko](#)
- [Risks On Rails](#)
[Rob Slade](#)
- [Train and iPod do not mix](#)
[Gene Wirchenko](#)
- [Cycle-omatic complexity needed?](#)
[Jeremy Epstein](#)
- [NZ bank lends \\$10M instead of \\$10K; plus Facebook](#)
[Rob Slade](#)
- [Re: Tail strikes from improper settings](#)
[Dick Mills](#)
- [Radio-isotope shortage, again...](#)
[Danny Burstein](#)
- [Hutber's Law, Clarke's Third Law and Weasley's Law](#)
[Michael Bacon](#)
- [Re: How small does the disk chunk have to be?](#)
[Jeremy Epstein](#)
[Fred Cohen](#)
[Jeremy Epstein](#)
- [Re: secure but memorable passwords](#)
[David Alexander](#)
[Dave Martin](#)
[Paul Karagianis](#)
- [Info on RISKS \(comp.risks\)](#)

✂ Municipal politician unseated over fake e-mail

Kelly Bert Manning <bo774@freenet.carleton.ca>

Wed, 27 May 2009 20:25:26 -0700

A municipal councilor in White Rock, British Columbia, has been booted out of office for sending unsolicited e-mail with a fake sender name, from a city hall computer, lying about his opponents. One of his opponents spent several \$100s on a forensic analysis and court case, recovering his expenses.

The lying spammer has lost his seat, fined \$20,000 and has to refund his court costs, which were paid by White Rock but may now be recoverable due to the reversal of the election.

Do a web search on
White Rock Coleridge Todd

Full text of decision.

<http://www.courts.gov.bc.ca/jdb-txt/SC/09/06/2009BCSC0688.htm>

✂ A new biometrics risk?

Lee Rudolph

Wed, 27 May 2009 11:07:23 -0400 (EDT)

As reported at <http://news.bbc.co.uk/2/hi/health/8064332.stm> :

A commonly-used cancer drug can make patients' fingerprints disappear, potentially causing problems for foreign travel, a doctor warns. One patient was held by US immigration officials for four hours before they allowed him to enter the country. The case is highlighted in the journal *Annals of Oncology*. ... Although the drug is commonly used to treat a range of cancers, it can cause chronic inflammation of the palms or soles of the feet, leading to peeling, bleeding or blistering of the skin. Over time this can lead to the loss of fingerprints. ...

✂ No-risk intelligence gathering?

Peter Neumann <neumann@csl.sri.com>

Mon, 1 Jun 2009 14:21:32 -0700

...Mike Birmingham, a spokesman for the Office of the Director of National Intelligence (located at the intersection of the Dulles Toll Road and Route 123), would say only that if a communications line used by the agency was cut, the nation's intelligence-gathering would carry on uninterrupted. "No

particular project puts us at risk -- highway construction, building construction," Birmingham said. "We don't have a single point of failure. Our systems are redundant." [Source: *The Washington Post*, 30 May 2009; TNX to Mark Luntzel for spotting this one. PGN]

<http://www.washingtonpost.com/wp-dyn/content/article/2009/05/30/AR2009053002114.html>

✶ iDEAL is not so ideal

Erling Kristiansen <erling.kristiansen@xs4all.nl>

Tue, 26 May 2009 22:19:03 +0200

Ideal is an electronic payment service for on-line purchases operated in The Netherlands (and maybe other countries -- I don't know). It works as follows:

- * You complete the details of your purchase on the web site of the merchant
- * You select iDEAL as payment method
- * You are re-directed to the on-line banking service of the bank of your choice
- * After logging in with your usual credentials, you are presented with a pre-filled bank transfer form
- * Accepting the form, the payment is done, and you are returned to the merchant, who confirms your purchase and payment

In a recent purchase I made, rather than confirming payment, I got a pop-up something like "Payment failed. Please try again later or pay by other means".

I did just that: Tried again later. Same result. Tried again a lot later. Same result. Checking my bank account, it turned out that 3 payments had been debited.

The merchant dealt with the case in a professional manner, accepting one payment and refunding me the two other. But it took several phone calls, faxing supporting material and a few days before I was really sure that the holiday I had booked was actually confirmed. Apparently, they had some trouble locating a bank transfer that was not properly linked to the purchase.

Is the iDEAL protocol really so sloppy that it cannot deal properly with a fault somewhere half-way the process? Or is it the implementation by a particular vendor that is broken? What I really object to is the "try again later" phrase that seemingly implies that the whole transaction was voided.

✶ Failures of eCommerce are Human not Computers

Chris J Brady <chrisjbrady@yahoo.com>

Thu, 28 May 2009 04:03:57 -0700 (PDT)

It never ceases to amaze me at the ineptitude of e-commerce web sites to deliver items paid for. There are excellent e-commerce web sites such as British Airways flight booking, Expedia, eBay and Amazon.

The common factor is that most (99.99%) manage to take a customer's money from a bank or credit card account almost quicker than a web page takes to refresh. And at least with airlines a customer then gets an e-ticket.

But it is companies that sell hard goods that are continually of concern. I have had little trouble with Amazon who use 'normal mail services. But eBay sellers, and companies such as Argos, Littlewoods, GUS, etc. (aka online mail order catalogue companies) ALL have a real problem in actually delivering goods to purchasers. The courier companies -- DHL, FedEx, Parcel Force, etc. -- even if in-house -- are the weak link in the e-commerce chain.

The issues are

- 1) These companies deliver at their convenience forgetting that many people are not at home but out at work, and/or
- 2) The laziness of the courier drivers is such that they don't bother to leave an attempted delivery card, and ultimately the goods are 'returned to sender' -- unclaimed.

In February I was sent from the USA some valuable and rare archive video recordings on tape. They failed to arrive at my address in the UK. The courier fee was \$60. After persistent enquiries at both ends they had simply disappeared -- each 'country' blamed the other. The tracking number(s) didn't work. *Three* months later the package turned up again -- but at the sender's address as 'returned unclaimed at destination.' It appears that once again the courier driver had simply failed to leave an 'attempted delivery card.' And the courier company had failed to alert me by mail and/or email. So the goods went back to sender.

Last year I bought some clubbing clothes from a eBay company in Germany. Again the goods were dispatched using a German courier -- I can't read German so tracking on its web site was a problem. The goods never arrived. Again they were sent back, and I had to raise a formal complaint with eBay and PayPal to obtain a refund.

I know that I'm not the only one affected in the UK. And this appears to be a world-wide problem. A friend of mine in New York City always has goods delivered to his parents in Vermont because he can never get them delivered properly in New York.

It is not usually the fault or risks of using computers and the Internet that fails the development of e-commerce so badly. It is the human element - aka the lazy courier companies and their drivers that fail the system. I see no solution to this even as the Internet gets faster.

No 911 Service

Gene Wirchenko <genew@ocis.net>

Mon, 01 Jun 2009 09:51:34 -0700

I hope no one found out the hard way:

"Geezer phones don't work

Part of [http://www.itbusiness.ca/it/client/en/home/News.asp?sub=true&id=53372:](http://www.itbusiness.ca/it/client/en/home/News.asp?sub=true&id=53372)

Thousands of phones sold by Jitterbug, a mobile operator that specializes in simple handsets for limited uses such as emergency calls, are being recalled because they can't be used to call 911 in some rare cases. Jitterbug sells bare-bones handsets and no-contract service plans geared toward seniors and other consumers who don't make heavy use of cell phones. One of its phones, the Jitterbug OneTouch, has dedicated buttons for the Jitterbug operator, one preset number, and 911 in place of a numeric keypad. That phone, as well as the standard Jitterbug phone with a keypad, have been recalled because they can't be used to call 911 emergency lines in some U.S. areas where they should be able to."

Risks On Rails

Rob Slade <rMslade@shaw.ca>

Fri, 29 May 2009 16:47:58 -0800

In 2004, a politically controversial decision was made to cease operations of BCRail, and sell a 999 year lease to CN.

A section of the line near the town of Lillooet is known as one of the longest continuous mountain grades in Canada. BCRail used dynamic brakes.

CN used air brakes, and confirmed this decision in early 2006, despite concerns raised by employees.

On June 29, 2006, a train derailed on that section, and two employees died.

The Transportation Safety Board (TSB) has now ruled that the failure was caused by an inadequate braking system used in the steep mountain canyon.

<http://links.cbc.ca/a/l.x?T=jncickgignjgfckaafjiiiklfcfi&M=36>

"[N]o risk assessment was done before removing locomotives with dynamic braking from this extreme mountain territory."

rslade@vcn.bc.ca <http://victoria.tc.ca/techrev/rms.htm>

http://blog.isc2.org/isc2_blog/slade/index.html <http://twitter.com/rslade>

<http://blogs.securiteam.com/index.php/archives/author/p1/>



Train and iPod do not mix

Gene Wirchenko <genew@ocis.net>

Sun, 24 May 2009 22:51:24 -0700

Jason Hewlett, Fatality: 19-year-old killed while walking on train tracks; iPod may have drowned out sound of train's warning whistle, *The Daily New*, Kamloops, British Columbia, Canada, 22 May 2009, A1-A2, PGN-ed

Liam Peel, an 19-year-old Kamloops man, may not have heard a CP Rail train approaching from behind him at 56 km/h, because he was apparently listening to an iPod while walking along one of the track rails, dressed in a black hoodie. A registered audiologist suggested that an iPod can crank out up to 100 decibels, and ear buds tend to drown out external sounds. [At maximum volume, our youths are probably going deaf as well.]

✂ Cycle-omatic complexity needed?

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Fri, 29 May 2009 10:20:27 -0400

Floyd Landis' 2006 Tour de France victory is being questioned because of allegedly hacked computer systems that held the drug test results.

<http://www3.signonsandiego.com/stories/2009/may/29/1s29landis215559-landis-case-twist-hacking-lab-com/>

Clearly, to keep drug testing computers safe from Tour de France attackers, we need higher cycle-omatic complexity of the systems.

The RISK? Some of us will go to any length to pull a pun out of a marginally security related article.

✂ NZ bank lends \$10M instead of \$10K; plus Facebook (Wells, [RISKS-25.69](#))

Rob Slade <rMslade@shaw.ca>

Mon, 25 May 2009 14:15:27 -0800

Actually, I'd just seen this in another place, with rather complementary info. "The fugitive couple and their small entourage have been traced to Hong Kong, Macau and mainland China, largely via one of their indiscreet updates on social networking site Facebook." I thought the "tracking crooks by Facebook" aspect made it RISKS fodder in another direction:

<http://www.smh.com.au/news/technology/web/2009/05/25/1243103468196.html>

✂ Re: Tail strikes from improper settings (Knowlton, [RISKS-25.68](#))

Dick Mills <dickandlibbymills@gmail.com>

Fri, 29 May 2009 11:17:52 -0400

> An airplane on a take-off run clearly could perform an automatic sanity
> check (comparing thrust settings and actual acceleration with gross
> weight, air speed/temperature/pressure, flap settings ...) and raise an
> alarm if something's seriously amiss.

As an engineer, I love this idea. A dash of physics, a bit of programming, a tiny display. Life is good.

In fact, you could improve it. GPS databases already know which airport you're at, and your heading tells it which runway you're on. It would be easy to look up runway length from that input.

As a pilot, I'm highly skeptical of any such alarm that may go off at the particularly sensitive time as take off. The alarm could trigger an inappropriate takeoff abort; and that could lead to a crash.

Displaying a new piece of information, say actual versus planned acceleration, would be very welcome in the first 100 feet of takeoff roll. The same information would be very unwelcome a few seconds later as we near takeoff speed at 200 feet per second, At that point, things happen too rapidly and the pilot is too focused to deal with distractions or cognitive dissonance.

That makes the design an engineering challenge -- the more time the gizmo takes to make sure that estimates are accurate and alarms are not false, the less valuable the information is to the pilot. Also, if we create a situation where trust transitions from the machine to the pilot's instincts, and there is no clear-cut transition boundary, then the design is a bad one.

Any new gizmo in the cockpit might be heroic or counterproductive depending on the human interface, and our ability to integrate it into pilot training. We need to develop practiced responses to inputs that lead to practiced recovery procedures.

Dick Mills, SV Tarwathie blog: dickandlibby.blogspot.com

radio-isotope shortage, again...

danny burstein <dannyb@panix.com>

Sun, 24 May 2009 23:13:40 -0400 (EDT)

[The dangers of not having multiple sources for, in this case, radioisotopes, strikes yet again. This primarily affects Canadian medical institutions, but there's lots of impact in the US as well. (Maybe it wouldn't have been so bad if Columbia University had gotten that nuclear reactor after all...)]

Peter Zimonjic, Isotope crisis may be worse than forecast; Some patients

will be 'low priority' <http://www.saultstar.com/ArticleDisplay.aspx?e=1581040>

Patient groups say lives are at stake because of the shrinking number of nuclear imaging scans available at Canadian hospitals. The situation is expected to worsen in the coming weeks as the medical isotope shortage intensifies because of the shutdown of the Chalk River nuclear reactor. [These isotopes, which have short radioactive half lives, thus can't be "stored", are used in many medical procedures. Oh, and for other purposes, too).

✂ Hutber's Law, Clarke's Third Law and Weasley's Law (Hollman, [R-25.68](#))

"Michael Bacon" <attilathehun1900@tiscali.co.uk>

Tue, 26 May 2009 13:34:03 +0100

In [RISKS-25.68](#), David Hollman (In a Lab, an Ever-Growing Database of DNA Profiles) asks if there is, "A niche catchphrase for the effect where information in digital form has more credibility than in other forms?" In the same issue, Bob Frankston (Re: Australian emergency services) asks whether anyone thought to play the audio recording over a telephone line.

Whilst I am insufficiently witty to think of an appropriate catchphrase, these both illustrate Hutber's Law -- "Improvement means deterioration".

They also suggest to me two other laws.

The first is Arthur C Clarke's Third Law, that any sufficiently advanced technology is indistinguishable from magic . and so it appears is much of today's technology to the non-technical and because of the increasing diversification of skills, even many of the 'techies'.

The second could be termed Weasley's Law, from the character Arthur Weasley in the Harry Potter book 'The Chamber of Secrets': "Never trust anything if you can't see where it keeps its brain."

But maybe the appropriate catchphrase is that old one ., "Computer says [YES/NO]".

✂ Re: How small does the disk chunk have to be? ([RISKS 25.68](#))

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Thu, 28 May 2009 12:46:27 -0400

Quoting an article about drive destruction, Fred Cohen disagreed with the adequacy of Canada's tax agency cutting disk drives into pieces "no bigger than the width of a pencil", saying the pieces "will have to be small enough to make the content on one chunk of no utility. At the density of a HDD, a pencil width holds quite a bit of data."

Fred is right in the literal sense, but one has to consider the overall threat model. Given a choice of obtaining and putting together a disk drive from pieces no bigger than the width of a pencil or hacking into a site to steal the data, the risks to the attacker for a hacking attempt are much lower, the specialized knowledge and equipment required much less, and the likelihood of success much greater. I fear that following Fred's cautionary words might lead organizations to overemphasize drive destruction and underemphasize the risks of software flaws.

Given everything we've read about tax, military, and medical systems being routinely compromised, a pencil width of data is fine with me for destruction of a disk that has my personal information. What keeps me up at night is the probability that the organization put a firewall in place and called it a day.

--Jeremy

Re: How small does the disk chunk have to be? ([RISKS 25.68](#))

Fred Cohen <fc@all.net>

Thu, 28 May 2009 09:54:58 -0700

I certainly agree that risks should be rationally managed. However, my caution stands. I don't believe I said that it was a bad risk management decision -- only that the residual data on a chunk of a disk is substantial. Evaluating the risks is not something that was discussed in the previous article -- rather it seemed to me to portray a level of risk thought to be acceptable with no particular reason behind it. I would welcome the detailed explanation from Canada's tax agency about how they made the risk management decision and what residual risks they decided to accept, assuming that such a rational decision was made. Which brings me to your point, Jeremy... What is the basis for your conclusion with respect to the relative risks you identify, and how did you do your calculations? Or were you just making a broad generalization without a firm basis like Canada's Tax Agency did in its press release (although perhaps not in its actual decision process - we don't know).

Fred Cohen & Associates tel/fax: 925-454-0171 <http://all.net/>
572 Leona Drive Livermore, CA 94550

Re: How small does the disk chunk have to be? ([RISKS 25.68](#))

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Fri, 29 May 2009 10:49:40 -0400

Fred, I think we're in agreement that the residual data on a chunk of disk is substantial. While it's true that the evaluation wasn't discussed, the implication was that chunks of that size are "safe", and therefore there was

an implicit risk assessment.

As for my conclusion about the relative risks, I assumed that the pieces of disk aren't labeled or segregated when being disposed of (i.e., so disk A is in a bag labeled "tax data disk A" while disk B is in a separate bag). I also assumed that their application security is neither better nor worse than the typical site - namely there's a 90% likelihood (give or take) that the site can be compromised with no more than a couple weeks of work by reasonably skilled non-nation-state attackers. So my calculation was that if there's a 90% probability of an arm's length essentially undetectable attack in a couple weeks vs. obtaining the physical media and analysis equipment and putting it back together (which, from what I've read, takes months or longer), the odds are very much on the software attack.

I don't know how much data is destroyed in the process of chopping the disks up, and how much of it is recoverable through error correcting codes, use of RAID (if an attacker is able to get multiple copies of the same data), etc. That would obviously also come into the risk assessment - but I believe the order of magnitude difference is large enough to make software attacks a clear winner for the bad guy.

So, yes I did do a (very informal) risk assessment in making my statement. Was it a broad generalization? Yes, but an informed one.

Re: secure but memorable passwords (Colbourn, [RISKS-25.69](#))

*David Alexander <dave_ale@online.rednet.co.uk>
Mon, 25 May 2009 06:43:28 +0100*

I have just read Phil Colbourn's advice on creating a secure password. It's good, but I don't think it goes far enough. It should be adequate for slowing down most attackers, but it won't work for anyone knowledgeable who can access the .sam file. Before an e-mail comes 'flooding in' to point it out - I know that should only be a very few people and it should be one of the best defended files in the whole system.

Someone has completed the task of generating 'rainbow tables' for every Microsoft password combination up to 14 characters in length. It's a 64 Gb download, but it is publicly available. For sysadmin and any other password with privileges, I regard anything less than 15 characters that uses the MS password hashing algorithm as broken. Eight characters is not long, not any more.

David Alexander, Towcester, Northamptonshire, England

Re: memorable but secure passwords (Colbourn, [RISKS-25.69](#))

*Dave Martin <dave_martin@mindspring.com>
Mon, 25 May 2009 18:10:05 -0400*

In [RISKS-25.69](#) Phil Colbourn presented a method for creating "memorable but secure passwords" but those 2 things, memorable and secure, seem to be directly at odds with each other.

Perhaps I have a naive view of the problems with passwords but it escapes me why passwords can not be phrases rather than based on some arcane and usually difficult set of arbitrary "rules".

It seems to me that the stricter the rules the easier it makes things for those would like to compromise a site with said rules. A phrase that includes upper and lower case letters (if desired) as well as spaces and punctuation creates a much large space that must be consider when attempting to figure out a password.

I've been designing sites to allow the use of a phrase of up to 255 characters for a number of years and have yet to have any of them compromised. It's a lot easier to remember "My first car was a '65 Mustang" than it is to remember "Ab19EloG#z" And a phrase that is easily remembered doesn't need to be written down.

Re: How to make memorable but secure passwords

"Paul Karagianis" <karypm@stjohns.edu>

Tue, 26 May 2009 17:26:00 -0400

How so? Or, more importantly, shouldn't we be asking on a target site by target site basis: "why is this better than three letters lower case, that aren't my initials"? eg: "cat".

The usual nonsense about complex passwords being needed to defeat "dictionary lookup" - a concept that depends on a sites admin being willing to hand out his encrypt - doesn't apply to the typical e-store that is willing to send you your password in clear text.

I'd be interested in typical e-store policies on people playing "guess the password"... how long do they pause between attempts, do they "lock" the account for some time period after so many tries etc. But in the real world I'm much more concerned about some manager getting his laptop stolen from the airport bar with my account info, along with the info for 78,000 other customers, on it.

The escalation we've seen in trying to get the Internet user base to adopt ever sillier passwords that they inevitably need to copy onto post-its on the bottom of their keyboards seems, to me anyway, to have become insanely disproportionate to the threat. Is this still a real problem for anyone else?

Working at a University requires that we set initial passwords for students to something not easily deduced by their classmates or we'll inevitably be told that any account abuse we follow up on was done by "someone guessed my

password". But that's more of a political solution to a different issue.

Aside from the above, I suppose one may be trying to protect oneself from someone who uses the same machine you do, but I fail to see how an environment that threatening (which suggests a key logger might be in the opponents arsenal) would benefit from a more more complex password.

I guess what I'm asking for here is, if you're suggesting a best practice, could you (rhetorical "you"... I'm not trying to hold the authors of this post or many similar ones immediately accountable) give a little more detail about the threat you're helping us avoid?



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 71

Tuesday 23 June 2009

Contents

- [Metro train fatal accident -- too much automation?](#)
[Joe Thompson](#)
- [Air France crash and computers?](#)
[Steven M. Bellovin](#)
- [Electronic health record systems fails; ambulances turned away from hospital](#)
[Dale Hawkins](#)
- [Demolition: GPS vs Address; Well, we were close...](#)
[David Leshner](#)
- [Shoreline music-food event fiasco: electronic pay system fails](#)
[PGN](#)
- [Green Dam Youth Escort](#)
[PGN](#)
- [China dominates NSA-backed coding contest](#)
[Eugene H. Spafford](#)
- [Electricity Industry to Scan Grid for Spies](#)
[Danny Burstein](#)
- [Google Street View functions as CCTV](#)
[Mark Brader](#)
- [Smart electric meter risks; disastrous GPS misuse](#)
[Nicky L Sizemore](#)
- [Copier short-changes users](#)
[Matt Bishop](#)
- [GM & Segway to make 2-wheeled car](#)
[Paul Czyzewski](#)
- [Another High-Tech Accident?](#)
[Gene Wirchenko](#)
- [Reducing Risks of Implantable Medical Devices](#)
[Kevin Fu](#)
- [Woman Gets Others' Medical Records In Mail](#)
[Adolphus St. Clair](#)
- [Bozeman asking job applicants for their userid/password](#)
[Arthur T.](#)
- [Risks of copyright lobbyists hiring someone to plagiarize PR spin](#)
[Kelly Bert Manning](#)
- [A new way to lose money via ATM...](#)

[David Lesher](#)

• [Re: Security through obscurity](#)

[Steven M. Bellovin](#)

• [REVIEW: "Zero Day Threat", Byron Acohido/Jon Swartz](#)

[Rob Slade](#)

• [Info on RISKS \(comp.risks\)](#)

✂ Metro train fatal accident -- too much automation?

Joe Thompson <joe@orion-com.com>

Tue, 23 Jun 2009 12:22:59 -0400

Though a definite determination has not been made yet, some preliminary reports of the DC Metro crash suggest a combination of automated control failure and failure by the operator to apply emergency braking. If borne out, this could be the second Metro crash to be attributed at least partially to driver inattention (along with the 2004 rollback crash).

I wonder if some of our systems have gotten **too** automated. During normal operation, Metro trains apparently move and stop fully automatically. In such a mode, it's easy to allow oneself the luxury of distractions, but even in the absence of that, it's also easy to fall into "highway hypnosis". The first thing that comes to mind is making operators do some sort of constant but non-repetitive task to stay alert, but that just moves the problem back to "distraction".

What is the status of research, I wonder, into keeping human backups to automated systems alert and awake without occluding their attention in case of a genuine issue? -- Joe

✂ Air France crash and computers?

"Steven M. Bellovin" <smb@cs.columbia.edu>

Thu, 4 Jun 2009 18:02:33 -0400

Could a Computer Glitch Have Brought Down Air France 447?

Jeffrey T. Iverson, **Time**, 5 Jun 2009

<http://www.time.com/time/world/article/0,8599,1902907,00.html>

--Steve Bellovin, <http://www.cs.columbia.edu/~smb>

[Several electrical systems in the Airbus 330 reported breaking down just before the crash, and the autopilot apparently disengaged. The investigation is ongoing. PGN]

✂ Electronic health record systems fails; ambulances turned away from

Hawkins Dale <hawkins@pobox.com>

Thu, 04 Jun 2009 11:30:08 -0400

hospital

Aaaaargh!

From the Indianapolis Star (via Slashdot)

<http://www.indystar.com/apps/pbcs.dll/article?AID=/20090603/LOCAL18/906030346>

Hospital is forced to turn away patients

Methodist Hospital went "on diversion" early Tuesday for the first time in its 100-plus years, sending ambulances that came to its doors to other hospitals.

A power surge knocked out Clarian Health's computer system Monday afternoon, derailing the hospitals' ability to access electronic health records for patients, said Clarian spokesman James Wide. Staff members at Methodist and Indiana University Hospital had to enter patients' records by hand.

By about 1 a.m. Tuesday, a backlog of paperwork led Methodist and IU hospitals to stop accepting patients who arrived by ambulance. Walk-in patients were still accepted.

Demolition: GPS vs Address; Well, we were close...

"David Lesher" <wb8foz@panix.com>

Mon, 15 Jun 2009 19:29:15 -0400 (EDT)

A Sandy Springs man got a phone call Monday that his family home in Carroll County [GA] was gone. Torn down. Demolished. ... Channel 2 Action News reporter Jovita Moore asked Byrd if the demolition company had an address. I said, "What address did you have?" and he said, "They sent me some GPS coordinates." I said, "Don't you have an address?" (and) he said, "Yes, my GPS coordinates led me right to this address here and this house was described." said Byrd. <<http://www.wsbtv.com/news/19715994/detail.html>>

Shoreline music-food event fiasco: electronic pay system fails

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

Tue, 23 Jun 2009 9:24:41 PDT

On 13 Jun 2009, the first Great American Food and Music Fest at the Shoreline Amphitheatre in Mountain View CA (reportedly with some top-price tickets at \$500) used an electronic bracelet payment system for food that "came down with a bad case of indigestion". The system collapsed, causing up to five-hour waits in food lines. [Source: Lisa Fernandez, San Jose Mercury, 16 June 2009]

✂ Green Dam Youth Escort

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

Tue, 23 Jun 2009 9:30:12 PDT

As of 1 July, all PCs sold in China must have the Green Dam Youth Escort software that is intended to filter out porn. However, that software has serious security flaws (<http://www.cse.umich.edu/~jhalderm/pub/gd/>) and also allegedly violates open-source licensing. [Sources: Andrew Jacobs, China Criticized Over Computer Filtering Plan, *The New York Times*, 10 Jun 2009 http://www.nytimes.com/2009/06/11/business/global/11censor.html?_r=1 and Edward Wong, China Orders Fixes in Censoring Software, *The New York Times*, 16 Jun 2009; PGN-ed. Mere mention of this here may also result in RISKS being blacklisted in China -- if it is not already. Also, the ability to violate privacy, and for anyone -- not just the Chinese government -- to remotely alter the software for surreptitious purposes including surveillance might turn it into Green Damn-Youth Escort or even the Green Youth Damned Escort Service. PGN]

✂ China dominates NSA-backed coding contest

"Eugene H. Spafford" <spaf@mac.com>

June 10, 2009 10:49:30 AM EDT

Programmers from China and Russia have dominated an international competition on everything from writing algorithms to designing components.

Whether the outcome of this competition is another sign that math and science education in the U.S. needs improvement may spur debate. But the fact remains: Of 70 finalists, 20 were from China, 10 from Russia and two from the U.S....

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=development&articleId=9134122>

✂ Electricity Industry to Scan Grid for Spies

danny burstein <dannyb@panix.com>

Thu, 18 Jun 2009 00:21:56 -0400 (EDT)

The electric-utility industry is planning a pilot initiative to see whether Chinese spies have infiltrated computer networks running the power grid, according to people familiar with the effort.

Officials of the North American Electric Reliability Corp., an industry regulatory group, are negotiating with a defense contractor for the job of

searching for breaches by cyberspies, according to people familiar with the plans. [Wall Street Journal]

rest:

<http://online.wsj.com/article/SB124528065956425189.html#mod=testMod>

Google Street View functions as CCTV

Mark Brader

Sun, 21 Jun 2009 06:55:03 -0400 (EDT)

* From: John Hatpin <RemoveThisjfhopkin@gmailAndThisToo.com>
* Newsgroups: alt.fan.cecil-adams
* Subject: Google CCTV
* Date: Sun, 21 Jun 2009 11:41:54 +0100
* Xref: number.nntp.dca.giganews.com alt.fan.cecil-adams:1611995

Google Street View functions as CCTV

http://www.theregister.co.uk/2009/06/19/street_view_mugging/

Now, what are the chances of that happening, eh? Normally, to get a result like that, you'd pretty much need cameras on every oh, never mind.

John Hatpin <http://uninformedcomment.wordpress.com/>

Smart electric meter risks; disastrous GPS misuse

"Sizemore, Nicky L CTR DISA JITC" <NICKY.SIZEMORE.ctr@disa.mil>

Mon, 15 Jun 2009 11:38:14 -0700

Two highly risks-relevant stories from 'The Register':

Smart electric meter risks: This one to be reported at the upcoming Black Hat conference:

http://www.theregister.co.uk/2009/06/12/smart_grid_security_risks/.

Apparent gross GPS misuse: This one reported with minimal detail and only a URL, but sounds worthy of tracking down...

http://www.theregister.co.uk/2009/06/15/gps_house_flattening/

...some substantiation from WSB Atlanta at...

<http://www.wsbtv.com/news/19715994/detail.html>

...and ABCNews at. Many other google hits, but most are brief and obviously derivative.

<http://abcnews.go.com/Business/story?id=7823594&page=1>

[These are left as an exercise for the reader. I don't have time to abstract. Also, sorry for the long gap between issues. PGN]

Copier short-changes users

Matt Bishop <bishop@cs.ucdavis.edu>

Tue, 09 Jun 2009 05:28:04 -0700

I gave a midterm in an introductory programming class this term. The class has 90 people. I wrote the midterm, and asked the office staff to make 100 copies (just to be sure I had enough). I picked them up a day before the exam.

When I got to the class, I passed out the midterms. I ran out of copies after passing out 75 -- that means 15 people didn't have one. So I had to cancel the midterm, and write a completely new one.

When I reported the discrepancy, the office staff was quite upset and investigated. It turned out that the counter on the copier was malfunctioning and reporting more copies than were actually made.

Moral of the story: always count the number of copies that a copier tells you it makes!

[Nasty problem if the copier is rented and usage costs are based on what the counter says! I suppose a malicious bug would give you the correct number of copies, but charge for 33% more. PGN]

GM & Segway to make 2-wheeled car

Paul Czyzewski <tallpaul@gmail.com>

Tue, 2 Jun 2009 11:24:03 -0700

[This is an old item that somehow got lost in the shuffle, even with the "notsp" tag in the subject line. PGN]

GM, Segway think 2 wheels, Associated Press, 7 Apr 2009

<http://www.latimes.com/business/la-fi-gm-segway7-2009apr07,0,2638670.story>

The companies plan to develop a two-wheeled, two-seat electric vehicle as a clean, safe and inexpensive alternative to traditional cars ... The companies plan to announce today that they are developing a two-wheeled, two-seat electric vehicle designed to be a safe, inexpensive and clean alternative to traditional cars for cities across the world. The companies said their project, dubbed PUMA, for Personal Urban Mobility and Accessibility, would include a communications network allowing vehicles to interact with one another to regulate traffic flow and prevent crashes. ...

[paul: okay, here's the kicker. Emphasis added:]

*Because it would be designed to automatically avoid obstacles such as

pedestrians and other cars, the PUMA vehicle

**** would not need air bags **** and

**** would have safety belts for "comfort purposes" only, *****

said Larry Burns, GM's vice president of research, development and strategic planning.

[and, yes, I did check to make sure that the story was not dated April 1.

Paul Czyzewski]

✂ Another High-Tech Accident?

Gene Wirchenko <genew@ocis.net>

Sat, 13 Jun 2009 13:37:44 -0700

The URL summarises the article well:

http://www.upi.com/Odd_News/2009/06/01/Man-jogs-into-tree-while-using-Twitter/UPI-68651243891045/

✂ Reducing Risks of Implantable Medical Devices

Kevin Fu <kevinfu@cs.umass.edu>

Mon, 22 Jun 2009 01:46:03 -0400

[I asked Kevin to submit a note on his CACM Inside Risks column this month, on improving security and privacy for Implantable Medical Devices (IMDs). It is a very timely column. PGN]

Millions of patients benefit from programmable, implantable medical devices (IMDs) that treat chronic ailments such as cardiac arrhythmia, diabetes, and Parkinson's disease with various combinations of electrical therapy and drug infusion. Modern IMDs rely on radio communication for diagnostic and therapeutic functions---allowing healthcare providers to remotely monitor patients' vital signs via the Web and to give continuous rather than periodic care. However, the convergence of medicine with radio communication and Internet connectivity exposes these devices not only to safety and effectiveness risks, but also to security and privacy risks. The column explains the impact of these risks on patient care, and makes recommendations for legislation, regulation, and technology to improve security and privacy of IMDs.

The full text appears on:

<http://www.csl.sri.com/users/neumann/insiderisks08.html#218>

and on ACM's portal.acm.org website as well.

✂ Woman Gets Others' Medical Records In Mail

"Adolphus St. Clair" <nermal1@earthlink.net>

Sat, 20 Jun 2009 09:32:22 -0400

Anyone out there guess what corrective action Blue Cross - Blue Shield would have taken to correct this screw-up if this person had not gone to the news?

A Seminole County FL woman expecting a new insurance card from Blue Cross/Blue Shield received a box with hundreds of private medical records for other people. [WFTV, 19 Jun 2009]

<http://www.wftv.com/news/19804431/detail.html>

✶ Bozeman asking job applicants for their userid/password

"Arthur T." <risk200906.10.atsjbt@xoxy.net>

Sat, 20 Jun 2009 14:39:07 -0400

Bozeman, Montana has a job application form that asks: "Please list any and all, current personal or business websites, web pages or memberships on any Internet-based chat rooms, social clubs or forums, to include, but not limited to: Facebook, Google, Yahoo, YouTube.com, MySpace, etc." There are column headings for Username and Password. Despite what's been written, there is no indication in the form that it's not mandatory.

<http://www.bozeman.net/bozeman/humanResource/forms/Background_Check_Form_Interview_MASTER.pdf>

There has been much written about this. Most of it attacks the requirement on ethical and privacy issues, but there is another point that I've seen less often. It is against most sites' Terms of Service to give your password to anyone, and it's against most sites' TOS to attempt to access the site with someone else's userid. If you recall, Lori Drew was convicted in federal court of violating the MySpace TOS in the cyberbullying case.

It seems to me that if city personnel actually used any of the passwords, they could be indicted on the same charges, as could the applicants who supplied the passwords.

Once the public flap started, I'm surprised that Bozeman didn't take the easy way out by saying that they never planned to use the information. It's just that anyone who supplied their userids and passwords was automatically disqualified for lack of sufficient intelligence.

✶ Risks of copyright lobbyists hiring someone to plagiarize PR spin

Kelly Bert Manning <bo774@freenet.carleton.ca>

Sun, 07 Jun 2009 21:04:39 -0700

It isn't just students who need to worry about plagiarized content being revealed when they submit their papers.

It has recently been revealed that 3 "independent" Conference Board of

Canada "research" reports submitted to legislators and recommending increased copyright protection were found to contain large sections of word for word boilerplate text copied, without acknowledgment or attribution, from the funding lobby group's own PR Spin material on the issue.

This wasn't a case of copying without permission or knowledge of the copyright holder. It appears to be an embarrassing case of the copyright holder trying to give their own questionable claims a credibility boost by having "independent" researcher's names used in place of their own name.

Ironic, eh!

<http://www.michaelgeist.ca/content/view/62/128/>
<http://www.michaelgeist.ca/content/view/4009/125/>

Conference Board Recalls All Three IP Reports

The Conference Board of Canada has just announced that it is recalling all three IP reports that it issued last week. It says that "an internal review has determined that these reports did not follow the high quality research standards of The Conference Board of Canada."

Update: Jesse Brown interviewed Anne Golden, CEO of the Conference Board of Canada. Golden admits that the digital economy report was plagiarised.

Update II: Media coverage of the Conference Board pulling the reports from the CBC, Vancouver Sun, Montreal Gazette, Macleans, Mediacaster, Techdirt, and the Georgia Straight."

The Conference Board at first "stood by" all 3 submissions, but is now in full retreat and asking former staff researchers for "help".

Some former researchers whose names were left attached to what became in large part a word for word repeat of lobbyist material are seeking to have their names disassociated from the plagiarised work.

Independent research work which contradicted the lobbyist claims was removed, but the researcher's names were somehow left on as authors of a work they do not wish to have their names associated with.

One researcher listed as an author of the reports, who is seeking to have [his/her] name removed from the plagiarism tainted documents, gives reasons such as:

"The Conference Board asks for my help but won't acknowledge that it was wrong to put my name on reports that bear little resemblance to the original research I submitted, were substantially reworked, and were published ten months after I resigned."

<http://www.techdirt.com/articles/20090603/0733135109.shtml>

Former Conference Board Author Explains How Lobbyists Influenced Plagiarized Reports

<http://www.michaelgeist.ca/content/view/4025/125/>

Ex-Conference Board Author Speaks Out; Confirms "Push Back" From Copyright Lobby Funders

<http://www.p2pnet.net/story/22321>

Conference Board denies Geist allegations

<http://www.calgaryherald.com/Clients+dictated+think+tank+research+Former+employee/1659760/story.html>

Clients dictated think-tank research: Former employee

Copyright lobbyists seeking to extend protection have previously learned to be careful what they ask for.

USA provisions for making the copyright period longer allowed the original owner, or their heirs, to have the copyright reassigned to them for the extended period of protection, since the price paid for transferring the copyright was based on the original copyright period length. The widow and daughter of one of the originators of "Superman" retrieved their half of the copyright, after a marathon of litigation. An heir of the other creator is also talking to Lawyers.

✂ A new way to lose money via ATM...

"David Leshner" <wb8foz@panix.com>

Tue, 23 Jun 2009 13:12:09 -0400 (EDT)

Paul Marks, Cash machines hacked to spew out card details,

New Scientist, 17 June 2009

<<http://www.newscientist.com/article/mg20227135.700-cash-machines-hacked-to-spew-out-card-details.html>>

After months poring over the Windows-based software in the bank's ATMs, Henwood and his team were astonished. They found a 50-kilobyte piece of malware disguised as a legitimate Windows program called Isass.exe. {...}

This is a clever choice of camouflage, says SpiderLabs' forensics manager Stephen Venter: to an IT staffer, Isass.exe doesn't look out of place in a Windows system, so routine checks wouldn't necessarily pick it up. Yet it has no useful function in an ATM. {...}

Equally ingenious is how the crooks harvest their stolen data - by using the ATM's receipt printer. Inserting a trigger card into the machine's slot causes the malware to launch a small window on the screen, with a variety of options. The first is to print out a list of all recently used cards. The data on the printout is encrypted, so crime bosses could enlist low-level accomplices to visit ATMs to retrieve the printouts, safe in the knowledge that they cannot use the data to clone cards themselves.

Comment:

And yet companies build both ATM's and voting machines based on Windows....

✂ Re: Security through obscurity (MacIntyre, [RISKS-25.69](#))

"Steven M. Bellovin" <smb@cs.columbia.edu>

Sat, 6 Jun 2009 22:21:01 -0400

The subject of security through obscurity comes up frequently. I think a lot of the debate happens because people misunderstand the issue.

It helps, I think, to go back to Kerckhoffs' second principle, translated as "The system must not require secrecy and can be stolen by the enemy without causing trouble", per <http://petitcolas.net/fabien/kerckhoffs/>). Kerckhoffs said neither "publish everything" nor "keep everything secret"; rather, he said that the system should still be secure *even if the enemy has a copy*.

In other words -- design your system assuming that your opponents know it in detail. (A former official at NSA's National Computer Security Center told me that the standard assumption there was that serial number 1 of any new device was delivered to the Kremlin.) After that, though, there's nothing wrong with trying to keep it secret -- it's another hurdle factor the enemy has to overcome. (One obstacle the British ran into when attacking the German Engima system was simple: they didn't know the unkeyed mapping between keyboard keys and the input to the rotor array.) But -- *don't rely on secrecy*.

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

[The peticolas website is very helpful. Check it out! Steve included the original quote in French, but I could not make it look correct. PGN]

REVIEW: "Zero Day Threat", Byron Acohido/Jon Swartz

Rob Slade <rmslade@shaw.ca>

Mon, 8 Jun 2009 11:19:34 -0800

BKZRDYTH.RVW 20090120

"Zero Day Threat", Byron Acohido/Jon Swartz, 2008, 978-1-4027-5695-5, U\$19.95/C\$21.95

%A Byron Acohido

%A Jon Swartz

%C 1 Atlantic Ave, #105, Toronto, ON, Canada M6K 3E7

%D 2008

%G 978-1-4027-5695-5 1-4027-5695-X

%I Sterling Publishing Co., Inc.

%O U\$19.95/C\$21.95 800-805-5489 specialsales@sterlingpublishing.com

%O <http://www.amazon.com/exec/obidos/ASIN/140275695X/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/140275695X/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/140275695X/robsladesin03-20>

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

%P 297 p.

%T "Zero Day Threat"

The title here is definitely misleading: the authors have just taken a

sensational term and stuck it on a book about "the shocking truth of how banks and credit bureaus help cyber crooks steal your money and identity." Now, as a malware researcher, I'm delighted to see them state, right off the top, the rather bitter truth that security is in such a sorry state because the general populace demands convenience over security, and major companies are willing to give it to them. I'm not quite as happy to find that Acohido and Swartz don't fully understand what a zero day threat actually is. I'm willing to suspend judgment for a while based on their very useful division of each chapter into exploiters (traditional blackhats and opportunists), enablers (those who build weak infrastructures), and expeditors (those who, in various ways, make the problem worse). It's good to see that the authors aren't just retailing the common "oooh, teenage hackers!" stories, and realize that the situation is complex, and involves the interacting behaviours of many different parties.

The synergy of this approach is not demonstrated in chapter one. Of the three parts of the chapter, the first talks about some drug addicts involved in dumpster diving for credit card and bank account information, the second briefly notes the speed and volume of credit card transactions, and the third examines a few of the malware instances around the year 2000. It is not clear what these have to do with each other. Subsequent chapters follow up on these stories. The tales start to interweave at about chapter five, but few connections are made between the items in the content, and those that do exist seem to be almost random. A final chapter in the book, eighteen, is entitled "What Must Be Done." Unfortunately, it is overly broad, and not very specific, reducing to an assertion that we need better financial activity oversight and review, better Internet infrastructure, and better security in operating systems and other software. Appendix A, on personal security, contains a fairly pedestrian collection of advice on credit card, financial, computer, and Internet security. All of the recommendations would help increase the safety of most people: sadly they do not exhaust the possible avenues of attack, and many of the suggestions are not completely within the capability of the average user. (For example, yes, it is a good idea to use strong passwords that are long, and contain a mix of characters, and to change those passwords on a regular basis. The trick is to teach people ways of creating passwords such that the user can remember them, and attackers can't. As a second instance, it is dangerous to click on any banner ad or popup window: what proportion of those who use the Internet regularly can identify those entities when they appear?)

Acohido and Swartz demonstrate, as David Rice did in "Geekonomics" (cf. BKGKNMCS.RVW), that financial entities have little incentive either to take serious steps to reduce electronic fraud, or to protect consumers (or merchants) from losses due to fraudulent transactions.

The authors have done an excellent job of research in the narrative, at least as far as events in the public record are concerned. There is also evidence of commendable exclusive investigation to confirm or enhance specific areas. Unfortunately, the technical material has little depth, and is somewhat suspect when dealing with specialized areas.

Overall, the stories of the blackhat community are entertaining, the tales from the financial world emphasize dangers that should be stressed, and the narratives from the malware environment provide a history (more social than

technical) of major recent infestations. The work contains a wealth of stories that could be used to promote security awareness, but doesn't otherwise provide a significant source of security assistance.

copyright Robert M. Slade, 2009 BKZRDYTH.RVW 20090120

<http://victoria.tc.ca/techrev/rms.htm>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 72

Monday 6 July 2009

Contents

- [More on the DC Metro collision 22 June 2009](#)
[David Lesher](#)
[Al Stangenberger](#)
- [Re: Train collisions](#)
[Dave Parnas via PGN](#)
- [Earlier autopilot problem on New York City subway trains](#)
[George Mannes](#)
- [More focus on computers in the Air France crash](#)
[Steven M. Bellovin](#)
- [Clear clears its ownership, but not stored data](#)
[PGN](#)
- [Use of GPS leads to wrong house being destroyed](#)
[PGN](#)
- [Sequoia Voting Systems vs DC](#)
[David Lesher](#)
- [A Less than Simple Flight from Rome to Heathrow](#)
[Chris J Brady](#)
- [Train and iPod do not mix](#)
[Barry Munns](#)
- [Billions stolen in online robbery](#)
[PGN](#)
- [HOW many? 12.000 laptops lost PER WEEK in US airports](#)
[Peter Houppermans](#)
- [That old "object reuse" problem ...](#)
[Rob Slade](#)
- [Politicians, personal e-mail, and the ECPA](#)
[Bob Gezelter](#)
- [RISKS at \[catless.ncl.ac.uk\]\(#\)](#)
[Lindsay Marshall](#)
- [Google Earth a tool for thieves and scoundrels?](#)
[John Hatpin via Mark Brader](#)
- [Re: A new way to lose money via ATM...](#)
[Jim Haynes](#)
- [Re: Bozeman](#)
[Andrew Koenig](#)

• [I think we're all Bozemans on this bus](#)

[Steve Lamont](#)

• [Info on RISKS \(comp.risks\)](#)

✂ **More on the DC Metro collision 22 June 2009 (Thompson, [RISKS-25.71](#))**

"David Leshner" <wb8foz@panix.com>

Thu, 25 Jun 2009 22:09:40 -0400 (EDT)

On Monday 22 June 2009, 6-car southbound train #112 rear-ended stopped 6-car southbound train #214, just north of Ft. Totten station. The lead car of 112 split open horizontally, with the frame crushed to half its length, and the sides/roof climbing the last 214 car.

Since this was inbound at afternoon rush hour, the trains were far from full; there are 9 dead, including the operator of 112, and ~75 injured.

The NTSB reports that 112 was in automatic mode, where trackside block limits and Central Command dictates the train's movements. An interview with the 214 operator disclosed that it was stopped in manual mode.

Based on track and wheel markings, the operator of 112 started an emergency stop several hundred feet before the collision. Despite that, 214 was displaced 6-7 feet by the collision. (An empty 6-car train weighs about 460,000 lbs.)

On Tuesday and Wed, NTSB ran tests on the blocks of signaling system. On Wednesday, they found that a train stopped where 214 was did NOT register on the ATP system.

Comments:

It's way too early to jump to conclusions, but the above is exactly what 100+ years of railroad signaling supposedly makes impossible. There will be a lot of work in the coming months to discern what happened.

ref: past NTSB reports on Metro incidents. One discusses the signaling system; the other shows another 1000-series car similarly split by a collision.

<http://www.nts.gov/publicctn/2006/RAR0601.htm>

<http://www.nts.gov/publicctn/1996/RAR9604.htm>

✂ **More on the CD Metro collision**

Al Stangenberger <forags@nature.berkeley.edu>

Fri, 26 Jun 2009 10:07:54 -0700

In case you missed it, NTSB issued a press release yesterday on investigation progress. <http://nts.gov/Pressrel/2009/090625.html>

One significant finding:

- > Investigators conducted tests at the accident site last night with a
- > similar train and found that when the train was stopped at the same
- > location as the stopped struck train, the train control system lost
- > detection of the test train.

This is certainly only one factor in a complex incident, for example the operator of the leading train says he was running the train in manual mode all his shift - why??

This will be an interesting one to watch.

✉ Re: Train collisions (Re: [RISKS-25.71](#))

*"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 23 Jun 2009 13:25:50 PDT*

Comment from Dave Parnas:

This problem already seems to be solved on German trains. If you watch them, you will see that they punch in some numbers when they pass a sign along the tracks. In this way, you know if they are not alert.

On the other hand, the system is supposedly designed to make it impossible for a train to cross the red light indicating a train on the tracks ahead, with automated braking based on maintaining a safe distance between trains.

Later reports seem to indicate that the signaling across one stretch of track was inoperative, which prevented the system from working properly.

<http://www.washingtonpost.com/wp-dyn/content/article/2009/07/01/AR2009070102369.html?hpid%3Dtopnews&sub=AR>

✉ Earlier autopilot problem on New York City subway trains

*George Mannes <gmannes@gmail.com>
Tue, 23 Jun 2009 16:30:19 -0400*

There was a train problem in the news two weeks before the DC disaster.
[Source: Heather Haddon, Autopilot causes L trains to bypass platforms, *AM New York*, 10 Jun 2009]

✉ More focus on computers in the Air France crash

*"Steven M. Bellovin" <smb@cs.columbia.edu>
Mon, 29 Jun 2009 11:13:58 -0400*

According to the Wall Street Journal, 27 Jun 2009, investigators "suspect a rapid chain of computer and equipment malfunctions stripped the crew of automation today's pilots typically rely on to control a big jetliner." Much of the article concerns the hypothesized sequence of events, but this paragraph should resonate with RISKS readers:

Unlike jetliners built in previous decades -- which required pilots to frequently manipulate controls and often manually fly the planes for long stretches -- newer computer-centric aircraft such as the A330 and Boeing's 777 are designed to operate almost entirely on automated systems. From choosing engine settings and routes to smoothing out the ride during turbulence and landing in low visibility, pilots essentially monitor instruments and seldom interfere with computerized commands. So when those electronic brains begin to act weirdly at 35,000 feet, the latest crop of aviators may be less comfortable stepping in and grabbing control of the airplane.

There's on other point worth noting. As has often been noted, it's rarely one thing that brings down a modern airliner. The current presumed scenarios are known to be incomplete:

Planes can -- and occasionally do -- fly safely without pitot probes functioning properly. That's why investigators believe some other important factor, which hasn't been identified yet, likely contributed to the crash.

The plane is a system, where the different pieces interact in complex ways.

✶ Clear clears its ownership, but not stored data

"Peter G. Neumann" <neumann@csl.sri.com>
Fri, 26 Jun 2009 13:18:15 PDT

Out of Business, Clear May Sell Customer Data <<http://slashdot.org/>>
Posted by kdawson Friday June 26, @11:40AM
from the but-don't-worry-it's-perfectly-safe dept.

privacy <<http://slashdot.org/index2.pl?fhfilter=privacy>>

narramissic <<http://www.itworld.com/>> writes "Earlier this week, the Clear airport security screening service ceased operations, leaving many to wonder what would become of the personal information, including credit card numbers, fingerprints, and iris scans, of Clear's customers. And now we know. The information could be sold to the provider of a similar service. <http://www.itworld.com/security/69829/out-business-clear-may-sell-customer-data> Until then, Clear has erased PC hard drives at its airport screening kiosks and is wiping employee computers, but the information is retained on its central databases (managed by Lockheed Martin). Clear customer David Maynor, who is CTO with Errata Security in Atlanta, wants Clear to delete his information but that isn't happening, the company said in a note <<http://www.flyclear.com/>> posted to its Web site Thursday. 'They had your

Social Security information, credit information, where you lived, employment history, fingerprint information,' said Maynor. 'They should be the only ones who have access to that information.'"

<<http://yro.slashdot.org/story/09/06/26/1435209/Out-of-Business-Clear-May-See-Il-Customer-Data>>

✂ Use of GPS leads to wrong house being destroyed

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 11 Jun 2009 19:28:46 PDT

The demolition crew was given only the GPS coordinates, and demolished the wrong house. No one home, no confirmation. Ugly case. [PGN-ed; Thanks to Lauren Weinstein.]

<http://news.aol.com/article/mans-house-mistakenly-destroyed/523439>

✂ Sequoia Voting Systems vs DC

"David Leshner" <wb8foz@panix.com>
Fri, 5 Jun 2009 23:23:12 -0400 (EDT)

Sequoia Voting Systems agreed yesterday to turn over sensitive information to the D.C. Council about how the District's voting machines work and tabulate results, setting the stage for one of the most comprehensive probes on the reliability of electronic voting equipment. The agreement is a response to the election night chaos in the September primaries, when Sequoia machines tabulated more ballots than there were voters, resulting in thousands of phantom votes. ... [Source: Tim Craig, *The Washington Post*, 6 Jun 2009]

<http://www.washingtonpost.com/wp-dyn/content/article/2009/06/05/AR2009060503617_pf.html>

✂ A Less than Simple Flight from Rome to Heathrow

Chris J Brady <chrisjbrady@yahoo.com>
Tue, 23 Jun 2009 08:48:18 -0700 (PDT)

I thought Heathrow was bad enough with its new multi-million pound Terminal 5. Remember the opening fiasco of the thousands of delayed bags being trucked around Europe and then back again, eventually to be auctioned at Gatwick as unclaimed? But at least at Heathrow they always get the departure gates correctly displayed on the computer driven LED displays.

But recently Rome FCO airport produced a first for me. The screens displaying departures were like huge 6 foot / 2 metre laptop screens on

end. In detail they listed the airlines, flight codes, departure gates, and important information like 'now boarding.' When I discovered them upstairs in Terminal C, incidentally in the time-distracting shopping area, one screen showed up-to-date / minute by minute listings for 12.00 through to about 14.00, and the two screens next door had listings for 19.00 through to 21.00 and 21.00 to 24.00. On the two latter screens some of the flights were listed as 'now boarding' including one for Toronto at about 20.00. However the actual time was 13.00. Hmm ...

Interestingly a possible explanation could have been seen at the bottom left hand corners of the errant screens where there was that ubiquitous Windows 'Start' button in green. I tried pressing it but the screens were not touch screens.

Clearly Windows had crashed and apparently left the previous day's flights on display on the two screens. When I told an official he shrugged - like airport officials tend to do - and walked away. The screens stayed like that until I left the area at 16.30 for my BA flight to London.

But as we queued at the BA flight's departure gate, to have our boarding passes processed, I noticed that the Windows driven screen there clearly stated that the flight we were about to board was on Gulf Air to Dubai. The BA contract staff had not noticed, so I assumed that this misinformation was not unusual. I was correct.

However that wasn't quite the end of my computer malfunctioned experience. At Heathrow T5 BA/BAA, with their spanking brand new computer controlled baggage delivery system, they kindly delivered my hold baggage onto the wrong belt so that after waiting for about 30 minutes I then reported it missing. After interrogating their computer system the BA staff told me that it had not even been loaded onto the plane at Rome, that this was not unusual from Rome, and that it would (probably) arrive the next day and be delivered to my home by courier. [Incidentally it appears that thousands (millions?) of 'delayed' bags actually do fly around the world without their owners on board - but that's another risk.] However as I was about to leave the hall and go through customs, and in a less than happy mood, I spotted my lonely bag all by itself on a delivery belt at the far end of the baggage hall.

So I guess it was all a case of a human workforce who don't care about giving out the wrong information, or at least in Rome FCO Airport simply not switching off (or rebooting) displays that were clearly giving out the incorrect information, together with "the principal of computer automation" (e.g. for baggage delivery) "that things automatically go wrong;" a mix that can't fail to cause an interesting experience if not one of concern. And this was during a simple flight from Rome to London.

✉ Train and iPod do not mix (Re: Wirchenko, [RISKS-25.70](#))

Barry Munns <brmunns@gmail.com>

Fri, 19 Jun 2009 16:47:42 +1000

Not an area I'm an expert in, but many years ago I worked as an auditor for the New South Wales (Australia) State Rail. As the job on occasion required us to walk around the maintenance workshops and railway tracks, we received safety training. My recollection of the training was an emphasis on not relying on actually hearing a train coming at you, as the sound waves mostly radiate sideways (not forward of the train). Hence, despite being very big and noisy the trains can 'sneak up on you' (even at very low speeds). Which is why when workers are doing track maintenance they put explosive charges down the track to provide an audio cue that the train is coming.

So, whilst wearing an ipod didn't help the situation, walking on a railway track is not very clever in the first place.

Billions stolen in online robbery

*"Peter G. Neumann" <neumann@csl.sri.com>
Fri, 3 Jul 2009 15:59:07 PDT*

[Thanks to Gunnar Peterson for spotting this one.]

Space trading game Eve Online has suffered a virtual version of the credit crunch. One of the game's biggest financial institutions lost a significant chunk of its deposits as a huge theft started a run on the bank. One of the bank's controllers stole about 200billion credits and swapped them for real world cash of 3,115 pounds. As news of the theft spread, many of the bank's customers rushed to remove their virtual cash. ... The scandal is not the first to play out in Eve Online. In early 2009 one of the game's biggest corporations, called Band of Brothers, was brought down by industrial espionage.

<http://news.bbc.co.uk/2/hi/technology/8132547.stm>

HOW many? 12.000 laptops lost PER WEEK in US airports

*Peter Houppermans <peter@houppermans.com>
Tue, 30 Jun 2009 10:31:32 +0200 (CEST)*

This is probably an interesting paper to draw figures from to see if you can somehow convince people to (a) leave full disk crypto alone and (b) properly shut down a laptop when not in use, despite the lengthy boot time of a modern enterprise laptop lumbering under anti-virus, corporate software management tools and a fragmented file system.

Ponemon rang up 106 big airports in 46 states to discover that Business travelers lose about 12,000 laptops a week in US airports. Not all, or even most, are stolen by airport staff -- 40 per cent of losses occur at security checkpoints. But of the laptops that are found, just 33 per cent are reclaimed by their owner. The rest are sold off, leaving "potentially millions of files containing sensitive or confidential data that may be

accessible to a large number of airport employees and contractors." 40% of loss occurs at security checkpoints. Should that not be IN security checkpoints then?

That old "object reuse" problem ...

Rob Slade <rMslade@shaw.ca>

Tue, 23 Jun 2009 17:23:50 -0800

UBC graduate students and instructors visited Ghana, China (the world's largest electronic waste dump, in Guiyi), and India to find out what happens to electronic trash. Criminals scour the hard drives for credit card information and other personal information. (The electronic waste also pollutes the environment and poisons scavengers seeking to extract metals.)

In Ghana, students bought a hard drive originally used by U.S. defence contractor Northrop Grumman, containing about 50 files marked as competitive and sensitive, including information on government contracts for the U.S. Department of Homeland Security. Northrop spokesman Thomas Henson said that the company has a detailed procedure to dispose of electronics and the drive was likely stolen from a vendor that handles its disposed electronics. (Yeah, right.)

(Maybe the Chinese don't have to hack into important computers to get sensitive info ...)

<http://www.publicaffairs.ubc.ca/media/releases/2009/mr-09-077.html>

<http://www.vancouversun.com/News/team+uncovers+sensitive+defence+records/1723318/story.html>

<http://www.pbs.org/frontlineworld/stories/ghana804/>

<http://www.timescolonist.com/Technology/secrets+found+trash/1723812/story.html>

ml

<http://fergdawg.blogspot.com/2009/06/ubc-journalism-students-find-sensitive.html>

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org

<http://victoria.tc.ca/techrev/rms.htm>

http://blog.isc2.org/isc2_blog/slade/index.html <http://twitter.com/rslade>

<http://blogs.securiteam.com/index.php/archives/author/p1/>

Politicians, personal e-mail, and the ECPA

Bob Gezelter <gezelter@rlgsc.com>

Sun, 28 Jun 2009 14:22:45 -0500

The matter of the e-mails between Governor Mark Sanford (R-SC) and his paramour becoming public raises any number of questions. However, what has been notable in much of the press coverage is the lack of question of whether a crime was committed in the process of supplying them to The State (a South Carolina newspaper).

A more detailed discussion of this affair appears in my blog under the under "Governor Sanford Email Disclosure: An ECPA Violation" at <http://www.rlgsc.com/blog/ruminations/sanford-ecpa.html>

Robert "Bob" Gezelter, 35-20 167th Street, Suite 215,
Flushing, New York 11358-1731 +1 (718) 463 1079 <http://www.rlgsc.com>

RISKS at catless.ncl.ac.uk

*Lindsay Marshall <Lindsay.Marshall@newcastle.ac.uk>
Tue, 9 Jun 2009 18:56:27 +0100*

There are now full-text RSS 1, RRS 2 and Atom feeds available from the risks.org website at <http://catless.ncl.ac.uk/Risks/> .

Google Earth a tool for thieves and scoundrels?

*Mark Brader
Mon, 29 Jun 2009 15:16:49 -0400 (EDT)*

X-Brightmail-Tracker

* From: John Hatpin <RemoveThisjfhopkin@gmailAndThisToo.com>
* Newsgroups: alt.fan.cecil-adams
* Subject: Google Earth a tool for thieves and scoundrels?
* Message-ID: <sfch45ht91u584ouantrdcu1mt7lfcu8ul@4ax.com>
* Date: Mon, 29 Jun 2009 13:29:34 +0100
* Xref: number.nntp.dca.giganews.com alt.fan.cecil-adams:1618846

Just happened across this report today from an unlikely source, the BCS (British Computer Society):

<http://www.bcs.org/server.php?show=conWebDoc.27169>

|Thieves in Hull are thought to be using Google Earth to help them
|steal sought after fish from people's gardens.

|

|Up to 12 cases of fish going missing have been reported during a
|three-week period, with many of those missing Koi carp, worth
|several hundred pounds each.

|

|Police believe the online technology is being used as it would
|otherwise be impossible to locate gardens with fish and ponds in.

|

|Sam Gregory, Humberside police community support officer, said:
|'Google shows what is in your garden and you can see people's
|ponds. One of the properties targeted has an eight foot fence and
|is set back from the road.'

|

|'The pond is in the corner and can't be seen. Unless you were

|standing right next to the wall, you wouldn't be able to hear
|the running water,' he added.

|
|Previously, Google Earth had led to the arrest of two muggers in
|Holland after their victim saw them on Google's Street View.

Firstly, it took me a while to realise that "12 cases of fish going
missing" wasn't talking about big boxes of fish.

Now, I'd heard people complaining that "Google Earth can be used by
burglars to case out their targets", but always dismissed it as
Luddite hysteria; this is the first time I've actually seen it to be
the case. Of fish.

Have there been any previous instances where GE has been used by
ne'er-do-wells to redistribute wealth nefariously?

John Hatpin

<http://uninformedcomment.wordpress.com/>

Re: A new way to lose money via ATM... (RISKS-25.71)

Jim Haynes <jhhaynes@earthlink.net>

Tue, 23 Jun 2009 19:42:46 -0500 (CDT)

I wonder why an ATM needs an operating system anyway. Maybe we should
go back to software as it was done in 1950 and write the instructions to
tell the hardware what to do, no more and no less.

But if it does need an operating system, there was a paper written by David
Parnas long ago where he explained how to write software so that it was
hierarchically modular. That is, the kernel was as simple as possible; and
increased functionality was achieved by adding modules on top of what was
already there, never having to modify something underneath the modules being
added. Philip Levy designed an operating system for the Z-80 using these
principles. The result was a system that could serve anything from an
embedded microcontroller to a multitasking workstation simply by adding the
right set of modules as needed. Seems like I was told that Data General had
an operating system designed along the same lines, again so that a machine
could span a wide range of different kinds of applications.

Maybe the problem is that today memory is essentially free, so it's easier
to throw in baggage we don't need than it is to decide just what we do need.

Re: Bozeman (RISKS-25.71)

"Andrew Koenig" <ark@acm.org>

Wed, 24 Jun 2009 09:16:23 -0400

When I read the article about Bozeman requiring job applicants to grant access to their online personae, I immediately wondered whether the same principle might not apply in the physical domain as well.

That is, I wonder what would happen if a prospective employer were to require all applicants to sign a contract that assigns the applicant's fourth-amendment rights to the employer as a condition of consideration for employment. In other words, in exchange for the company looking at your job application, you would agree to give the company power of attorney to authorize police searches of your home and possessions.

Would such a contract be considered binding? Would it even be considered conscionable? If not (and I certainly hope not), what is the difference between such a contract and what Bozeman is doing? In both cases it is a matter of using a contract to force someone to divulge information to a government entity that would ordinarily require a search warrant.

✂ I think we're all Bozemans on this bus

Steve Lamont <spl@ncmir.ucsd.edu>

Tue, 23 Jun 2009 18:43:50 -0700

Regarding that recent story about Bozeman, Montana, requesting usernames and passwords for social networking sites:

<http://www.montanastation.com/Global/story.asp?S=10577236>

They appear to have backed down and apologized.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 73

Thursday 16 July 2009

Contents

- [Massive Visa overcharge](#)
[Steven M. Bellovin](#)
- [German electronic health card system failure](#)
[Martyn Thomas](#)
- [Boston Ballet School data breach](#)
[Concerned Parent](#)
- [Risks of the Cloud: Liquid Motors](#)
[Gene Wirchenko](#)
- [Facebook fraud about to get more interesting?](#)
[Paul Wallich](#)
- [Taiwan man rescued after getting lost via GPS](#)
[jidanni](#)
- [July 4 Fireworks cyber-attack](#)
[PGN](#)
- [Twitter Attack Raises Flags on Security](#)
[PGN](#)
- [Teenager Falls Into Manhole While Texting](#)
[Michael Barkoviak via Monty Solomon](#)
- [When Texting Is Wrong](#)
[Randy Cohen via Monty Solomon](#)
- [TV station forced to go old school after fire](#)
[Denise Caruso](#)
- [Re: More on the DC Metro collision 22 June 2009](#)
[Steven M. Bellovin](#)
[Rick Dickinson](#)
[David Leshner](#)
- [Saltzer-Kaashoek Computer System Engineering book finally published](#)
[PGN](#)
- [paypal accounts](#)
[Toby Douglass](#)
- [SPAM: Phishing - the state of the art?](#)
[Dirk Fieldhouse](#)
- [Re: Bozeman](#)
[D.F. Manno](#)
[Mark Brader](#)

- [Oakland 2010, IEEE Symposium on Security and Privacy, CFP](#)
[Ulf Lindqvist](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Massive Visa overcharge

"Steven M. Bellovin" <smb@cs.columbia.edu>
Wed, 15 Jul 2009 22:12:09 -0400

According to CNN, about 13,000 customers of Visa found a charge for \$23,148,855,308,184,500 on their statements (<http://www.cnn.com/2009/US/07/15/quadrillion.dollar.glitch/index.html>). Since that's rather larger than the combined GDPs of all the world's economies, Visa did acknowledge the problem and reversed the charge, and even reversed the \$15 overdraft fee...

Where did that amount come from? If you multiply by 100 to get cents and convert to hex, you get 2020202020201250. 0x20 is an ASCII blank, which suggests that someone copied a character string, rather than converting to a long int or unsigned long int. And the 0x1250? Perhaps that's the converted amount of \$46.88. (We can also learn that Visa is using 64-bit integers, which means they're ready to handle charges greater than ~\$21M or perhaps \$43M, and that they're using a non-EBCDIC platform at some point...)

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

[Several other RISKS readers reported on this one, including Jeremy Epstein. PGN]
<http://www.cnn.com/2009/US/07/15/quadrillion.dollar.glitch/index.html>
<http://blogs.usatoday.com/ondeadline/2009/07/man-racks-up-23-quadrillion-bill-at-the-gas-pump.html>

✂ German electronic health card system failure

Martyn Thomas <martyn@thomas-associates.co.uk>
Sun, 12 Jul 2009 10:06:32 +0100

"Test runs with Germany's first-generation electronic health cards and doctors' "health professional cards" have suffered a serious setback. After the failure of a hardware security module (HSM) holding the private keys for the root Certificate Authority (root CA) for the first-generation cards, it emerged that the data had not been backed up. Consequently, if additional new cards are required for field testing, all of the cards previously produced for the tests will have to be replaced, because a new root CA will have to be generated."

href="http://en.wikipedia.org/Hardware_Security_Module" rel="external"

[Also noted by Joe Loughry. PGN]
<http://www.h-online.com/security/Loss-of-data-has-serious-consequences-for-German-electronic-health-card--/news/113740>

✂ Boston Ballet School data breach

Concerned Parent <bostonballetschooldatabreach@yahoo.com>
Thu, 16 Jul 2009 07:45:40 -0700 (PDT)

On July 13, the Boston Ballet School inadvertently mailed to many people a spreadsheet containing personal information on over 3,700 students, alumni and supporters.

Details are available at <http://bostonballetschooldatabreach.blogspot.com/>.

✂ Risks of the Cloud: Liquid Motors

Gene Wirchenko <genew@ocis.net>
Mon, 13 Jul 2009 18:07:09 -0700

Company Caught in Texas Data Center Raid Loses Suit Against FBI
<http://www.wired.com/threatlevel/2009/04/company-caught/>

The first four paragraphs are a good synopsis. In particular, note paragraph three.

'A company whose servers were seized in a recent FBI raid on Texas data centers applied for a temporary restraining order to force the bureau to return its servers, but was denied by a U.S. district court last week.

The company, Liquid Motors, provides inventory management and marketing services to national automobile dealers, such as AutoNation. It was one of about 50 companies put out of business last week when the FBI seized the servers at Core IP Networks, one of two <<http://blog.wired.com/27bstroke6/2009/04/data-centers-ra.html>> data centers and co-location facilities raided by the FBI's Dallas office in the last month in an investigation into VoIP fraud.

Although Liquid Motors was not a target of the investigation, the FBI took all of the company's servers and backup tapes in the raid.

"As a result, Liquid Motors, Inc. has been put out of business and is in breach of its contracts with automobile dealers throughout the country," the <http://www.wired.com/images_blogs/threatlevel/files/Liquid_Motors_v_Lynd.pdf> company wrote in its application for the restraining order (.pdf). "Those automobile dealerships may hold Liquid Motors responsible for all of their lost business, and may terminate their contracts with Liquid Motors, causing permanent and irreparable harm -- for which there is no adequate remedy at law."

[Cloud Computing of course raises some enormous security and privacy issues, especially in having to trust untrustworthy third parties... PGN]

Facebook fraud about to get more interesting?

Paul Wallich <pw@panix.com>

Sun, 28 Jun 2009 20:13:03 -0400

A friend's facebook account was hacked recently (a neat little short-term scam of contacting friends by FB chat, claiming to have been robbed in a foreign country and needing money wired) and it got me to thinking about possible interactions between Facebook's security and plans to open user-generated content to public search and aggregation.

Scams that involve impersonating someone in a medium such as e-mail or chat are necessarily fairly low-volume. Impersonations seen only/mostly by a computer scale much better. So when people talk about the possibility of selling data-mined analyses for content from facebook for marketing or other purposes, fraudulent ways to manipulate the underlying data may become attractive. If someone could use Facebook security holes to fake posts, comments, fanhood, cause-joining and so forth, their clients could profit when the misinformation shows up in the data-mining stream (and the data-mining stream could become significantly less valuable).

As with spamming services, fraudsters wouldn't actually have to generate profits for their customers, just the perception that hijacking facebook identities wholesale would be a good idea...

Taiwan man rescued after getting lost via GPS

<jidanni@jidanni.org>

Sat, 04 Jul 2009 10:01:56 +0800

East Branch of the police force to remind the public that although the satellite navigation to find a way to save time, the public or in front of the first re-start done its homework in order to avoid disappointed and go out to the ages.

<http://translate.google.com/translate?>

[u=http%3A%2F%2Ftw.myblog.yahoo.com%2Fjwlg_pkUviaAxDWs.F9XXuQMb0y%2Farticle%3Fmid%3D4439&sl=zh-TW&tl=en](http://http%3A%2F%2Ftw.myblog.yahoo.com%2Fjwlg_pkUviaAxDWs.F9XXuQMb0y%2Farticle%3Fmid%3D4439&sl=zh-TW&tl=en)

No kidding :-)

July 4 Fireworks cyber-attack

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

Wed, 8 Jul 2009 2:33:30 PDT

Federal agency Web sites knocked out by massive, resilient cyber attack
[Source: Lolita C. Baldor (Associated Press), 7 Jul 2009; thanks to Marv Schaefer]

<http://finance.yahoo.com/news/Federal-Web-sites-knocked-out-apf-2773092122.html?x=0&v=3>

A widespread and unusually resilient computer attack that began on 4 Jul 2009 knocked out the Web sites of several government agencies, including some that are responsible for fighting cyber crime. The Treasury Department, Secret Service, Federal Trade Commission and Transportation Department Web sites were all down at varying points over the holiday weekend and into this week, according to officials inside and outside the government. Some of the sites were still experiencing problems Tuesday evening. Cyber attacks on South Korea government and private sites also may be linked. U.S. officials refused to publicly discuss details of the cyber attack. But Amy Kudwa, spokeswoman for the Homeland Security Department, said the agency's U.S. Computer Emergency Readiness Team issued a notice to federal departments and other partner organizations about the problems and "advised them of steps to take to help mitigate against such attacks."

[Vireworks? Vir-works? Pyreworks? Ireworks? PGN]

Twitter Attack Raises Flags on Security

*"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 16 Jul 2009 9:13:58 PDT*

Someone hacked into a Twitter employee's e-mail account, which apparently led to Twitter execs realizing that their system is not very secure. (A Sophos study from last year is quoted, claiming 40% of web users use the same password on multiple sites, increasing their vulnerabilities.)

[Source: Claire Cain Miller and Brad Stone, *The New York Times*, 16 Jul 2009; PGN-ed]

Teenager Falls Into Manhole While Texting

*Monty Solomon <monty@roscom.com>
Thu, 16 Jul 2009 08:18:15 -0400*

Michael Barkoviak - July 13, 2009 7:46 AM

A teenager walking along the streets in Staten Island recently suffered an embarrassing mistake when she walked into an open sewer while sending text messages on her cell phone. Alexa Longueira, 15, suffered deep cuts and bruises after she fell through a manhole that was uncovered and reportedly left unattended. Two New York City Department of Environmental Protection workers were planning on flushing the sewer, left the manhole cover off, and walked away without putting up a warning sign or orange cones. ...

<http://www.dailytech.com/article.aspx?newsid=15661>

#When Texting Is Wrong

Monty Solomon <monty@roscom.com>

Wed, 15 Jul 2009 01:06:47 -0400

Randy Cohen, The Moral of the Story - The Ethicist's take on the news:
When Texting Is Wrong, *The New York Times*, 13 Jul 2009

The Issue:

You're having dinner with your teenage kids, and they text throughout: you hate it; they're fine with it. At the office, managers are uncertain about texting during business meetings: many younger workers accept it; some older workers resist. Those who defend texting regard such encounters as the clash of two legitimate cultures, a conflict of manners not morals. If a community - teenagers, young workers - consents to conduct that does no harm, does that make it O.K., ethically speaking? ...

<http://ethicist.blogs.nytimes.com/2009/07/13/when-texting-is-wrong/>

#TV station forced to go old school after fire

Denise Caruso <caruso@hybridvigor.org>

Thu, 9 Jul 2009 09:17:18 -0700

This is a little late as I just read it in a friend's Facebook update, but I thought you should see it.

http://www.techflash.com/TV_station_forced_to_go_old_school_after_fire_at_Seattles_Fisher_Plaza_49893982.html

For some reason, the photo makes me smile every time I look at it. I think it's the flag and the fireworks. You don't often get to see images on TV that look like someone actually made them. Like, arts-and-crafts made them. Kinda sweet.

I'm not sure what you'd file it under -- the risks of operations in formerly cool climes being unprepared for heat spikes? -- but certainly it's a case study for why drawing and painting should continue to be taught in school!

#Re: More on the DC Metro collision 22 June 2009 (Thompson, [R-25.71](#))

"Steven M. Bellovin" <smb@cs.columbia.edu>

Mon, 6 Jul 2009 15:43:49 -0400

David Leshner notes, when speaking of the train not showing up, that "the

above is exactly what 100+ years of railroad signaling supposedly makes impossible." True -- but there's another layer here that might play either way: the computerized control system.

Yes, the circuitry is supposed to be designed so that failures always result in a "train present signal. Why there was a failure that could do the opposite is an important question. But what about the computer? Did it misprocess some analog signal? There's clearly a logic failure, since it let a train disappear. If there's a train in a given spot at time T, at time T+delta, there is only a short stretch of track where it can be. Surely a computerized system should be able to take that into account, and mark all of the blocks occupied until it reacquires the train's location. A simple system -- one that just emulated the old relay-based logic -- might not have that ability, since it would be stateless, but the DC Metro system's train-tracker is almost certainly stateful, since it's operating location displays and time of arrival displays at every station. What happens to the state object when a train vanishes? Is it silently deleted? Does the train simply become invisible? Is there a memory leak? The first two, in my opinion, are a definite safety bug.

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

Re: More on the CD Metro collision (Stangenberger, [RISKS-25.72](#))

Rick Dickinson <rtd@notesguy.com>

Mon, 06 Jul 2009 14:47:14 -0500

Taking as given that some (supposed to be all?) track sections have train detectors that can identify specific trains, it's easy to think of at least two ways to keep track of which trains are where within the system:

- 1) Poll each track section periodically to see which trains it currently sees, or
- 2) For each train, maintain a list of the last track section (or last few sections) where it was seen.

Option 1 runs into difficulty as soon as you have a faulty detector anywhere. Option 2 may report a train being on an adjacent section if you have a faulty detector, but it will never show *no train*.

It appears that the train control system in this case used some variation of Option 1.

The RISK? Failing to plan for graceful degradation in the event of sensor failure. Reporting the stalled train in a slightly incorrect position along that track would have certainly been preferable to having it simply "disappear" from view entirely, and might have saved some lives.



Re: More on the DC Metro collision 22 June 2009

wb8foz <wb8foz@panix.com>

Tue, 14 Jul 2009 00:56:35 -0400

The National Transportation Safety Board today issued an urgent safety recommendation to the Washington Metropolitan Area Transit Authority (WMATA) calling for enhanced safety redundancy of its train control system. "The accident has shown that the train control system is susceptible to a single point failure because it did not fail safe and stop the following train when train detection was lost." It called upon WMATA to install software such that the higher level Supervision system would in effect, observe and track train positions, and if/when a train "vanishes" from the basic ATP's view; raise an alarm. It also issued a broader recommendation to the FRA:

"Advise all rail transit operators that have train control systems capable of monitoring train movements to determine whether their systems have adequate safety redundancy if losses in train detection occur. If a system is susceptible to single point failures, urge and verify that corrective action is taken to add redundancy by evaluating track occupancy data on a real-time basis to automatically generate alerts and speed restrictions to prevent train collisions. (R-09-7) (Urgent)"

<http://ntsb.gov/Pressrel/2009/090713.html>

Some early comments/observations/speculations:

The basic reason NTSB's said what they did appears to be that they simply do not [yet...] know why/how the track circuit failed, or how to predict when other failures may happen. The failure was replicable for several days but now is not.

0) WTH ?!%^&*%^??? "Failsafe" track block signals go back to 1872. AC track circuits are newer but still were around to see the Cubbies win the World Series....

1) No such product as NTSB wants exists at present; WMATA can't just slap cash on a vendor's palm and walk away with a fragulator to install. They are already dealing with the vendor of their current ATS platform to create same.

2) The ATP runs on railroad standard components [vital relays, etc...]. The ATS system now runs on Windows.

3) But the ATP unquestionably failed in a way that Just Can't Happen. So is a secondary system that also relies on Windows a step back or going ahead?

4) The 'bright line' border between ATP and systems above is already fuzzy in places; the higher-level stuff relies on ATP, for example.

5) Seldom does a major safety disaster have a single cause; this is no exception. Train 214 was stopped short of the Ft. Totten platform because there had been a breakdown 10-15 miles ahead, at Friendship Heights station. They were using another train to push the dead one out of the

station.

6) Thus far there is no smoking gun. [Someone whose sole job it was to constantly watch that track circuit but was instead texting etc; a safety switch jumpered across, etc....]. Yes, the ops center might have noticed the disappearing train 214, but it's a busy place, especially with #5 going on.

7) An obvious issue will be building a system that does NOT cry wolf multiple times a day. Metrorail moves a lot of people every rush-hour, and repeated line shutdowns will not be well-received.

8) There's a RISKS textbook sure to be written re: the whole saga.

#Saltzer-Kaashoek Computer System Engineering book finally published

*"Peter G. Neumann" <neumann@csl.sri.com>
Sat, 11 Jul 2009 8:55:27 PDT*

Jerry Saltzer and Frans Kaashoek have been turning the class notes that have evolved over the past 40 years for M.I.T. subject 6.033 Computer System Engineering into a book. They have now concluded the effort. The first six chapters have been published by Morgan Kaufman as *Principles of Computer System Design*:

1. Systems
2. Elements of Computer System Organization
3. The Design of Naming Schemes
4. Enforcing Modularity with Clients and Servers
5. Enforcing Modularity with Virtualization
6. Performance

The remaining chapters 7 through 11 are posted online with a Creative Commons license as part of MIT's OpenCourseWare:

<http://ocw.mit.edu/Saltzer-Kaashoek>

This material should be of considerable interest to RISKS readers, who will find some familiar cases -- including pithy examples on network protocols (Chapter 7), fault tolerance (Chapter 8), atomicity (Chapter 9), consistency (Chapter 10), and security (Chapter 11).

Chapter 11, Information Security, is particularly relevant here, including a modernization and reworking of the formative 1975 Saltzer-Schroeder paper that included widely cited security principles.

#Paypal accounts

*Toby Douglass <trd@45mercystreet.com>
Wed, 24 Jun 2009 22:42:36 +0200*

I recently came to buy a pair of clip-on LED lamps. The merchant supported

only VISA card payment via Paypal. In 2004, much against my will, I opened a Paypal account. I knew then with the exquisite clarity of foretelling how much pain it would bring into my life.

At the time, I lived in the UK, with a UK bank account and a UK address for my VISA card.

I now live in the Netherlands and while retaining my UK bank account to retain a VISA card (VISA doesn't really exist in the Netherlands) I now have a Dutch address for the card.

Paypal *insists* on retaining your card address in an account (rather than letting you enter it when paying) and so I needed to update my card address so I can pay. I manage to remember both my old e-mail address and password and log into Paypal.

Turns out you cannot change the country of your account.

Paypal is a credit card billing processor who require the card address to be stored in an account but do not permit the country to change. I may be wrong, but this seems an amazing design flaw.

So I couldn't pay and canceled the order. A risk here is the silent loss of business due to apparently broken intermediation systems.

However, I was then curious why this was so. I contacted Paypal.

The exchange of e-mails that ensued is a wonderful thing, proving - as if proof were needed - that with the correct use of incentives, rational, sentient creatures wonderfully evolved over millions of years can be reduced to drooling imbecility.

The dialog so far has been thus;

Me: 'Why can I not change the country in my Paypal account?'

PP: 'Be aware you cannot change the country in your account. You must set up an account for each country you live in.'

Me: 'Isn't that an awkward way to change the country?'

PP: 'It's a security measure. If people can have multiple accounts per country, they could use it for fraud.'

Me: 'But they can create multiple accounts anyway, just by making them. [Anyway, how does having multiple accounts permit fraud?']

PP: 'All computers have an IP address. Paypal only permits users to log in from the computer they created the account from. It's a security measure.'

Me: 'Your reply is totally factually incorrect and completely irrelevant in every way to my previous question.'

PP: 'Having carefully reviewed your concern, and I see you would like to know if you use your Paypal account on multiple computers. You can.'

Me: 'That was not my question. I want to know why I can't change the

country in my account.'

PP: 'Be aware you cannot change the country in your account. You must set up an account for each country you live in.'

Suddenly, the inability to change country all made sense.

#SPAM: Phishing - the state of the art?

"Dirk Fieldhouse" <fieldhouse@gmx.net>

Tue, 23 Jun 2009 19:55:27 +0100

I received two e-mail messages purporting to be from Abbey National, a UK bank that is a subsidiary of Banco Santander.

Both were flagged as spam. As I have some sort of relationship with this company (unlike, say, Wells Fargo, a popular phishing target), I investigated further. Here's what Abbey's web site says:

"Important warning about Internet banking fraud

Customers of several UK banks have recently been the target of a fraud which uses fake e-mails to encourage customers to enter their card or security details into a counterfeit copy of their website. Abbey will never send you an e-mail asking you to enter, reconfirm or change your security details. ..."

That sounds good. Let's see if it's true ...

Message #1, "*** IMPORTANT *** Ensure The Safety Of Your Online Banking Account", was a clear phisher, a multipart message with a text/plain repeating the subject and text/html containing a 'security notice' with a supposed login link to Abbey, actually to 185.143.broadband7.iol.cz.

"Dear Abbey National online account holder,

This is an important message from the Abbey National Security Centre and has been issued due to a recent upgrade of our secure servers. All current customers are required to update their personal details by simply logging into their online banking accounts.

For security reasons, your access to sensitive account features has been limited until your details are updated on our servers. However, failure to update your details will further lead to a temporary restriction of your online access.

Update your account now in just one easy step, click the "Log On" link below and enter your personal login details to restore your access and enjoy the benefits of online banking and finance avoiding fra

<Log On>

..."

Apart from the fragmentary paragraph preceding the phish-hook, this is really quite good, reasonably grammatical and plausible enough unless you happen to see the actual link behind the 'Log On' hyperlink. It certainly wouldn't be the first time a company had used some external service to send its e-mail, so the fraudulent From: address nxqbpf@messagelabs.com is nicely constructed, the choice of MessageLabs adding a further glint of security.

Now message #2.

"From: "Abbey National" <noreply@abbey.co.uk>

To:

Cc:

Subject: Security

Date: Tue, 23 Jun 2009 02:36:14 +0100

Important Information

In order to make your online experience even more secure we have introduced a new security feature that allows us to detect unusual activity on your online account. If we detect unusual activity, we will call you to make sure that it's really you.

As a result, we need you to visit our online service site by following the reference given below and provide your urgent phone number where you can be reached anytime during the day.

<For banking with a higher level of security, please click here.>

How does it work?

If we detect a sign in with your user name from another country we may decide to confirm that it's really you. You must provide your urgent phone number within 2 weeks from receiving this e-mail otherwise you will not be able to use the online service until we contact you and complete additional security checks. This can be avoided simply by following our online service link above. ..."

Is this is a real attempt by the bank to find my phone number?

If it is, see effectively how they have simulated a phishing e-mail by

- * not including the customer's name in the text;
- * using slightly unnatural English phrases like "your urgent phone number", "anytime" and "otherwise" as a conjunction;
- * actually including a banking login link in HTML mail, for heaven's sake;
- * using three pointlessly different top-level domains (abbey.com, abbeynational.co.uk, abbey.co.uk) in one communication.

On the other hand the security system that's proposed sounds all too plausibly like something that a retail bank might propose: apparently when I

try to maintain my Abbey account from abroad, Abbey will phone my number, not be able to contact me (since I am away), and consequently prevent me from maintaining my account. So I might as well have stayed with telephone banking, then.

Most weirdly the login link is to

<https://myonlineaccounts2.abbeynational.co.uk/CentralLogonWeb/Logon?action=prepare>

which is just the same as I get at www.abbey.com (which in turn is linked from www.santander.com).

But the SMTP headers look extremely phishy: instead of an Abbey server the initial sender is

Received: from User ([24.72.38.106]) by SHOPWEB.PCSECURITYSHIELD.COM

And <http://www.ip-db.com/24.72.38.106> indicates that User is a cable modem in Regina, Saskatchewan, which is a pretty unlikely outsourcer for Abbey.

So is this really a new turn in the phishing war -- a psych-ops attempt to disprove the bank's credibility and possibly increase the hit-rate of future phishery like message #1?

Or did the phisherman just incorrectly bait the hook by forgetting to change the domain part of the link?

At least the ObRisk of e-mail messages with embedded links can only be restated. Always navigate to secure sites manually using a trusted domain name that you found outside the e-mail.

Dirk Fieldhouse, London,UK

Re: Bozeman ([RISKS-25.71](#))

*"D.F. Manno" <dfmanno@mail.com>
Wed, 08 Jul 2009 15:32:39 -0400*

Andrew Koenig asked what would happen if a prospective employer were to require all applicants to sign a contract that assigns the applicant's fourth-amendment rights to the employer as a condition of consideration for employment, specifically whether said employer could require said applicant to agree to give the company power of attorney to authorize police searches of your home and possessions in exchange for the company looking at your job application.

The Fourth Amendment applies only to governments. Absent a specific law to the contrary, a private employer could demand the right to search an applicant's (or employee's) home and possessions. The applicant's recourse is to refuse the job, the employee's is to quit.

(By the way, the police will not search a premises solely at the request of a private employer, no matter what powers of attorney have been signed.

Without a warrant, police can't conduct searches, with a few specified exceptions.)

Since the City of Bozeman is a government, the Fourth Amendment does apply and it could be enjoined from enforcing such a contract provision. With media reports indicating that it has backed off the original provision regarding online accounts, it appears that the policy will not be tested in court, making its constitutionality moot.

✉ Re: Bozeman (Koenig, [Risks-25.72](#))

Mark Brader

Mon, 6 Jul 2009 15:05:16 -0400 (EDT)

The difference is that in the Bozeman case, they would *additionally* be giving the employer power of attorney to *impersonate* them. If I give you my password, you don't just get read access to my files!

Mark Brader, Toronto, msb@vex.net | "Well, *somebody* had to say it."

✉ Oakland 2010, IEEE Symposium on Security and Privacy, CFP

Ulf Lindqvist <ulf.lindqvist@sri.com>

Wed, 08 Jul 2009 13:33:44 -0700

I am happy to let you know that the Call for Papers for the 31st IEEE Symposium on Security and Privacy ("Oakland 2010") is now available.

31st IEEE Symposium on Security and Privacy - Call For Papers

Important Dates (all deadlines are 23:59 PST)

Workshop proposals due: Friday, 21 August 2009

Research papers due: Wednesday, 18 November 2009

Systematization of Knowledge papers due: Tuesday, 24 November

Acceptance notification: 1 February 2010

Final papers due: 1 March 2010

Since 1980, the IEEE Symposium on Security and Privacy has been the premier forum for computer security research, presenting the latest developments and bringing together researchers and practitioners.

We solicit previously unpublished papers offering novel research contributions in any aspect of computer security or privacy. Papers may present advances in the theory, design, implementation, analysis, verification, or empirical evaluation of secure systems. S&P is interested in all aspects of computer security and privacy. Papers without a clear application to security or privacy, however, will be considered out of scope and may be rejected without full review.

Systematization of Knowledge Papers. In addition to the standard research papers, we are also soliciting papers focused on systematization of knowledge. The goal of this call is to encourage work that evaluates, systematizes, and contextualizes existing knowledge. These papers will provide a high value to our community but would otherwise not be accepted because they lack novel research contributions. Suitable papers include survey papers that provide useful perspectives on major research areas, papers that support or challenge long-held beliefs with compelling evidence, or papers that provide an extensive and realistic evaluation of competing approaches to solving specific problems. Submissions will be distinguished by a checkbox on the submission form. They will be reviewed by the full PC and held to the same standards as traditional research papers, except instead of emphasizing novel research contributions the emphasis will be on value to the community. Accepted papers will be presented at the symposium and included in the proceedings.

Workshops. The Symposium is also soliciting submissions for co-located workshops. Workshop proposals should be sent by Friday, 21 August 2009 by e-mail to Carrie Gates (carrie.gates@ca.com). Workshops may be half-day or full-day in length. Submissions should include the workshop title, a short description of the topic of the workshop, and biographies of the organizers.

See the full CFP at

<http://oakland10.cs.virginia.edu/cfp.html>

for more information including detailed submission instructions.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 74

Wednesday 22 July 2009

Contents

- [Elements of Programming, Alexander Stepanov/Paul McJones](#)
[PGN](#)
- [The NSA wiretapping story nobody wanted: Whistleblower Klein](#)
[jidanni](#)
- [Amazon Erases Orwell Books From Kindle Devices](#)
[Brad Stone via Monty Solomon](#)
- [Re: Amazon takes-back Kindle e-books](#)
[Hal Murray](#)
- [Net-filtering tables turned](#)
[Geoff Kuenning](#)
- [Jonathan Zittrain, "Lost in the Cloud"](#)
[PGN](#)
- [Re: cloud computing & server loss](#)
[Harlan Rosenthal](#)
- [Ruhr University team breaks code of KeeLoq system](#)
[David Leshner](#)
- [U.S. Passport RFID security](#)
[Erica Naone via Monty Solomon](#)
- [U.S. Passports: Special alloy sleeves urged to block hackers?](#)
[Todd Lewan via Monty Solomon](#)
- [Arming ATMs with Pepper Spray?](#)
[Thomas Dzubin](#)
- [Eye tracking to prevent screen snooping](#)
[Peter Houppermans](#)
- [U.S. Withheld Data on Risks of Distracted Driving](#)
[Matt Richtel via Monty Solomon](#)
- [Adobe Terms Gone Wild](#)
[Gene Wirchenko](#)
- [Taiwan president in ruckus over prerecorded web messages](#)
[jidanni](#)
- [Canadian Mint says missing gold may have been stolen](#)
[Darryl Dueck](#)
- [Re: July 4 cyber attack](#)
[Joseph Brennan](#)
- [Risks of hierarchical map displays](#)

[Paul Wallich](#)

- [An interesting reversal of the usual credit card problem](#)

[Roger Leroux](#)

- ["Don't freak out," says ING Direct. At least I THINK it's ING Direct!](#)

[Daniel P. B. Smith](#)

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

✶ **Elements of Programming, Alexander Stepanov/Paul McJones**

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

Wed, 22 Jul 2009 9:39:04 PDT

Alexander Stepanov and Paul McJones

Elements of Programming

Addison-Wesley

2009

ISBN 978-0-321-63537-2

What could be one of the most important books for developers of low-risk systems has come to my attention, and deserves your consideration if you are serious about understanding the mathematical foundations of programming and applying them sensibly to your practice. It is not an easy read, but it is a very compelling approach. To support its mathematically oriented crispness, the book includes the definition of a small but elegant C++ subset that has been crafted by Sean Parent and Bjarne Stroustrup for illustrative use in the book. I believe this material should be taught within all computer science curricula.

A long quote and a short one on the back jacket give an idea of what is involved:

Ask a mechanical, structural, or electrical engineer how far they would get without a heavy reliance on a firm mathematical foundation, and they will tell you, 'not far.' Yet so-called software engineers often practice their art with little or no idea of the mathematical underpinnings of what they are doing. And then we wonder why software is notorious for being delivered late and full of bugs, while other engineers routinely deliver finished bridges, automobiles, electrical appliances, etc., on time and with only minor defects. This book sets out to redress this imbalance. Members of my advanced development team at Adobe who took the course based on the same material all benefited greatly from the time invested. It may appear as a highly technical text intended only for computer scientists, but it should be required reading for all practicing software engineers.

-- Martin Newell, Adobe Fellow

The book contains some of the most beautiful code I have ever seen.

-- Bjarne Stroustrup

The bottom of the inside cover suggests that through this book you will come to understand that mathematics is good for programming, and theory is good for practice. I applaud that sentiment.

✶ The NSA wiretapping story nobody wanted: Whistleblower Klein

<jidanni@jidanni.org>

Wed, 22 Jul 2009 04:51:46 +0800

IDG News Service: By some estimates there are 15 to 20 of these secret wiretapping rooms across the country. You're the only AT&T employee who has come forward and talked about them in detail. Why?

Mark Klein: Fear. First of all it was a scary time. It still is a scary time, but during the Bush years it was sort of a witch hunt atmosphere and people were afraid. People are afraid of losing their jobs, and it's a rule of thumb that if you become a whistleblower you'll probably lose your job. And if you have a security clearance, you not only lose your job, but you probably will be prosecuted by the government. The Bush administration made that very clear in statements they made over and over again: 'Anybody who reveals anything about our secret programs will be prosecuted and we are running investigations to find out who leaked this to the New York Times.' Well that puts a fear in people.

http://www.computerworld.com/s/article/9135645/The_NSA_wiretapping_story_nobody_wanted

While campaigning against President George W. Bush, Barack Obama had pledged that there would be "no more wiretapping of American citizens," but President Obama's administration has continued to use many of his predecessor's arguments when it comes to warrantless wiretapping.

http://www.computerworld.com/s/article/9135575/Obama_administration_defends_Bush_wiretapping

✶ Amazon Erases Orwell Books From Kindle Devices (Brad Stone)

Monty Solomon <monty@roscom.com>

Sat, 18 Jul 2009 14:42:33 -0400

In George Orwell's "1984," government censors erase all traces of news articles embarrassing to Big Brother by sending them down an incineration chute called the "memory hole." On Friday, it was "1984" and another Orwell book, "Animal Farm," that were dropped down the memory hole - by Amazon.com. In a move that angered customers and generated waves of online pique, Amazon remotely deleted some digital editions of the books from the Kindle devices of readers who had bought them.

An Amazon spokesman, Drew Herdener, said in an e-mail message that the books were added to the Kindle store by a company that did not have rights to them, using a self-service function. "When we were notified of this by the rights holder, we removed the illegal copies from our systems and from customers' devices, and refunded customers," he said.

Amazon effectively acknowledged that the deletions were a bad idea. "We are

changing our systems so that in the future we will not remove books from customers' devices in these circumstances," Mr. Herdener said. [...]

[Source: Brad Stone, *The New York Times*, 18 Jul 2009]

<http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html>

[Lots of media coverage on this one, especially the 1984 connection. See also an item from David Pogue's Posts: Some E-Books Are More Equal Than Others, 17 Jul 2009. PGN]

<http://pogue.blogs.nytimes.com/2009/07/17/some-e-books-are-more-equal-than-others/>

✂ Re: Amazon takes-back Kindle e-books

Hal Murray <hmurray@megapathdsl.net>

Fri, 17 Jul 2009 16:37:27 -0700

I see two RISKS-related issues. One is that it undermines the whole e-book industry. The other is a good reminder of what can happen with closed ecosystems.

It's been slashdotted and is in many online news sources and blogs.

http://news.cnet.com/8301-13860_3-10289983-56.html

✂ Net-filtering tables turned

Geoff Kuenning <geoff@cs.hmc.edu>

Tue, 07 Jul 2009 13:40:16 -0700

The July 7th, 2009 edition of "Ask Amy" (an advice columnist) tells the tale of an interesting RISK of using net filtering and online systems to control your children. Briefly, a high-school student's father was using the school's "check up on your kids" Web site to an excessive degree. The fed-up student used the family's parental control software to find out how often the dad was visiting the site (answer: three times daily) and in the process learned some unsavory details about Dad's browsing habits.

<http://www.chicagotribune.com/features/columnists/advice/chi-0707-ask-amyjul07,0,2095115.column>

I suppose the RISK lies in assuming you're smarter than your kids...and forgetting that most tools can be used in multiple ways.

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

In any large population, there are some people who aren't very bright. That's not their fault, it's just in their genes. As an engineer, I have a responsibility to design things that won't kill off the slower ones, just as I have a responsibility to design things that won't harm my neighbor's dog.

✂ Jonathan Zittrain, "Lost in the Cloud" (NYTimes Op-Ed)

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

Mon, 20 Jul 2009 8:12:56 PDT

[I read this over breakfast on paper. Thanks to Lauren Weinstein for the URL.]

Jonathan Zittrain, Lost in the Cloud, *The New York Times*, 20 Jul 2009

Earlier this month Google announced a new operating system called Chrome. It's meant to transform personal computers and handheld devices into single-purpose windows to the Web. This is part of a larger trend: Chrome moves us further away from running code and storing our information on our own PCs toward doing everything online - also known as in "the cloud" - using whatever device is at hand.

Many people consider this development to be as sensible and inevitable as the move from answering machines to voicemail. With your stuff in the cloud, it's not a catastrophe to lose your laptop, any more than losing your glasses would permanently destroy your vision. In addition, as more and more of our information is gathered from and shared with others - through Facebook, MySpace or Twitter - having it all online can make a lot of sense.

The cloud, however, comes with real dangers. [...]

<http://www.nytimes.com/2009/07/20/opinion/20zittrain.html>

Re: cloud computing & server loss (RISKS-25.73)

Harlan Rosenthal <Harlan.Rosenthal@verizon.net>

Thu, 16 Jul 2009 22:14:27 -0400

Cloud Computing certainly exposes one to the consequence of other people's actions, but law enforcement's lack of selectivity is nothing new. Consider the Secret Service raid on Steve Jackson Games years ago. <http://www.sjgames.com/SS/>

Ruhr University team breaks code of KeeLoq system

David Leshner <wb8foz@panix.com>

Fri, 10 Jul 2009 14:20:35 -0400

<http://www.sundayherald.com/news/heraldnews/display.var.2174801.0.scientists_crack_security_system_of_millions_of_cars.>

Ruhr University scientists say it is now relatively straightforward to clone the remote control devices that act as the electronic keys. They have overcome the KeeLoq security system, which is made by US-based Microchip Technology and is used by Honda, Toyota, Volvo, Volkswagen and other

manufacturers to transmit access codes using radio frequency identification technology. The KeeLoq's security relies on poor key management, in which every key is derived from a master that's stored in the reading device. Moreover, it uses a proprietary algorithm that had already been shown to generate cryptographically-weak output.

✂ U.S. Passport RFID security (Erica Naone)

*Monty Solomon <monty@roscom.com>
Fri, 17 Jul 2009 13:37:36 -0400*

Meanwhile, although experts say that some RFID technologies are quite secure, a University of Virginia security researcher's analysis of the NXP Mifare Classic (see Hack, November/December 2008), an RFID chip used in fare cards for the public-transit systems of Boston, London, and other cities, has shown that the security of smart cards can't be taken for granted. "I think we are in the growing-pains phase," says Johns Hopkins University computer science professor Avi Rubin, a security and privacy researcher. "This happens with a lot of technologies when they are first developed." ... [Source: Erica Naone, RFID's Security Problem: Are U.S. passport cards and new state driver's licenses with RFID truly secure? Technology Review, Jan/Feb 2009; PGN-ed]

<http://www.technologyreview.com/computing/21842/>

✂ U.S. Passports: Special alloy sleeves urged to block hackers?

*Monty Solomon <monty@roscom.com>
Sat, 18 Jul 2009 14:42:33 -0400*

(Todd Lewan)

To protect against skimming and eavesdropping attacks, federal and state officials recommend that Americans keep their e-passports tightly shut and store their RFID-tagged passport cards and enhanced driver's licenses in "radio-opaque" sleeves. That's because experiments have shown that the e-passport begins transmitting some data when opened even a half inch, and chipped passport cards and EDLs can be read from varying distances depending on reader technology.

[Source: Todd Lewan, The Associated Press, 12 Jul 2009; PGN-ed]

<http://www.washingtonpost.com/wp-dyn/content/article/2009/07/11/AR2009071101929.html>

✂ Arming ATMs with Pepper Spray?

*<dzubint@vcn.bc.ca>
Mon, 13 Jul 2009 08:32:38 -0700 (PDT)*

Now I've seen everything...

Apparently, a leading South African bank has fitted 11 ATMs around the Cape Peninsula with pepper spray cans in an effort to prevent card skimming and ATM bombing.

I guess the person who thought of this wasn't a reader of Risks Digest.

According to the following Guardian article

<http://www.guardian.co.uk/world/2009/jul/12/south-africa-cash-machine-pepper-spray>

...the mechanism backfired in one incident last week when pepper spray was inadvertently inhaled by three technicians who required treatment from paramedics.

Patrick Wadula, spokesman for the Absa bank, which is piloting the scheme, told the Mail & Guardian Online: "During a routine maintenance check at an Absa ATM in Fish Hoek, the pepper spray device was accidentally activated.

"At the time there were no customers using the ATM. However, the spray spread into the shopping centre where the ATMs are situated."

What's next? PCs that pepper spray their users when they download a virus or malware? Hmmmm... perhaps not a bad idea :-)

Thomas Dzubin, Calgary, Saskatoon, or Vancouver CANADA

Eye tracking to prevent screen snooping

Peter Houppermans <peter@houppermans.com>

Wed, 08 Jul 2009 11:56:07 +0200

This is IMHO a rather promising new development in security, mainly because it appears to promise more security without too much usability impact. And it may ruin Powerpoint presentations, another point in its favour :-). It neatly uses the fact that most modern laptops have a camera built in.

Source: http://www.siliconvalley.com/ci_12743292

=====

Anderson calls it his "aha" moment -- a flash of insight from which he drew a career-altering connection between decades-old research and his job as a computer security expert. Nearly two years ago, Anderson had a comfortable job as vice president at an established computer security company. But while reading "Consciousness Explained," a book by philosopher Daniel Dennett, Anderson learned about one scientist's research into variations in the way the human eye reads and processes text and images.

"This obscure characteristic ... suddenly struck me as (a solution to) a security problem," said Anderson, 42, who has a doctorate in cryptology.

"I said, 'Holy cow. No one has thought of using this to protect the contents of a screen.' It was just some obscure research."

Anderson quit his job at SafeNet, raised \$1.2 million in seed money from friends and family and plunged full time into developing his idea -- a software program that allows only an authorized user to read text on the screen, while everyone else sees gibberish. [..]

The private version of the product can already be bought from the company at <http://oculislabs.com>, at a price well below your average privacy screen. From their website it appears the "look, your mother is watching" Pro version is not yet released.

U.S. Withheld Data on Risks of Distracted Driving (Matt Richtel)

Monty Solomon <monty@roscom.com>

Wed, 22 Jul 2009 00:08:23 -0400

In 2003, researchers at a federal agency proposed a long-term study of 10,000 drivers to assess the safety risk posed by cellphone use behind the wheel. They sought the study based on evidence that such multitasking was a serious and growing threat on America's roadways. But such an ambitious study never happened. And the researchers' agency, the National Highway Traffic Safety Administration, decided not to make public hundreds of pages of research and warnings about the use of phones by drivers - in part, officials say, because of concerns about angering Congress. ...

[Source: Matt Richtel, *The New York Times*, 21 Jul 2009; PGN-ed]

<http://www.nytimes.com/2009/07/21/technology/21distracted.html>

Adobe Terms Gone Wild

Gene Wirchenko <genew@ocis.net>

Mon, 13 Jul 2009 16:47:50 -0700

Hello:

Would you like to report a bug in an Adobe product? Here is the URL:

<https://www.adobe.com/cfusion/mmform/index.cfm?name=wishform>

They do have rather stringent terms. You have to affirm lots of things about interest in your bug report, oops, Idea. My favourite bit is "You represent and affirm that you are 18 years of age or older." Oh, to be 17 again.

How many people take one look at that page and decide not to bother? Does this affect the quality of Adobe software?

Taiwan president in ruckus over prerecorded web messages

<jidanni@jidanni.org>

Mon, 20 Jul 2009 14:33:23 +0800

Taiwan President Ma Ying-jeou was criticized after prerecorded Internet messages leaked out.

Experienced Internet surfers found the messages due to be broadcast the next two weeks had already been recorded. The surfers only had to change the dates on the presidential website to see the new messages.

Presidential Office Spokesman Wang Yu-chi said Ma had prerecorded the videos, which were supposed to address current affairs, adding that Ma would remake the videos, and asked the person who first discovered the messages to come forward and receive a "small prize" from the Presidential Office.

<http://www.taipeitimes.com/News/taiwan/archives/2009/07/20/2003449078>

http://www.etaiwannews.com/etn/news_content.php?id07831

Canadian Mint says missing gold may have been stolen

"Darryl/Becky Dueck" <dbdueck@gmail.com>

Mon, 6 Jul 2009 19:36:58 -0500

<http://www.cbc.ca/canada/ottawa/story/2009/06/29/ottawa-mint-gold-missing.html>

Money is missing, and all they're saying is, "we'll look into it - we have one of the most secure facilities in the world". I can't believe how little uproar there has been. -Darryl Dueck, Winnipeg, MB CANADA

The Royal Canadian Mint said Monday that \$15.3 million worth of gold missing from its vaults could have been stolen. The gold was reported missing last fall, but officials at the mint said they had hoped they would find that an accounting error was responsible.

A review conducted by auditors Deloitte and Touche, however, recently concluded that the gold wasn't simply forgotten during inventory. "The unaccounted for difference in gold does not appear to relate to an accounting error in the reconciliation process, an accounting error in the physical stock count schedules or an accounting error in the record keeping of transactions during the year," the company concluded in a report released Monday.

Christine Aquino, director of communications with the mint, said that many possible scenarios are being considered. "We're not going to speculate on the cause just yet. We're not giving up on this. We're going to pursue this rather vigorously." Aquino said the mint asked the RCMP to look into the matter two weeks ago. She said in the meantime, the mint is prepared to follow three of Deloitte and Touche's recommendations concerning its accounting procedures and building security. "They've also asked that we go through our security measures for review. But it's just one of the avenues

we're pursuing. We have one of the most secure facilities in Canada, if not the world." [Source: CBC News, 29 Jun 2009]

<http://www.cbc.ca/news/credit.html>

Re: July 4 cyber attack ([RISKS-25.73](#))

Joseph Brennan <brennan@columbia.edu>

Fri, 17 Jul 2009 10:50:23 -0400

The attacks on web sites from Korea made the news, but there was at least one attack on email, at columbia.edu. More than 26,000 hosts in Korea connected to the columbia.edu mx pool, collectively 160,000 times an hour, and then just sat there. Our network monitoring showed that they sent some bytes that may have been a HELO string, but they did not send MAIL.

Our system responds by forking a sendmail process for each connection, and even though they were mostly doing nothing waiting for data, the system load went up. However, it is summer at an edu, and we are pretty well provisioned anyway, so the effect was "hm, that's funny, wonder why the load is that high" rather than "OMG the sky is falling".

We shortened the timeout waiting for MAIL, and rate-limited the worst-offending IP blocks, and got the load back to normal. The attack was not continuous throughout the weekend. Maybe the botnet had other missions part of the time. Like the http attacks, it stopped during the following week.

Possibly the goal was that we would be forced to blackhole South Korean IP space in order to function. Columbia University has a significant number of people with personal and academic contacts in South Korea.

Joseph Brennan, Lead E-mail Systems Engineer
Columbia University Information Technology

Risks of hierarchical map displays

Paul Wallich <pw@panix.com>

Mon, 20 Jul 2009 22:30:01 -0400

The other day, for no good reason, I got misplaced on some local dirt roads. "No problem," I thought, because my car had a GPS and a map database that actually knew about all those dirt roads. But when I zoomed the display out far enough to see where the nearest paved road back to exurbia might be, all the dirt roads disappeared, and I was apparently driving through a void. So I couldn't figure out which road would take me back to pavement, because I couldn't display both the roads I was on and the one I wanted to get to at the same time.

Obviously, I could have pulled over and used pan as well as zoom controls,

or asked for directions to some known point (and hoped none of the dirt roads on the route was closed or washed out). But that would have required both presence of mind and a place to park where I could be sure of getting back on the road after figuring out location and route.

I wonder whether such hierarchical displays contribute to some of the GPS-aided navigation debacles that sometimes grace this publication -- a driver may have some idea that they're going the wrong way, but their display doesn't offer enough information to plan a new route easily, and the psychological pressure to keep moving forward can increase as conditions get worse.

✶ An interesting reversal of the usual credit card problem

Roger Leroux <yrl1967@gmail.com>

Thu, 16 Jul 2009 23:00:38 +0000

There's a board game company called GMT Games (www.gmtgames.com). They have a "pre-order" system in place that lets you order a game before it is published (they call it the P500 system), and in order to participate you need to provide them with a credit card number.

Recently, I and other customers received this e-mail from them:

"Please Update Your Online Credit Card Information

Ugh! Microsoft strikes again! As you probably know, we encrypt your credit card data, several times, to make sure that your data is always safe online. Well, a recent Windows update done by our service provider apparently modified the encryption key used to decrypt the data for us to read and use for charging. Please don't worry about your cc info. *There was absolutely no security issue here. In fact, it's quite the opposite. For any card that you entered into our system before July 4, neither we nor anyone else can read the card # (as the encryption key was changed).* There is no problem with cc #s entered after July 4.

So we're asking you guys to please go into your online account in the next day or two and update the credit card # that is listed there (for many of you it will now look like a long string of alphanumeric) with your correct # so that we can charge the games slated to begin charging on Monday, July 13th. If you guys have any questions about this, or would prefer to do this by phone or online chat, please don't hesitate to contact our office ladies either on our website or at our toll-free number. They'll be happy to help you get the data re-entered if you'd like some help. We apologize for any inconvenience this may cause."

It was nice that for a change no personal information was leaked, but I think this highlights the problems of applying OS updates without the ability to do a rollback or for that matter, having a backup of the original (suitably encrypted of course) data.

🔥 "Don't freak out," says ING Direct. At least I THINK it's ING Direct!

"Daniel P. B. Smith" <usenet2006@dpbsmith.com>

Wed, 22 Jul 2009 11:53:08 -0400

Every time I turn around, a bank website presents me with glaringly obvious RISKS about which one can only say "what _were_ they thinking?"

1) When I click on "View My Account" at <http://www.ingdirect.com>, I am taken to a login screen headed by a bold blue notice:

"Our site will be getting a minor facelift soon. So if you notice anything different after you sign in, don't freak out. You're in the right place."

That should train customers to be vigilant.

2) I opened a bank account at a local bank, and went through all the silly rigamarole about picking a picture and so forth, and got to the idiotic "security questions." This site is one of the kind that forces you to select from a limited list of bad options, which usually manage to be both insecure yet difficult to remember (Let me think, did I enter the answer as "Main Street," "main street," or "Main st.?"?)

But one made my jaw drop: one of the available choices was "How many children do you have?"

What are the chances that a stranger could successfully guess *that* one? By comparison, my birthday is as strong as Fort Knox.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 75

Thursday 6 August 2009

Contents

- [Software never fails, people decide that it does](#)
[Paul Robinson](#)
- [Seven water mains break due to computer glitch](#)
[Joseph Lorenzo Hall](#)
- [Stock Traders Find Speed Pays, in Milliseconds](#)
[Charles Duhigg via Monty Solomon](#)
- [GPS typo saves couple?](#)
[Joel Baskin](#)
- [How To Hijack 'Every iPhone In The World'](#)
[Andy Greenberg via Monty Solomon](#)
- [10 ways your voice and data can be spied on](#)
[Gene Wirchenko](#)
- [The NSA Is still Listening to You](#)
[jidanni](#)
- [Beware of Outdated E-mail Addresses](#)
[Gene Wirchenko](#)
- [Funniest security faux pas this week](#)
[Ron LaPedis](#)
- [You think Adobe bug reports are tough to submit...](#)
[Michael Albaugh](#)
- [Re: Risks of hierarchical map displays](#)
[Leonard Finegold](#)
[Gavin Treadgold](#)
[Gene Wirchenko](#)
- [Industrial object-oriented language made void-safe](#)
[Bertrand Meyer](#)
- [Ari Juels, Tetraktys, a 'cryptographic thriller'](#)
[Ben Rothke via PGN](#)
- [Info on RISKS \(comp.risks\)](#)

✶ **Software never fails, people decide that it does**

Paul Robinson <paul@paul-robinson.us>
Sun, 26 Jul 2009 18:17:14 -0700 (PDT)

There was an article [1] on Slashdot saying how Software Engineering and Computer Science are two different things. It also refers to an article [2] on Dr. Dobbs Journal that says that Software Engineering will never be a rigorous, formal discipline. Which is true.

The statement that software engineering - which is a mislabel - cannot be a rigorous, formal system is so obvious that it might as well be one of those things we never think about until we have to and when we do think about it it's intuitively obvious.

Consider what will happen when you die, there are only three possibilities: You exist after you die and you like the results; you exist after you die and you do not like the results; you do not exist after you die. All three possibilities are equally valid since we have no evidence of any of them. If as it turns out, that when you die you cease to exist, it is not something you need to worry about. Now, the thought probably terrifies you - it used to terrify me, too - until you realize something: if you cease to exist, you will know nothing. You'll never know that you don't exist.

So consider the conditions of the existence of software. Software is always perfect and is always the same, it never changes. It does not rot, rust, age, get moldy, crumble, break, shatter or fail. It never needs maintenance, lubrication, cleaning, sharpening, polishing, repair or replacement. As long as the hardware that copies it makes identical copies, it is perfect and always will be perfect, except for the extremely rare and unusual case of deterioration of the storage media due to cosmic ray damage. Which can be detected by mathematical algorithm, in which case, if there is another source, another perfect copy can be made and it's right back where it was. Software is never defective and can never be defective other than the case I've given of the rare possibility of cosmic-ray damage to media or hardware failure in copying, and thus it never needs change, modification or updating.

Every year, every country makes changes to its tax laws. Any software which must comply with those new changes has to be changed according to the decisions of tax accountants and lawyers as to what is needed to be in compliance. If you have a cellular network and want to add new features, you have to modify the software - in the switches, the handsets, the gateways, and/or all of these - to be able to enable them to offer new features. In both cases the software needs updating.

Both statements are true, but you might ask how they can be when they appear to be conflicting. They're not, and I'll explain why.

Any software package, from a 1-line APL function to a 20 million-line COBOL behemoth application suite that runs a trillion dollar bank, large insurance company or government agency, only requires maintenance or change because in someone's subjective opinion it needs a change. A bridge needs replacement when it collapses or when it is beyond its useful life; a building needs replacement under the same circumstances. A piece of metal furniture needs replacement when its structure rusts into dust, fails or is unable to support a load due to metal fatigue. These are objective facts, either the

structure is usable or it isn't. An engineer can determine by experience and judgment that the structure is at its lifespan limit or can point to signs of physical rust, deterioration, or structure failure indicators that prove their opinion.

Any declaration that a software package needs updating, change, or replacement is strictly based upon the subjective opinion of someone saying that it needs the work. All software change is the result of some person's opinion that the change needs to be made and have no basis in reality except their opinion. Their opinion is correct if you agree with them or if in your opinion you can't disagree with their opinion. They may be correct that because of errors in how the software performs its desired function, need for new function, or need for changes in existing function, the software needs change, replacement or updating, but they can only be "correct" because it is considered that in someone's opinion they agree with their opinion that the change is needed.

But the claim by someone that a software package needs change, updating or replacement is, and always will be, a subjective opinion based on nothing more than "because I say so."

(1) <http://tech.slashdot.org/story/09/06/06/0210229>

(2) <http://www.ddj.com/architect/217701907>

Seven water mains break due to computer glitch

Joseph Lorenzo Hall <joehall@gmail.com>

Tue, 28 Jul 2009 19:32:16 -0400

http://www.nj.com/news/index.ssf/2009/07/seven_water_mains_break_in_jer.html

Jersey City is my hometown during my visiting postdoc at Princeton's CITP.

From the story:

Seven water mains broke in the Jersey City Heights today -- the result of a computer glitch that caused a false low pressure reading and kicked on pumps at a United Water facility, officials said. Due to low water pressure in the Heights following the ruptures, fire officials posted four water tanker trucks at two locations in the area for use in the event of a fire, Fire Director Armando Roman said. [...]"

Pretty serious consequences from this glitch, no doubt... and a mighty efficient way to mess up fire response. And I can attest with video evidence that the water was indeed brown:

<http://www.flickr.com/photos/joebeone/3766791608/>

UC Berkeley/Princeton <http://josephhall.org/>

Stock Traders Find Speed Pays, in Milliseconds

Monty Solomon <monty@roscom.com>

Fri, 24 Jul 2009 22:40:44 -0400

Charles Duhigg, *The New York Times*, 14 Jul 2009

It is the hot new thing on Wall Street, a way for a handful of traders to master the stock market, peek at investors' orders and, critics say, even subtly manipulate share prices. It is called high-frequency trading - and it is suddenly one of the most talked-about and mysterious forces in the markets.

Powerful computers, some housed right next to the machines that drive marketplaces like the New York Stock Exchange, enable high-frequency traders to transmit millions of orders at lightning speed and, their detractors contend, reap billions at everyone else's expense. These systems are so fast they can outsmart or outrun other investors, humans and computers alike. And after growing in the shadows for years, they are generating lots of talk.

Nearly everyone on Wall Street is wondering how hedge funds and large banks like Goldman Sachs are making so much money so soon after the financial system nearly collapsed. High-frequency trading is one answer. And when a former Goldman Sachs programmer was accused this month of stealing secret computer codes - software that a federal prosecutor said could "manipulate markets in unfair ways" - it only added to the mystery. Goldman acknowledges that it profits from high-frequency trading, but disputes that it has an unfair advantage. Yet high-frequency specialists clearly have an edge over typical traders, let alone ordinary investors. The Securities and Exchange Commission says it is examining certain aspects of the strategy. ...

<http://www.nytimes.com/2009/07/24/business/24trading.html>

GPS typo saves couple?

Joel Baskin <jdbaskin@hotmail.com>

Tue, 28 Jul 2009 13:17:58 -0700

A Swedish couple touring in Italy drove to Carpi instead of Capri due to a typo. Who knows if they would have tried to drive to the intended island -- so this may have saved them. :)

This is just another case of user error -- but should GPS systems check spelling, and if so how? Could there be a database of places with similar names within defined distances? Extended metadata would be of use -- but effort would increase quite quickly for several reasons.

<http://news.bbc.co.uk/2/hi/europe/8173308.stm>

[Also noted by Rick Moen in the *San Francisco Chronicle* and by Gene Wirchenko. PGN]

How To Hijack 'Every iPhone In The World'

Monty Solomon <monty@roscom.com>

Wed, 29 Jul 2009 08:14:30 -0400

Andy Greenberg, 28 Jul 2009

On Thursday, two researchers plan to reveal an unpatched iPhone bug that could virally infect phones via SMS. If you receive a text message on your iPhone any time after Thursday afternoon containing only a single square character, Charlie Miller would suggest you turn the device off. Quickly.

That small cipher will likely be your only warning that someone has taken advantage of a bug that Miller and his fellow cybersecurity researcher Collin Mulliner plan to publicize Thursday at the Black Hat cybersecurity conference in Las Vegas. Using a flaw they've found in the iPhone's handling of text messages, the researchers say they'll demonstrate how to send a series of mostly invisible SMS bursts that can give a hacker complete power over any of the smart phone's functions. That includes dialing the phone, visiting Web sites, turning on the device's camera and microphone and, most importantly, sending more text messages to further propagate a mass-gadget hijacking. ...

<http://www.forbes.com/2009/07/28/hackers-iphone-apple-technology-security-hackers.html>

10 ways your voice and data can be spied on

Gene Wirchenko <genew@ocis.net>

Tue, 28 Jul 2009 10:55:12 -0700

1. Wireless keyboard eavesdropping
2. Wired keyboard eavesdropping
3. Laptop eavesdropping via lasers
4. Commercial keyloggers
5. Cell phones as remotely activated bugs
6. Cell phone SIM card compromise
7. Law enforcement wiretapping based on voice print
8. Remote capture of computer data
9. Cable TV as an exploitable network
10. Cell phone monitoring

Some of these ways have been covered in RISKS before.

Item 9 caught my eye:

Commercially available software claims to capture cell phone conversations and texting. Attackers need to get physical access to the phone to upload the software that enables this.

<http://www.itbusiness.ca/it/client/en/CDN/News.asp?sub=true&id=54027>

#The NSA Is still Listening to You

<jidanni@jidanni.org>

Thu, 23 Jul 2009 10:31:34 +0800

This summer, on a remote stretch of desert in central Utah, the National Security Agency will begin work on a massive, 1 million-square-foot data warehouse. Costing more than \$1.5 billion, the highly secret facility is designed to house upward of trillions of intercepted phone calls, e-mail messages, Internet searches and other communications intercepted by the agency as part of its expansive eavesdropping operations. The NSA is also completing work on another data warehouse, this one in San Antonio, Texas, which will be nearly the size of the Alamodome.

<http://informationclearinghouse.info/article23125.htm>

#Beware of Outdated E-mail Addresses

Gene Wirchenko <genew@ocis.net>

Fri, 24 Jul 2009 11:41:27 -0700

Twitter hack illustrates danger of chained exploits

http://www.infoworld.com/d/security-central/twitter-hack-illustrates-danger-chained-exploits-535?source=IFWNLE_nlt_daily_2009-07-24

The article discusses a few attacks. The one that struck me as interesting is the one at the bottom of page one and top of page two.

"The second example of a chained exploit is even more intriguing. In this case, a malicious hacker broke in to one or more Twitter employees' e-mail accounts, then publicly posted both personal and company confidential information.

The hacker accomplished this feat after discovering that a Twitter employee used Gmail and that a request for a new password for the account would be sent to the employee's Hotmail account. However, the employee had not used the Hotmail account in a very long time, so their Hotmail address was available for anyone to adopt.

The hacker registered for the Hotmail address and had Gmail send a password reset for the Twitter employee's Gmail account to what was now the hacker's Hotmail account. With the new password, the hacker gained access to the Twitter employee's Gmail account. Using information found in the employee's e-mail, the hacker was able to acquire personal information about the employee and data to exploit Twitter's own network. TechCrunch has an excellent step-by-step account of the hack."

The TechCrunch link referred to is full of yummy technical details.

<http://www.techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/>>

#Funniest security faux pas this week

Ron LaPedis <rlapedis@seacliffpartners.com>

Wed, 22 Jul 2009 17:01:31 -0700

According to the About Us blurb on their web site, "The Payment Card Industry (PCI) Knowledge Base (www.KnowPCI.com) is the largest an independent research community focused on the security of payment and related financial and personal data. Our registered membership includes approximately 2000 persons, including retailers, hoteliers, academics, bankers, payment processors, PCI assessors (QSAs), providers of payment systems and security technologists."

Yet when I registered on the site, their confirmation e-mail contained my username and password in clear text. I think we already know the RISKS in that, no?

FOLLOW UP: An e-mail to the founder of the organization resulted in him asking the webmistress to remove the password from the confirmation e-mail which she did within the hour. Now THAT is service!

Ron LaPedis, MBCP, MBCI, CISSP-ISSAP, ISSMP +1 415 939 8887
Seacliff Partners International, LLC
<http://seacliffpartners.com> Business Continuity & Security Advisors

#You think Adobe bug reports are tough to submit...

Michael Albaugh <m.e.albaugh@gmail.com>

Wed, 22 Jul 2009 14:37:33 -0700

Gene Wirchenko should be glad he was only trying to report a bug. ([RISKS Digest 25.74](#)).

When I upgraded to PageMaker7 (Yes, that long ago, they may have reformed by now), I got porn-spam within 15 minutes of entering "my e-mail address" into their online registration.

Yes, it was one I created for this specific purpose. When I tried to report this, I found that abuse@adobe.com did not apparently exist. postmaster@adobe.com would not accept my e-mail either.

The website kindly directed me to send a registered letter to some lawyers in Los Angeles, at a post-office box. I found it simpler to delete the account, as it had served its purpose. I also chose at that point to never again buy from Adobe.

Re: Risks of hierarchical map displays (Wallich, [RISKS-25.74](#))

Leonard Finegold <L@drexel.edu>

Wed, 22 Jul 2009 18:20:12 -0400

Where was this, and what was the GPS? Sympathy. Have experienced just this for Cathedral Valley, UT (beautifully deserted). GPS = Garmin Nuvi 350. Had happily driven around the dirt roads, using the GPS. Afterwards, I wanted to check another route in and out, and found just what you did.

PS. Could you just have stopped on the road, presumably no-one around?

Re: Risks of hierarchical map displays (Wallich, [RISKS-25.74](#))

Gavin Treadgold <gav@rediguana.co.nz>

Thu, 23 Jul 2009 12:14:31 +1200

I am most familiar with Garmin handheld and auto GPS units, but this probably applies to other brands as well. Under Settings > Maps, there usually exists an option entitled Map Detail. By default on Garmins, it is set to Normal. It also has options such as Least Detail, Less Detail, More Detail and Most Detail. If you increase the level of detail, you will see the roads that exist lower in the hierarchy at a wider zoom level - which is probably what Paul was attempting to achieve. E.g. roads that previously may have been shown at the say a 500m scale (as set by the map developer) now become visible up to say 1.2km or 2km scales. A number of units also offer more granular control of what layers are visible up to what zoom level.

This works well in the countryside, but can be a real problem in cities with dense road networks as the map display takes longer to redraw, and when it has redrawn it becomes too cluttered to be readable.

It is certainly possible to force the display of more roads at higher zoom levels, once again, the risk is actually user awareness of the features of the device they are using, and how to customise their device to achieve the desired display.

Gavin, Immediate Past President of the NZ Recreational GPS Society

<http://www.gps.org.nz/>

Re: Risks of hierarchical map displays (Wallich, [RISKS-25.74](#))

Gene Wirchenko <genew@ocis.net>

Wed, 22 Jul 2009 18:14:40 -0700

Paul Wallich wrote "I wonder whether such hierarchical displays contribute to some of the GPS-aided navigation debacles that sometimes grace this

publication -- a driver may have some idea that they're going the wrong way, but their display doesn't offer enough information to plan a new route easily, and the psychological pressure to keep moving forward can increase as conditions get worse."

I have similar problems with Google Maps. I frequently look up locations mentioned in articles that I read. Sometimes, even after zooming out as far as I can, I still do not know where the location that I am looking at is.

In another case, the urban, residential location indicated was a bit off from the actual location. Normally, this would not be of much consequence, but in this case, between the two locations was a deep gully.

✂ Industrial object-oriented language made void-safe

"Bertrand Meyer" <Bertrand.Meyer@inf.ethz.ch>
Sun, 26 Jul 2009 23:57:43 +0200

Re: Tony Hoare: "Null References: The Billion Dollar Mistake"

In January-February there was a discussion on comp.risks on the risks of null references, following the publication of a talk abstract by Tony Hoare (<http://qconlondon.com/london-2009/presentation/Null+References:+The+Billion+Dollar+Mistake>).

For the past five years we have been working at making Eiffel completely void-safe ("void" being the same as "null"). Part of the significance of this work is that we are not dealing with an experimental design but with an existing industrial language and millions of lines of code that cannot just be discarded. The mechanism was included in the ECMA/ISO standard for Eiffel, but a full implementation required upgrading the libraries, providing a migration path for existing code, and refining the mechanism. With the release of EiffelStudio 6.4 in June, the language is entirely void-safe. Our recent paper "Avoid a Void: The eradication of null dereferencing" describes the challenges of void safety, the design of the Eiffel mechanism, and the difficulties encountered in making it practical. It is available at <http://se.ethz.ch/~meyer/publications/hoare/void-safety.pdf>.

Bertrand Meyer, Eiffel Software <http://www.eiffel.com>
ETH Zurich <http://se.ethz.ch/~meyer>

✂ Ari Juels, Tetraktys, a 'cryptographic thriller'

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 29 Jul 2009 13:11:36 PDT

Ari Juels, Tetraktys, Emerald Bay Books, 2009, 351 pages, ISBN 978-0982283707
Reviewed by Ben Rothke

Review from <http://books.slashdot.org/story/09/07/29/1313201/Tetraktys>

"Imagine for a moment what his novels would read like if Dan Brown got his facts correct. The challenge Brown and similar authors face is to write a novel that is both compelling and faithful to the facts. In Tetraktys, author Ari Juels is able to weave an interesting and readable story, and stay faithful to the facts. While Brown seemingly lacks the scientific and academic background needed to write such fiction, Juels has a Ph.D. in computer science from Berkeley and is currently the Chief Scientist and director at RSA Laboratories, the research division of RSA Security."

The book, which might be the world's first cryptographic thriller, tells the story of Ambrose Jerusalem, a gifted computer security expert, still haunted by his father's death, a few months shy of his doctorate, who has a beautiful and loving girlfriend, and a bright future ahead of him. This is until the government gets involved and Jerusalem's plans are put on hold when the NSA asks him to join them to track down a strange and disturbing series of computer breaches.

Tetraktys, like similar thrillers, has its standard set of characters; from corrupt State Department and World Bank officials, a dashing protagonist with a long-suffering girlfriend, to mysterious and obscure terrorist groups. This terrorist group in the book is comprised of followers of Pythagoras.

As to the title, a tetraktys is a triangular figure of ten points arranged in four rows, with one, two, three, and four points in each row. It is a mystical symbol and was most important to the followers of Pythagoras. While mainly known as the creator of the Pythagorean theorem, Pythagoras of Samos was an influential Greek mathematician and founder of the religious movement of Pythagoreanism. Those wanting more information can watch a video http://www.tetraktysnovel.com/?page_id=83 about the symbol.

As to the storyline, the NSA is trying to recruit Ambrose as they feel that the terrorists, who form a secret cult of followers of Pythagoras have broken the RSA public-key algorithm. Breaking RSA is something that is not expected for many decades, but if a revolution in factoring numbers were to occur sooner, RSA's demise could happen that much quicker. And if RSA was indeed broken by the antagonists, it would undermine the security of nearly every government and financial institution worldwide and create utter anarchy.

A good part of the book centers on the cult of Pythagoras. Its followers believe that truth and reality can only be understood via their system of numbers. The NSA needs Jerusalem's assistance as he is one of the few people who have the mathematical, classical and philosophical background to help them. It is he who ultimately connects the dots that the Pythagoreans have left, which leads to the book's dramatic conclusion.

The book is a most enjoyable read and one is hard pressed to put it down once they start reading it. The reader gets a good understanding of who Pythagoras was and his worldview via Juels weaving of Pythagorean

philosophy into the storyline.

While the book is not autobiographical, there are many similarities between Ambrose Jerusalem and Ari Juels. From identical initials, to their lives in events in Berkeley and Cambridge, to RSA and more.

For a first book of fiction, Tetraktys is a great read. As a novelist, Juels style approaches that of Umberto Eco, in that he weaves numerous areas of thought into an integrated story. Like Eco's works, Tetraktys has an arcane historical figure as part of it storyline, and an intricate plot that takes the reader on many, and some unexpected, turns. While not as complex and difficult to read as Eco, Tetraktys is a remarkable work of fiction for someone with a doctorate in computer science, not literature.

The book though does have some gaps, but that could be expected for a first novel. The reader is never sure what the Pythagoreans are really after or why they have resurfaced, and one of the characters is killed, for reasons that are not apparent. Readers who want more information can visit the Tetraktys web site <<http://www.tetraktysnovel.com/>>.

As to the book's protagonist, Ambrose Jerusalem is to Juels what Jack Ryan is to Tom Clancy, meaning that his adventures are just beginning, and that is a good thing.

For those interested in a cryptographic thriller, Tetraktys is an enjoyable read. The book interlaces Greek philosophy, mathematics, and modern crime into a cogent theme that is a compelling read. And if the exploits of Ambrose Jerusalem continue, we may have found the successor to Umberto Eco.

Ben Rothke is the author of Computer Security: 20 Things Every Employee Should Know

<<http://www.amazon.com/dp/0072262826?tag=benrothkswebp-20&camp=14573&creative=327641&linkCode=as1&creativeASIN=0072262826&adid=1J568GC6NDN92JTGVP3&>>.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 76

Saturday 15 August 2009

Contents

- [Amusement rides without Fail-safe States](#)
[Debora Weber-Wulff](#)
- [Taipei rapid transit line closed until further notice](#)
[jidanni](#)
- [Twitter disruption](#)
[Jenna Wortham via PGN](#)
- [UK national ID card cloned in 12 minutes](#)
[PGN](#)
- [Social security to pay \\$500 million to victims of database error](#)
[Rob McCool](#)
- [Computer Error Caused Rent Troubles for Public Housing Tenants](#)
[Manny Fernandez via Monty Solomon](#)
- [Kentucky election fraud indictments](#)
[PGN](#)
- [Sequoia e-voting machine manipulated without insider info](#)
[Peter Houppermans](#)
- [Boy Dies After Mom Says GPS Left Them Stranded in Death Valley](#)
[Richard Grady](#)
- [China backs off on censorship software ...](#)
[Lauren Weinstein](#)
- [Revealingerrors.com](#)
[Robert P. Schaefer](#)
- [Apple keyboard firmware hack demonstrated](#)
[Monty Solomon](#)
- [Re: Software never fails ...](#)
[Martyn Thomas](#)
[George Jansen](#)
[Andrew Brydon](#)
[Paul Edwards](#)
[Rob Seaman](#)
[Devin Moore](#)
[Nick Keighley](#)
[Martin Cohen](#)
- [Re: Ari Juels, Tetraktys, a `cryptographic thriller'](#)
[Dag-Erling Smørgrav](#)

• [Info on RISKS \(comp.risks\)](#)

✂ Amusement rides without Fail-safe States

Debora Weber-Wulff <weberwu@htw-berlin.de>
Sun, 09 Aug 2009 23:14:51 +0200

Spiegel-Online reports that not one, but two amusement park rides in Europe failed in August 2009 - in a non-safe state.

In Berlin, a car in the ride "Stargate" at the German- American Fair that just used a rail to hold people in was stuck at the top with the 14 passengers on their heads. It took 20 minutes to get the car down by hand. The passengers could not be retrieved by firetruck ladder, as opening the rail would cause everyone to fall down. Some were treated for shock, one woman apparently thought it was part of the ride. The same fair had an 11-year-old child die a week ago on a children's roller-coaster ride, as reported by the *Abendblatt*.

In Moscow, a Ferris wheel at the Allunions fairgrounds stopped with about 50 people on board and could not be coaxed to move. Here the fire trucks could use ladders, as people were sitting right-side up. There had been repeated technical problems with the wheel.

(Berlin, Stargate) <http://www.spiegel.de/panorama/0,1518,641351,00.html>

(Berlin, Roller Coaster)

<http://www.abendblatt.de/vermischtes/article1120791/Elfjaehriger-stirbt-in-Kinderachterbahn.html>

(Moscow, Ferris wheel)

<http://www.spiegel.de/panorama/0,1518,641379,00.html>

Prof. Dr. Debora Weber-Wulff, HTW Berlin, FB 4, Treskowallee 8, 10313 Berlin
+49-30-5019-2320 <http://www.f4.htw-berlin.de/people/weberwu/>

✂ Taipei rapid transit line closed until further notice

<jidanni@jidanni.org>
Sat, 15 Aug 2009 02:56:50 +0800

Taipei, Aug 6. (CNA) The Taipei Mass Rapid Transit (MRT) Neihu line was closed Thursday noon until further notice due to problems with the computer system. http://www.etaiwannews.com/etn/news_content.php?id=1023961
OK, they did fix it, but things have been on and off, up and down,
<http://www.taipeitimes.com/News/taiwan/archives/2009/08/15/2003451137>

✂ Twitter

"Peter G. Neumann" <neumann@csl.sri.com>
Sat, 8 Aug 2009 12:22:59 PDT

Many of Twitter's 45 million customers were disrupted for several hours by a denial-of-service attack on 6 Aug 2009. This resulted from a spam flood relating to the Russian-Georgian dispute over Abkhazia. The messages contained links to Twitter, Facebook, YouTube, and Google (among others). However, Twitter users seem to have been affected the most. Source: Jenna Wortham, *{\it The New York Times,}* 7 Aug 2009; PGN-ed

UK national ID card cloned in 12 minutes

*"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 11 Aug 2009 6:10:38 PDT*

The prospective national ID card was broken and cloned in 12 minutes. The **Daily Mail** hired computer expert Adam Laurie to test the security that protects the information embedded in the chip on the card. Using a Nokia mobile phone and a laptop computer, Laurie was able to copy the data on a card that is being issued to foreign nationals in minutes. He then created a cloned card, and with help from another technology expert, changed all the data on the new card. This included the physical details of the bearer, name, fingerprints and other information. He then rewrote data on the card, reversing the bearer's status from "not entitled to benefits" to "entitled to benefits". He then added fresh content that would be visible to any police officer or security official who scanned the card, saying, "I am a terrorist - shoot on sight."

According to the paper, Home Office officials said the foreign nationals card uses the same technology as the UK citizens card that will be issued beginning in 2012.

<http://www.computerweekly.com/Articles/ArticlePage.aspx?ArticleID=237215>
<<http://www.computerweekly.com/Articles/2009/07/30/237113/picture-uk-id-card-unveiled.htm>>
<<http://www.dailymail.co.uk/news/article-1204641/New-ID-cards-supposed-unforgeable--took-expert-12-minutes-clone-programme-false-data.html#>>

For more information on the National ID Card scheme:

<<http://www.computerweekly.com/Articles://www.computerweekly.com/blogs/the-data-trust-blog/2009/07/id-cards-communications-genius.html>>
<<http://www.computerweekly.com/Home/tags/id-card.htm>>

Social security to pay \$500 million to victims of database error

*Rob McCool <robm@robm.com>
Thu, 13 Aug 2009 22:27:19 -0700 (PDT)*

The Social Security Administration has agreed to pay more than \$500 million in back benefits to more than 80,000 recipients whose benefits re unfairly denied after they were flagged by a federal computer program designed to

catch serious criminals, officials said Tuesday. ... At issue was a 1996 law, which contained language later nicknamed the "fleeing felon" provision, that said fugitives were ineligible to receive federal benefits. As part of its enforcement, the administration began searching computer databases to weed out people who were collecting benefits and had outstanding warrants. ... The lead plaintiff in the class-action suit, Rosa Martinez, 52, of Redwood City, Calif., was cut off from her \$870 monthly disability benefit check in January 2008 because the system had flagged an outstanding drug warrant in 1980 for a Rosa Martinez from Miami. An investigation showed that the warrant was for a different Rosa Martinez. Martinez tried for months to convince officials that she was innocent, but failed.

<http://www.washingtonpost.com/wp-dyn/content/article/2009/08/11/AR2009081103282.html>

✶ Computer Error Caused Rent Troubles for Public Housing Tenants

Monty Solomon <monty@roscom.com>

Sat, 8 Aug 2009 17:30:28 -0400

(Manny Fernandez)

The city's public housing agency overcharged hundreds of welfare families because of a rent calculation error and took many of them to court, threatening them with eviction for failing to pay the higher amount. The computer problem at the agency, the New York City Housing Authority, is in the process of being corrected, and none of the tenants were evicted, officials said. But the error, which began last September and continued until May, had serious legal, financial and personal consequences for many low-income families.

Residents affected by the miscalculations were ordered to appear in Housing Court for nonpayment of the extra rent, tried in vain to convince building managers that there had been a mistake and lived in constant fear of losing their homes because they could not or would not pay the extra money - often as little as \$50 to \$200 a month - that the agency claimed it was owed. The problem affected only households whose sole income is public assistance.

[Source: Manny Fernandez, *The New York Times*, 6 Aug 2009; PGN-ed]

<http://www.nytimes.com/2009/08/06/nyregion/06rent.html>

✶ Kentucky election fraud indictments

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

Mon, 10 Aug 2009 8:06:39 PDT

In the November 2009 election in Kentucky, there was a serious discrepancy between how ES&S's iVotronic voting machines worked and how some voters were instructed. Some voters were apparently falsely told that touching 'Vote' completed the voting process. However, that only displayed the review screen, whereas subsequently touching 'Cast Ballot' was required. Conspiratorial election judges were then able to modify the ballot and cast it. In addition to the fraud, it is clear that the 'vote' screen should

have instead been labeled something such as `review'. Five insiders were indicted -- including conspiracy to commit vote fraud, extortion, and tampering with grand jury witnesses in a subsequent attempt at a cover-up. [I've been meaning to get this item into the RISKS archives for a long time, and finally got around to it. PGN]

Sequoia e-voting machine manipulated without insider info

*Peter Houppermans <peter@houppermans.com>
Wed, 12 Aug 2009 10:22:38 +0200*

So much for Sequoia's security through obscurity - researchers bought some machines legally at an auction, and without access to Sequoia's information (which is heavily and heavy handedly protected) they managed to manipulate the machines regardless..

Source:

[http://www.theregister.co.uk/2009/08/12/sequoia_evoting_machine_felled/:](http://www.theregister.co.uk/2009/08/12/sequoia_evoting_machine_felled/)

Computer scientists have figured out to how trick a widely used electronic voting machine into altering tallies with a technique that bypasses measures that are supposed to prevent unauthorized code from running on the device. [...] The computer scientists were able to evade this safety mechanism using return-oriented programming. Rather than designing the malicious code from scratch, the technique reassembles programming expressions already found in the targeted software in a way that gives the researchers the ability to take complete control over the machine. It's tantamount to kidnapers who write a ransom note using letters cut from the headline of a newspaper.

[No surprise to the red-team folks involved in last summer' California's Top-To-Bottom Review (<http://www.sos.ca.gov/elections/elections>). PGN]

Boy Dies After Mom Says GPS Left Them Stranded in Death Valley

*Richard Grady <richard@richbonnie.com>
Sun, 09 Aug 2009 20:36:29 -0700*

Alicia Sanchez, 28, was found severely dehydrated and remained hospitalized in Las Vegas a day after being found with her dog, her dead son and a Jeep Cherokee buried up to its axles in sand. She told rescuers in California's San Bernardino County that her son Carlos died Wednesday, days after she fixed a flat tire and continued into Death Valley, relying on directions from a GPS device in the vehicle.

<http://www.foxnews.com/story/0,2933,538323,00.html>

China backs off on censorship software,

Lauren Weinstein <lauren@vortex.com>

Thu, 13 Aug 2009 08:50:04 -0700

but may still require real names on comments

Greetings. *The New York Times* is reporting that China has now definitively backed off from requiring the installation of filtering/censorship software on all PCs sold in China. Internet cafe and other public computers would still be required to use the software, and two major manufacturers are already including it on PCs sold in China.

<http://www.nytimes.com/2009/08/14/world/asia/14censor.html>

China blames the controversy over the software on "confusion" related to badly written regulations.

On a related front, the same article reports that China is considering a requirement that all posters to Internet chat rooms, bulletin board systems, etc. use their real names (and, I'd be willing to bet, eventually include other identifying information as well) on all postings. The stifling effects of such a requirement on speech are obvious, but I should note that I regularly hear from people in the U.S. promoting a similar misguided ("Internet Driver's License") concept.

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org/lauren>
<http://www.pfir.org> Network Neutrality Squad: <http://www.nnsquad.org> [and more]

✶Revealingerrors.com

"Schaefer, Robert P \ (US SSA)" <robert.p.schaefer@baesystems.com>

Thu, 6 Aug 2009 14:52:27 -0400

Another website aggregating faults and errors, some of which are due to computers:

<http://revealingerrors.com/>

[Weblog maintained by Benjamin Mako Hill. Lots of RISKS-worthy stuff, e.g., a recent item on Akamai and SSL. PGN]

✶Apple keyboard firmware hack demonstrated

Monty Solomon <monty@roscom.com>

Mon, 3 Aug 2009 08:17:54 -0400

Charlie Demerjian at Defcon 17, 31 Jul 2009: Apple needs to patch it ASAP

Apple keyboards are vulnerable to a hack that puts keyloggers and malware directly into the keyboard. This could be a serious problem, and now that

the presentation and code is out there, the bad guys will surely be exploiting it.

The vulnerability was discovered by K. Chen, and he gave a talk on it at Blackhat this year. The concept is simple, a modern Apple keyboard has about 8K of flash memory, and 256 bytes of working ram. For the intelligent, this is more than enough space to have a field day.

K. Chen demonstrated the hack to S|A at Defcon today and it worked quite well. You start out by running GDB, and set a breakpoint in Apple's HIDFirmwareUpdaterTool. This tool is meant to update the firmware in human interface devices, hence the name. The tool is run, a breakpoint set, and then you simply cut and paste the new code into the firmware image in memory. That's it.

Nothing is encrypted, decrypted, and the process is simple. You then resume HIDFirmwareUpdaterTool, and in a few seconds, your keyboard is compromised. Formatting the OS won't do you any good, the code is in keyboard flash. There are no batteries to pull, no nothing, the keyboard is simply compromised. ...

<http://www.semiaccurate.com/2009/07/31/apple-keyboard-firmware-hack-demonstrated/>

Reversing and Exploiting an Apple Firmware Update

<http://www.blackhat.com/html/bh-usa-09/bh-usa-09-archives.html#Chen>

Re: Software never fails ... (Robinson, [RISKS-25.75](#))

*Martyn Thomas <martyn@thomas-associates.co.uk>
Thu, 06 Aug 2009 21:30:59 +0100*

This rambling piece is nonsense and so are the articles it refers to. If software engineering is not engineering because the specification contains human requirements that cannot be completely formalised, then nor are civil engineering, electrical engineering, or any other form of engineering.

The excuses that people come up with to justify their unwillingness to learn and use some simple mathematics should be collected in a book and studied by psychiatrists. Meanwhile, as an engineer, I shall continue to believe that if my square-root function crashes, loops forever, or returns a value that is not the square root of its argument, then it has failed. And that its failure is independent of my personal opinion or anyone else's. And that the straightforward application of some engineering methods can deliver a square root function that does not fail, together with a proof.

And before anyone says that this is a toy example: (a) it only takes one counterexample to disprove an absolute claim, and (b) the same methods are being used routinely, successfully and cost-effectively on many industrial and commercial projects.

Re: Software never fails ... (Robinson, [RISKS-25.75](#))

"George Jansen" <GJANSEN@aficio.org>

Thu, 06 Aug 2009 15:18:34 -0400

Perhaps the subject line would more justly be "Software never fails more or less than it did on release." I am struck in particular by two things:

1. "Any software package ... only requires maintenance or change because in someone's subjective opinion it needs a change." I think that the expression "someone's subjective opinion" is not usefully defined. In the preceding paragraph it covers changes in the tax law--the subjective opinion of the legislators that taxes should go up or down, and of businesses that they had better comply--and of network providers that they must provide new features. Subjective opinions held by the IRS and by enough consumers tend to become compelling enough to affect the continued existence of a business, don't they?

This also does not cover such cases as they year 2038 issue. I don't think it useful to say that it is merely my subjective opinion that we can't stick with 32 bits and reset the clock to 1970.

2. "A bridge needs replacement when it collapses or when it is beyond its useful life; a building needs replacement under the same circumstances." Yet "useful life", unless referring to safety, reflects "subjective opinion". Every day (unless in depressed markets), buildings are demolished that could have stood for many years yet; a developer has the opinion he'd make more money building a new one. Does the engineer's employment by a developer make him less an engineer?

Software never fails ... (Robinson, [RISKS-25.75](#))

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

Fri, 7 Aug 2009 06:40:54 +0100

> But the claim by someone that a software package needs change, updating or replacement is, and always will be, a subjective opinion based on nothing more than "because I say so."

One difference between engineering software and something physical such as a bridge is the general population's experience of the domain. The average person on the street can readily conceive the failure modes of bridges, their causes and outcomes. The effects of software on the domain world, be it returning the wrong tax deductions from payroll after a governmental rule change or simply freezing/crashing are less easily perceived and much less understood by a non-programmer. However, that does not inhibit someone other than the originator from making an informed and educated decision, based on engineering principles, that the product requires updating or replacing.

✂ Re: Software never fails ... (Robinson, [RISKS-25.75](#))

"Paul Edwards" <paule@cathicolla.com>

Fri, 7 Aug 2009 22:01:56 +1000 (EST)

Paul Robinson asserts that "the claim by someone that a software package needs change, updating or replacement is, and always will be, a subjective opinion based on nothing more than "because I say so." " This assertion does not stand up at a practical level, nor at a philosophical level. It fails to recognize that software exists to provide support for specific real-world activities; software does not exist for its own sake (with the exception of games and entertainment software).

Well designed and implemented software will reflect the constraints and/or requirements of the real-life application it is supporting, and if those constraints and/or requirements change, the software (objectively) requires updating, otherwise it will fail to achieve its purpose.

Suppose it's 2001, and you have some financial reporting software. As a result of Sarbanes-Oxley passing in 2002, this software will need updating in order to accurately support its real-world activity (financial reporting). Of course, the "do nothing" option here would result in additional expense for reporting companies through increased headcount, and an ongoing reduction in efficiency of the financial reporting activity.

Further, whilst I can't speak for the two men involved in drafting SOX, I'm confident their motivation had precious little to do with software, and more to do with strengthening financial reporting activities to avoid another Enron.

The bridge analogy in the original article also fails to stand up to scrutiny. A bridge near where I used to live was a good solid bridge, there were no issues with its structural integrity, and it was nowhere near the end of its life. However, due to unanticipated demographic movements, the bridge became a bottleneck. It was updated to double the number of traffic lanes it could handle, to reflect the changing requirements that the bridge supported (pun intended).

Note that the above holds when instantiating "system" for "software" as well.

Paul Edwards, IT Service Management Consultant, Melbourne, Australia

✂ Re: Software never fails ... (Robinson, [RISKS-25.75](#))

Rob Seaman <seaman@noaa.edu>

Tue, 11 Aug 2009 10:33:59 -0700

Paul Robinson makes an interesting observation - that success in software is subjective - but then overgeneralizes to suggest that

software engineering can never be a rigorous discipline. Bridges must be maintained because the external world changes. This is also true of software. Traffic load increases, the balance of expense of necessary resources (toll plazas, police, paramedics) shifts. Yes, tax laws change and cellular networks evolve to vex software engineers, but this is precisely the same with other types of engineering.

More to the point, almost every modern system includes software dependencies. Systems engineering would be impossible without taking software into account. And programmers - whether or not they are using formal system engineering methods - should be held as responsible to the intrinsic requirements of each project as any other engineer. Projects are defined by their requirements. Requirements are discovered from use cases. Use cases evolve more rapidly for certain kinds of projects - those are simply the projects for which software solutions are most appropriate. Requirement management techniques exist precisely to control the subjective aspects of a project. These techniques are even **more** appropriate to software than to other engineering disciplines.

It is also naive to suggest that software never rots or rusts. The existence of software is contingent on the vessel containing it. At great ongoing expense one can preserve digital copies indefinitely, but entropy will always win (cf. Claude Shannon). To suggest, therefore, that software never fails is naive. One could similarly assert that bridges never fail, by redefining their collapse as an exercise in performance art. Alternately, even the collapse of natural bridges (<http://earthobservatory.nasa.gov/NaturalHazards/view.php?id=37806>) may reflect our subjective, but not therefore less real failures (human induced climate change).

It is true that software failures tend to reflect failures during design, but this is true of bridges as well. The total system involving both must surely include life-cycle maintenance and the periodic review of external requirements, such as exponentially growing usage patterns exceeding initial assumptions. All failures reveal shortcomings of the human imagination.

The Risk? Software is only as perfect as its creators.

Rob Seaman <seaman@hanksville.org>

✉ Re: Software never fails ... (Robinson, [RISKS-25.75](#))

Devin Moore <devin.moore@gmail.com>

Thu, 13 Aug 2009 08:20:46 -0400

I would like to comment on the [RISKS-25.75](#) editorial advancing the idea that software engineering failures or changes are always subjective. I agree that for software engineering projects that are proven to have no existing

bugs, any change from that point forward may be a subjective change because the product is proven to meet its functional requirements. However, software can contain bugs and will fail just like any other engineering project. For example, if I build a bridge and it collapses, that failure was because of a flaw rather than someone's opinion about whether the bridge is failing or not.

Furthermore, I believe in many circumstances software engineering is rigorous and formally designed, as in safety-critical systems (1)(2). In these cases, opinion is not enough to advance that a system is capable of serving its desired functionality without failure.

Devin Moore

[I am currently a Ph.D student in Information Systems Science at Nova Southeastern University]

(1) Ponsard, C; Massonet, P; & Dallons, G. (2008, October). From Rigorous Requirements Engineering to Formal System Design of Safety-Critical Systems. *ERCIM News **Special: Safety-Critical Software*.* (75) * Retrieved August 9, 2009, from <http://deploy-eprints.ecs.soton.ac.uk/40/1/EN75-CETIC.pdf>

(2) Merino, P.; & Shoitsch, E. (2009). Introduction to the Special Theme: Safety-Critical Software. Retrieved August 9, 2009, from <http://ercim-news.ercim.org/content/view/474/699/>

<http://www.devinmoore.com> | <http://novastudentlounge.proboards.com>

✂ Software never fails ... (Robinson, [RISKS-25.75](#))

Nick Keighley <nick_keighley_nospam@hotmail.com>

Fri, 14 Aug 2009 14:14:16 +0100

> An engineer can determine by experience and judgment that the structure is at its lifespan limit or can point to signs of physical rust, deterioration, or structure failure indicators that prove their opinion.

This just isn't true. Look at an old street in a European country. Every building has had substantial changes made to it over time. Building have changed use. Medieval pubs stand on Roman bath houses and office blocks on old monasteries. Buildings get removed when they can no longer be adapted for their new purpose. This is a better model of software maintenance.

Software isn't as different from other designed objects as Mr Robinson thinks.

✂ Re: Software never fails ... (Robinson, [RISKS-25.75](#))

Martin Cohen <mjc_q@yahoo.com>

Thu, 6 Aug 2009 14:50:14 -0700 (PDT)

If software requirements change, and the software no longer meets the requirements, then it has objectively failed - no opinion needed.

This was definitely one of the weirder risks posts.

Re: Ari Juels, Tetraktys, a `cryptographic thriller' ([RISKS-25.75](#))

Dag-Erling Smørgrav <des@des.no>

Thu, 06 Aug 2009 20:40:35 +0200

> The book, which might be the world's first cryptographic thriller [...]

Not by 10 years:

<http://www.amazon.com/Cryptonomicon-Neal-Stephenson/dp/0380973464/>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 77

Tuesday 1 September 2009

Contents

- [UK Chinook helicopters grounded for *years* due to software problems](#)
[Danny Burstein](#)
- [DNA Evidence Can Be Fabricated, Scientists Show](#)
[Monty Solomon](#)
- [Computer-driven class schedules](#)
[David Lesher](#)
- [Computer to blame for man's fiery death](#)
[Gene Wirchenko](#)
- [RFI isn't all harmless: turns on oven](#)
[David Lesher](#)
- [Pepper-spray ATMs](#)
[Jeremy Epstein](#)
- [The VA erroneously informs over a thousand vets of fatal diagnosis](#)
[Rob McCool](#)
- [ROTC Computer Files Found in the Public Domain](#)
[Monty Solomon](#)
- [Hackers break into police computer as sting backfires](#)
[Andrew Pam](#)
- [3 Indicted in Theft of 130 Million Card Numbers](#)
[Monty Solomon](#)
- [AT&T unable to protect Kevin Mitnick's account](#)
[David Magda](#)
- [Swiss Data Protection orders Google Streetview offline](#)
[Peter Houppermans](#)
- [Canadian model gets Google to unmask nasty blogger](#)
[Simon Avery via PGN](#)
- [Cannot print on Tuesdays!](#)
[Phil Colbourn](#)
- [GSM's A5/1 cipher being brute forced](#)
[David Magda](#)
- [The Pirate Bay Returns With Guns Blazing](#)
[jidanni](#)
- [Bad questions for account retrieval](#)
[Jeremy Epstein](#)
- [Take only pictures *we* like](#)

[David Lesher](#)

• [Re: Kentucky election fraud indictments](#)

[Drew Dean](#)

• [Stephen Albin. The Art of Software Architecture](#)

[David Schneider](#)

• [Info on RISKS \(comp.risks\)](#)

✂ UK Chinook helicopters grounded for *years* due to software problems

danny burstein <dannyb@panix.com>

Tue, 25 Aug 2009 12:45:56 -0400 (EDT)

[UK news sources: UK bought Boeing helicopters, figured they'd save money by designing their own software...]

When the [Boeing] Chinooks were delivered in 2001 at a cost of 259 million [British pounds] - the [software] codes would have pushed the price to over 300 million - they could not be certified because of the lack of software.

They could be flown but pilots were barred from taking the controls in cloudy conditions or at low altitude. While all the discussions were going on the Chinooks had been idle in their hangars. Between 2001 and 2007 the helicopters had to be inspected once a week and moved out of the hangars every two years for more detailed checks, at a total cost of 560,000 [pounds].

Rest, with links to related stories and lots of interesting reader comments):

<http://www.timesonline.co.uk/tol/news/politics/article6808604.ece>

✂ DNA Evidence Can Be Fabricated, Scientists Show

Monty Solomon <monty@roscom.com>

Wed, 19 Aug 2009 00:10:08 -0400

Scientists in Israel have demonstrated that it is possible to fabricate DNA evidence, undermining the credibility of what has been considered the gold standard of proof in criminal cases. The scientists fabricated blood and saliva samples containing DNA from a person other than the donor of the blood and saliva. They also showed that if they had access to a DNA profile in a database, they could construct a sample of DNA to match that profile without obtaining any tissue from that person. "You can just engineer a crime scene," said Dan Frumkin, lead author of the paper, which has been published online by the journal Forensic Science International: Genetics. "Any biology undergraduate could perform this." [Source: Andrew Pollack, *The New York Times*, 18 Aug 2009; PGN-ed]

<http://www.nytimes.com/2009/08/18/science/18dna.html>

✂ Computer-driven class schedules

"David Leshner" <wb8foz@panix.com>
Thu, 27 Aug 2009 18:41:32 -0400 (EDT)

[would Ferris Bueller get the week off?]

Prince Georges [MD] Public Schools \$4.1 million SchoolMax student scheduling system has left thousands of its high school students with no schedules, and thus no classes.

Those students have spent the first few days of school sitting in the gym, cafeteria, or other holding areas.

While the number of still-unscheduled students has fallen from the first day's 8000 [of 41,000 total] to roughly 2000, that does not include those in the wrong classes; including one where administrators have, in effect, randomly assigned students to any available class.

The saga sounds oh so familiar to RISK regulars; a big changeover, no manual fallback scheme, approaching deadlines, with complaints about inadequate training, and big increases in the time needed [from ~10 minutes to 45 per student!] for core tasks.

But SchoolMax is not a new creation, nor are these issues. It was deployed for 300,000 in the Los Angeles Unified School District, and Richmond County, Georgia had similar issues in 2004.

So who's not learning here: SchoolMax, the school systems clients, or their students?

Class Chaos Persists at Prince George's High Schools

<http://www.washingtonpost.com/wp-dyn/content/article/2009/08/27/AR2009082701518_pf.html>

Computer to blame for man's fiery death

Gene Wirchenko <genew@ocis.net>
Thu, 27 Aug 2009 19:03:19 -0700

A Laptop computer that burst into flames after being left on a couch is to blame for a Vancouver man's death, prompting a public warning from the British Columbia Coroners Service not to leave the devices on soft furniture. [Source: *The Daily News*, Kamloops, British Columbia, Canada, 27 Aug 2009, A4 PGN-ed]:

RFI isn't all harmless: turns on oven

"David Leshner" <wb8foz@panix.com>
Tue, 18 Aug 2009 23:28:08 -0400 (EDT)

RFI is usually an annoyance but seldom harmful. Here's an exception.

A UPI article of 18 Aug reports:

Andrei Melnikov said his Maytag Magic Chef stove beeps and turn its broiler onto the highest setting if his phone, which he has had for about three years, receives an incoming call while within two feet of the appliance, WABC-TV, New York, reported Tuesday. ... He said the stove is currently unplugged and Maytag has agreed to send a repair crew to get to the bottom of the problem.

GSM cell phones are noted for causing audible RFI in other receivers nearby. Looks like some Maytag ranges are equally vulnerable.

[Also reported by David Hollman and by Kevin Connolly, who added, ``Here in Ireland the electrical regulations require a wall switch to isolate the mains supply to a cooker when not in use. It is good advice to use it." PGN]

Pepper-spray ATMs

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Wed, 26 Aug 2009 10:44:01 -0400

Haven't seen this in RISKS - I first heard about it on NPR's Wait Wait (waitwait.npr.org) as part of their truth-is-weirder-than-fiction contest, so was initially skeptical, but it appears to be true. Seems that some South African ATMs are equipped with pepper spray to (under software control) spray anyone who tampers with the machines. According to the (UK) Guardian, "the technology uses cameras to detect people tampering with the card slots. Another machine then ejects pepper spray to stun the culprit while police response teams race to the scene." The Guardian report says that three servicing technicians were hit while (legitimately) repairing the machines.

It doesn't take a rocket scientist to figure out that when there's software involved, there's opportunities for it to go wrong. And as someone on a blog pointed out, this technology can also be used by the bad guys - get the ATM to trigger on a legitimate customer, and while the customer is incapacitated, take their ATM card and whatever other valuables they have.

<http://www.guardian.co.uk/world/2009/jul/12/south-africa-cash-machine-pepper-spray>

(and many others, which all seem to use pretty much the same text)

The VA erroneously informs over a thousand vets of fatal diagnosis

Rob McCool <robm@robm.com>

Thu, 27 Aug 2009 14:26:30 -0700 (PDT)

<http://fcw.com/articles/2009/08/26/va-erroneously-informs-vets-of-fatal-disease-diagnosis.aspx>

Through a data maintenance error, the Veteran's Affairs department recently sent out automated letters to as many as 1200 veterans that they had the fatal neurological disorder known as Lou Gehrig's disease.

A diagnostic code was chosen many years ago for "unknown neurological disorder". That itself is an example of the often problematic "miscellaneous" hole in most categorization systems. Some things simply defy categorization. Later, the diagnostic code was expanded to include Lou Gehrig's disease.

Still later, the VA decided to make Lou Gehrig's disease a service-connected disability. So they sent the automated letters to inform affected vets that benefits were available. Up to 1200 people were erroneously informed of this and the office is getting more than 50 calls a day from veterans in an understandable panic.

✂ ROTC Computer Files Found in the Public Domain

Monty Solomon <monty@roscom.com>

Sat, 22 Aug 2009 02:04:00 -0400

Art Jahnke, Technology error exposes personal information, BU News, 20 Aug 2009

A file transfer program erroneously installed on a server in an Army Reserve Officers' Training Corps (ROTC) office at Boston University inadvertently exposed personal information about thousands of people affiliated with the program. University officials say the compromised computer was taken off-line when the breach was identified on July 28; they are working with the U.S. Army Cadet Command to contact every person whose information was placed at risk.

The incident involved information on 6,675 people, say University administrators, 406 of whom are affiliated with BU. Officials believe the rest come from ROTC branches around the country. ...

<http://www.bu.edu/today/campus-life/2009/08/17/rotc-computer-files-found-public-domain>

✂ Hackers break into police computer as sting backfires

Andrew Pam <andrew@sericyb.com.au>

Tue, 18 Aug 2009 14:30:49 +0930

"An Australian Federal Police boast, on the ABC's Four Corners program last night, about officers breaking up an underground hacker forum, has backfired after hackers broke into a federal police computer system.

Security consultants say police appear to have been using the computer

as a honeypot to collect information on members of the forum but the scheme came undone after the officers forgot to set a password."

<http://www.theage.com.au/technology/security/hackers-break-into-police-computer-as-sting-backfires-20090818-eohc.html>

#3 Indicted in Theft of 130 Million Card Numbers

Monty Solomon <monty@roscom.com>

Fri, 28 Aug 2009 23:38:49 -0400

On 24 Aug 2009, Albert Gonzalez was indicted along with two unspecified Russian conspirators. Charges included theft of 130 million credit and debit card numbers from late 2006 to early 2008 from various sources -- Heartland Payment Systems, 7-Eleven, Hannaford Brothers, and others. Some of those numbers were sold online and used in identity frauds. Gonzalez is already waiting trial for previous cases involving T.J. Maxx (in Massachusetts) and the Dave & Buster restaurant chain (in New York).

[Source: Brad Stone, *The New York Times*, 18 Aug 2009; PGN-ed]

<http://www.nytimes.com/2009/08/18/technology/18card.html>

AT&T unable to protect Kevin Mitnick's account

"David Magda" <dmagda@ee.ryerson.ca>

Thu, 20 Aug 2009 11:15:24 -0400 (EDT)

It's a good thing that most people are not as "high profile" as Kevin Mitnick, as otherwise their phone records would be practically public records:

> Over the past month, both HostedHere.net, his longtime webhost, and AT&T,
> his cellular provider since he was released from prison more than nine
> years ago, have told him they no longer want him as a customer. The
> reason: his status as a celebrity hacker makes his accounts too hard to
> defend against the legions of script kiddies who regularly attack them.

http://www.theregister.co.uk/2009/08/19/att_dumps_kevin_mitnick/

Of course the rest of AT&T customers' accounts are probably not better protected and just as vulnerable. If Mr. Mitnick does change providers, I'm curious to know if they'll do any better than AT&T has.

[Also noted by David Leshner. PGN]

Swiss Data Protection orders Google Streetview offline

Peter Houppermans <peter@houppermans.com>

Sat, 22 Aug 2009 15:28:52 +0200

The risk of not living up to your promises when you do mass surveillance: the Swiss newspaper NZZ reports today that the Swiss office for Data Protection (<http://www.edoeb.admin.ch>) has asked Google to immediately shut down the Swiss part of Google Streetview because it does not meet Data Protection standards - the masking of license plates and faces is insufficient. The (German language) article is at <http://preview.tinyurl.com/nwsl65>.

I can attest to that, I had a quick browse of a place I know, and the promised masking of faces was in quite a few cases simply absent..

The Swiss Data Protection office doesn't consider the "you can opt out if you want" approach as acceptable, a point I can only agree with when it comes to privacy. I've read through a Q&A (<http://preview.tinyurl.com/muor75>, no English version available) with Google provided answers, and that contains a few classics:

(a) people would know in advance where the cars would be, "so they could act accordingly" - a fantastic idea to move your obligation to the people you're surveilling ("just go and hide if you don't like it")

(b) you can always have your picture removed - which only requires you to remember where exactly you saw the camera car, several months later.

It appears Google has also offered to remove house images if so required. I think that's a bit much, but from what I've seen so far it would be a good idea if they would at least obscure windows. The resolution of the images is in some cases sufficient to make out what's INSIDE houses close to the street.

But hey, according to Google they should have had their curtains drawn when Google came filming.

English translation available at <http://preview.tinyurl.com/m3vokf>.

✂ Canadian model gets Google to unmask nasty blogger

*"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 20 Aug 2009 15:59:02 PDT*

Legal ruling will force Internet search giant to reveal identify of blogger who posted derogatory comments about Liskula Cohen.
[Source: Simon Avery, *Globe and Mail*, 20 Aug 2009]

✂ Cannot print on Tuesdays!

*phil colbourn <philcolbourn@gmail.com>
Sun, 16 Aug 2009 11:27:21 +1000*

Today I came across an interesting bug mentioned on a blog. The problem was that printing for some people failed occasionally. Later someone noted that his Wife had been complaining that she couldn't print on Tuesdays!

In reading through the bug report people were initially claiming that it must be an OpenOffice bug since all other applications printed fine. Others noted that it comes and goes. One user found a solution: To remove and purge the system of OpenOffice and re-install (any easy task on Ubuntu). He reported on a Thursday that this fixed his printing problem.

Two weeks later he reported (on a Tuesday) that his solution did not work after-all. Nearly 4 months later the Wife of a Ubuntu hacker complained that OpenOffice would not print on Tuesdays. I can imagine the scenario:

Wife: Steve, the printer will not work on Tuesdays.

Steve: That's the printer's day off - Of course it will not print on Tuesdays.

Wife: No, I'm serious! I can not print from OpenOffice on Tuesdays.

Steve: (Unbelieving..) Ok... Show me.

Wife: I can't show you.

Steve: (Rolling eyes..) Why?

Wife: It's Wednesday!

Steve: (Nods. He says slowly...) Right.

The problem seemed to be tracked down to a program called 'file'. This *NIX utility uses patterns to detect file types. eg. if the file starts with '%!' followed by 'PS-Adobe-' then it is a PostScript file. It seems that OpenOffice writes the date to the postscript file. On Tuesdays it takes the form of %%CreationDate: (Tue MMM D hh:mm:...)

An error in the pattern for an Erlang JAM file meant that 'Tue' in the PostScript file was being recognised as an Erlang JAM file and so, presumably, it was not being sent to the printer.

The Erlang JAM file pattern is:

```
4 string Tue Jan 22 14:32:44 MET 1991 Erlang JAM file - version 4.2
```

It should have been

```
4 string Tue\ Jan\ 22\ 14:32:44\ MET\ 1991 Erlang JAM file - version 4.2
```

With the large number of files types that this program attempts to match (over 1600) it is not surprising that errors are made in the patterns, but also the order of matching could mean that false positives are common. In this case, an Erlang JAM file was matched before the PostScript match occurred.

References:

<http://mdzlog.alcor.net/2009/08/15/bohrbugs-openoffice-org-wont-print-on-tuesdays/>

Reported as this bug:

<https://bugs.edge.launchpad.net/ubuntu/+source/cupsys/+bug/255161>

Later made a duplicate to this bug:

<https://bugs.edge.launchpad.net/ubuntu/+source/file/+bug/248619>.

<http://www.blaxlandweather.com/> <http://philatwarrimoo.blogspot.com>

GSM's A5/1 cipher being brute forced

David Magda <dmagda@ee.ryerson.ca>

Tue, 25 Aug 2009 21:41:43 -0400

Looks like the GSM folks may want to think about upgrading to a better algorithm:

- > It will take 80 high-performance computers about three months to do
- > a brute force attack on A5/1 and create a large look-up table that
- > will serve as the code book, said Nohl, who announced the project at
- > the Hacking at Random conference in the Netherlands 10 days ago.
- >
- > Using the code book, anyone could get the encryption key for any GSM
- > call, SMS message, or other communication encrypted with A5/1 and
- > listen to the call or read the data in the clear. [...]
- > Carriers should upgrade the encryption or move voice services to 3G,
- > which has much stronger encryption, [Karsten] Nohl said.

http://news.cnet.com/8301-27080_3-10316812-245.html

Is there any reason why future mobile standards shouldn't just use AES?

Given that most governments can tap phone calls for lawful purposes once the signal hits the tower, what possible use would there be to having a weak cipher for radio transmissions?

The Pirate Bay Returns With Guns Blazing

<jidanni@jidanni.org>

Thu, 27 Aug 2009 01:10:45 +0800

When The Pirate Bay was shut down by the authorities yesterday many believed that this was the end for the Internet's largest BitTorrent tracker.

A mere three hours after it went offline the site reappeared from a different location.

The Pirate Bay team released the following statement, adapted from Churchill's famous "We Shall Fight On the Beaches" speech.

"We have, ourselves, full confidence that if all do their duty, if nothing is neglected, and if the best arrangements are made, as they are being made, we shall prove ourselves once more able to defend our Internets..."

<http://torrentfreak.com/the-pirate-bay-returns-with-guns-blazing-090825/>

Bad questions for account retrieval

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Thu, 20 Aug 2009 19:31:02 -0400

A recent study [1] showed that the "security questions" used for recovering account access tend to be easily guessable, even by strangers, and the answers are almost as frequently forgotten by the account owner. As pointed out in that article, it's important in choosing questions that they have relatively unchanging answers, or else customers will be unable to recall the answer a year or two down the road when they're needed. That's of course why questions like birthplace and mother's maiden name are "good" from the memory perspective, even though they're bad from the security perspective.

So the other day I was helping my son apply for a student credit card at Citibank, and was somewhat amused that the following were the **only** questions allowed (I think you had to have answers to three of them):

- (A) Best friend's last name
- (B) Pet's name
- (C) Favorite teacher's last name
- (D) Last 4 digits of friend/relative phone #
- (E) Other

(A) might be mined from Facebook or a similar page (a large fraction of people will probably list their spouse's name!), if it's not their spouse, for many people this will change over time. (*) [1] notes that "best childhood friend" is frequently forgotten and fairly easily guessed; "best friend" is both easily guessed and subject to change. As noted in [1], (B) is easily guessed (although less likely to change than (A)). (C) is likely to change over time. (D) has the disadvantages of the person changing, as well as choosing which phone number (cell/home/work); also many of the college students who are the target of this application don't know their friends' phone numbers since they're all programmed into cell phone memory. And their implementation of (E) doesn't allow you to put in a hint, but the answer is limited to 10 characters.

The risk? In the move to trying to improve the security of backup questions, even big companies can miss the point....

[1] "It's no secret: Measuring the security and reliability of authentication via 'secret' questions", Stuart Schechter, A.J. Bernheim Brush, and Serge Egelman, 2009 IEEE Symposium on Research in Security and Privacy, <http://research.microsoft.com/apps/pubs/default.aspx?id=79594>

(*) For some people, the spouse's name will also change over time, but that's outside the scope of this note.

✂ Take only pictures *we* like

"David Leshar" <wb8foz@panix.com>
Sun, 23 Aug 2009 15:14:51 -0400 (EDT)

Ever vigilant against terrorism, the LAPD gets specific instructions:

<<http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf>>

A Suspicious Activity Report (SAR) is a report used to document any reported or observed activity, or any criminal act or attempted criminal act, which an officer believes may reveal a nexus to foreign or domestic terrorism. The information reported in a SAR may be the result of observations or investigations by police officers, or may be reported to them by private parties. Incidents which shall be reported on a SAR are as follows: [...]

Takes pictures or video footage (with no apparent aesthetic value, i.e., camera angles, security equipment, security personnel, traffic lights, building entrances, etc.).

There are so many fallacies here I don't know where to start.

a) People taking pictures is a terrorism problem. Well, sure, but so is driving on freeways, and buying BBQ grill fuel, and....

b) But only *some* takers may be terrorists. Jack and Jill Instamatic, suspect; All Kinda Productions, of course not -- terrorists can't be part of our economic base. [Err... What BETTER way to hide an attack then fake up a movie over same, and hire off-duty cops for security?]

c) LAPD's finest's esthetic value judgment is up to the task of differentiating between terrorism and turkeys. Err, I've seen their HQ building; and besides, not even the Hollywood power barons manage that task well - witness this summer's flops such as GI Joe.

d) But NO DOUBT, the database from those SAR's shall be used both to harass/arrest Jack & Jill's associates, and the fact that data came from a computer renders it irreproachable. Garbage In, Garbage Out *still* does no good and much ill.

✂ Re: Kentucky election fraud indictments ([RISKS-25.76](#))

Drew Dean <ddean@csl.sri.com>
Mon, 17 Aug 2009 11:54:48 -0700

On Aug 15, 2009, at 3:26 PM, RISKS List Owner wrote:

> In the November 2009 election in Kentucky, there was a serious discrepancy

AAAAAAAA AAAAA

I must say, electronic voting systems have become quite advanced if they can commit fraud in future elections! :-)

[My goof. The indictment actually covered the 2002, 2004, and 2006 elections. Ray Gardner noted that the elections affected by the ES&S user interface exploit were just 2004 and 2006. The county didn't get those machines until 2003. The 2002 fraud was apparently of another sort. And I am neither prescient nor postscent. PGN]

Stephen Albin. The Art of Software Architecture

*David Schneider <pd@hq.acm.org>
Thu, 20 Aug 2009 13:03:42 -0400*

Stephen Albin
The Art of Software Architecture: Design Methods and Techniques
August 2009 ACM Featured Online Book for Professional Members

The ACM Featured Online Book Program focuses on books in the ACM Collection that are highly used and highly reviewed. A different book will be featured in each newsletter. This issue features a title from our Books24x7 collection.

Stephen Albin. The Art of Software Architecture: Design Methods and Techniques

This book synthesizes and distills information so that the practicing software architect, and especially the beginning software architect, can fill in the gaps in their understanding of software architecture design. This innovative book uncovers all the steps readers should follow in order to build successful software and systems. With the help of numerous examples, Albin clearly shows how to incorporate Java, XML, SOAP, ebXML, and BizTalk when designing true distributed business systems. The book not only teaches how to easily integrate design patterns into software design, but also documents all architectures in UML and presents code in either Java or C++.

Bernard Kuc of Computing Reviews said "Albin presents extensive coverage of the current state of the art in software architecture. Throughout the book, he remains focused on software architecture. He does not give in to the temptation of going deeper into software engineering and design, an area already well covered elsewhere, and hence achieves coverage of a wide breadth of material in relatively few pages."

One Amazon reviewer, who rated the book 5 stars, said the book as "This book uses real world examples and practical advice coupled with academic rigor. It provided tremendously helpful insights into how I can improve the efforts of my team."

Feedback:

We are always looking for feedback and recommendations on our book offerings. If you know of a book you would like ACM to consider offering, please email me at Schneider@hq.acm.org.

David Schneider, Education Manager, Association for Computing Machinery



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 78

Monday 14 September 2009

Contents

- [South Africa's Telkom: For the Birds or Not For the Birds](#)
[Gene Wirchenko](#)
- [OLPC: Sic Transit Gloria Laptopi](#)
[jidanni](#)
- [Smart Cars?](#)
[Gene Wirchenko](#)
- [Boston city employees routinely deleted e-mail](#)
[D.Slack/M.Levenson via Monty Solomon](#)
- [Networks and Nationalization With Respect to Cyberwar](#)
[jidanni on Suresh Ramasubramanian](#)
- [Heavy Data Use Puts a Strain on AT&T Service](#)
[Jenna Wortham via Monty Solomon](#)
- [Snow Leopard: A gigabyte by any other name](#)
[Monty Solomon](#)
- [Humbert Humbert <heart> Fishfingers](#)
[Lee Rudolph](#)
- [Quantum Chip Helps Crack Code](#)
[Anne-Marie Corley via Monty Solomon](#)
- [Nonprofit for collecting info on SCADA & PCS security incidents](#)
[Stephanie Neil via PGN](#)
- [Utah Gets Tough With Texting Drivers](#)
[Matt Richtel via Monty Solomon](#)
- [Re: UK Chinook helicopters grounded for *years*](#)
[Peter Duncanson](#)
- [Bertrand Meyer, *Touch of Class*, Springer, 2009](#)
[PGN](#)
- [Re: VA erroneously informs over a thousand vets](#)
[Alexandre Peshansky](#)
- [Interesting disclaimer added by my ISP to the latest RISKS](#)
[Glenn Chambers](#)
- [Info on RISKS \(comp.risks\)](#)

✉ **South Africa's Telkom: For the Birds or Not For the Birds**

Gene Wirchenko <genew@ocis.net>

Fri, 11 Sep 2009 23:02:44 -0700

You have probably read the April Fool's Day RFC 1149
(A Standard for the Transmission of IP Datagrams on Avian Carriers)
(available at <http://www.rfc-editor.org/rfc/rfc1149.txt>).

You may have read <http://www.blug.linux.no/rfc1149/> which is about an implementation of it. Maybe they should try it in South Africa. They appear to have the hardware.

A South African information technology company on Wednesday proved it was faster for them to transmit data with a carrier pigeon than to send it using Telkom, the country's leading [!]Internet service provider. Internet speed and connectivity in South Africa are poor because of a bandwidth shortage. The 11-month-old pigeon, Winston, took one hour and eight minutes to fly the 80 km from Unlimited IT's offices near Pietermaritzburg to the coastal city of Durban with a data card strapped to his leg. In that time, just two per cent of the data was sent over the Internet." [Source: Pigeon Transfers Data Faster Than Internet Provider (Reuters), Kamloops This Week Daily (Kamloops, British Columbia, Canada), 2009-09-11 issue, p. 4]

The joke used to be about the bandwidth of a station wagon full of magtapes, and now, the hardware has been miniaturised to pigeon-size. I am amazed at the advances in computer technology.

[Also noted by Matthew Kruk. PGN]

<http://au.news.yahoo.com/a/-/mp/6016150/pigeon-transfers-data-faster-than-south-africa-telkom/>

OLPC: Sic Transit Gloria Laptopi

<jidanni@jidanni.org>

Sat, 05 Sep 2009 05:46:36 +0800

...there was no one hired to work on deployment while I was at OLPC, with Uruguay's and Peru's combined 360,000-laptop rollout in progress. I was parachuted in as the sole OLPC person to deal with Uruguay, and sent to Peru at the last minute. And I'm really good at thinking on my feet, but what the sh*t do I know about deployment? Right around that time, Walter was demoted and theoretically made the "director of deployment," a position where he directed his expansive team of -- himself. Then he left, and get this: now the company has half a million laptops in the wild, with no one even pretending to be officially in charge of deployment. "I quit," Walter told me on the phone after leaving, "because I can't continue to work on a lie." <http://radian.org/notebook/sic-transit-gloria-laptopi>

Smart Cars?

Gene Wirchenko <genew@ocis.net>

Mon, 14 Sep 2009 09:43:15 -0700

In today's connected world, the time you spend in your car might be the only time you're really off the grid. But that's about to change --- the automotive and ICT sectors are collaborating to network vehicles and come up with ideas for useful applications. Whether its finding carpool buddies, swerving to avoid a collision, or avoiding traffic jams --- CATA wants those applications to be tested in Canada. [Source: Intelligent car 1,000-km corridor between Ontario and Quebec envisioned]

<http://www.itbusiness.ca/it/client/en/home/News.asp?sub=true&id=54501>

The risky stuff starts near the bottom of page 2.

A concern of mine is how motorists in vehicles without this system will interact with vehicles that do. It seems to me that expectations of intelligent response are not going to be met.

✶ Boston city employees routinely deleted e-mail

Monty Solomon <monty@roscom.com>

Sat, 12 Sep 2009 23:36:43 -0400

Menino's office acknowledges city employees routinely deleted e-mails
By Donovan Slack and Michael Levenson, *The Boston Globe*, 13 Sep 2009

Mayor Thomas M. Menino's administration, prompted by public records requests from *The Globe*, has acknowledged that city employees were routinely deleting e-mails, a potential violation of the state public records law.

This came after *The Globe* filed several requests for e-mails sent and received by Menino's Cabinet chief of policy and planning, Michael J. Kineavy -- who is one of Menino's most powerful and trusted advisers, intimately involved in nearly everything at City Hall. However, a search of city computers found just 18 e-mails he had sent or received between 1 Oct 2008, and 31 Mar 2009. The unusually low figure prompted administration officials to question him about what happened to the rest of the e-mails he was presumably sending and receiving during that period. Kineavy told them that he deletes all his e-mails on a daily basis, in such a way that they are not saved on city backup computers.

http://www.boston.com/news/local/massachusetts/articles/2009/09/13/meninos_office_acknowledges_city_employees_routin

✶ Networks and Nationalization With Respect to Cyberwar

<jidanni@jidanni.org>

Sat, 12 Sep 2009 03:59:34 +0800

Cyberwarfare is the sort of game where you don't really need to be a huge government with the largest standing army in the world and sophisticated weaponry in order to win. Any teenager in his basement can control a botnet. And a botnet targeted at a poorly secured site will take it down, never mind whether the site belongs to the US government, or to the Iranians, or the Chinese, the Russians, Indians, etc. etc.

In other words probably the best way to go in a so-called "cyberwar" is defense. Harden your security. And make efforts to take down the sources of the DDoS or other attack as a way to mitigate it.

Not by breaking into it -- that's not a good idea-it will very likely end up affecting an innocent party, and you might not even have taken out the actual source -- given that a lot of botnet C&Cs are usually compromised hosts, controlled by a chain of proxies from god knows where else (connecting those dots is quite tough, when a botnet is done right).

Rather, by actually using the public private partnership you have, internationally, to work with upstream providers of the source to mitigate these attacks, work with the providers of your critical infrastructure's connectivity to filter attack sources etc. etc.

A textbook case of "how not to do this" -- during the recent North Korea (!) DDOS: A vietnamese antivirus / security vendor, BKIS and their analysis said the command and control servers were in the UK-again, quite possibly compromised hosts were used for the C&C.

That turned into a "The UK, not North Korea, is behind this cyberattack" in the media. Which doesn't sound quite right to me...

Suresh Ramasubramanian: More on Networks and Nationalization with Respect to Cyberware, 21 Jul 2009

http://www.circleid.com/posts/20090721_networks_and_nationalization_with_respect_to_cyberwar/

[Legislating against the concepts of Deep Packet Inspection (DPI) or other preferential treatment of packets is not the brightest thing to do. I've seen others draw analogies to gun control using the 'guns don't kill people' argument. Network algorithms don't kill people either but that's the most I'll take that line of argument forward, it is loaded and the traps are 'easy' to find for people on both sides of the argument. jidanni]

Heavy Data Use Puts a Strain on AT&T Service

Monty Solomon <monty@roscom.com>
Wed, 2 Sep 2009 22:18:15 -0400

Jenna Wortham, *The New York Times*, 3 Sep 2009

Slim and sleek as it is, the iPhone is really the Hummer of cellphones. It's a data guzzler. Owners use them like minicomputers, which they are, and

use them a lot. Not only do iPhone owners download applications, stream music and videos and browse the Web at higher rates than the average smartphone user, but the average iPhone owner can also use 10 times the network capacity used by the average smartphone user. [...] The result is dropped calls, spotty service, delayed text and voice messages and glacial download speeds as AT&T's cellular network strains to meet the demand. Another result is outraged customers.

<http://www.nytimes.com/2009/09/03/technology/companies/03att.html>

✂ Snow Leopard: A gigabyte by any other name

Monty Solomon <monty@roscom.com>

Wed, 2 Sep 2009 22:23:37 -0400

Excerpt from Mac OS X 10.6 Snow Leopard: the Ars Technica review

<http://arstechnica.com/apple/reviews/2009/08/mac-os-x-10-6.ars>

A gigabyte by any other name

Snow Leopard has another trick up its sleeve when it comes to disk usage. The Snow Leopard Finder considers 1 GB to be equal to 10^9 (1,000,000,000) bytes, whereas the Leopard Finder—and, it should be noted, every version of the Finder before it—equates 1 GB to 2^{30} (1,073,741,824) bytes. This has the effect of making your hard disk suddenly appear larger after installing Snow Leopard. For example, my "1 TB" hard drive shows up in the Leopard Finder as having a capacity of 931.19 GB. In Snow Leopard, it's 999.86 GB. As you might have guessed, hard disk manufacturers use the powers-of-ten system. It's all quite a mess, really. Though I come down pretty firmly on the powers-of-two side of the fence, I can't blame Apple too much for wanting to match up nicely with the long-established (but still dumb, mind you) hard disk vendors' capacity measurement standard.

✂ Humbert Humbert <heart> Fishfingers

Lee Rudolph

Tue, 8 Sep 2009 20:11:03 -0400 (EDT)

... Panic at the London Evening Standard yesterday where the theatre critic Henry Hitchings filed his review of Lolita at the National Theatre, only to learn that no one at HQ could locate his copy. The panic starts early there -- 5am -- with production staff looking at the clock and imploring him to file again. Why couldn't he communicate with them. No one could understand it. Enter a hero computer boffin. The firewall, he explained, was rejecting the word Lolita. So Hitchings had to re-file substituting Lolita throughout with the less troublesome "Fishfingers". Relieved production staff re-inserted all the Lolitas at the other end. ...

<http://www.guardian.co.uk/politics/2009/sep/09/boris-johnson-cycling-goldschmied-rogers>

Quantum Chip Helps Crack Code

Monty Solomon <monty@roscom.com>

Thu, 10 Sep 2009 08:01:33 -0400

Anne-Marie Corley, Quantum Chip Helps Crack Code;
Experimental chip does part of code-cracking quantum algorithm, 3 Sep 2009

Modern cryptography relies on the extreme difficulty computers have in factoring huge numbers, but an algorithm that works only on a quantum computer finds factors easily. Today in Science, researchers at the University of Bristol, in England, report the first factoring using this method-called Shor's algorithm-on a chip-scale quantum computer, bringing the field a tiny step closer to realizing practical quantum computation and code cracking.

Quantum computers are based on the quantum bit, or qubit. A bit in an ordinary computer can be either a 1 or a 0, but a qubit can be 1, 0, or a "superposition" of both at the same time. That makes solving certain problems-like factoring-exponentially faster, because it lets the computer try many more solutions at once. The race is on to find the ideal quantum computer architecture, with qubit contenders that include ions, electrons, superconducting circuits, and in the University of Bristol's case, photons.

MIT professor Seth Lloyd, who has been researching quantum computing and communication systems since the early 1990s, says that "optical methods [using photons] have a long way to go before being useful." But, Lloyd adds, the Bristol experiment demonstrates that the components for optical quantum computing can be squeezed onto a chip, which is an important step forward.

Shor's algorithm was first demonstrated in a computing system based on nuclear magnetic resonance-manipulating molecules in a solution with strong magnetic fields. It was later demonstrated with quantum optical methods but with the use of bulk components like mirrors and beam splitters that take up an unwieldy area of several square meters. ...

<http://www.spectrum.ieee.org/computing/hardware/chip-does-part-of-codecracking-quantum-algorithm>

[The rest of the article sounds as if the paradigmatic hard problem at this point is still factoring 15. PGN]

Nonprofit for collecting info on SCADA & PCS security incidents

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

Mon, 14 Sep 2009 08:10:50 -0400

Stephanie Neil, *Managing Automation*, 12 Sep 2009

http://www.managingautomation.com/maonline/news/read/NonProfit_Targets_CyberSecurity_in_Plants_33037

The move from proprietary, non-networked control systems in the plant to off-the-shelf, open applications that share information across industrial and business networks is a double-edged sword for manufacturers. On one side, people are more productive; on the other side, SCADA and process control systems are falling victim to hackers and network viruses.

Getting a handle on how to manage cyber-threats, however, has always been a bit tricky. Reporting an industrial incident to organizations such as the government-backed CERT program, which tracks Internet and network security attacks, accidents, and failures, could expose a company's network vulnerability or create a legal liability. As a result, many manufacturers keep a lid on their own security issues, which limits knowledge sharing that could help the industrial community as a whole.

Enter the Security Incidents Organization, a newly formed non-profit group that provides public access to its Repository of Industrial Security Incidents (RISI). Established in July, the group maintains an industry-wide repository for collecting, investigating, analyzing, and sharing critical information regarding cyber-security incidents that directly affect SCADA and process control systems.

The RISI database dates back to 2001, when it was housed at the British Columbia Institute of Technology (BCIT) as part of a research project that was shut down in 2006. At that time, BCIT faculty member Eric Byres purchased the database and continued to collect data on incidents. His company, Byres Research, was acquired by safety and security services firm exida earlier this year.

Jeremy Epstein, Senior Computer Scientist, SRI International, 1100 Wilson Blvd, Suite 2800, Arlington VA 22209 +703-247-8708 jeremy.epstein@sri.com

[Eric Byres is noted in two previous issues of RISKS, notably Critical infrastructure cybersecurity risks, [RISKS-23.57](#), and also for Infoworld interviews with him and Alan Paller, in SCADA Hacks, [RISKS-24.44](#). Please see <http://www.securityincidents.org> if you are interested in being involved in RISI. PGN]

Utah Gets Tough With Texting Drivers

*Monty Solomon <monty@roscom.com>
Sun, 30 Aug 2009 09:49:27 -0400*

Matt Richtel, *The New York Times*, 29 Aug 2009
Driven to Distraction: Utah Gets Tough With Texting Drivers
<http://www.nytimes.com/2009/08/29/technology/29distracted.html>

In most states, if somebody is texting behind the wheel and causes a crash that injures or kills someone, the penalty can be as light as a fine. Utah is much tougher. After a crash here that killed two scientists -- and

prompted a dogged investigation by a police officer and local victim's advocate -- Utah passed the nation's toughest law to crack down on texting behind the wheel. Offenders now face up to 15 years in prison.

The new law, which took effect in May, penalizes a texting driver who causes a fatality as harshly as a drunken driver who kills someone. In effect, a crash caused by such a multitasking motorist is no longer considered an "accident" like one caused by a driver who, say, runs into another car because he nodded off at the wheel. Instead, such a crash would now be considered inherently reckless.

"It's a willful act," said Lyle Hillyard, a Republican state senator and a big supporter of the new measure. "If you choose to drink and drive or if you choose to text and drive, you're assuming the same risk."

The Utah law represents a concrete new response in an evolving debate among legislators around the country about how to reduce the widespread practice of multitasking behind the wheel -- a topic to be discussed at a national conference about the dangers of distracted driving that is being organized by the Transportation Department for this fall.

Studies show that talking on a cellphone while driving is as risky as driving with a .08 blood alcohol level -- generally the standard for drunken driving -- and that the risk of driving while texting is at least twice that dangerous. Research also shows that many people are aware that the behavior is risky, but they assume others are the problem.

Treating texting behind the wheel like drunken driving raises complex legal questions. Drunken drivers can be identified using a Breathalyzer. But there is no immediate test for driving while texting; such drivers could deny they were doing so, or claim to have been dialing a phone number. (Many legislators have thus far made a distinction between texting and dialing, though researchers say dialing creates many of the same risks.)

If an officer or prosecutor wants to confiscate a phone or phone records to determine whether a driver was texting at the time of the crash, such efforts can be thwarted by search-and-seizure and privacy defenses, lawyers said.

Prosecutors and judges in other states already have the latitude to use more general reckless-driving laws to penalize multitasking drivers who cause injury and death. In California, for instance, where texting while driving is banned but the only deterrent is a \$20 fine, a driver in April received a six-year prison sentence for gross vehicular manslaughter when, speeding and texting, she slammed into a line of cars waiting at a construction zone, killing another driver.

But if those prosecutors want to charge a texting driver with recklessness, they must prove the driver knew of the risks before sending texts from behind the wheel.

In Utah, the law now assumes people understand the risks. ...

Re: UK Chinook helicopters grounded for *years* ([RISKS-25.77](#))

Peter Duncanson <mail@peterduncanson.net>

Wed, 02 Sep 2009 14:11:33 +0100

Danny Burstein's comment "UK bought Boeing helicopters, figured they'd save money by designing their own software..." is based on an inaccurate news report and is incorrect. There was no attempt to design their own software.

The report from the UK Parliament's Public Accounts Committee makes the position much clearer.

(It is the purchasing nation's responsibility to assess and certify the airworthiness of the aircraft.)

Conclusions and Recommendations:

<http://www.publications.parliament.uk/pa/cm200809/cmselect/cmpubacc/247/24704.htm>

3. The problems with the [Chinook] Mk3 procurement stemmed from the Department's failure to specify in the contract that it required access to the software source code in order to assess the safety risks and establish whether the helicopters would meet UK airworthiness standards. Given that software is key to the operation of most modern defence equipment, this is irresponsible. The Department should specify access to software as a clear requirement within any contract, especially where access to proprietary software is needed to provide airworthiness certification."

The Original Procurement of Chinook Mk3 helicopters:

<http://www.publications.parliament.uk/pa/cm200809/cmselect/cmpubacc/247/24705.htm>

1. In 1995, the Ministry of Defence (the Department) decided that, in order to meet the long standing requirement for dedicated helicopters to support special operations, an original order for 14 Chinook Mk2a helicopters from Boeing would be changed. Six were retained as Mk2a and have flown satisfactorily ever since they were delivered, but it was decided that the other eight would be modified to become Chinook Mk3 helicopters. The Chinook Mk3 helicopters feature unique cockpit avionics which, because of the Department's budgetary priorities elsewhere, ended up being a hybrid of analogue and digital systems, rather than a pure digital arrangement as used in the United States special operations Chinook (MH47-E) and by the Royal Netherlands Air Force.
2. In 2005, the Department acknowledged that the Chinook Mk3 project had been badly handled... The hybrid digital and analogue cockpit avionics could not be shown to meet United Kingdom airworthiness standards. As a result, the helicopters could only be granted a limited release to fly, and are restricted to flying on cloudless days above 500 feet where the pilot can navigate via landmarks. This makes them completely unsuitable for use on operations.
3. One of the key reasons for not granting a full release to fly was

that the software codes that maintained the instrument displays in the Mk3 cockpit could not be proven to be safe. The Department acknowledged that analysis of the code, which would help anticipate how the software, and hence the helicopter, would behave in all flight conditions, may have enabled it to certify them as safe. Boeing, in protecting their intellectual property rights, denied the Department access to the software source code. The Department accepted that the original contract, which did not mandate access to the codes, was not sufficient for the purpose of procuring helicopters that could be proven to be safe.

5. ... If the Department had not been so willing to compromise on the specification of the cockpit, it might have been able to prove airworthiness in the same way as it has for other aircraft. For example, by using the safety cases put together by the United States for the C17 aircraft, the Department has been able to satisfy the British airworthiness authorities and use the aircraft operationally, without having to resort to analysis of the flight software. The Department acknowledged that it should not over-specify changes to equipment or platforms unless it had, for example, to fit United Kingdom specific communications equipment.

The report is available as a PDF file:

<http://www.publications.parliament.uk/pa/cm200809/cmselect/cmpubacc/247/9780215526663.pdf>

✉ Bertrand Meyer, *Touch of Class*, Springer, 2009

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

Mon, 14 Sep 2009 13:51:23 PDT

A book arrived in the post from Switzerland today in a package that was soaking wet, as if it had been submerged or left out in the rain. However, the book itself was encased in plastic, and was not only in perfect condition, but very readable and very relevant to RISKS.

Bertrand Meyer's new book, *Touch of Class: Learning to Program Well with Objects and Contracts* ``gives students the edge by teaching both the fundamentals of programming and the professional-level skills preparing them for the challenges of modern software engineering.'' (Quoted from the back cover). 876+lxiv

The book is dedicated to Tony Hoare and Niklaus Wirth, and I think it would please both of them very much. It is very likely to be a real value for students, professors, and software engineers alike. PGN

✉ Re: VA erroneously informs over a thousand vets (McCool, [RISKS-25.77](#))

Alexandre Peshansky <peshanal@umdnj.edu>

Thu, 03 Sep 2009 12:30:39 -0400

On 27 Aug 2009, Rob McCool reported VA gaffe as "Through a data maintenance error, the Veteran's Affairs department recently sent out automated letters"

The issue probably has nothing to do with data maintenance error. The error is in the underlying ICD-9 (International Classification ... of Diseases), which is, along with CPT (Current Procedural Terminology) and, to smaller degree, HL7 (Health Level 7), totally unsuitable for anything except billing for current medical intervention. This is a problem well known in clinical research community and was a topic of many a lively discussions. The same underlying problem caused spurious assignment of a range of illnesses to Mr. deBronkart in his Google Health record ([RISKS-25.64](#)), extracted from ICD and CPT in his billing data. These coding systems are not hierarchical (or where they try to be, hierarchy is often broken), non-conservative (the meaning of the codes changes over time, with codes being re-assigned (as in quoted case), split and merged. The latter makes them unusable over any non-trivial timeframe without metadata, which is often unavailable (the source document - medical chart _should_ contain the date of each entry, which would have made maintaining the metadata possible - _if_ it was preserved in transcription.

So the risk in the quoted cases is, probably, in the use of data items outside of domain for which they were designed (similarly to use of SSN for authentication).

Alexandre Peshansky, Manager, OCR Informatics Core, NJ Medical School, UMDNJ CC F-1220 205 S. Orange Ave., Newark, NJ (973) 972-4897

***✶* Interesting disclaimer added by my ISP to the latest RISKS**

*Glenn Chambers <gchamber@bright.net>
Tue, 01 Sep 2009 19:39:05 -0400*

On Tue, 2009-09-01 at 08:51 -0700, RISKS List Owner wrote:

> - -----
> WARNING! This email may be asking for account details.
> bright.net would NEVER email you asking for this information.
> Do not reply to this email unless you are certain of the
> sender.
> - -----
>
> RISKS-LIST: Risks-Forum Digest Tuesday 1 September 2009 Volume 25 : Issue 77

I can imagine cases where this could cause problems...



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 79

Friday 25 September 2009

Contents

- [Complex Machinery: a parody](#)
[Ken Knowlton](#)
- [Los Angeles Drought Restrictions: Unintended Consequences?](#)
[Thomas Russ](#)
- [More on the DC Metro collision 22 June 2009](#)
[David Leshner](#)
- [New York Nuclear Plant Mistakenly Bares Emergency Alarm](#)
[PGN](#)
- [Air Force loses control of autonomous aircraft, shoots it down](#)
[Rob McCool](#)
- [Policemen's sanitary habits result in high breathalyzer reading](#)
[Matt Fichtenbaum](#)
- [Children's hospital in Ohio infected with spyware](#)
[Rob McCool](#)
- ['Robot' computer to mark English essays](#)
[Polly Curtis](#) via [Tom Heathcote](#)
- [Swiss watchdog sets court ultimatum for Google Street View](#)
[Peter Houppermans](#)
- [*NYTimes* Web Ads Show Security Breach](#)
[Matthew Kruk](#)
- [Google Buys reCAPTCHA, Creating a Potential Privacy Issue](#)
[Lauren Weinstein](#)
- [DMAchoice.org - a case study in how to run an insecure website](#)
[Jonathan Kamens](#)
- [Retailer Must Compensate Sony Anti-Piracy Rootkit Victim](#)
[jidanni](#)
- [Re: Quantum chip helps crack code](#)
[Steve Wildstrom](#)
- [Info on RISKS \(comp.risks\)](#)

✉ **Complex Machinery: a parody**

<KCKnowlton@aol.com>

Tue, 22 Sep 2009 12:12:43 EDT

An advertisement for a high-class car [Lexus] in an equally classy magazine [9/21/09 New Yorker] begins with a satirical quote by the president [John Maeda] of a respected School [RISD], the punch line of which, I fear, may float well above the grasp of many grade C students of the modern world:

"Digital technology will enable the creation of ultra-complex machines, processes, and imagery. But that amazing technology will be framed in an elegant and simple form that makes it user-friendly. The more complex the machinery, the simpler the interface will be."

[High school dropouts, I think, might thus hope for jobs as pilots of thousand passenger airplanes, or controllers of nuclear power plants - punching and twiddling a few intuitively understood buttons and knobs. KCK]

[Rhode Island is a small but nevertheless complex state. But perhaps the upshot of the supposed satire is that School of Design students are actually learning that "Everything should be made as simple as possible, and then massively oversimplified." (It won't work even in the architecture of buildings, let alone computer architectures. But the secret of success is giving the appearance of simplicity that implicitly masks the inherent complexity.) PGN]

✂ Los Angeles Drought Restrictions: Unintended Consequences?

Thomas Russ <tar@ISI.EDU>

Tue, 22 Sep 2009 13:17:27 -0700

The city of Los Angeles, California has run into a rather curious set of unintended consequence of lawn watering restrictions imposed as a conservation measure. A couple years of drought has strained the water resources of the city. So, to reduce water consumption, the city restricted lawn watering to just two days per week: Mondays and Thursdays. Unexpectedly, this may have led to a dramatic increase in the number of water main breaks, 34 since September 1st. For comparison, the numbers for September 2008, 2007 and 2006 were 21, 17 and 13. There is some suspicion that pressure shocks from the much larger swings in usage and pressure overtax the aging infrastructure. I suppose the law of unintended consequences is always operating, and this one seems to have caught everyone by surprise: "The rationing began in June, shortly before they noticed an uptick in major blowouts. There were 24 blowouts in July and 31 in August, increases from the same months last year."

More details from the Los Angeles Times:

<http://www.latimes.com/news/local/la-me-water-main19-2009sep19,0,88564.story>

<http://www.latimes.com/news/la-me-water-burst17-2009sep17,0,4531113.story>

[Nice lesson there. Put all your watery eggs in one leaky basket.]

More on the DC Metro collision 22 June 2009 ([RISKS-25.73](#))

"David Leshner" <wb8foz@panix.com>
Tue, 22 Sep 2009 23:36:06 -0400 (EDT)

The NTSB has issued an urgent interim recommendation re: the fatal Metro collision in June.

<http://www.nts.gov/recs/letters/2009/R09_15_16.pdf>

The letter discusses the failure they found:

"Testing found that a spurious high-frequency modulated signal was being created by parasitic oscillation from the power output transistors in the track circuit module transmitter. This spurious signal propagated through the power transistor heat sink, through the metal rack structure, and through a shared power source into the associated module receiver, thus establishing an unintended signal path. The spurious signal mimicked a valid track circuit signal. The peak amplitude of the spurious signal appeared at the correct time interval and was large enough to be sensed by the module receiver as a valid track circuit signal, which energized the track relay. This combination -- of an alternate signal path between track circuit modules and a spurious signal capable of exploiting that path -- bypassed the rails, and the ability of the track circuit to detect the train was lost."

and makes recommendations for WMATA, and other involved parties.

Comment: Attention has long focused on the track signaling circuit that inexplicably failed to detect the stopped train. What was not know was why it failed; when AC track signals have been in use for a century. After a great deal of work on the scene and off, NTSB has part of the answer.

The RISK here is this was and is the classic "all the eggs in one basket" protection scheme. It was a very sturdy basket, but...

Now the issue is how to retrofit real redundancy into this system...and how to pay for it.

[Doug Hosking noted a CNN item. PGN]
<http://www.cnn.com/2009/US/09/22/transit.rail.alert/index.html?iref=mpstoryview>

New York Nuclear Plant Mistakenly Blares Emergency Alarm

"Peter G. Neumann" <neumann@csl.sri.com>
Sun, 20 Sep 2009 9:18:14 PDT

Fox News, 19 Sep 2009

A suburban New York City nuclear power plant's siren system has mistakenly

blared out the warning, "Emergency! Emergency! Emergency!" The ominous message rattled some of the residents of New City, about 30 miles north of midtown Manhattan. Auto shop worker Rudy Gaspari says the mechanical voice had an unsettling, post-apocalyptic overtone to it.

The voice came from an Indian Point plant siren located downtown during a test Friday, The Journal News reported. Indian Point spokesman Jerry Nappi says the voice message "shouldn't have happened." He says plant officials have disabled the voice mechanism in the siren.

Four other sirens with faulty connections also have been fixed. A new \$15 million system is undergoing tests. It's supposed to give voice directions in park areas only.

[Doug Hosking remarked, "disabled the voice mechanism"? What could possibly go wrong there? PGN] <http://www.foxnews.com/story/0,2933,552603,00.html?test=latestnews>

✂ Air Force loses control of autonomous aircraft, shoots it down

*Rob McCool <robm@robm.com>
Fri, 18 Sep 2009 21:43:09 -0700 (PDT)*

The US Air Force in Afghanistan "lost positive control" of an autonomous MQ-9 aircraft in Afghanistan, and decided to destroy it before it crossed Afghanistan's border. A piloted plane was sent and presumably shot down the errant aircraft.

<http://io9.com/5362338/robot-fighter-jet-killed-before-it-could-go-awol>

✂ Policemen's sanitary habits result in high breathalyzer reading

*Matt Fichtenbaum <mattfic@rcn.com>
Mon, 21 Sep 2009 21:41:45 -0400*

[Online Swedish press, probably Svenska Dagbladet, a week or so ago.]

A motorist in Piteå in the north of Sweden crashed his car, injuring himself. Before sending him off to the hospital the police gave him a breathalyzer test, which resulted in a very high reading of 0.45 percent.

The hospital folks ran their own test on a sample of his blood, with a result of 0.12 percent. Still over the "drunk" threshold, but not so badly so.

It turns out that the police had a bottle of alcohol-based hand sanitizer in their car, and evidently used it. And some of it must have found its way onto the breathalyzer.

"Officer? Do you have a standard reference sober person to check the

calibration?"

#Children's hospital in Ohio infected with spyware

Rob McCool <robm@robm.com>

Fri, 18 Sep 2009 21:49:28 -0700 (PDT)

An Ohio man who had a relationship of some sort with a woman who works at Akron Children's Hospital decided to monitor her activities. He sent spyware to her Yahoo account, and instead of reading his e-mail at home (and unfortunately placing trust in him that it seems he didn't deserve), she read it at work, infecting several systems in the cardiac surgery department. Work she performed during the time her computer was infected, including patient details and some medical records, were sent to the man's computer.

http://www.cio.com.au/article/319073/misdirected_spyware_infects_ohio_hospital

This illustrates an increasing risk I think, that more and more employees are taking casual network access for granted on their work computers. Similar to cellular phones and USB sticks in the workplace, it's becoming difficult to isolate sensitive data from multitasking workers who mix personal with professional computing activity. Maintaining the kind of separation of duties that would be required to prevent this sort of incident seems to be either expensive or inconvenient, or maybe just not imagined beforehand by IT departments.

#'Robot' computer to mark English essays (Polly Curtis)

Tom Heathcote <TomHeathcote@email.com>

Fri, 25 Sep 2009 18:23:18 +0100

Polly Curtis, **The Guardian**, 25 September 2009

The owner of one of England's three major exam boards is to introduce artificial intelligence-based automated marking of English exam essays in the UK from next month. Pearson, the American-based parent company of Edexcel, is to use computers to "read" and assess essays for international English tests in a move that has fueled speculation that GCSEs and A-levels will be next.

<http://www.guardian.co.uk/education/2009/sep/25/robots-to-mark-english-essays>

#Swiss watchdog sets court ultimatum for Google Street View

Peter Houppermans <peter@houppermans.com>

Tue, 15 Sep 2009 00:31:19 +0200

Classic example of ignoring a smoldering until it turns into a raging fire.

The Swiss data protection commissioner has made fresh proposals to Google Switzerland to improve privacy of its online Street View. The office of Hanspeter Thür said on Monday that there were many problem pictures that did not respect anonymity, particularly in private roads and gardens.

Google Switzerland has said it is "very disappointed" at Thür's position because it had supplied much information and had received the go-ahead to go online, only for Thür to change his position a few days later.

The office of the Federal Data Protection and Information Commissioner says Google has to improve its system of blurring faces and car registration plates.

It also has to pay particular attention to blurring such places as hospitals, schools and prisons.

Google has 30 days to accept the proposals; if they are rejected, Thür may go to the Swiss Federal Administrative Court.

The organisation says Street View has been very popular in Switzerland and people should continue to enjoy it.

Wonderful ignoring of the real issues. Another publication in the NZZ illustrates what Google has been asked to do, over and above ensuring that their masking software actually works. They have been asked to remove small private streets from their database, and -- as in Japan -- they have been told to take pictures at eye height so fences can do what they were originally placed for.

http://www.swissinfo.ch/eng/news_digest/Watchdog_barks_again_at_Google_Street_View.html?siteSect=104&sid=11215004&cKey=1252954358000&ty=nd

***NYTimes* Web Ads Show Security Breach**

"Matthew Kruk" <mkruk@gmail.com>
Tue, 15 Sep 2009 07:20:01 -0600

"OVER the weekend, some visitors to the Web site of *The New York Times* received a nasty surprise. An unknown person or group sneaked a rogue advertisement onto the site's pages.

The malicious ad took over the browsers of many people visiting the site, as their screens filled with an image that seemed to show a scan for computer viruses. The visitors were then told that they needed to buy antivirus software to fix a problem, but the software was more snake oil than a useful program."

http://www.nytimes.com/2009/09/15/technology/internet/15adco.html?_r=1&th&emc=th

Google Buys reCAPTCHA, Creating a Potential Privacy Issue

Lauren Weinstein <pfir@pfir.org>

Wed, 16 Sep 2009 14:01:48 -0700

Google Buys reCAPTCHA, Creating a Potential Privacy Issue

<http://lauren.vortex.com/archive/000612.html>

Greetings. Google has announced (<http://bit.ly/2r4BOL>)_their acquiring of Carnegie Mellon University's "reCAPTCHA" system. You've no doubt seen reCAPTCHA in action -- it is very widely used by a vast array of sites. CMU's reCAPTCHA is a specific implementation of the more generalized CAPTCHA concept, which attempts to validate user input as coming from a human, not a (typically spam-related) robot.

The reCAPTCHA system presents pairs of words optically scanned from books, and asks the user to identify them. In the process, it also uses the resulting data to help "decode" those scanned words into their correct machine-readable textual representations as part of larger book scanning efforts.

This obviously makes reCAPTCHA a perfect match for Google, who is faced with the challenge of processing vast numbers of books in their Google Books project, some of which have fairly high OCR (Optical Character Recognition) error rates due to the difficulty of machine recognition of odd fonts, faded printing, and so on.

However, there is a potential privacy problem with reCAPTCHA (or any centralized CAPTCHA system, for that matter), that Google will need to face.

Early this year, while in the process of setting up an Internet-based forum, I considered using reCAPTCHA as part of the validation procedures. Since centralized CAPTCHA servers will typically collect IP address and potentially other data from users at the time of page display, and again when users interact with the CAPTCHA systems (for registration, message sending, etc.), these servers receive a running log of information regarding the users of the sites who are incorporating those CAPTCHAs into their pages.

So I was very surprised to discover that I could not find any reCAPTCHA privacy policy explaining to ordinary Web users displaying those pages, or interacting with the reCAPTCHA system, how that collected data would be handled from a privacy and data protection standpoint.

I queried CMU about this, and the reCAPTCHA support team replied that they did have an extensive privacy policy, but that it only appeared when reCAPTCHA API keys were created -- that is, when a Web site administrator wanting to incorporate reCAPTCHA into a site applied for reCAPTCHA access. There was nothing to tell conventional users how their IP address or other data would be handled by reCAPTCHA as a result of their viewing or interacting with a Web site page incorporating reCAPTCHA functionalities -- that is, no privacy policy to be found at all for those users at that time.

Partly for this reason, I chose not to use reCAPTCHA for my forum.

With reCAPTCHA moving under the Google umbrella, it will be crucial that Google clearly explain, in a visible and specific privacy policy, how they will collect, correlate, and otherwise use IP address and other data associated with reCAPTCHA display and use.

Fundamentally, this situation is similar to that with ad display systems, where the very act of viewing a page that includes external ads may pass IP address info (and sometimes other data) to third parties. However, while Web users can usually choose to block external ads in various ways if they wish (something I do not recommend or promote -- see "Blocking Web Ads -- And Paying the Piper" - <http://lauren.vortex.com/archive/000281.html>), blocking CAPTCHAs would usually mean losing access to the associated sites in significant ways.

As an enthusiastic supporter of Google Books ("The Joy of Libraries, a Fireman's Flame, and the Google Books Settlement" - <http://lauren.vortex.com/archive/000611.html>), I fully appreciate the value that reCAPTCHA will bring to Google, and ultimately to all users of Google Books.

But I also believe that it's very important for the privacy issues associated with reCAPTCHA to be properly handled by Google, hopefully in a manner significantly better than Carnegie Mellon's own approach earlier this year.

Lauren Weinstein, lauren@vortex.com +1 818-225-2800 <http://www.pfir.org/lauren>
Network Neutrality Squad <http://www.nnsquad.org> Blog: <http://lauren.vortex.com>
Global Coalition for Transparent Internet Performance - <http://www.gctip.org>
pfir mailing list: <http://lists.pfir.org/mailman/listinfo/pfir>

DMAchoice.org - a case study in how to run an insecure website

*Jonathan Kamens <jik@kamens.brookline.ma.us>
Wed, 23 Sep 2009 23:06:34 -0400*

The Direct Marketing Association runs a Web site, <http://dmachoice.org/>, that people are supposed to be able to use to enroll in the DMA's "Mail Preference Service" (MPS) to opt out of bulk mailings (paper junk mail, not spam), or to opt into bulk mailings from specific companies.

I registered at the site about a year ago. I had to create two different accounts because they only allow up to five addressees to be specified on a single account. At that time, I was asked to provide a username distinct from my e-mail address, which is good idea security-wise.

Recently, I returned to the site to confirm that I was still opted out of bulk mailings. Lo and behold, the login page had changed, and where before it had said "Username", it now said "E-Mail". It appeared that they had decided to no longer differentiate usernames from e-mail

addresses and I would have to register again using my e-mail address as my username. In fact, I learned later that I could have logged in with my old username, at which point it would have prompted me to enter my e-mail address and changed my username to it.

Problem #1:* *Forcing users to use e-mail addresses as usernames is bad security.

Problem #2: Switching your username format without bothering to tell existing users that they can still log in with their old usernames is stupid for all sorts of reasons, albeit perhaps not a security issue per se.

Thinking that my old accounts were no longer valid (having been given no reason to believe otherwise), I set out to register again. Note that they still only allow up to five recipient names to be specified on a single account, which leads us to...

Problem #3: If the site requires you to use your e-mail address as your username, how are you supposed to register more than one account on the site if you need to enroll more than five addressees in the MPS?

Fortunately, my mail server supports extended addresses with the semi-standard syntax of using "+" as the separator between the mailbox name and extension to the left of the "@" sign (i.e., "jik+foo@...", "jik+bar@...", etc. all end up in my inbox), so I figured that I would simply register two accounts with the e-mail addresses "jik+dma@..." and "jik+dma2@...". Alas...

Problem #4: The DMA Web site does not accept "+" as a valid character to the left of the "@" in an e-mail address, even though in fact it's perfectly valid according to all relevant e-mail standards. (I wish I could say that this problem is unique to the DMA site, but alas it's one I've encountered many times before.)

However, all was not lost. Since I maintain my own mail server, I was able to create two new aliases for myself without "+" signs in them, which I did. I then proceeded to successfully register using the first alias. I ran into a bit of difficulty along the way, because...

Problem #5: The site uses CAPTCHAs to prevent automated registrations. The CAPTCHAs are case-sensitive, but the letters in the CAPTCHA are of varying sizes and for many of them it's impossible to tell whether they're in lower or upper case. (I don't know whether this is because the DMA implemented a stupid home-grown CAPTCHA generator or there's actually a third-party generator out there which is this stupid, but I don't think I've ever encountered another Web site with CAPTCHAs with the same problem.)

When I registered the first account, a confirmation screen was displayed after I clicked the "Submit" button on the registration screen, and I was sent an e-mail message with a link I had to click on to confirm my e-mail address and activate my account. Unfortunately, when I tried to register a second time with the other e-mail alias so that I could enroll the rest of my family in the MPS...

Problem #6: I got a blank confirmation screen after clicking the "Submit" button, and no activation e-mail was sent.

Thinking that perhaps my cookies and/or browser cache were confusing the site, I cleared them both. It didn't make any difference. Thinking that perhaps they were throttling the number of registrations from a single IP address, I tried from two other IP addresses on completely different networks; that didn't make any difference either. Thinking that perhaps Firefox might be a problem, I tried with both IE7 and IE8; no luck. In short, for some inexplicable reason, although I was able to register just fine once, I was unable to repeat the feat a second time.

Only just now, as I'm writing this, have I realized that the first e-mail address I used was 30 characters long, while the second was 31. Therefore, I have realized that...

Problem #7: The reason I was unable to register the second account is almost certainly because there's a hard-coded, bogus 30-character limit on e-mail addresses somewhere in the DMA's application or database schema, along with a bug which prevents the application from notifying the user of the problem when the limit is exceeded.

I used the "Contact Us" link on the Web site to let them know the address I was trying to register and the behavior I was seeing. A day later, I received a response. Paraphrasing: "Sometimes the Web site doesn't work. Try again after about an hour. If it still doesn't work, you'll have to print out the form and register by mail."

Problem #8: If I'm right about the 30-character limit on e-mail addresses, and I'm fairly certain that I am, and I told their customer service people the e-mail address I was trying to register, then surely the "Supervisor" who responded to my e-mail should know about this problem and should have been able to tell me what was wrong and how to work around it (use a shorter e-mail address).

In response, I asked to speak with someone who could actually debug the issue and figure out why it wasn't working so that I could register through the Web site. My correspondent said that would not be possible.

Problem #9: Web site problems which make the site completely useless for some users are dismissed with "Oh, well, sometimes the site doesn't work," and, "It's just too bad for you if it doesn't." The people running the site simply don't care about getting to the bottom of these issues.

I sent back a more strongly worded complaint to this effect. Several hours later, I received a response from someone different at the DMA. Excerpting from her response:

I did a little research on your behalf and found that you had already created two accounts last year for the same seven family members back on 08/14/2008; for [names elided] the old username for the 2008 account is: [elided] and the old password is: [elided].

The second account for the other two names [elided] was created on 08/14/2009. The old username name was: [elided] and password [elided].

What I did on the existing second account was to change the username into the other e-mail address that you were trying to use. So now the second account is username: [elided] and the password is the same.

I'm sure I don't have to tell people what's wrong here, but just to be pedantic...

Problem #10: Passwords are stored in plain-text and accessible to DMA employees rather than stored as the result of a one-way hash.

Problem #11: The DMA employee provided me with usernames that I had never provided to her.

Problem #12: The DMA employee sent my passwords through e-mail.

(The last three problems are, of course, by far the worst of the ones listed in this message.)

Problem #13: This second DMA employee made no more effort than the first one to acknowledge the root cause of my problem, i.e., that I should have been able to register the second account myself and that the DMA should actually make some effort to figure out why I couldn't and fix it.

Problem #14: This second DMA employee also didn't say anything about e-mail addresses more than 30 characters long not working. (On the other hand, if you combine the "Never attribute to malice..." rule with the fact that neither employee I dealt with showed any inclination to try to identify the root cause of the issue, perhaps it's reasonable to conclude that they really don't know this is the problem.)

I'm so flabbergasted that I have to go back a bit and repeat myself in capital letters here: **PASSWORDS ARE STORED IN PLAIN-TEXT AND ACCESSIBLE TO DMA EMPLOYEES, WHO HAVE NO COMPUNCTIONS ABOUT LOOKING THEM UP AND SENDING THEM TO PEOPLE IN E-MAIL. ARGH!**

Thanks, I feel much better now.

When there are Web sites like this on the Internet and people like this maintaining them, is it any wonder that there are new revelations about serious data breaches several times every week?

✂ Retailer Must Compensate Sony Anti-Piracy Rootkit Victim

<jidanni@jidanni.org>

Wed, 16 Sep 2009 05:46:29 +0800

[[From the boy who cried RISK]]

...Claiming for his losses, the plaintiff demanded 200 euros for 20 hours wasted dealing with the virus alerts and another 100 euros for 10 hours spent restoring lost data. Since the plaintiff was self-employed, he also claimed for loss of profits and in addition claimed 800 euros which he paid to a computer expert to repair his network after the infection. Added to this was 185 euros in legal costs making a total claim of around 1,500 euros.

The judge's assessment was that the CD sold to the plaintiff was faulty, since he should be able to expect that the CD could play on his system without interfering with it.

The court ordered the retailer of the CD to pay damages of 1,200 euros.

<http://torrentfreak.com/retailer-must-compensate-sony-anti-piracy-rootkit-victim-090914/>

Re: Quantum chip helps crack code ([RISKS-25.78](#))

Steve Wildstrom <steve.wildstrom@gmail.com>

Tue, 15 Sep 2009 12:40:54 -0700 (PDT)

I'm sure it can also factor 4, 6, 8, 9, 12, and 14. But if you only have four qubits, you can only count to 15, assuming unsigned integers. The real hard problem is scaling a quantum computer into something useful. It seems that no matter which technology we use, we have been stuck at 4 to 8 qubits for many years. Wake me when a quantum computer can factor RSA151.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 80

Friday 9 October 2009

Contents

- [The computers did it -- differently](#)
[Wendell Cochran](#)
- [Lobstermen Get Wrong Number for a Hot Line](#)
[Ian Austen via PGN](#)
- [Swine flu brings down Kaiser Permanente servers](#)
[Tony Lima](#)
- [Restricted manual on avoiding leaking sensitive data is leaked](#)
[Mark Thorson](#)
- [Subject: Mass. Blue Cross physicians' personal info on stolen laptop](#)
[Kay Lazar via Monty Solomon](#)
- [Airline status display follies](#)
[Steven Bellovin](#)
- [For Washington Metro, it's the appearance of risk](#)
[Jeremy Epstein](#)
- [Man forged 12,500 pounds worth of train tickets](#)
[Mark Brader](#)
- [System diversity helps in power control system](#)
[Jeremy Epstein](#)
- [How Hackers Snatch Real-Time Security ID Numbers](#)
[Saul Hansell via Monty Solomon](#)
- [Perils of password reuse plus password security hall of shame](#)
[Jonathan Kamens](#)
- [WordPress inadvertent disclosure bug](#)
[Jonathan Kamens](#)
- [The risks of being cute, Re: Complex Machinery: a parody](#)
[Donald Norman](#)
[PGN](#)
[Bluejay](#)
- [Re: Snow Leopard: A gigabyte by any other name](#)
[Phil Hobbs](#)
- [Re: South Africa's Telkom: For the Birds or Not For the Birds](#)
[Richard Botting](#)
- [Re: Software never fails, people decide that it does](#)
[Paul Robinson](#)
- [Info on RISKS \(comp.risks\)](#)

✂ The computers did it -- differently

Wendell Cochran <atrypa@eskimo.com>

Fri, 2 Oct 2009 10:16:31 -0700

Airbus's A380 megajet is now two years behind schedule, reports *BusinessWeek*, which goes on to say 'Use of incompatible programs takes the rap, but behind that is a management team cobbled together from formerly separate companies.'

http://www.businessweek.com/globalbiz/content/oct2006/gb20061005_846432.htm

✂ Lobstermen Get Wrong Number for a Hot Line

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

Fri, 9 Oct 2009 20:35:35 PDT

The Canadian government announced a stimulus program for their lobster fishery, with a toll-free number that embarrassingly had an incorrect area code, resulting in solicitations for "nasty girls". The president of the Prince Edward Island Fisherman's Association put a reverse spin on the situation: "Maybe it would have been good if the people calling the sex line would have heard the fishing issues, giving them a bit of an education." [Source: Ian Austen, *The New York Times*, 28 Sep 2009, National Edition, B5]

✂ Swine flu brings down Kaiser Permanente servers

Tony Lima <tony.lima@csueastbay.edu>

Fri, 09 Oct 2009 09:36:19 -0700

Moday morning my wife was trying to log in to her Kaiser online account. The server was obviously very busy; her login attempts failed repeatedly with timeouts. The new items on the Kaiser home page were two links to H1N1 information. These appeared to be the cause of the problem. The links could have been placed on the members' home page, available only after logging in.

RISK: making information available to the general public instead of members only can lead to server overload. - Tony Lima (who, by the way, is otherwise quite happy with Kaiser)

Prof. Tony Lima, Dept. of Economics, CSU, East Bay, tony.lima@csueastbay.edu

<http://www.cbe.csueastbay.edu/~alima> (510) 885-3889

✂ Restricted manual on avoiding leaking sensitive data is leaked

Mark Thorson <eee@sonic.net>
Mon, 05 Oct 2009 13:35:15 -0700

UK's Ministry of Defense 3-volume guide to avoiding leakage of sensitive data, itself a restricted document, has been leaked.

<http://www.dailymail.co.uk/news/article-1218315>

✶ Mass. Blue Cross physicians' personal info on stolen laptop (Kay Lazar)

Monty Solomon <monty@roscom.com>
Sat, 3 Oct 2009 20:06:06 -0400

Blue Cross physicians warned of data breach;
Stolen laptop had doctors' tax IDs

The largest health insurer in Massachusetts is warning roughly 39,000 physicians and other health care providers in the state that personal information, including Social Security numbers, may have been compromised after a laptop containing the data was stolen in August from an employee of the Blue Cross and Blue Shield Association's national headquarters in Chicago.

The breach involves "tens of thousands" of physicians nationwide, although the precise number is unclear, according to a national Blue Cross-Blue Shield spokesman. Thirty-nine affiliates feed information about providers into a database maintained by the association's national headquarters.

Massachusetts doctors were not notified by letter until yesterday, because state Blue Cross-Blue Shield officials said they did not at first know what kind of data were on the stolen laptop. They said the data did not contain any information about patients or personal health records.

[Source: Kay Lazar, *The Boston Globe*, 3 Oct 2009]

http://www.boston.com/news/local/massachusetts/articles/2009/10/03/blue_cross_physicians_warned_of_data_breach/

✶ Airline status display follies

Steven Bellovin <smb@cs.columbia.edu>
Fri, 9 Oct 2009 22:53:47 -0400

Flying -- more precisely, checking flight status -- is a wonderful way to learn how not to design systems.

I was scheduled to fly from Pittsburgh to Newark; my flight was scheduled to depart at 6:22pm. That itself is probably a case of letting precision exceed accuracy; indeed, the departure board at the airport showed a scheduled departure time of 6:25pm. Other flights, though, did have times like 6:29 or 7:31 shown; admittedly, those were from different airlines.

But why would my airline show one time on its schedule and web status, and another at the airport?

When I got to the airport, around 4:00, I saw that the 3:15 flight hadn't left yet: "delayed", no time shown. I went to the gate, but saw neither a plane nor a gate agent. Odd, especially since the web showed that the incoming flight had indeed arrived in Pittsburgh on time. When someone eventually showed up, I asked if I could still get on the 3:15 flight. "Oh, that left a long time ago." I asked why it was still on the displays. He immediately got on his radio to ask that it be deleted. The status displays aren't database-driven?

I checked my flight again; it showed as on time. It showed as on time even when the inbound plane was running 1.5 hours late. Well, not quite; the inbound plane was listed as departing 1.5 hours late, but arriving on time, only four minutes after it was supposed to leave Newark. Hmm, no sanity checks in that display.

And my flight? Even after the inbound flight departed, 2.25 hours late, it still showed an on-time departure, about 1.5 hours after the web claimed the inbound equipment will arrive. Note that the web site actually has a link to the inbound flight's status, so some database *knew* which plane was involved. And the airport display? It showed the flight as "delayed", but still with a departure time that was earlier than the plane's arrival time.

The gate agent told me never to trust the web site. I forbore to point to the airport displays, because at that point one of her colleagues was wondering why their information showed that the inbound plane was still taxiing at Newark, well after it should have been in the air. She replied "maybe someone forgot to enter the update".

I arrived home about two hours late, musing about systems design.

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

✂ For Washington Metro, it's the appearance of risk

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Sun, 27 Sep 2009 16:09:41 -0400

After the deadly Metro train crash in June, the Washington Metro system reconfigured trains so that the older ("1000 series") train cars were no longer at the ends of trains, where they were in the deadly crash. The idea, as described at the time, was to put them in the middle of the train, since the newer cars have greater survivability in a crash.

The problem is, there was no engineering to support this hypothesis. According to the WashPost, it was a pure PR move, and in fact Metro doesn't know if the move made the trains safer or less safe. They were mostly concerned about the appearance of doing something to address risk, lest the public (and the localities that fund Metro) decide that the lack of action

meant Metro didn't care.

The RISK is that when something that looks to the public like an engineering action has no engineering basis, we may get results that are counterproductive.

There's minimal direct computer risk in this particular action, although other postings have noted computer and technology risks elsewhere in the Metro system.

<http://www.washingtonpost.com/wp-dyn/content/article/2009/09/26/AR2009092602684.html?hpid=topnews>

Man forged 12,500 pounds worth of train tickets

Mark Brader

Sat, 3 Oct 2009 05:46:49 -0400 (EDT)

Jonathan Moore of Hove, England, described as an "IT expert", has been sentenced for using a computer to forge 12,472 pounds worth of train tickets that he used for his daily commute to London. The ongoing fraud was eventually detected by a ticket inspector who noticed that Moore's ticket was not quite the right color. Designs for over 70 tickets were found on his laptop.

According to the customer services director at the train operating company, "It is a tribute to our quick-witted staff that this thief was caught out. Fare dodgers are robbing the rail industry of 400 million pounds a year."

http://news.bbc.co.uk/2/hi/uk_news/england/sussex/8287111.stm
<http://www.timesonline.co.uk/tol/news/uk/crime/article6858680.ece>

System diversity helps in power control system

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Fri, 2 Oct 2009 08:51:54 -0400

The Inquirer reports that a virus infestation in the electrical grid control room of Integral Energy (Australia) was controlled by replacing the Windows-based control consoles with the development systems that run Linux. The SCADA systems themselves run Solaris, and the control consoles only are used as X Window displays, so the replacement didn't require reprogramming.

This appears to be a case where diversity of implementations and plug compatibility (Windows + X replaced by Linux + X) allowed greater resilience than either alone. However, the fact that the SCADA systems run Solaris is of scant comfort - while perhaps not as strewn with viruses as Windows, it's still not risk-free.

<http://www.theinquirer.net/inquirer/news/1556944/linux-saves-aussie-electricity>

#How Hackers Snatch Real-Time Security ID Numbers (Saul Hansell)

Monty Solomon <monty@roscom.com>

Thu, 1 Oct 2009 08:27:02 -0400

[From Saul Hansell's blog, *The New York Times*, 20 Aug 2009]

The world's savviest hackers are on to the "real-time Web" and using it to devilish effect. The real-time Web is the fire hose of information coming from services like Twitter. The latest generation of Trojans - nasty little programs that hacking gangs use to burrow onto your computer - sends a Twitter-like stream of updates about everything you do back to their controllers, many of whom, researchers say, are in Eastern Europe. Trojans used to just accumulate secret diaries of your Web surfing and periodically sent the results on to the hacker.

The security world first spotted these new attacks last year. I ran into it again while reporting an article in Thursday's Times about a lawsuit meant to help track down the perpetrators of these attacks.

By going real time, hackers now can get around some of the roadblocks that companies have put in their way. Most significantly, they are now undeterred by systems that create temporary passwords, such as RSA's SecurID system, which involves a small gadget that displays a six-digit number that changes every minute based on a complex formula.

If your computer is infected, the Trojan zaps your temporary password back to the waiting hacker who immediately uses it to log onto your account. Sometimes, the hacker logs on from his own computer, probably using tricks to hide its location. Other times, the Trojan allows the hacker to control your computer, opening a browser session that you can't see. ...

<http://bits.blogs.nytimes.com/2009/08/20/how-hackers-s snatch-real-time-security-id-numbers/>

#Perils of password reuse plus password security hall of shame

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

Tue, 6 Oct 2009 10:09:06 -0400

Years ago, I developed the bad habit of using the same "medium-security password" on lots of different Web sites. I first started doing this around a decade ago, when Web site data breaches were far less frequent and far less professionally executed than they are now. Still, that's a bad excuse for forming a bad habit, which it took a real kick in the pants to get me to break.

That kick in the pants came a couple of weeks ago, when I inadvertently posted my password to my blog for the world to see (more on that under

separate cover). After realizing what had happened, I spent every available moment for several days logging into ten years' worth of Web sites, many of which I haven't used in a long, long time but still had personal information about me stored on them, and changing my password on all of them.

This prompted me to write two articles on my blog which may be of interest to RISKS readers:

* In <http://blog.kamens.brookline.ma.us/~jik/wordpress/300pw>, I discuss why password reuse is a bad idea (the fact that I had to spend days changing my password on over 300 Web sites is only one of many reasons) and offer advice on how to avoid it without having to remember different, random password for hundreds of Web sites.

* My marathon password-changing journey gave me the opportunity to look at how well passwords are secured at a large number of Web sites in many different application domains. In <http://blog.kamens.brookline.ma.us/~jik/wordpress/pwshame>, I've published my "Password Security Hall of Shame" of the sites I encountered with poor password security.

I am interested in hearing feedback from others about these articles so that I can make them better. In particular, I'd love to add other noteworthy pieces of advice to my article about managing the seemingly inevitable juggernaut of Web passwords, and I'd also like to add to the Hall of Shame any other sites with poor password security of which people are aware. Please feel free to post comments on my blog or email me.

WordPress inadvertent disclosure bug

*"Jonathan Kamens" <jik@kamens.brookline.ma.us>
Tue, 6 Oct 2009 10:17:54 -0400*

There is a bug in the current version of the WordPress blogging platform (and probably in all versions since 2.8.0) which can cause hidden text to be inadvertently published in a blog entry without the user's knowledge.

In a nutshell, sometimes when text is pasted into the WordPress WYSIWYG editor, an invisible copy of the text is pasted into the editor without the user's knowledge. This invisible text is published along with the blog entry, and although it is not visible on the user's blog, it is visible to search engines and to syndicators which strip HTML style attributes.

The exact conditions under which the bug occurs are not yet known.

This is not a terribly serious security hole as these things ago, but it is real and needs to be addressed. Unfortunately, the maintainers of WordPress do not seem to be taking it particularly seriously; despite having been notified about the issue over a week ago, they have not yet acknowledged that it has security implications or committed to fixing it.

I've posted more details about the issue on my blog at <http://blog.kamens.brookline.ma.us/~jik/wordpress/wpbug>.

The risks of being cute, Re: Complex Machinery: a parody ([RISKS-25.79](#))

Donald Norman <don@jnd.org>

Fri, 25 Sep 2009 20:08:14 -0700

You know, it's fun to be cute or to pun, but not when it causes the RISKS digest to mislead and misinform.

When two otherwise intelligent people, K C Knowlton and our esteemed moderator decide to be cute, they should check the facts first. Taking lines out of context is bad. Writing about something of which you know nothing is worse.

Both Knowlton and Neumann decided to have fun with the poor little Rhode Island School of Design (RISD) and its new president, John Maeda. John was quoted in a Lexus ad of all places saying "the more complex the design, the simpler the interface will be." Sounds right to me! Alas, not to our esteemed commentators.

RISD is one of the world's best conventional design schools. Many of us in the design community are delighted that John has taken over: he will take it out of "conventional". John Maeda is from the MIT Media Lab and one of the world's best designers with a best-selling book entitled "Simplicity." But our esteemed commentators couldn't resist stating that his quote meant oversimplification and reduction to absurdity. Shame on both of you. You read a message in the quotation that was not there.

The trick in design is to get it just right: neither too simple nor too complicated. Moreover, I have argued that complexity is good -- it is complicated that is bad. Simplicity does not mean simple-minded. Maeda has made this point many times in his professional writing and talks.

The real quote is that of Einstein who said that everything should be as simple as possible, but no simpler. It is the "but no simpler" part of the quote that people forget, but it is the most important.

Simplicity needs to be context sensitive. The average driver needs a very simple control for the auto. The skilled driver wants more control, so a bit less simplification. And the technicians need to be able to get into the guts of the stuff, so they need even less simplification. Yes, the more complex the underlying machinery, the more sophisticated the interface design has to be to tame that complexity so it is at just the right level for whatever person is using it at the moment. Making something easy to use and understand often requires increased complexity beneath the surface to make that possible. Hence, the fact that the human interface code takes up a considerable portion of the code base of any software system.

These are issues Maeda and RISD do understand. Different people have

different needs. The real story requires a book (and John has written one). Look folks, don't make up RISKS that do not exist. we have enough real ones to cope with.

Don't take isolated quotations out of context. And please don't write about topics in which you are not expert.

Don Norman, Nielsen Norman Group, Northwestern University, and KAIST (S. Korea)
don@jnd.org www.jnd.org/

✂ The risks of being cute, Re: Complex Machinery: a parody ([RISKS-25.80](#))

*"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 30 Sep 2009 17:12:14 PDT*

Don, I think you have overreacted, and even misunderstood my comments. And you evidently do not believe in causal logic in English. "The more complex the design, the simpler the interface will be." implies a causality: If a design is more complex, it follows that the interface will inherently be simpler. That is sheer and utter nonsense. Ken was undoubtedly reacting to the reality that complex systems often have inappropriately over-complex interfaces. On the other hand, if Maeda had said, "If a design must inherently be more complex (because of the intrinsic complexity of the requirements -- for example, management of fault tolerance and safety and survivability usually adds significantly more complexity), the interface had very well better be simple." then I would have been comfortable. Actually, I have high respect for Maeda and RISD, and would prefer to think that he was misquoted by the typically nontechnically savvy admen-istrators. PGN]

✂ The risks of being cute, Re: Complex Machinery: a parody ([RISKS-25.79](#))

*Bluejay <bluejay@prtcnet.com>
Fri, 25 Sep 2009 19:20:43 -0400*

>[... (...But the secret of success is giving the appearance of
>simplicity that implicitly masks the inherent complexity.) PGN]

I have a theory that the amount of complexity of a closed system remains constant. For example, long ago computers were very complex to use and maintain, but certainly by today's standard they were pretty simple. Today, computers have become so complex as to often defy understanding, but even my 86-year-old Dad can use one.

Bluejay Adametz, CFII, A&P, AA-5B N45210

✂ Re: Snow Leopard: A gigabyte by any other name ([RISKS-25.78](#))

*Phil Hobbs <pcdhSpamMeSenseless@electrooptical.net>
Thu, 01 Oct 2009 18:24:03 -0400*

It's historical.

Disc drive specifications have been in decimal since the 1950s, whereas the 1024-byte kilobyte is from the 1970s.

Re: South Africa's Telkom: For the Birds or Not For the Birds

*Richard Botting <rbotting@csusb.edu>
Fri, 02 Oct 2009 12:44:18 -0700*

Gene Wirchenko reported on 11 Sep 2009 on the comparison of Pigeons and the Internet to transmit data. I am bothered by the confusion in the news item between latency and bandwidth: "took one hour and eight minutes to fly the 80 km [...] with a data card strapped to his leg. In that time, just two per cent of the data was sent over the Internet." Surely we should launch a whole series of pigeons to calculate the bandwidth?

By the way, Rocky Mountain Adventures uses pigeons to send data sticks of photos to their home base. See

<http://odeo.com/episodes/25042064-Pigeon-Protocol-Finds-a-Practical-Purpose>

Re: Software never fails, people decide that it does (Brydon, [R-25.76](#))

*Paul Robinson <paul@paul-robinson.us>
Wed, 30 Sep 2009 21:08:19 +0000 (GMT)*

> However, that does not inhibit someone other than the originator from
> making an informed and educated decision, based on engineering principles,
> that the product requires updating or replacing.

True, but technically you can't objectively prove it. Point to a software program and all you can really say is that these bits - which look like any other bits - need replacing. Or this code needs replacing because it needs to perform a different function than it does or because the function is wrong. But there will be nothing there you can show that is quantitatively different from anything else which would indicate evidence of the defect other than you claiming there is one, which again, is going to be your opinion and no more.

The possibility of failure in a software package can be no less deadly than that of any other failure in a device or item under the same sort of usage or operation, e.g., a software failure in a pacemaker can be as fatal as having bad wiring. Bad software in a car's engine could be as serious as a stuck gas pedal or a failed brake pedal. But where's the objective proof to make the claim? There really isn't any, it's just an opinion. Evidence of

failure that has happened is real and can be shown, but unlike rust on a bridge, there nothing "there" to show where the failure point is in a piece of software. Again, all bits look alike, there are no obviously corroded or "rusty" ones you can single out for repair or replacement.

The difference is that for the real world, we can point to and objectively show the rust in a bridge, the corrosion in wiring, the break in a rubber hose, the molecular discohension in a framistat (the latter is a fictional example for something that hasn't been invented yet, but we will someday have and use.) But inaccurate or incorrect functionality in a computer program can only be shown by errors in some output or damage in something else; the software has nothing intrinsic in and of itself to show that it is in error or operates improperly except for, unfortunately, someone's opinion that the software is wrong or inadequate.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 81

Monday 12 October 2009

Contents

- [Microsoft's Danger Data Service disrupts users](#)
[John F. McMullen](#)
- [Microsoft's Danger SideKick and cloud computing](#)
[Daniel Eran Dilger via Monty Solomon](#)
- [Microsoft's Sidekick due to dogfooding/sabotage](#)
[Daniel Eran Dilger via Monty Solomon](#)
- [Cloud Danger, literally... MS loses T-mobile data](#)
[David Lesher](#)
- [Excess CAT scan radiation -- the return of Therac 25?](#)
[David Lesher](#)
- [A Time Machine time bomb](#)
[Ron Garret](#)
- [Why E-mail No Longer Rules](#)
[Jessica E. Vascellaro via Monty Solomon](#)
- [Re: Airline status display follies](#)
[Peter R Cook](#)
[Arthur Flatau](#)
- [Re: The risks of being cute](#)
[Rob Seaman](#)
[Ken Knowlton](#)
- [Re: The computers did it -- differently](#)
[Wendell Cochran](#)
- [Re: Software never fails, people decide that it does](#)
[Martyn Thomas](#)
[Michael Smith](#)
[Geoffrey Brent](#)
[Dimitri Maziuk](#)
- [Info on RISKS \(comp.risks\)](#)

Microsoft's Danger Data Service disrupts users

"John F. McMullen" <johnmac13@gmail.com>

Mon, 12 Oct 2009 18:54:31 -0400

[From Johnmac's blog: <<http://johnmacrants.blogspot.com>>]

T-Mobile's Sidekick Smart Phone Service, powered by Microsoft's Danger Data Service has been out of commission for over a week and now the users are warned that their data, stored on Danger's Servers, may have been lost and that the data that remains on their Sidekick devices is at jeopardy, putting customers contact and calendar information at risk to disappear.

Some johnmac comments:

1. There was never a problem like this prior to the Microsoft acquisition of Danger.
2. There has been little media coverage of this problem although I suspect that multi-thousands of users are affected.
3. It would seem that, given all of its technical expertise, Microsoft could come up with some way to replicate the original Danger SideKick to Danger backup. Failing that, it should be able to provide a USB backup to Outlook.
4. Perhaps Google can jump in with a Sidekick to G-Mail, G-Calendar, etc. If so, game over and a lot of Androids get sold.*

The latest missive:

Sidekick customers, during this service disruption, please DO NOT remove your battery, reset your Sidekick, or allow it to lose power.
Updated: 10/10/2009 12:35 PM PDT

T-MOBILE AND MICROSOFT/DANGER STATUS UPDATE ON SIDEKICK DATA DISRUPTION

Dear valued T-Mobile Sidekick customers:

T-Mobile and the Sidekick data services provider, Danger, a subsidiary of Microsoft, are reaching out to express our apologies regarding the recent Sidekick data service disruption. We appreciate your patience as Microsoft/Danger continues to work on maintaining platform stability, and restoring all services for our Sidekick customers.

Regrettably, based on Microsoft/Danger's latest recovery assessment of their systems, we must now inform you that personal information stored on your device - such as contacts, calendar entries, to-do lists or photos - that is no longer on your Sidekick almost certainly has been lost as a result of a server failure at Microsoft/Danger. That said, our teams continue to work around-the-clock in hopes of discovering some way to recover this information. However, the likelihood of a successful outcome is extremely low. As such, we wanted to share this news with you and offer some tips and suggestions to help you rebuild your personal content. You can find these tips in our Sidekick Contacts FAQ. We encourage you to visit the Forums on a regular basis to access the latest updates as well as FAQs regarding this service disruption.

In addition, we plan to communicate with you on Monday (Oct. 12) the status of the remaining issues caused by the service disruption, including the data

recovery efforts and the Download Catalog restoration which we are continuing to resolve. We also will communicate any additional tips or suggestions that may help in restoring your content.

We recognize the magnitude of this inconvenience. Our primary efforts have been focused on restoring our customers' personal content. We also are considering additional measures for those of you who have lost your content to help reinforce how valuable you are as a T-Mobile customer. We continue to advise customers to NOT reset their device by removing the battery or letting their battery drain completely, as any personal content that currently resides on your device will be lost. Once again, T-Mobile and Microsoft/Danger regret any and all inconvenience this matter has caused.

Service Disruption FAQs| Disruption Credit FAQs| Disruption Discussion
Password/Sign-in Text Message FAQs | Password/Sign-in Discussion

[One of my closest associates reacted to this, and said,
"Who would want to use a system called `Danger'?" PGN]

johnmac@acm.org johnmac13@gmail.com johnmac@sdf.lonestar.org
johnmac@panix.com, johnmac@echonyc.com johnmac13@mac.com
jmcmullen@monroecollege.edu johnmac@alumni.iona.edu [...]

[Johnmac's message also included an incisive item by Robert X. Cringeley,
Microsoft screwup puts T-Mobile users in Danger. PGN]
[http://www.infoworld.com/d/adventures-in-it/microsoft-screwup-puts-t-mobile-users-in-danger-482?
source=3DIFWNLE_nlt_blogs_2009-10-12](http://www.infoworld.com/d/adventures-in-it/microsoft-screwup-puts-t-mobile-users-in-danger-482?source=3DIFWNLE_nlt_blogs_2009-10-12)

Microsoft's Danger SideKick and cloud computing (Daniel Eran Dilger)

*Monty Solomon <monty@roscom.com>
Mon, 12 Oct 2009 19:22:50 -0400*

Daniel Eran Dilger, Microsoft's Danger SideKick data loss casts dark on
cloud computing, 11 Oct 2009
<http://www.roughlydrafted.com/2009/10/11/microsofts-danger-sidekick-data-loss-casts-dark-on-cloud-computing/>

Microsoft has demonstrated that the dark side of cloud computing has no silver linings. After a major server outage occurred on its watch last weekend, users dependent on the company have just been informed that their personal data and photos "has almost certainly been lost."

Microsoft's Danger SideKick data loss casts dark on cloud computing

While occasional service outages have hit nearly everyone in the business, knocking Google's Gmail offline for hours, plunging RIM's BlackBerrys into the dark, or leaving Apple's MobileMe web apps unreachable to waves of users, Microsoft's high profile outage has impacted users in the worst possible way: the company has unrecoverable lost nearly all of its users' data, and now has no alternative backup plan for recovering any of it a week later.

The outage and data loss affects all SideKick customers of the Danger group Microsoft purchased in early 2008. Danger maintained a significant online services business for T-Mobile's SideKick users. All of T-Mobile's SideKick phone users rely on Danger's online service to supply applications such as contacts, calendars, IM and SMS, media player, and other features of the device, and to store the data associated with those applications.

When Microsoft's Danger servers began to fall offline last Friday October 2, users across the country couldn't even use the services; even after functionality was beginning to be brought back on Tuesday October 6, users still didn't have their data back. This Saturday, after a week of efforts to solve the crisis, T-Mobile finally announced to its SideKick subscribers:

"Regrettably, based on Microsoft/Danger's latest recovery assessment of their systems, we must now inform you that personal information stored on your device - such as contacts, calendar entries, to-do lists or photos - that is no longer on your Sidekick almost certainly has been lost as a result of a server failure at Microsoft/Danger."

A new report from Engadget says that T-Mobile has suspended sales of its SideKick models and is warning: "Sidekick customers, during this service disruption, please DO NOT remove your battery, reset your Sidekick, or allow it to lose power." ...

[Also noted by Ben Moore. PGN]

Microsoft's Sidekick due to dogfooding/sabotage (Daniel Eran Dilger)

*Monty Solomon <monty@roscom.com>
Mon, 12 Oct 2009 23:01:13 -0400*

Daniel Eran Dilger, Microsoft's Sidekick/Pink problems blamed on dogfooding and sabotage, 12 Oct 2009

Additional insiders have stepped forward to shed more light into Microsoft's troubled acquisition of Danger, its beleaguered Pink Project, and what has become one of the most high profile Information Technology disasters in recent memory.

The sources point to longstanding management issues, a culture of "dogfooding," and evidence that could suggest the issue was a deliberate act of sabotage.

AppleInsider previously broke the story that Microsoft's Roz Ho launched an exploratory group to determine how the company could best reach the consumer smartphone market, identified Danger as a viable acquisition target, and then made a series of catastrophic mistakes that resulted in both the scuttling of any chance that Pink prototypes would ever appear, as well as allowing Danger's existing datacenter to fail spectacularly, resulting in lost data across the board for T-Mobile's Sidekick users. ...

<http://www.roughlydrafted.com/2009/10/12/microsofts-sidekickpink-problems-blamed-on-dogfooding-and-sabotage/>

Cloud Danger, literally... M\$ loses T-mobile data

*"David Leshar" <wb8foz@panix.com>
Sun, 11 Oct 2009 15:43:17 -0400 (EDT)*

T-Mobile's "Sidekick" mobile service uses a backend system provided by Microsoft, and seemingly aptly named "Danger." [Will Robinson was not mentioned, but...]

Danger has lost ALL the customers' stored data. The only copy remaining is that remaining on the mobile device itself.

"our teams continue to work around-the-clock in hopes of discovering some way to recover this information. However, the likelihood of a successful outcome is extremely low."

RISKS:

Backups are good, working backups *far* better.

If you run a cloud-based service, you can ruin *many* more people's days than anyone with a mere departmental failed server ever can.

Excess CAT scan radiation -- the return of Therac 25?

*David Leshar <wb8foz@panix.com>
Sun, 11 Oct 2009 14:32:34 -0400*

The *LA Times* reports that patients at Cedars-Sinai Medical Center were hit with excess radiation from CT brain scans.

The FDA has issued an alert "Over an 18-month period, 206 patients at a particular facility received radiation doses that were approximately eight times the expected level. Instead of receiving the expected dose of 0.5 Gy (maximum) to the head, these patients received 3-4 Gy."
<<http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm185898.htm>>

A) Old Risks come back Yet Again; note this went on for 18 months.

B) I assume the employees around such emitting devices still wear film badges or other dosimeters; maybe patients should do so as well....

[Also noted by Brian Harvey and Lauren Weinstein. PGN]
<http://www.washingtonpost.com/wp-dyn/content/article/2009/10/10/AR2009101000813.html?hpid=sec-health>

✂ A Time Machine time bomb

Ron Garret <ron@flownet.com>

Sat, 10 Oct 2009 03:37:27 -0700

From the better-late-than-never department:

<http://rondam.blogspot.com/2009/09/time-machine-time-bomb.html>

Summary: plugging in a new ESATA drive can cause you to silently lose ALL your Time Machine backups.

✂ Why E-mail No Longer Rules (Jessica E. Vascellaro)

Monty Solomon <monty@roscom.com>

Mon, 12 Oct 2009 11:09:54 -0400

-- and what that means for the way we communicate

[Source: Jessica E. Vascellaro, *Wall Street Journal*, 12 Oct 2009; PGN-ed]

E-mail has had a good run as king of communications. But its reign is over. In its place, a new generation of services is starting to take hold-services like Twitter and Facebook and countless others vying for a piece of the new world. And just as e-mail did more than a decade ago, this shift promises to profoundly rewrite the way we communicate-in ways we can only begin to imagine. ...

<http://online.wsj.com/article/SB10001424052970203803904574431151489408372.html>

✂ Re: Airline status display follies (Bellovin, [RISKS-25.80](#))

Peter R Cook <PCook@wisty.plus.com>

Sat, 10 Oct 2009 10:29:18 +0100

The risks of assumptions:

In [RISKS-25.80](#), Steve Bellovin muses entertainingly on the chaotic state of the flight status systems he encountered, and the foibles he ascribes to poor systems design.

However, the piece is based on the assumption that the design purpose of the flight information system is to provide passengers with accurate real time data on the status of the flight. If this is the purpose then his thoughts are valid.

If on the other hand the purpose of the system is to give to the passenger information about the flight that the airline wishes the passenger to know

-- as part of a strategy to manage passenger expectations - then the system may well be doing what its designers created it to do.

For example, displaying times to the minute leaves the passenger with an impression of precision - a perception that an airline might want to create in the mind of the passenger. However changing that "precise" timing in real time as the accurate flight status changed in the database would spoil the impression.

I can also visualise situations where the airline would not want the "real" status of the flight displayed in real time on the annunciations at the airport. Disney manages queues brilliantly to minimise the negative psychological effects of the wait. They know when to tell you its a long wait, and when to "fold the queue" out of visual sight to minimise its apparent length. Are the airline flight systems intended to do something similar? What would they display if something went badly wrong?

Was it really poor systems design; was the airline using it badly; or did they have a purpose that was not apparent or espoused? I suspect Steve is right -- the end to end system was broken. But it did get me to thinking about what the airline might have specified as the design parameters for the system.

Re: Airline status display follies (Bellovin, [RISKS-25.80](#))

*Arthur Flatau <flataua@acm.org>
Mon, 12 Oct 2009 11:32:36 -0500*

I have noticed similar problems with flight status. For the most part, I do not believe that this is a computer problem. I believe that the airlines have cut their personnel so far as to barely have enough people to do what is needed if everything goes right. When anything goes wrong, there are not enough people to do what needs to be done. At some point, someone has to manually enter that a plane has left the gate, or arrived at a gate. This seems to be a low priority (and it probably should be) compared to getting people on and off the plane, for example.

Of course, there various databases should be connect to the web sites and in airport displays, but I think that is a more minor problem in this case.

Of course, I have no actual knowledge of how any of this works.

Re: The risks of being cute ([RISKS-25.79,80](#))

*Rob Seaman <seaman@noao.edu>
Sun, 11 Oct 2009 11:16:56 -0700*

It is immensely informative (as well as hugely entertaining) to see two paragons of design excellence such as Donald Norman and PGN arguing issues

of simplicity versus complexity. I could only wish Henry Petroski and Edward Tufte would chime in, too...

I'm reminded of the deliciously dynamic conversation of architectural design between Richard Meier's Getty Center and the context provided by its central garden independently designed by Robert Irwin. Perhaps all design arises from the synthesis of contending views.

It seems to this acolyte that a view helpful to understanding the context of complex systems and their need for simple user interfaces is to realize that the user is not external to the system. A car is not acting as a car until its driver takes the controls. The UI is only one of many interfaces, each critically important and benefiting from principles of design elegance.

One certainly agrees that quotes mean more in context. Frost's "good fences makes good neighbors" was what the neighbor said - the poet said "something there is that doesn't love a wall".

On the other hand, Einstein's original quote was "...the supreme goal of all theory is to make the irreducible basic elements as simple and as few as possible without having to surrender the adequate representation of a single datum of experience." Einstein was describing physics not engineering. In engineering corners must often be cut. In physics they may never be.

There are more risks in remaining silent than in hazarding the occasional ironic remark.

Rob Seaman, National Optical Astronomy Observatory seaman@hanksville.org

Re: The risks of being cute ([RISKS-25.79,80](#))

<KCKnowlton@aol.com>

Sun, 11 Oct 2009 20:35:47 EDT

Complex talk about Complex Machinery

I'm sorry to see the bearer of our golden standard on interfaces, Don Norman, plunging headlong into such shallow waters [[RISKS-25.80](#)]. At issue is John Maeda's quote [[RISKS-25.79](#)] in a Lexus ad in The New Yorker:

"Digital technology will enable the creation of ultra-complex machines, processes, and imagery. But that amazing technology will be framed in an elegant and simple form that makes it user-friendly. The more complex the machinery, the simpler the interface will be." [italics mine].

This last sentence, without more context, explanation, or scope of applicability, is worse than a simple conundrum; it is a disservice to public understanding of the perils of complexity that the RISKS forum, as I've known it, serves to explore.

(I admit that there are special circumstances, such as in the design of aids

for the visually, mentally or physical handicapped, wherein a more severe handicap might seem to require more complicated machinery and a simpler interface. Even then, with more complexity, more things can go wrong: we should have indicators to know that something has gone amiss with a breathing tube or robotic arm, and the means to do something about it - automatically, or course, which could save the day, or the person, until these indicators or controls or automated actuators themselves malfunction, etc.)

To print that quote was surely bad judgment on the part of Maeda, or Lexus, or *The New Yorker*, or some combination of them, I don't know which. It may have been wrong of me to call it exactly as I saw it, an unintended parody, suggesting that complexity of machinery and the complexity of its interface are inversely related. I had assumed that RISKS readers would see somewhat as I did.

And, as for PGN's puns, look folks, lets fix what we can fix.

✂ Re: The computers did it -- differently ([RISKS-25.80](#))

*Wendell Cochran <atrypa@eskimo.com>
Sat, 10 Oct 2009 09:07:19 -0700*

[Quite a few readers noted that the A380 item was three years old, and slipped by Wendell and PGN. Apologies. The A390 has of course been flying quite noticeably for quite a while now. PGN]

My blushes, as Holmes said to Dr Watson.

It's odd that I didn't check the date, for I often complain that a Web page hides the answer to When?

At least the moral of the story holds good -- which is to say bad.

Ad astra per aspera.

[Mea culpa from PGN for not noticing the old URL and checking it. I have spent the last three weeks filling up at least six dumpsters for recycling and 30 large boxes for saving almost 60 years of accumulated paper, so that my office could be emptied enough for an earthquake retrofit. I've been massively preoccupied, and am now a preoccupant of temporary (and also nearly empty) office for the next three weeks or so. I'll have to rely on our aggressive backup system in case my desktop does not survive the construction. I'm finally forced to live in a paperless world for a while. PGN]

✂ Re: Software never fails, people decide that it does ([RISKS-25.80](#))

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

Sat, 10 Oct 2009 11:28:37 +0100

We have been through all this before, in thread "Failure Taxonomy (Discussion of Terms)" in January 1997. [Indeed. And yet the ensuing discussion was also repeated, as seen in a few selected responses that follow -- included in case we have some new readers such as the T-mobile/Danger/MS folks, the CAT scan folks, or others, with apologies to old readers (who can skip the next three messages). PGN]

All **design** faults show no physical degradation. That doesn't make the fault merely a matter of opinion. If any artifact is stated to carry out some function, and it doesn't, then it is flawed - independently of whether the failure was caused by erroneous software or a broken wire.

The distinction that Paul Robinson seeks to make is false. A bridge may be rusty, or a wire corroded, yet still be fit for purpose. The evidence of the fault is the consequent failure to perform as required, not the corrosion.

So long as the requirements are clear, any deviation from the requirements is an objective fault that does not depend on anyone's opinion. If the requirements are not clear, then whether the observed behaviour is faulty or not **is** a matter of opinion, whether the system is mechanical or software-controlled.

Let's keep post-modernism out of engineering.

✂ Re: Software never fails, people decide that it does ([RISKS-25.80](#))

Michael Smith <emmenjay@zip.com.au>

Tue, 13 Oct 2009 01:56:12 +1100

I suspect that we may be mixing two types of failure.

When we design software or bridges, we write specifications. If we specify a width of 'n' metres for a bridge, but a survey reveals a different width, then the bridge does not meet its specification -- i.e. it is faulty.

Similarly, when designing software, we may (and should) specify precise behaviour. If the software fails to meet that specification, then it is faulty. We apply code inspections and various types of testing to determine how well the specification is met. Since perfection is not possible, there will be gaps in our specification. However such a "specification bug" is a different thing from a failure to meet the specification.

Quite different from the above is "decay". A bridge may rust, components may bend or break. Metal fatigue and a multitude of other factors may reduce the usefulness of a product that was originally of acceptable quality.

In general, software does not experience this [1]. If your software works

correctly, it will continue to work correctly. However its usefulness may decline over time due to external factors. The computer on which it runs may become obsolete. Peripherals may malfunction. The problem, which the software solves, may change [2].

In the first type of failure, software and other engineering endeavours share a good deal of similarity. In the second, they seem to share less.

[1] Sometimes data or configuration files become progressively more corrupt, giving software the appearance of decay. This is sometimes known as "bit rot".

[2] A bridge has an analogue to the "problem change" situation. e.g., a bridge with a particular capacity may become less useful as changed traffic patterns create a need for higher capacity.

Re: Software never fails, people decide that it does ([RISKS-25.80](#))

*Geoffrey Brent <gpbrent@optusnet.com.au>
Sat, 10 Oct 2009 21:35:08 +1100*

I'm not sure I follow this argument. If the point here is that the concept of "defect" in software becomes meaningless when we narrow our field of vision sufficiently, then that's true; it's meaningless to say that a solitary 0 or 1 is "defective". But that's just as true for the non-computing examples given here; it's meaningless to say that a single proton/electron/neutron is "rusty".

"Error" in software is a matter of human opinion. But then, so is the general consensus that brakes should be able to stop a car and bridges shouldn't fall down.

Re: Software never fails, people decide that it does ([RISKS-25.80](#))

*Dimitri Maziuk <dmaziuk@bmr.wisc.edu>
Sat, 10 Oct 2009 12:51:31 -0500*

Disproof by counterexample: binary diff against a program that works correctly will quantitatively show the bits that are different.

If I don't know anything about corrosion or bridges, your claim that those brown spots on the cables are bad is going to be your opinion and nothing more -- to me.

Or, looking at it from the other side, I write code for scientists. Often enough I don't have enough domain knowledge to tell if the numbers my code produces are correct or not. I have to ask for someone else's opinion on that and trust them if they say my code needs replacing.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 82

Tuesday 20 October 2009

Contents

- [Toyota uncontrolled acceleration](#)
[David Lesher](#)
- [Another Therac-25 rerun](#)
[Jeremy Epstein](#)
- [Custom license plate lands man a database full of fines](#)
[Rob McCool](#)
- [Risks of namespace conflicts among city names](#)
[Cody Boisclair](#)
- [More on hospital error leads to radiation overdoses](#)
[Gene Spafford](#)
- [Internet Pioneers Speak Out on Net Neutrality](#)
[Lauren Weinstein](#)
- [Accessing your legacy](#)
[Peter Bernard Ladkin](#)
- [Re: A Time Machine time bomb](#)
[Alan J Rosenthal](#)
- [Re: Microsoft's Danger Data Service](#)
[David Lesher](#)
[John Murrell via John E. McMullen](#)
- [Inexcusable Complexity, Re: The risks of being cute](#)
[Ed Lowry](#)
- [Re: The risks of being cute](#)
[Curt Sampson](#)
- [Re: System diversity helps in power control system](#)
[Ian Botham](#)
- [Rethinking What Leads the Way: Science, or New Technology?](#)
[John Markoff on W. Brian Arthur](#)
[via PGN](#)
- [Computers, Freedom and Privacy 2010 Conference: Call for Proposals](#)
- [Info on RISKS \(comp.risks\)](#)

✈ **Toyota uncontrolled acceleration**

"David Lesher" <wb8foz@panix.com>

Mon, 19 Oct 2009 17:10:15 -0400 (EDT)

There have been several recent cases where Toyotas have suddenly accelerated out of control.

The most notable had a passenger who called 911 and reported her spouse, a Calif. Highway Patrol officer who taught driving safety, was unable to stop their car. They crashed with all on board killed.

Toyota has recalled several million cars to replace a floor mat that may jam the accelerator.

But the crash raises the question: why couldn't an experienced officer stop a runaway car?

- a) It was a loaner from the dealer.
- b) It was equipped with a keyless RFID ignition lock. To force such off, you must *hold* the Start button down for 3+ seconds; touching it is ineffective.
- c) The transmission was some mix of manual and automatic, with a series of gates to keep you from mis-shifting. Apparently there is no clutch pedal.
- d) There were passerby reports the car brakes were on fire as it went by.

I see two big risks here. The first is changing longstanding, well-understood, user interfaces without considering the uninitiated driver. While Windows may have taught some of us that of course we use the Start button to stop; it's not clear such learning transfers to driving. And when you hide a vital safety function behind a time delay....

The second is more alarming. I thought that there was a {?unwritten} requirement that no US road-legal car could even overpower its own brakes; i.e., given full throttle and full brakes; the car stops, period. (This may not be the case for a dedicated race car...)

Is this no longer true? Are there production cars where the brakes can't stop a runaway? (That does not say you couldn't fade the brakes into worthlessness, but we can assume the driver knew that.)

There are obvious add-ons that could reduce the possibility of a recurrence [Tie brake activation to a throttle cutoff, add a real STOP button to the dash, etc.] but those add complexity or direct costs...and may provoke new problems.

While Toyota's head is now on the chopping block; they won't be the last.

✂ Another Therac-25 rerun (Re: Lesher, [RISKS-25.81](#))

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Sun, 18 Oct 2009 09:00:52 -0400

David Lesher noted a recent Cedars-Sinai Therac-25-like failure.

WiReD is reporting another one at an unnamed Cleveland hospital, where medical staff noticed that the patient was out of position and hit the emergency stop button, but the machine didn't correctly put the shielding in place or move the patient out of the machine. The problem was a "known bug" which had been deferred to a future release. Just to be clear, unlike the Therac incident, there was no significant excess radiation involved, and it does not appear that anyone was harmed.

No word on whether the bug was in the application software designed for the instrument, or something inherent in the system (e.g., a buggy operating system).

Still, the RISKS of software-controlled medical instruments are pretty clear, and are likely to increase as high tech equipment becomes more prevalent.

<http://www.wired.com/threatlevel/2009/10/gamma/>

✂ Custom license plate lands man a database full of fines

*Rob McCool <robm@robm.com>
Fri, 16 Oct 2009 22:54:23 -0700 (PDT)*

<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2009/10/16/national/a072720D99.DTL&tsp=1>

An Alabama man ordered a license plate with seven occurrences of the letter X, to pay homage to Racer X, a favorite character of his. He is now getting as many as 10 tickets a day because the city's traffic enforcement division uses this as a placeholder in their database for cars with no license plates. Yet another instance of an information system failing to account for the unexpected, people working around that limitation, and an edge case arriving some time later to cause trouble.

[Apparently \$19,000 thus far.

Craig Reise suggested that ``Maybe a `missing license plate' checkbox or drop-down would be a good idea in this application...

Bob Frankston said, ``Reminds me of people with the name Ng vs. payroll systems." RISKS has had a few similar stories in the past. PGN]

✂ Risks of namespace conflicts among city names

*Cody Boisclair <cody@zone38.net>
Sat, 17 Oct 2009 21:07:38 -0400*

It's not just GPSes that get confused by multiple locations having the same name; even weather forecasts can be surprisingly deceptive for the same

reason.

I recently upgraded my MacBook from OS X 10.5 (Leopard) to 10.6 (Snow Leopard). The weather widget included in the OS changed its information provider with the update; in 10.5 it used AccuWeather, while in 10.6 it gets its information from The Weather Channel.

To make the transition as seamless as possible, Apple designed it so that the widget in 10.6 would import its information from the 10.5 version. Or more accurately, it imports the name of the city-- and *nothing else*, even though it's very much possible to enter one's location as a postal code in the widget.

You've probably already guessed at the sort of problems this could cause -- and sure enough, it did.

In 10.5, I entered my location into the weather widget as the ZIP code 30605, representing the city of Athens, Georgia in the US. This seemed the most unambiguous way of doing it, given the sheer number of towns out there called Athens.

Upon upgrading to 10.6, nothing seemed incredibly out of the ordinary at first glance during the summer and the beginning of fall -- any glitches could easily have been excused by the cached weather information being a couple hours stale. As fall weather began to arrive, however, I noticed more and more discrepancies between what the weather widget claimed and the actual weather I encountered outside. And yet, the widget was still showing "Athens" as the location, as if nothing had changed.

I decided today to take a look at the properties for the widget... and sure enough, despite the fact that I originally entered the location as a postal code, the stored location had been changed to Athens, *Greece*. Oops.

Judging from the order in which The Weather Channel lists its disambiguations for these city names, I imagine the same thing would occur for anyone living in Rome, Georgia; Birmingham, England; Portland, Maine; Paris, Texas; London, Ontario... and, depending on weather patterns, could easily have gone unnoticed for as long as it did for me.

Cody "codeman38" Boisclair cody@zone38.net <http://www.zone38.net/>

More on hospital error leads to radiation overdoses

Gene Spafford <spaf@cerias.purdue.edu>

Wed, 14 Oct 2009 19:44:01 -0400

(Re: Leshner, [RISKS-25.81](#))

206 people received 8 times the expected dose of X-rays as a result of a misunderstanding setting a CT machine...and then not finding it for 18 months. It was finally found when one of the patient complained about his hair falling out after a test. "You have to be pretty confident to think

you know more than the guys who designed the equipment." [Source: latimes.com, 13 Oct 2009]

<http://www.latimes.com/news/local/la-me-cedars13-2009oct13,0,1200257.story>

Internet Pioneers Speak Out on Net Neutrality

Lauren Weinstein <pfir@pfir.org>

Fri, 16 Oct 2009 14:58:43 -0700

Internet Pioneers Speak Out on Net Neutrality

<http://www.vortex.com/FCC-Net-Neutrality-Letter.pdf>

<http://lauren.vortex.com/archive/000625.html>

15 October 2009

Honorable Julius Genachowski
Chairman, Federal Communications Commission
Washington, DC

Dear Mr. Chairman:

We appreciate the opportunity to send you this letter. As individuals who have worked on the Internet and its predecessors continuously beginning in the late 1960s, we are very concerned that access to the Internet be both open and robust. We are very pleased by your recent proposal to initiate a proceeding for the consideration of safeguards to that end.

In particular, we believe that your network neutrality proposal's key principles of "nondiscrimination" and "transparency" are necessary components of a pro-innovation public policy agenda for this nation. This initiative is both timely and necessary, and we look forward to a data-driven, on-the-record proceeding to consider all of the various options.

We understand that your proposal, while not even yet part of a public proceeding, already is meeting with strong and vocal resistance from some of the organizations that the American public depends upon for broadband access to the Internet. As you know, the debate on this topic has been lengthy, and many parties opposing the concept have systematically mischaracterized the views of those who endorse and support your position.

We believe that the existing Internet access landscape in the U.S. provides inadequate choices to discipline the market through facilities-based competition alone. Your network neutrality proposals will help protect U.S. Internet users' choices for and freedom to access all available Internet services, worldwide, while still providing for responsible network operation and management practices, including appropriate privacy-preserving protections against denial of service and other attacks.

One persistent myth is that "network neutrality" somehow requires that all packets be treated identically, that no prioritization or quality of service

is permitted under such a framework, and that network neutrality would forbid charging users higher fees for faster speed circuits. To the contrary, we believe such features are permitted within a "network neutral" framework, so long they are not applied in an anti-competitive fashion.

We believe that the vast numbers of innovative Internet applications over the last decade are a direct consequence of an open and freely accessible Internet. Many now-successful companies have deployed their services on the Internet without the need to negotiate special arrangements with Internet Service Providers, and it's crucial that future innovators have the same opportunity. We are advocates for "permissionless innovation" that does not impede entrepreneurial enterprise.

We commend your initiative to protect and maintain the Internet's unique openness, and support the FCC process for considering the adoption of your proposed nondiscrimination and transparency principles.

Respectfully,

Vinton G. Cerf, Internet Pioneer
Stephen D. Crocker, Internet Pioneer
David P. Reed, Internet Pioneer
Lauren Weinstein, Internet Pioneer
Daniel Lynch, Internet Pioneer

Accessing your legacy

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

Sun, 18 Oct 2009 08:58:37 +0200

People who use computers and the Internet as major professional tools are all getting closer to dying. The organiser (organiser? provoker) of our traditional music group died suddenly last year and his professional and personal correspondence was inaccessible. Nobody could find out who Mario knew or whom he was encouraging to come to our sessions. And not just us -- he organised a lot for concertina players throughout Germany. (I wrote a couple of poems in tribute, one in English and one in German, accessible through irishsessionbielefeld.de) Today I heard belatedly about the death of one of my most extensive correspondents of the last 17 years. His son found the e- mail address of a mailing-list correspondent of ours in his papers. Not on his machine, mind -- in his A4 bleached- wood-fibre Nachlass.

Which leads to the moral:

* Please leave access details to computerised personal and professional information in a secure place to which your executors will have access when you fall over.

The question is precisely how you organise your computerised life so that your executors can find out, for example, whom you know, and how to pass on info to others if you organised groups, while keeping those things

inaccessible which you don't wish to bequeath to posterity. I don't think there are obvious general answers. But telling your executor about the most obvious stuff is not hard.

Peter Bernard Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

Re: A Time Machine time bomb (Ron Garret, [RISKS-25.81](#))

Alan J Rosenthal

Sat, 17 Oct 2009 11:56:08 -0400 (EDT)

This seems to me to be an inherent risk of any automated backup aging process: adding a bunch of new data to be backed up will cause a bunch of old backups to be deleted.

If you want the computer to decide without consulting you how many of your backups to keep, then you relinquish the power to decide how many of your backups to keep.

Re: Microsoft's Danger Data Service (Re: [RISKS-25.81](#))

"David Leshner" <wb8f0z@panix.com>

Tue, 13 Oct 2009 14:24:26 -0400 (EDT)

Re: Cloud Danger, literally... M\$ loses T-mobile data

One aspect of Sidekick's design that was not directly Microsoft's fault is both a caution, and maybe a lesson, for the design and legal communities.

Unlike most of the competition; the Sidekick user allegedly had no way to do her/his own backups, and still doesn't. Palms, iPhones, etc not just allow such but make it simple to do so to a local computer. But from what I've read, Sidekick users had no such option bundled with their purchase. (There was reportedly some extra cost add-on that could back up *Danger's* copy of same to a user machine, but no direct way. And with the Danger database corrupted...it's too late now.)

Now we know that many many [but not all] of the customers would never bother to perform a local backup. [I'm hard pressed to imagine Sidekick's most famous user, Paris Hilton, on the phone to Tech Support asking for backup help....] But if it's true that their users had no real option to do so, that surely dilutes one legal excuse for Microsoft, that backups were really the users' responsibility.

Another dimension of the saga... where do such cloud based devices fall in the world of Carnivore err DCS-1000? I suspect the legal stance DOJ takes is the user voluntarily shared the data (be it calendar data, pictures, or voice recordings) with Microsoft/Danger; ergo she had no expectations of

privacy. Hmm, I wonder if users can FOIA their lost data back from the FBI?

✈ Re: Microsoft's Danger Data Service (Re: [RISKS-25.81](#))

"John F. McMullen" <johnmac13@gmail.com>

Thu, 15 Oct 2009 12:16:00 -0400

John Murrell <jmurrell@bayareanewsgroup.com>

Sidekick depression eases; Microsoft says recovery under way

The prospects for recovering the personal data lost by T-Mobile Sidekick customers in a server snafu at Microsoft's Danger unit have gone from bleak to hazy to substantially brighter.

In a post early today, Roz Ho, Microsoft's VP for (ideally) Premium Mobile Experiences, said "We are pleased to report that we have recovered most, if not all, customer data for those Sidekick customers whose data was affected by the recent outage. We plan to begin restoring users' personal data as soon as possible, starting with personal contacts, after we have validated the data and our restoration plan. We will then continue to work around the clock to restore data to all affected users, including calendar, notes, tasks, photographs and high scores, as quickly as possible. We now believe that data loss affected a minority of Sidekick users."

She went on: "We have determined that the outage was caused by a system failure that created data loss in the core database and the back-up. We rebuilt the system component by component, recovering data along the way. This careful process has taken a significant amount of time, but was necessary to preserve the integrity of the data. ... We have made changes to improve the overall stability of the Sidekick service and initiated a more resilient backup process to ensure that the integrity of our database backups is maintained."

http://click1.newsletters.siliconvalley.com/wsqqmtdr_ohmctgnpjmp_myfvsqln.html

That said, Microsoft continued to run away from Danger lest its other cloud computing efforts be injured. Microsoft spokeswoman Tonya Klause said Wednesday, "The Danger Service platform, which experienced the outage, is a standalone service operating on non-Microsoft technologies, and is not related to Microsoft's cloud services platform or Windows Live. Other and future Microsoft mobile products and services are entirely based on Microsoft technologies and Microsoft's cloud service platform and software."

The good news on the recovery front arrived too late to stop the first wave of the inevitable lawsuits including a pair in Northern California that seek class action status and assert negligence and false claims by Microsoft and T-Mobile.

[Source: MediaNews Group, 1560 Broadway, Ste. 2100, Denver, CO 80202]



Inexcusable Complexity, Re: The risks of being cute ([RISKS-25.80](#))

Ed Lowry <eslowry@alum.mit.edu>

Thu, 15 Oct 2009 15:08:33 -0400

In [RISKS-25.80](#) Donald Norman lectures us on simplicity versus complexity issues and admonishes "please don't write about topics on which you are not an expert". In software, that would lead to almost total silence on software's biggest challenge, expressing it simply.

At present there is no software language technology available which provides for simplicity of expression as advanced as what was designed at IBM in the early 1970s and implemented at Digital Equipment Corporation in the early 1980s. I have seen no evidence of organizations or leadership in software that aspire to expertise that advanced. If there is I would like to hear about it. The capabilities of the most advanced facilities for executing simply-expressed software have moved backwards over the past 20 years. The expertise has been fading too.

Twenty five years ago, expressions such as:

- * count every person whose spouse is veteran;
- * sum revenue of every year after 1981;
- * every element of where some isotope of it is stable;

could be executed as part of general purpose programming and database language, but not today.

There are three sources of inexcusable complexity plaguing software today where software leaders have mostly obstructed progress. They can be eliminated by: -- combining structural with functional expressiveness, - using data objects that are designed to be easily arranged, -- increasing language generality. They are described in "Inexcusable Complexity" at <http://users.rcn.com/eslowry> .

One result of neglecting simplification is that students everywhere are routinely taught how to arrange pieces of information by teachers who have little idea what is a reasonable structure for well-designed pieces of information.

Decades of obstructing simplification has undermined public safety and some currently high priorities of the US government:

- * technical education,
- * innovation,
- * cyber security,
- * reducing health care costs,
- * reducing government spending.

The risks of neglecting progress in a fundamental part of information technology for 35 years: a widening swath of death destruction, ignorance, agony, waste, criminality, and dangers to national security.

✂ Re: The risks of being cute ([RISKS-25.79,80,81](#))

Curt Sampson <cjs@cynic.net>

Fri, 16 Oct 2009 22:39:12 +0900

>> The more complex the machinery, the simpler the interface will be."

> This last sentence, without more context, explanation, or scope of
> applicability, is worse than a simple conundrum; it is a disservice to
> public understanding of the perils of complexity that the RISKS forum, as
> I've known it, serves to explore.

Indeed. But even if we take the sentiment as a whole, rather than focusing on the last sentence, I think I'd go further than you and say that this way of looking at things is not only a disservice to the public, but a danger to the public, and even each of us in our private lives. It's not only wrong on occasion; it's wrong frequently enough that I believe we should never think about things this way: we should be appropriately suspicious when we do ever think about it this way.

How wrong this idea can go was made most viscerally clear to me when, after some years of film photography on '60s- and '70s-era cameras, I bought a digital SLR. I spent quite some time (almost two hours, actually) writing up a detailed example of the differences, but it became too large for a RISKS post. When you start analyzing in detail the use of the three simple settings (focus, aperture and shutter speed) that are the primary controls on both digital and analogue cameras, you run into huge, unforeseen (and often not seen terribly clearly afterward) differences well before you even reach those modes on the dial beyond 'M', 'A', 'S' and 'P' that instead have funny pictures (and even more mysterious effects on those three settings --though those setting are all that they affect).

Through thinking about this a bit more, I now have great sympathy for any Airbus pilot who pushed a little hard on the rudders. How was he to know? I'd do the same.

I think it comes down to Fred Brooks' essential vs. inessential complexity; the essential doesn't go away: it just gets disguised, and in the disguising of it, we lose the instincts we've developed and have to relearn them, perhaps without realising, in the moment, that we need to do so.

> It may have been wrong of me to call it exactly as I saw it, an
> unintended parody, suggesting that complexity of machinery and the
> complexity of its interface are inversely related.

No, they are proportionally related. As I now know too well, and yet not well enough.

Curt Sampson <cjs@starling-software.com> +81 90 7737 2974

✶ Re: System diversity helps in power control system

Ian Botham <ianb30804@gmail.com>

Sat, 17 Oct 2009 00:43:10 +1100

This article missed the major issue, which was that a virus outbreak crippled the Windows desktops of a large government utility. I have talked to some insiders, and thought the facts might be of interest to Risks readers.

The organisation is a large electrical distribution utility in Australia. It has around 2700 Windows desktops in a head office, and some dozen regional offices, all connected via a WAN. I haven't heard how the virus (W32.virut.cf) got into the internal network initially (if anybody knows), but I heard that the anti-virus software was out of date, and while it could recognise infected exe's it couldn't kill the virus process or stop it spreading via Windows file shares. The virus infected exe files, then the anti-virus software detected this and quarantined the files -- with the result that soon there were no exe's left to run, and the desktop boxes were junk.

Initially the scale and seriousness of the situation wasn't realised, and after several days a high percentage of the organisation's desktops were close to useless. The effect on day to day operations was crippling. As the original article mentioned, the SCADA system is on Solaris and so was not at risk. However, the trouble ticket system runs on Windows servers, and while not affected was at risk. Eventually the decision was made that all desktops had to be re-imaged to get rid of the virus, and it took more than 2 weeks from the initial detection of the virus to get most of the desktops back in operation.

The most obvious risk is that of letting anti-virus software get out of date. However, that shouldn't blind us to the bigger risk of having the day to day operation of a large organisation dependent on a large collection of Windows computers -- which will always be vulnerable to a zero-day exploit of some kind. I know there's no easy fix for this risk, but that doesn't make the risk go away.

Finally, I'm not an anti-Windows zealot, but I just can't resist ! How will the Windows marketing droids spin the lower TCO of Windows, and discount the cost of thousands of employees twiddling their thumbs for a few weeks ?

✶ Rethinking What Leads the Way: Science, or New Technology?

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

Tue, 20 Oct 2009 11:24:52 PDT

(John Markoff on W. Brian Arthur)

John Markoff has a very interesting column in The New York Times' Science Times, 20 Oct 2009, on what appears to be a very interesting new book:

W. Brian Arthur

The Nature of Technology: What It Is and How it Evolves

Free Press, 246 pages, 2009

Markoff notes that this book "reframes the relationship between science and technology as part of an effort to come up with a comprehensive theory of innovation. The relationship is more symbiotic than is generally conceded." Arthur was trained as an engineer, mathematician, and economist, and those disciplines are all brought to bear. Markoff concludes with this paragraph: "Dr. Arthur's view is that technology is something that defines us as human and that, in the end, we will be able to control a set of technologies that rather than conquering us will extend our humanity." This has of course been an ongoing topic here in one guise or another, and can benefit from Arthur's analysis -- particularly as it might (or might not) relate to the computer field. (That might be a subject for John Markoff's blog!)

Computers, Freedom and Privacy 2010 Conference: Call for Proposals

<technews@HQ.ACM.ORG>

Mon, 19 Oct 2009 13:36:16 -0400

Organizers of the 20th annual ACM Computers, Freedom, and Privacy conference, which takes place June 15-18, 2010, in San Jose, have announced a call for proposals to help shape the program for next year's gathering. The theme of the conference is Computers, Freedom, and Privacy in the Networked Society and seeks to address how constant connection in social, communication, information, and physical environments impacts freedom and privacy, and how computers can be used to improve freedom and privacy. Organizers are seeking suggestions for speakers, topics, workshops, tutorials, and panel sessions. The proposals should take advantage of the location of the conference, include a diverse set of panelists and new voices, offer a number of perspectives on challenging issues, and explore cutting-edge technology, legal, and policy issues. Possible topics include social networks, cloud computing, surveillance networks, anonymity in a networked world, ethics and computing, accessibility, open source, and media concentration, advertising, and political campaigning on the Internet. The final program will be assembled partly from the proposals. The early bird deadline for proposals is Dec. 1, 2009, and the final deadline is Jan. 31, 2010. <http://usacm.acm.org/usacm/weblog/index.php?p=3D749#more-749>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 83

Friday 6 November 2009

Contents

- ["Jimmy Carter era" computer causes traffic jams](#)
[Jeremy Epstein](#)
- [Central Traffic unControl === gridlock](#)
[David Lesher](#)
- [Washington Metro system communications depend on single data center](#)
[Jon Eisenberg](#)
- [T-Mobile suffers major outage: nationwide or nearly so](#)
[Lauren Weinstein](#)
- [File share leaks data on US Congress members under investigation](#)
[Jeremy Epstein](#)
[PGN](#)
- [Fugitive caught via Facebook updates](#)
[Mark Brader](#)
- [Facebook 'Suggests Contacting Dead Friends'](#)
[Matthew Kruk](#)
- [Massive Gene Database Planned in California](#)
[David Talbot via Jim Schindler](#)
- [Drivers ticketed for not speaking English - misapplication of UI](#)
[Frank Jimenez](#)
- [Privacy of health care info & health insurers](#)
[Henry Baker](#)
- [Spam forged from .gov and .mil](#)
[PGN](#)
- [AMEX sends USB trojan keyboards in ads](#)
[David Lesher](#)
- [Risks of Using Encryption](#)
[Roger Grimes via Gene Wirchenko](#)
- ['Robot' computer to mark English essays](#)
[Polly Curtis via Randall](#)
- [Is Net Neutrality a Communist Plot? "Declassified DoD Film"](#)
[Lauren Weinstein](#)
- [Speaking of cable modem insecurity](#)
[Danny Burstein](#)
- [Re: Toyota uncontrolled acceleration](#)
[Anton Ertl](#)

[Matt Roberds](#)

• [Re: Danger and Paris Hilton](#)

[Peter Houppermans](#)

• [Info on RISKS \(comp.risks\)](#)

✂ "Jimmy Carter era" computer causes traffic jams

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Thu, 5 Nov 2009 06:44:46 -0500

4 Nov 2009. A "Jimmy Carter era" computer that controls traffic light timing in Montgomery County, Maryland (suburban Washington DC) failed, which meant that traffic lights throughout the county stopped being timed properly (i.e., to allow more green southbound in the mornings and northbound in the evenings). Setting 750 traffic lights by hand each morning and evening is ineffective.

I don't know what the article means by a Jimmy Carter era computer (other than presumably something purchased in the late 1970s), but it's fair to say that finding replacement parts for whatever went wrong isn't easy. And for those young'uns on the list, computers in that era weren't a single chip or a single board - the CPU alone probably fills several 6' (1.8 meter) tall cabinets, with discrete components and wires. Troubleshooting requires lots of training and intuition, not something you can pick up from a book...

The computer had been scheduled for replacement. Hopefully not by a Windows box that decides to reboot itself at inconvenient times....

The RISK, I'm guessing, is of being so reliant on a piece of hardware that can't be readily repaired (with no backup).

<http://www.washingtonpost.com/wp-dyn/content/article/2009/11/04/AR2009110402413.html>

✂ Central Traffic unControl === gridlock

"David Leshner" <wb8foz@panix.com>

Thu, 5 Nov 2009 15:40:25 -0500 (EST)

Montgomery County MD, north of DC, has an extensive network of traffic controls including cameras on hundreds to thousands of traffic signals. (Those cameras are allegedly for motion sensing only but I have no proof of that; mission creep seems obvious...)

They have their own fiber backbone to interconnect all this with one central computer. It failed, and thus far they have not been able to restart it. As a result, the signals have all reverted to autonomous local operation, and traffic is a major mess. [This is a region where normal rush hours runs from 0530-0930, and 1500-1900...]

RISK:

While they HAVE fallback control; [bravo..] here it is not all that is needed. Gridlock for several days will not win any votes.

Traffic signals disrupted, creating chaos in Montgomery - washingtonpost.com

<http://www.washingtonpost.com/wp-dyn/content/article/2009/11/04/AR2009110402413.html>

Washington Metro system communications depend on single data center

"Jon Eisenberg" <JEisenbe@nas.edu>

Wed, 4 Nov 2009 08:55:42 -0500

-- power failure causes multiple problems

<http://www.washingtonpost.com/wp-dyn/content/article/2009/11/04/AR2009110401104.html?hpid=newswell>

Jon Eisenberg, Director, Computer Science and Telecommunications Board,
The National Academies

T-Mobile suffers major outage: nationwide or nearly so?

Lauren Weinstein <lauren@vortex.com>

Tue, 3 Nov 2009 17:23:42 -0800

NNSquad - Network Neutrality Squad <nnsquad.nnsquad.org>

T-Mobile suffered a major outage today. The exact scale is still unclear, but clearly various areas around the U.S. were affected, including voice, data, and SMS. Service currently appears to be completely up here in my area of L.A., though I haven't tried to use T-M in several hours and could have missed any outage (Update: user reports on the T-M discussion forum do indicate that L.A. was down at some point -- for up to four hours).

Anecdotal reports suggest that service has been restored in some areas but not necessarily for all of voice/data/SMS, and that in some areas voice calls were disrupted but 3G data continued working throughout the outage.

Obviously some failure of their backbone network and/or authentication services. More to come.

One other point for now. AP is reporting that they were unable to reach the cell phones of various T-Mobile media spokespersons, because calls to those cell phones couldn't complete ... due to the T-Mobile outage itself.

A lesson re network diversity, it seems.

✂ File share leaks data on US Congress members under investigation

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Fri, 30 Oct 2009 13:54:08 -0400

The Washington Post's Oct 30 lead article notes that "more than 30 lawmakers and several aides" are under investigation for various possible misdeeds associated with "defense lobbying and corporate influence peddling".

What's technology relevant is that the information leaked because a report was (presumably accidentally) placed on an unprotected computer (not clear whether it was a web site, a file share, or something else). No word on whether the problem was a misconfiguration (i.e., mis-set file permissions, whether accidentally or intentionally) or due to a bug in software that allowed bypassing protections.

No indication that the data was encrypted... perhaps this is an opportunity for Congress to learn the need for more usable security systems, including encryption, to reduce the RISK of accidental sharing?

<http://www.washingtonpost.com/wp-dyn/content/article/2009/10/29/AR2009102904597.html?hpid=topnews>

✂ Re: File share leaks data on US Congress members under investigation

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

Fri, 30 Oct 2009 13:44:58 PDT

Congressional investigation kimono opened? Some not-so-senior Congressional employee working from home with peer-to-peer file sharing software apparently blew the security on the ongoing internal congressional investigations.

<http://www.comcast.net/articles/news-politics/20091030/US.Congress.Leaked.Ethics.Report/>

✂ Fugitive caught via Facebook updates

Mark Brader

Sat, 24 Oct 2009 16:04:04 -0400 (EDT)

Maxi Sopo was living in Cancun, and allegedly living high on the proceeds of bank fraud in the US. He maintained a Facebook entry under his own name. His status was public, but his profile was only accessible to his Facebook "friends" -- but one of them was a former US Department of Justice official.

Story at:

<http://news.bbc.co.uk/2/hi/americas/8306032.stm>

<http://www.guardian.co.uk/technology/2009/oct/14/mexico-fugitive-facebook-arrest>

Commentary and discussion at:

http://www.schneier.com/blog/archives/2009/10/helpful_hint_fo.html

Facebook 'Suggests Contacting Dead Friends'

"Matthew Kruk" <mkruk@gmail.com>

Mon, 26 Oct 2009 11:28:49 -0600

<http://news.sky.com/skynews/Home/Technology/Facebook-Changes-Upset-Users-Reconnect-Feature-Suggests-Dead-Friends/Article/200910415417724>

Facebook 'Suggests Contacting Dead Friends'

12:51pm UK, Monday October 26, 2009

Ruth Barnett, Sky News Online

Facebook's latest revamp has upset some members by recommending they get in touch with friends who have died. The social networking site, which is used by 300 million people worldwide, made the controversial changes at the weekend.

One of the most prominent additions is an automatically-generated box suggesting the user "reconnect" with a specific person they have not contacted for a while. But within hours, dozens of users reported feeling distressed when the new feature told them to get in touch with someone deceased.

More than 900,000 have reacted against the changes by joining a group calling for the site to go "back to normal". "Facebook just suggested that I reconnect with someone who passed away two years ago. That's messed up," one person wrote on Twitter. Another user, Emma, 27, was confronted by the image of a deceased friend when she logged into the site at the weekend. "Like many of his friends I haven't deleted his profile as that would feel weird. I'm sure thousands of Facebook users are in the same position," she told Sky News Online. "When someone dies there doesn't seem to be much you can do about their profile. It would be nice to keep it as a memorial but there is no way of acknowledging what has happened to that person. "There should be a way of recognising this on their profile or Facebook should remove the feature altogether to avoid causing offence."

Facebook does offer a "memorialisation" option and invite users to alert them to a death but it is not widely known or publicised.

The glitch reveals the "insensitivity of the algorithm," according to Mashable blogger Pete Cashmore. He also found examples of the site suggesting ex husbands and wives. "Facebook is investigating the situation," a spokeswoman for the site told Sky News Online.

Massive Gene Database Planned in California (David Talbot)

Jim Schindler <jimschin@gmail.com>

Tue, 20 Oct 2009 21:30:00 -0800

David Talbot, Massive Gene Database Planned in California; The data will be compared against electronic health records and patients' personal information. *Technology Review*, 21 Oct 2009
www.technologyreview.com/biomedicine/23777/?nlid=2446

Plans for genetic analyses of 100,000 older Californians--the first time genetic data will be generated for such a large and diverse group--will accelerate research into environmental and genetic causes of disease, researchers say.

"This is a force multiplier with respect to genome-wide association studies," says Cathy Schaefer, a research executive at Kaiser Permanente <<http://www.kaiserpermanente.org/>>, a health-care provider based in Oakland, CA, whose patients will be involved. Researchers will be able to study the data and seek insights into the interplay between genes, the environment, and disease, thanks to access to detailed electronic health records, patient surveys, and even records of environmental conditions where the patients live and work. "The importance of this project is that it will, almost overnight--well, in two years--produce a very large amount of genetic and phenotypic data that a large number of investigators and scientists can begin asking questions of, rather than having to gather data first," Schaefer says.

The effort will make use of existing saliva samples taken from California patients, whose average age is 65. Their DNA will be analyzed for 700,000 genetic variations called single-nucleotide polymorphisms, or SNPs, using array analysis technology from Affymetrix in Santa Clara, CA. Through the National Institutes of Health (NIH), the resulting information will be available to other researchers, along with a trove of patient data including patients' Kaiser Permanente electronic health records, information about the air and water quality in their neighborhoods, and surveys about their lifestyles.

The result will be the largest genetic health research platform of its kind, says Schaefer, who directs Kaiser Permanente's research program on genes, the environment, and health. The study is being undertaken together with the University of California, San Francisco (UCSF), with a \$25 million, two-year NIH grant that tapped federal stimulus funds allocated earlier this year.

The potential for study is nearly limitless. Researchers will likely seek the genetic influences that determine why some people suffering from, say, cardiovascular disease and type 2 diabetes deteriorate more rapidly than others; and tease out which genetic factors reduce the effectiveness of various drugs or, indeed, make them hazardous, Schaefer says. As doctors obtain more such insights, this will allow them to tailor drug regimens and focus resources on higher-risk patients.

Given the high average age of the group, the platform will also be a boon to studying diseases of aging. "One might want to ask," Schaefer says, "what

are the genetic influences on changes in blood pressure as people age, and how are those changes in blood pressure related to diseases of aging, like stroke and Alzheimer's and other cardiovascular diseases?"

✂ Drivers ticketed for not speaking English - misapplication of UI

*"Frank Jimenez (franjime)" <franjime@cisco.com>
Sat, 24 Oct 2009 09:20:10 -0700*

Apparently, in the USA, there is a Federal Law requiring holders of commercial driving licenses to speak English. However, the user interface for citations in the Dallas Police Department also made this option available when citing drivers of private vehicles. Recently, a particular case was publicized in the local media, and it was later discovered that 38 tickets had been issued improperly to non-commercial drivers. The risk here is the ability to choose an option from a drop-down box that doesn't actually apply to a particular law enforcement situation.

More details here:

<http://www.nbcdfw.com/news/local-beat/Dallas-Cop-Cites-Driver-for-Not-Speaking-English-65793662.html>

✂ Privacy of health care info & health insurers

*Henry Baker <hbaker1@pipeline.com>
Thu, 29 Oct 2009 13:02:24 -0700*

Since Congress & various states passed laws to protect our health info from being sold to drug companies, we thought our mail boxes would be safe from spam advertisements targeted to us on the basis of our health information.

Apparently we were wrong.

The drug companies are now paying our health insurers to send out advertisements for their drugs to us on the basis of our health insurance information.

I recently received an advertisement from my insurance company for a shingles drug which costs a bundle just for the copay.

In the letter accompanying this advertisement:

"The development and distribution of these materials is supported by Merck & Co., Inc."

The letter included a phone number to be dropped from the distribution of these advertisements.

I think that this letter indicates whose pocket "our" health insurer is in, and it isn't ours, the customer/taxpayer.

Spam forged from .gov and .mil

*"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 27 Oct 2009 13:56:12 PDT*

Recent "FDIC" spam messages were forged to appear to be sent from fdic.gov. In the past, spammers have steered clear of forging their messages from ".gov" and ".mil" addresses due to the associated legal consequences if they were caught and prosecuted. As a result, SRI is now spam-filtering .gov and .mil. [PGN-ed from an SRI facilities message.]

AMEX sends USB trojan keyboards in ads

*David Leshner <wb8foz@panix.com>
Tue, 27 Oct 2009 01:14:59 -0400*

A fellow user group member reported getting a USB-fob from American Express. When he plugged in to a port, it attempted to send his xterm command line to [HTTP://VCGW.NET/.../...](http://VCGW.NET/.../...) {the dots were hex digits, it appears.... [and PGN changed x to dot to avoid filtering]} but didn't succeed. [It may be Windows and Mac compatible, but not Linux...]

That address redirects to an Amex URL: <https://www201.americanexpress.com/>

It identified itself on the USB chain as:

```
Bus 003 Device 003: ID 05ac:020b Apple, Inc. Pro Keyboard  
[Mitsumi, A1048/US layout]
```

Since it's clearly NOT an Apple Pro Keyboard; one wonders why the manufacturer <http://www.ikyp.com> chose that false identity. The masquerade as a keyboard might also have been to penetrate those machines that do not blindly mount USB storage devices.

Risks:

While we now look for incoming malware on the TCP/IP connections, clearly we need to similarly monitor the other ports as well; you can do just as much damage (or more) with a insider keyboard attack, given some social engineering. Is the power line next?

[I'm somewhat reminded of the DOS era story of a voice recognition product demo where someone in the audience yelled "FORMAT C:" and "YES"....]

This is tangential:

<http://www.digitalsociety.org/2009/08/apple-keyboards-hacked-and-possessed/>

✂ Risks of Using Encryption (Roger Grimes)

Gene Wirchenko <genew@ocis.net>

Fri, 23 Oct 2009 14:49:32 -0700

Roger Grimes had an interesting column on security recently:

http://www.infoworld.com/d/security-central/dont-trust-public-pc-your-digital-identity-126?source=IFWNLE_nlt_daily_2009-10-23

Excerpt of particular interest:

"Similarly, I need the recipient's public key so that I can send him or her encrypted content. We should never share private keys. That's why they are called private. Pretty simple -- or so you would think. More often than not, if the person isn't overly familiar with PGP/SMIME, even if they've been using it, they send me their private key.

Being the good citizen that I am, I delete their private key and ask again for their public key, explaining that with their private key, I could be them, for all digital purposes. About half the newly educated group then sends back my public key back or, if they're using PGP, their private key ring, which contains all their private keys. You might think that I'm making this stuff up, but it's pretty much been this way with PKI and PGP exchanges since they were invented. PGP's own Phil Zimmerman has often written on this subject."

✂ 'Robot' computer to mark English essays (Polly Curtis)

Randall Webmail <rvh40@insightbb.com>

October 23, 2009 11:04:18 EDT

[From Dave Farber's IP, johnmac, ...]

[I guess it's not so different from using grad students: autograding. RVH]

'Robot' computer to mark English essays
Exam board denies system will be extended to GCSEs
Union fears 'a disaster waiting to happen'

The owner of one of England's three major exam boards is to introduce artificial intelligence-based automated marking of English exam essays in the UK from next month. Pearson, the American-based parent company of Edexcel, is to use computers to "read" and assess essays for international English tests in a move that has fueled speculation that GCSEs and A-levels will be next. All three exam boards are now investing heavily in e-assessment but none has yet perfected a form of marking essays using computers -- or "robots" -- that it is willing to use in mainstream exams. Academics and leaders in the teaching profession said that using machines to mark papers would create a "disaster waiting to happen".

[Source: Polly Curtis, *The Guardian*, 25 Sep 2009; PGN-ed]

[IP Archives: <https://www.listbox.com/member/archive/247/=now>]

✂ Is Net Neutrality a Communist Plot? "Declassified DoD Film"

Lauren Weinstein <lauren@vortex.com>

Tue, 27 Oct 2009 14:18:39 -0700

Is Net Neutrality a Communist Plot? ("Declassified DoD Film")

<http://lauren.vortex.com/archive/000627.html>

Greetings. As a strong supporter of Net Neutrality (<http://lauren.vortex.com/archive/000625.html>), I've been increasingly concerned by recent accusations from some anti-neutrality forces and media commentators, who claim that Net Neutrality is actually an insidious and dangerous "communist plot" that must be destroyed at all costs.

Such a characterization has seemed utterly ridiculous to me, and hopefully also to most other reasonable observers.

However, a friend of mine working at a certain "Three-Initial Agency" (that must remain unnamed) recently uncovered a long-lost U.S. government film that appears to shed unexpected light on accusations of a linkage between communist/Marxist ideologies and Net Neutrality.

He managed to get the short film (only a few minutes long) rapidly declassified and shipped it out to me. I've now digitized the 16mm print and brought it online.

The complete film (with associated very brief explanatory text, etc. that I've included) can be viewed at the YouTube link:

Is Net Neutrality a Communist Plot?

<http://www.youtube.com/watch?v=4fCLFKIYW3c>

I must admit, the film certainly had an impact on me!

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org/lauren>

Co-Founder, PFIR <http://www.pfir.org> and NNSquad <http://www.nnsquad.org>

GCTIP Global Coalition for Transparent Internet Performance <http://www.gctip.org>

PRIVACY Forum - <http://www.vortex.com> Lauren's Blog: <http://lauren.vortex.com>

✂ Speaking of cable modem insecurity

danny burstein <dannyb@panix.com>

Fri, 23 Oct 2009 02:08:04 -0400 (EDT)

Chen, founder of a software startup called Pip.io, said he was trying to help a friend change the settings on his cable modem and discovered that

Time Warner had hidden administrative functions from its customers with Javascript code. By simply disabling Javascript in his browser, he was able to see those functions, which included a tool to dump the router's configuration file.

That file, it turned out, included the administrative login and password in cleartext. Chen investigated and found the same login and password could access the admin panels for every router in the SMC8014 series on Time Warner's network - a grave vulnerability, given that the routers also expose their web interfaces to the public-facing Internet.

All of this means that a hacker who wanted to target a specific router and change its settings could access a customer's admin panel from anywhere on the net through a web browser, log in with the master password, and then start tinkering. Among the possibilities, the intruder could alter the router's DNS settings - for example, to redirect the customer's browser to malicious websites - or change the Wi-Fi settings to open the user's home network to the neighbors.

Re: Toyota uncontrolled acceleration (Leshner, [Risks 25.82](#))

Anton Ertl

Sun, 25 Oct 2009 19:59:04 GMT

Motorcycles in Austria and Germany (and maybe other places) are equipped with kill switches that can be easily reached, in addition to having an ignition key. Given the number of incidents with runaway cars one reads about, maybe that should be a required feature of cars, too (even with a traditional ignition key, there is the risk of activating the steering lock when shutting off the engine with it).

On one of my first rides with my motorcycle, the engine tried to run away (probably a mechanical thing, few or no computers on that 1986 motorcycle) which created a few moments of horror, but then I pulled the clutch and activated the kill switch, and had everything under control.

M. Anton Ertl <http://www.complang.tuwien.ac.at/anton/home.html>

Re: Toyota uncontrolled acceleration (David Leshner, [RISKS-25.82](#))

Matt Roberds <mroberds@att.net>

Mon, 26 Oct 2009 22:50:50 -0500 (CDT)

The brake performance of new cars sold in the US since about 2000 is regulated by Federal Motor Vehicle Safety Standard 135, 49 CFR 571.135. (Previously it was FMVSS 105. The analogous Canadian standards are CMVSS 135 and CMVSS 105.) The US standards can be navigated to from <http://www.gpoaccess.gov/ecfr/>; a very quick read of FMVSS 135 doesn't show any tests that are supposed to be done with the throttle open during the

test. There **are** tests that are done with the vehicle loaded to its maximum weight rating, both with the braking system intact and with various failures present.

An acquaintance of mine has worked for various car manufacturers and has described doing brake tests that seem to be in excess of the federal requirements, such as testing a fully loaded vehicle descending a mountain in Colorado. To the best of my recollection, however, these were also done with the throttle closed.

Several of the other FMVSSs touch various aspects of the user interface of a car, including at least 101, 102, 114, and 124. 114 does cover the possibility of using something other than a physical key, but does not specify too much about its behavior. This may be a case where the available products are outpacing the regulations.

✉ Re: Danger and Paris Hilton (Re: [Risks 25.82](#), Danger-ous services)

*Peter Houppermans <peter@houppermans.com>
Wed, 21 Oct 2009 22:34:32 +0200*

* I consider it unlikely that Paris Hilton would call tech support - that's what you have assistants for.

* I'm amazed nobody commented on the irony of a Microsoft company asking people NOT to reboot :-).



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 84

Weds 25 November 2009

Contents

- [Apostrophe in Your Name? You Can't Fly!](#)
[Chris J Brady](#)
- [NY area bank claws back over 50,000 pension payments](#)
[Danny Burstein](#)
- [Hacking ring steals \\$9 million from ATMs globally](#)
[Gadi Evron](#)
- [Teleportation via Skyhook](#)
[Jerry Leichter](#)
- [Warren Buffett cell phone skills: did they doom Lehman?](#)
[jidanni](#)
- [Two Are Charged With Helping Madoff Falsify Records](#)
[Robert Schaefer](#)
- [Brevity of text message leads to rumor of death](#)
[Mark Brader](#)
- [Nasty iPhone Worm Hints at the Future](#)
[Robert Lemos via Jim Schindler](#)
- [Australian Emergency operator hangs up; no street address](#)
[Darryl Smith](#)
- ["Your smart meter is watching"](#)
[Cavoukian-Polonetsky via David Magda](#)
- [Failure begets failure?](#)
[Aahz](#)
- [At Checkout, More Ways to Avoid Cash or Plastic](#)
[Matthew Kruk](#)
- [Mafia Wars CEO Brags About Scamming Users From Day One](#)
[Matthew Kruk](#)
- [NY State Proposing Laws to Restrict Trucker Use of GPS](#)
[jidanni](#)
- [Re: Jimmy Carter era" computer causes traffic jams](#)
[JosephKK](#)
- [Re: Drivers ticketed for not speaking English](#)
[Jerry Leichter](#)
- [REVIEW: "Security and Usability", Lorrie Faith Cranor/Simson Garfinkel](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

✂ Apostrophe in Your Name? You Can't Fly!

Chris J Brady <chrisjbrady@yahoo.com>

Tue, 10 Nov 2009 14:36:56 -0800 (PST)

This is the stuff of nightmares - not to mention enormous frustration and possible stomach ulcers. If you have an apostrophe in your name - like many of Irish descent do - you may find it impossible to board an airplane in the coming months. Why? Because airline computers can't print an apostrophe on the boarding pass, the name on your boarding pass will not exactly match the name on your driver's license or passport. And beginning next year, the two must match or you don't fly. And they call this progress. CJB.

✂ NY area bank claws back over 50,000 pension payments

danny burstein <dannyb@panix.com>

Sat, 7 Nov 2009 07:39:26 -0500 (EST)

- the bank paid the money, then grabbed it back from the accounts. Just like we've all been promised would never, ever, happen...

[UFT press release]

http://www.uft.org/news/bank_error_to_blame_for_withdrawn_pension_payments/

Bank error to blame for withdrawn pension payments

Some 53,000 UFT retirees who rely on electronic pension payments had funds involuntarily withdrawn from their accounts on Nov. 6, causing all sorts of grief for those counting on the money. The Bank of New York Mellon, which is the transferring agent for the funds, erroneously reversed the October benefits payments to retirees paid through electronic fund transfer.

"We're outraged. This is unacceptable," said UFT President Michael Mulgrew. "We have been on top of this since the calls first started coming in early Friday morning and we will continue to work until all of our members have been made whole. Our first priority is to get all of the money back into our members' accounts."

The risks of this happening have been thrashed out before. What disturbs me even more here is that the recipient banks simply allowed this wholesale clawback.

Given the dangers of someone even less scrupulous than this player doing, well, the exact same thing... one would have hoped that part of the banking security profiles on ACH transfers would include "circuit breakers" which would get tripped on any demand of this many accounts.

✂ Hacking ring steals \$9 million from ATMs globally

Gadi Evron <ge@linuxbox.org>

Thu, 19 Nov 2009 12:55:57 +0200

According to an FBI press release, a global ring of hackers broke into an unnamed American credit processing company, stole PIN numbers, manipulated accounts, and proceeded to steal 9 million USD from over 2000 ATM machines world-wide. (They have just been brought to justice.)

http://www.fbi.gov/page2/nov09/atm_111609.html

✂ Teleportation via Skyhook

Jerry Leichter <leichter@lrw.com>

Sun, 22 Nov 2009 22:31:08 -0500

I commute into Manhattan, which suffers from frequent traffic problems. I've been using a combination of technologies to help out: An cell-phone system based modem, one of the little portable WiFi hotspots that will talk to it (so that I have a hotspot in my car), and the iPod Touch map application, which shows Google's maps along with traffic conditions.

Now, the Touch doesn't have a GPS and doesn't talk to cell towers; but it does quite well using technology from a company called Skyhook Wireless. Skyhook builds a database of WiFi networks, and if you're in an area where you can "see" one or more WiFi networks, it can locate you with surprising accuracy. It does make mistakes every once in a while, when very few WiFi signals are visible nearby. This may result in the map jumping around a bit until more data is available.

One day, as I was driving along the west side of Manhattan, the map suddenly changed. A quick glance showed it to be entirely unfamiliar. Since I was stopped at a red light, I was able to stare at the map. Surprise! My Touch thought I had instantly teleported across the Atlantic, and was driving along the Mediterranean coast, not far from Monte Carlo.

A look around me gave a hint to the cause of the problem. I was right next to a large cruise ship. Obvious guess: Such ships provide WiFi services. This one probably happened to be visiting near Monte Carlo when it made it into Skyhook's database. Sure enough, when I had driven a couple of blocks, the map suddenly shifted back to Manhattan.

A friend and I had previously joked about the confusion that would result if I happened to be driving, with my in-car hotspot, just behind a Skyhook mapping van. Well ... it looks as if truth can be stranger than fiction!

✂ Warren Buffett cell phone skills: did they doom Lehman?

<jidanni@jidanni.org>

Sun, 15 Nov 2009 13:29:56 +0800

If Buffett only knew how to retrieve his cell phone messages, the banking crisis might have been averted. True or false?

<http://www.thefirstpost.co.uk/53572,people,news,warren-buffett-the-unheard-voice-mail-that-could-have-saved-lehman-brothers>

Did Warren Buffett's Inability to Check Voice Mail Cause the Recession?

<http://www.switched.com/2009/09/16/did-warren-buffetts-inability-to-check-voice-mail-help-cause-th/>

If Only Warren Buffett Knew How to Work His Cellphone...

<http://swampland.blogs.time.com/2009/09/15/warren-buffett-could-have-saved-lehman/>

Warren Buffett Cell Phone Skills: Did They Doom Lehman?

http://www.huffingtonpost.com/2009/09/16/warren-buffett-cell-phone_n_288594.html

[http://www.ecommerce-](http://www.ecommerce-journal.com/news/18151_lehman_collapse_and_world_crisis_happened_because_buffett_cannot_read_voice_mail)

[journal.com/news/18151_lehman_collapse_and_world_crisis_happened_because_buffett_cannot_read_voice_mail](http://www.ecommerce-journal.com/news/18151_lehman_collapse_and_world_crisis_happened_because_buffett_cannot_read_voice_mail)

<http://blogs.wsj.com/deals/2009/09/15/if-buffett-had-checked-his-voicemail-would-lehman-have-survived/>



Robert Schaefer <schaefer_robert@dwc.edu>

Fri, 13 Nov 2009 12:46:44 -0500

Subject: Two Are Charged With Helping Madoff Falsify Records

Two computer programmers who worked for Bernard L. Madoff's investment firm were accused Friday of helping to cover-up the giant Ponzi scheme. for more than for more than 15 years." [*The New York Times*, 13 Nov 2009]

http://www.nytimes.com/2009/11/14/business/14madoff.html?_r=1&hp

Brevity of text message leads to rumor of death

Mark Brader

Fri, 13 Nov 2009 17:15:22 -0500 (EST)

Canadian cabinet minister John Baird texted a friend to say that his cat had died. But it was thought he meant Margaret Thatcher, who the cat was named after...

<http://news.bbc.co.uk/2/hi/americas/8358544.stm>

<http://www.guardian.co.uk/world/2009/nov/13/thatcher-cat-death-canada>

[And twitter was the cat's bird friend? PGN]

#Nasty iPhone Worm Hints at the Future (Robert Lemos)

Jim Schindler <jimschin@gmail.com>

Tue, 24 Nov 2009 22:44:05 -0800

Robert Lemos, *Technology Review*, 25 Nov 2009

As smart phones become smarter, malicious code will find a friendlier home.

<http://www.technologyreview.com/communications/24011/?nlid=2555&a=f>

As mobile phones get more powerful, the threat of serious attacks against such devices increases, security experts warn. This week, cybercriminals moved closer to proving this point--exploiting a weakness in modified iPhones to spread a worm programmed to steal banking information. Some experts say the worm may be a sign that criminals are getting more savvy about hacking mobile devices.

Last Saturday, researchers at several security firms reported that the new worm, dubbed "Ikee.B" or "Duh," spreads using the default password for an application that can be installed on modified versions of the iPhone. Once the device has been compromised, the worm grabs text messages, and searches for banking authorization codes used by at least one bank, before sending the codes to a central server. Earlier this month, another iPhone worm was released. It exploited the same password weakness to spread itself, but did not try to steal personal information.

"The banking [attack] is new to mobile devices," says Chet Wisniewski, a senior security advisor at antivirus firm Sophos. "It goes through your phone, grabbing all your text messages, and sends them off to a server in Lithuania."

Since the attack affects only the small number of iPhones that have been "jail broken"--modified to run nonapproved software--the worm will likely inconvenience only a few people. Yet some researchers say the worm confirms that attacks against mobile users are evolving, and that cybercriminals are targeting the personal and financial information kept on portable devices. The ability to communicate with a central command-and-control server--a characteristic more commonly associated with hijacked PCs--also makes such software more dangerous.

This past summer, at the Black Hat Security Briefings conference in Las Vegas, Charlie Miller, a consultant with Independent Security Evaluators, demonstrated a way to remotely attack iPhones using the short message service (SMS) protocol<<http://www.technologyreview.com/blog/unsafebits/23957/>>. Miller says it's only a matter of time before cybercriminals find a way to infect phones that haven't been jail broken, vastly increasing the potential scale of an infection. "A [more serious] worm against an iPhone or any other mobile device is going to happen," Miller says. "It is going to happen to [Google's] Android and iPhone and everything else. As more bad guys do research into the mobile platforms, these devices are going to get attacked."

The evolution of the Ikee.B or Duh worm can be traced back to early attacks

against mobile devices. In 2000, Timofonica, a relatively simple virus that spread between desktop computers and servers, also had the ability to spam mobile phones in Spain with text messages. In 2004, Cabir, the first mobile-phone-only worm, was released. Cabir could jump automatically between Nokia handsets.

In 2006, researchers at the University of Toronto and Microsoft confirmed that even short-ranged and short-lived Bluetooth connections between phones could, in theory, be used to spread a wireless worm. "Starting a Bluetooth worm outbreak is relatively easy once a vulnerability is found. An attacker can bring an infected device into a typical urban mall and discover many potential victims," the researchers wrote in a related paper.

The iPhone, and other smart phones, are a more attractive target for hackers because they resemble mini PCs. The devices are always connected to the Internet, run third-party applications, and store information that is potentially valuable to cybercriminals.

Normally, however, exploiting the iPhone is not that easy. The new worm employed a weakness introduced by an application called OpenSSH that can be used to connect to the phone remotely. This application uses the default password "alpine," and the worm used this default password to wriggle between handsets.

"This is trivial--there is no shell code, no buffer overflow, nothing," says Miller. "It took me two weeks to write the [code] for the SMS thing, but I could have written [Ikee.B] in, like, five minutes."

The attacks that have targeted the iPhone in the last month have also focused on jail-broken devices. The modification process to jail break a phone removes the code that prevents users from loading whatever applications they want, but also removes much of the security that prevents malicious code from running on the device. "The iPhone has all these layers of defense, but when you jail break your phone, you break every single one of them," Miller says.

The evolution of such hacking will continue, Miller says, although the current crop of iPhone attack code has a long way to go. The new worm does little to hide its activity, for example. And, by sending data over wireless networks, as well as aggressively attempting to infect other phones, the worm also quickly runs down the compromised phone's battery.

"Because the phone is trying to connect all the time, users that get infected with this thing are going to know," says Sophos' Wisniewski.

✂ Australian Emergency operator hangs up; no street address.

*"Darryl Smith" <Darryl@radio-active.net.au>
Thu, 26 Nov 2009 10:30:06 +1100*

From the **Sydney Morning Herald**, 26 Nov 2009

<http://www.smh.com.au/national/triple0-bungle-over-lack-of-street-address--a-gain-20091126-jshb.html>

A man called the emergency line from a remote property near Boomi in far northern NSW. An operator ended the call because Mr Jamieson could not provide a street number. "They said they wanted a house number. I said there's no house number." When what road his property was on, he responded "The Boomi-Goondiwindi Road, they couldn't find Goondiwindi on a map because ... it's in Queensland". An ambulance eventually arrived after he contacted a business next door to the Goondiwindi ambulance service in the next state.

This comes after a 17-year-old became separated from his two classmates on Mount Solitary during a three-day trek in 2006 and died. The inquest found three triple-0 operators bungled a series of calls for help he made to them because they did not have a street address of the rugged bushland.

Darryl Smith, VK2TDS POBox 169 Ingleburn NSW 2565 Australia
Mobile Number 0412 929 634 [+61 4 12 929 634 Int] - 02 9618 645
www.radio-active.net.au/blog/ - www.radio-active.net.au/web/tracking/

[Another problem well known to RISKS readers. PGN]

✈ "Your smart meter is watching"

*David Magda <dmagda@ee.ryerson.ca>
Tue, 17 Nov 2009 18:25:42 -0500*

Ann Cavoukian (Privacy Commissioner of Ontario) and Jules Polonetsky:

- > We must take great care not to sacrifice consumer privacy amid an
- > atmosphere of unbridled enthusiasm for electricity reform. But we need not
- > forfeit one for the other in a zero-sum manner; we can adopt a
- > positive-sum approach, where both interests may prevail. Information
- > proliferation, lax controls and insufficient oversight of this information
- > could lead to unprecedented invasions of consumer privacy. Intimate
- > details of individual hydro customers' habits, from when they eat, when
- > they shower, to when they go to bed, plus such security issues as whether
- > they have an alarm system engaged, could all be discerned by the data,
- > automatically fed by appliances and other devices, to the companies
- > providing electric power to our homes.

<http://www.thestar.com/comment/article/726528>

They have also released a white paper entitled "SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation" detailing the issue:

<http://tinyurl.com/ye2kjl>

<http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=912>



Aahz <aahz@pythoncraft.com>
Sat, 21 Nov 2009 11:32:05 -0800

Subject: Failure begets failure?

I've been having a number of problems with the Hyatt hotel chain lately, and I'm excerpting the bits that I think would be of interest to RISKS readers (mostly the ones that represent failure in communication and computer use), none of which is particularly surprising, although having the entire sequence is somewhat surprising to me.

What I'm curious about, particularly from a RISKS perspective, is the likelihood that any given customer having experienced problems with an organization makes it more likely that the same customer will experience additional problems. Anyone know of research in this area? This is related to e.g. problems in aviation and computer servers -- how likely are cascading failures? Can/should we use the first failure as a harbinger of future failures?

I mean, although my experiences with Hyatt are such that calling them incompetent would be high praise, they clearly can't be causing this many problems for other customers or they'd be out of business.

Here's the redacted list:

- * Failing to provide free Internet at Hyatt Santa Clara (California) despite group contract specifying it (5/2008)

- * Refusing to refund a damage deposit until I dispute the charge with my credit card company (Hyatt Santa Clara, 5/2009 - 7/2009)

The next series of incidents started when the Hyatt Summerfield Suites in Belmont, California was unable to give us a room because some other guests trashed their rooms; the Summerfield sent us to the Hyatt SFO.

- * Informing me only by telephone about the new arrangement despite making the reservation on-line (although this is par for the course for pretty much all idiot companies) -- I'm hearing-impaired, so this issue is particularly important to me, but I know plenty of people who hate using the phone

- * Although this is supposed to be a free room with breakfast (to compensate for switching hotels), they charge my credit card for parking, Internet, and room service (\$60!)

- * They later reverse the charge without informing me; I only notice this on my credit card bill

- * Changing the name on my Hyatt account without asking me

- * When I complain about the name change, they claim that they have no record of a name-change on my account (they are obviously either lying or incompetent because they sent me an automated e-mail when my name was

changed)

In addition, the Hyatt web site uses HTTP for account login instead of HTTPS/SSL, so they clearly don't care about security.

Aahz (aahz@pythoncraft.com) <http://www.pythoncraft.com/>

At Checkout, More Ways to Avoid Cash or Plastic

"Matthew Kruk" <mkruk@gmail.com>

Mon, 16 Nov 2009 23:36:59 -0700

<http://www.nytimes.com/2009/11/16/technology/start-ups/16wallet.html>

Claire Cain Miller, At Checkout, More Ways to Avoid Cash or Plastic,
The New York Times, 16 Nov 2009

For almost as long as Americans have been hearing about jetpacks and picturephones, they have been hearing that money - bills, coins and plastic cards - might cease to exist, or at least become a novelty.

Instead of leather wallets, consumers could, sooner than they think, carry virtual wallets, with their credit card and bank information stored on remote computers that are accessible everywhere and anytime. They could use them whenever they want to buy something, whether on the Web, on cellphones or at cash registers.

With a new cellphone application called ShopSavvy, for instance, a shopper can use the phone's camera to scan an item's bar code in a store to see if it is available for less online. If so, the shopper can buy it with one click if they have already entered their credit card and shipping information on PayPal's Web site.

"What we're trying to do and what we think is very important is to displace the use of cash or checks," said Scott Thompson, president of PayPal, which is a leader in digitizing money. "We'll just have one wallet, and it lives in the cloud." ...

There's more ... makes me very uneasy. Electronic pickpockets have perked up their ears ...

[And if you ask for the manager, the checker is likely to say,
"The Head's in the Clouds" or perhaps "The Cloud is in the Head." PGN]

Mafia Wars CEO Brags About Scamming Users From Day One

"Matthew Kruk" <mkruk@gmail.com>

Mon, 16 Nov 2009 23:31:12 -0700

<http://consumerist.com/5400720/mafia-wars-ceo-brags-about-scamming-users-from-day-one>
<http://tinyurl.com/ycpkrzd>

"From the beginning, the profitability and viability of popular Facebook social networking games Mafia Wars and Farmville were predicated on the backs of scams, boasts Zynga CEO Mark Pincus in this video. "I did every horrible thing in the book just to get revenues," he crows in the clip to a gathered bunch of fellow scumbag app developers." ...

NY State Proposing Laws to Restrict Trucker Use of GPS

<jidanni@jidanni.org>

Sun, 15 Nov 2009 04:22:17 +0800

AP item, 14 Oct, 2009: New York State wants to crack down on truckers who rely on satellite devices to direct them onto faster but prohibited routes and end up crashing into overpasses that are too low for their rigs.

Gov. David Paterson proposed penalties including jail time and confiscation of trucks to come down on drivers who use GPS - global positioning systems - to take more hazardous routes and end up striking bridges.

<http://www.dailymail.com/ap/ApTopStories/200910141133>

Re: Jimmy Carter era" computer causes traffic jams (RISKS-25.83)

"JosephKK" <quiettechblue@yahoo.com>

Sun, 15 Nov 2009 18:25:54 -0800

> Troubleshooting requires lots of training and intuition, not something
> you can pick up from a book...

Like hell. I started in computers in 1971 and only a few antiques took more than four shelves in a 36 inch cabinet for the CPU proper. By 1974 the whole thing including I/O adapter was below 22" by 22" by 48" and did about 1 32bit (VAX) mips. Moreover these were military ruggedized types. And the training required was weeks. Straightforward as hell. And the basic implementation was bit slice to boot. For that matter so was the previous generation, just not quite so obviously. Ref (CP1303/AN-UYK7 {32bit} and CP-642B/AN-UYK4 {30 bit})

Re: Drivers ticketed for not speaking English (Jiminez, R 25 83)

Jerry Leichter <leichter@lrw.com>

Sun, 22 Nov 2009 23:25:39 -0500

In [RISKS-25.83](#), Frank Jimenez reports on that the Dallas Police Department

has issued at least 38 tickets citing drivers for an inability to speak English. There is, in fact, no such requirement - except for commercial drivers. Jimenez concludes: "The risk here is the ability to choose an option from a drop-down box that doesn't actually apply to a particular law enforcement situation."

Is it really? Do we really want a computer system involved in deciding whether a particular law is applicable in a given situation or not? We're not talking about some simple UI to a billing program where it's trivial to determine which options make sense.

Police are expected to understand the law. It's part of the job description. They are human and humans make mistakes; that's why we have courts and appeals courts beyond them. But a policeman who doesn't get the law right in the vast majority of situations shouldn't be wearing a badge.

Paper tickets include space for many possible violations, only a few of which may be relevant in any given circumstance. Based on all history of computerization as we've seen it here, do we really think that replacing that piece of paper with a "smart" program that somehow decides with violations are relevant will improve things? Or is it more likely to lead to a spate of other stories in which police are unable to issue tickets because the computer fails to bring up the right option; or, even worse, are led to ignore their own knowledge and judgement and charge things incorrectly because "the computer said this was the right charge"?

REVIEW: "Security and Usability", Lorrie Faith Cranor/Simson Garfinkel

*Rob Slade <rMslade@shaw.ca>
Tue, 17 Nov 2009 14:06:04 -0800*

BKSECUSA.RVW 20090727

"Security and Usability", Lorrie Faith Cranor/Simson Garfinkel, 2005,
0-596-00827-9, U\$44.95/C\$62.95

%E Lorrie Faith Cranor

%E Simson Garfinkel

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 2005

%G 0-596-00827-9

%I O'Reilly & Associates, Inc.

%O U\$44.95/C\$62.95 800-998-9938 fax: 707-829-0104 nuts@ora.com

%O <http://www.amazon.com/exec/obidos/ASIN/0596008279/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0596008279/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0596008279/robsladesin03-20>

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

%P 714 p.

%T "Security and Usability"

The editors state that they intended this collection of essays more to address the academic, than the practical, side of the security field. Thus,

the papers are chosen to reflect theory and principle, rather than specific practice. A prudent choice, since theory dates less quickly than specific procedure.

The thirty-four compositions in this work are divided into six sections. Part one states that security and usability are not antithetical, part two addresses authentication mechanisms and techniques, part three examines how system software can contribute to security, part four deals with privacy controls, part five examines the vendor perspective of provision of security, while part six finishes off the book with a few papers considered to be of lasting value.

The papers contain interesting points, but sometimes both theoretical and practical utility are lacking. For example the first paper, entitled "Psychological Acceptability Revisited," challenges the idea that security mechanisms must be complex and difficult to use in order to be effective. Unfortunately, while the author clearly demonstrates that a system can be both insecure and useless, he does not prove the opposite, which is the condition we want. A good many papers simply state that human factors should be considered, and that security provisions should be usable: these points are true, but not helpful. With one exception (a good paper on password choice) all the pieces on authentication present research having nothing to do with usability. Most of the papers in the book describe security research that is interesting, and which frequently has relations with human factors, but the relevance to the provision of systems that are both usable and secure is not often clear.

Even as a compilation of security bedtime reading, the essays collected in this volume are somewhat lacking. In terms of both principles and practice, any volume of the "Information Security Management Handbook" (cf. BKINSCMH.RVW) has superior selection, and better structure, as well.

copyright Robert M. Slade, 2009 rslade@vcn.bc.ca rslade@computercrime.org
victoria.tc.ca/techrev/rms.htm blog.isc2.org/isc2_blog/slade/index.html



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 85

Saturday 28 November 2009

Contents

- [London's stock exchange crashes again](#)
[John Oates](#) via [Kevin Pacheco](#)
- [Your wallet in the cloud](#)
[Martin Ward](#)
- [Used ATM Machines for Sale on Craigslist](#)
[Ben Moore](#)
- [The Joy of satellite navigation failures](#)
[Steve Loughran](#)
- [Re: Toyota Toyota uncontrolled acceleration](#)
[David Leshner](#)
[JC Cantrell](#)
- [Patients' data used as Packing \(Robert](#)
[Bob\) Waixel](#)
- [Re: Apostrophe in Your Name? You Can't Fly!](#)
[Andy Behrens](#)
[JosephKK](#)
[Dag-Erling_Smørgrav](#)
[Bob Frankston](#)
- [Re: Warren Buffett cell phone skills: did they doom Lehman?](#)
[Curt Sampson](#)
[Henry Baker](#)
- [Re: Teleportation via Skyhook](#)
[Charles Wood](#)
- [Android Mythbusters](#)
[Matt Porter](#) via [jidanni](#)
- [Solving the Android "Graved Out Application" Deadlock](#)
[Lauren Weinstein](#)
- [Info on RISKS \(comp.risks\)](#)

✉ London's stock exchange crashes again (John Oates)

Kevin Pacheco <kevinpacheco@gmail.com>

Thu, 26 Nov 2009 18:17:57 +0000

John Oates, Who's to blame this time? *The Register*, 26 Nov 2009

The London Stock Exchange has suffered yet another systems crash, leaving brokers high and dry since 9.30 this morning. The Exchange last went down in September 2008 and took almost the entire day to get back online. That outage, on one of the Exchange's busiest days, was the day after the \$200bn bailout of US housing giants Freddie Mac and Fannie Mae, leading to lots of conspiracy theories. [It resumed operation at 14.00.]

http://www.theregister.co.uk/2008/09/08/lse_down/

<http://www.londonstockexchange.com/global/incident/previous-updates.htm>

http://forms.theregister.co.uk/mail_author/?story_url=/2009/11/26/lse_crash_again/

✶Your wallet in the cloud

Martin Ward <martin@gkc.org.uk>

Fri, 27 Nov 2009 11:20:16 +0000

(was: At Checkout, More Ways to Avoid Cash or Plastic)

"What we're trying to do and what we think is very important is to displace the use of cash or checks," said Scott Thompson, president of PayPal, "We'll just have one wallet, and it lives in the cloud."

The "dream scenario" for any financial institution is to be in the position to take a cut from **every** financial transaction carried out by **every** person in the country. This is why the president of PayPal thinks it is so important to "displace the use of cash or checks."

For the rest of us, this is a nightmare scenario.

If you think it would be bad to have all your data is held hostage in a proprietary format on a machine you have no control over: think what it will be like when **all** your money is controlled by a single organisation which decides (purely on the basis of maximising profit) how big a cut to take out of each and every transaction.

martin@gkc.org.uk <http://www.cse.dmu.ac.uk/~mward/> <http://www.gkc.org.uk>

✶Used ATM Machines for Sale on Craigslist

"Ben Moore" <ben.moore@juno.com>

Thu, 26 Nov 2009 04:49:10 GMT

<http://www.tomsguide.com/us/ATM-Hackers-Credit-Card-numbers,news-5203.html>

Used ATM machines are for sale on auction sites, many of which still contain credit card numbers.

Identity theft expert Robert Siciliano is claiming that he bought a used ATM machine on Craigslist for \$750. Apparently, this isn't unusual: he found plenty of machines on both Craigslist and eBay ranging between \$500 and \$2000 USD. However, this particular ATM machine was listed by a bar north of Boston, and contained 1000 credit card numbers.

That's right: the machine wasn't wiped. Siciliano said, in an interesting way, that his "hacker friend" came over with a manual and gutted the machine's eeprom, spilling the 150-foot spread of sensitive data all over the floor. Surprised and excited, Siciliano thus called a "TV producer friend," and now his local FOX affiliate is running a series on ATM hacking and Siciliano's discovery.

Siciliano also said in his report that he was considering a scheme to use the numbers to leech millions from unsuspecting victims, however his wife told him a firm "NO!"

FOX Boston, on the other hand, added that the credit cards stored in the ATM consisted of numbers processed in a four month period. With that said, it's highly likely that many more used ATM machines for sale on eBay, Craigslist, and other auction sites contain credit card numbers, ripe for the picking. Then again, consumers are more susceptible to identity theft thanks to ATM skimming devices sold on the very same auction sites.

So how do you protect yourself from ATM hackers? "By paying attention to your statements," Siciliano said. "Don't use just any ATM. Instead, look for ATMs in more secure locations." He also said to cover your pins when punching them into the keypad on the ATM or within retail stores.

✶ The Joy of satellite navigation failures

*Steve Loughran <steve.loughran@gmail.com>
Fri, 27 Nov 2009 12:44:36 +0000*

Part of BMW's new "Joy" marketing campaign includes one on GPS, that claims that if "Joy" does get lost, GPS will get it home again.

<http://tinyurl.com/yf98b2e>

As any reader RISKS readers will know, that is not always the case, so it is a shame that vehicle vendors can make this claim in their advertising. Here in the UK, the Advertising Standards Authority does let you complain about adverts making false claims; it is even possible for them to ban adverts.

Accordingly I did actually file a complaint on the the ASA's web site (http://www.asa.org.uk/asa/how_to_complain/complaints_form/). The complaint is attached below, it lists many of the failure modes of GPS as documented on RISKS, and Volpe's 2001 paper discussing the vulnerability to the US transport infrastructure to GPS failures. I was curious to see what the reaction of the ASA/BMW would be.

Last week I got a reply, telling me that:
1. I was the only person that complained

2. It was meant to be metaphor, and therefore the fact that GPS fails is unimportant.

I'm disappointed by this. The more adverts that imply GPS is infallible, the more people believe the claims, the more they drive off cliffs and under bridges too low for their trucks, and the less equipped they are to deal with failures of GPS or the maps themselves.

Yet clearly there is no point for a single individual to complain, because the complaint gets dismissed, without any attempt to consider the technical merits of the argument.

Which means that the myth "GPS doesn't fail" is going to keep on being repeated, while on this list we get to read about more vehicles getting into trouble, yet the root cause -people blindly doing what their satellite navigation devices tell them to do- remains.

I wish to complain about the accuracy of the advert for a BMW X1 which appeared in the Guardian on September 21 2009, an advert which included the statement "On the rare occasion Joy finds itself hopelessly lost, a GPS can guide it back home"

I believe this statement is dangerously misleading as it implies that GPS is something drivers can rely on in emergencies. This is untrue. As a computer scientist I believe it places excessive faith in complex computing infrastructure, and perhaps reflects the copywriter's own lack of awareness of the infrastructure behind GPS satellite navigation, and the risks that the abdication of decision making to computers presents to car drivers, passengers and other road users.

The Navstar Global Positioning Satellite System (GPS) is run by U.S. Air Force Systems Command's Space Division in Los Angeles [1]. A constellation of atomic clocks are in low-earth orbit, continually announcing the location of all the satellites and their local clock's time, the latter compensated for relativity effects so as to appear consistent with atomic clocks on the earth's surface. GPS receivers pick up the signal from three or more satellites, and by comparing the differences in time received, estimate their location on the geode, the ellipse that represents their view of the Earth's surface in their mapping tool's datum. The location of the satellites is calculated in advance by observing the satellites orbits and predicting their future locations, information which must be regularly updated and relayed to the satellites themselves for rebroadcasting.

The time and location data is broadcast on an encrypted "P" signal which can only be decrypted by military receivers, and a civilian "C/A" signal. The civilian signal was made available after the shooting down of the KAL 007 passenger airliner over Soviet Airspace, and receivers for which have become a feature built into cars and mobile phones. It is not digitally signed; there is no way to distinguish a spoof civilian signal publishing invalid information.

In computing circles, there are number of well-known failure modes for GPS. The natural failures are:

1. Geomagnetic storms. Affects all civilian GPS receivers, and magnetic compasses. As well as effecting the signal, the expansion of the atmosphere alters the satellite's orbits, and hence the locations they claim to be at becomes incorrect. [2]

2. "Canyoning", loss of signal while deep inside a natural canyon, or an artificial one (such as street with skyscrapers).

3. Reflected Signal. This is a known problem in Scottish Mountaineering: large cliff faces can reflect GPS signals. The extra delay can result in the receiver's location being misplaced.

4. Accidental interference with GPS from sources including consumer electronics. [3]

5. Loss of signal due to overhead materials. Civilian GPS can be lost in woods and forests, and of course in tunnels, covered car parks and the like there is minimal likelihood that a signal will be picked up.

Note that as no satellites in the GPS constellation orbit at a latitude above 54 degrees N, the risk of canyoning and reflection increases above this point -which means the Lake District and points north, including all of Scotland. From the Lake District up, no GPS satellite will ever be directly above the receiver, they will either be in the south, or near the horizon to the far north, those being the satellites on the other side of the earth becoming visible.

There are also receiver-side software or hardware problems

1. Errors in the maps. These are common and widely documented. Note that such errors effects are invariably amplified by the trust that drivers place in the SatNav units, following them up footpaths and off river banks. To cite one example of this general problem, we would draw attention to a BMW 5 series which recently got stuck on a cliff in Yorkshire when the driver followed the SatNav's instructions to drive down a bridleway. [6]

2. Software errors in the system. This has been discovered on a number of occasions, including in such vehicles as the International Space Station [4].

3. Hardware errors. In the absence of formally verified hardware, the reliability of the underlying microprocessor and other hardware in a GPS receiver cannot be guaranteed.

Finally, the entire GPS infrastructure is vulnerable to malicious attack. This is covered in Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System [5]. This paper by the US Department of Transport, spells out clearly the how vulnerable GPS is.

The author's concerns are of malicious failures, either from local jamming, or "Loss of GPS satellites or the Operational Control Segment" though on the latter they note that "attacking these elements can be more challenging and likely would produce a more aggressive U.S. Government response". Given the report was published, poignantly, on September 10, 2001, we know what a more aggressive response would be.

A key recommendation of the paper is:

"Create awareness among members of the domestic and global transportation community of the need for GPS backup systems or operational procedures, and of the need for operator and user training in transitions from primary to backup systems, and in incident reporting, so that safety can be maintained in the event of loss of GPS"

Given that US Government, the providers of GPS, believe that it constitutes a Single Point of Failure ("SPOF") for land, sea and air travel in the US, it seems unlikely that BMW can state unequivocally that GPS will get their customers out of trouble. All the advertisement does is reinforce the mistaken belief that GPS is reliable, and that the SatNav units' instructions should be followed blindly.

Please can this advert not be printed again, or could its claims be qualified to state that a number of natural and human problems may affect GPS coverage in an area, and that the stored maps cannot be trusted. The US Department of Transport report should act as a foundation for these qualifications. They may also mention that the risks of canyoning, reflection and other problems become more common above 54 degrees north, and therefore that GPS is less trustworthy in Scotland.

A more accurate statement would therefore be

"On the rare occasions that Joy finds itself lost, GPS will guide it home, provided Joy did not get lost in Scotland, or in woodland, the GPS maps are kept up to date, and none of the failure modes outlined in (Volpe 2001) have occurred. In keeping with Volpe's guidelines, should Joy consider getting home to be critical, we recommend gaining familiarity with alternate non-GPS navigation techniques, such as using a printed map in conjunction with a magnetic compass."

Thank you

Citations

1. 2001 GPS SPS Performance Standard Final
<http://www.navcen.uscg.gov/GPS/geninfo/2001SPSPerformanceStandardFINAL.pdf>
2. The Geomagnetic Storm of 13 March 1989. ACM Risks Digest Volume 8 Issue 72
<http://catless.ncl.ac.uk/Risks/8.72.html>
3. Detrimental Effects of Installing Consumer Electronics on Ships, Ken Hamer 1997
<http://www.naval.com/help/emi.html>
4. "Truncation error" found in GPS code on International Space Station ACM Risks Digest Volume 21 Issue 11.
<http://catless.ncl.ac.uk/Risks/22.11.html>
5. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning system, John A. Volpe, U.S. National Transportation Systems Centre, 2001,

http://www.navcen.uscg.gov/gps/geninfo/vulnerability_assess_2001.pdf

6. Â£900 fine for sat nav nut. The Sun, 2009

<http://www.thesun.co.uk/sol/homepage/news/2640633/900-fine-for-sat-nav-driver-who-was-left-dangling-over-cliff.html>

✶ Re: Toyota uncontrolled acceleration (Lesh, [RISKS-25.82](#))

David Lesh <wb8foz@panix.com>

Fri, 27 Nov 2009 17:59:38 -0500

Update: Toyota has announced a 3.8E6 vehicle recall for the unattended acceleration problem discussed before.

Press reports indicate that Toyota will modify the floor mats and pedals. Further, they'll install engine cut-offs that activate when the brake and accelerator are both depressed, at least on new production vehicles. (Reports vary widely re: their backfitting to existing vehicles.)

Unmentioned is any change to the ignition switch design; which requires the driver hold down the START button to stop. Also no mention of transmission changes.

✶ Re: Toyota uncontrolled acceleration (Lesh, [RISKS-25.82](#))

JC Cantrell <jccant@pacbell.net>

Mon, 9 Nov 2009 12:41:33 -0800 (PST)

David Lesh wrote:

"... The second is more alarming. I thought that there was a {?unwritten} requirement that no US road-legal car could even overpower its own brakes; i.e., given full throttle and full brakes; the car stops, period. (This may not be the case for a dedicated race car...)"

LA Times story on 8 November:

"In reviewing consumer complaints during its investigations, the NHTSA relied on established "positions" that defined how the agency viewed the causes of sudden acceleration. Cases in which consumers alleged that the brakes did not stop a car were discarded, for example, because the agency's official position was that a braking system would always overcome an engine and stop a car. The decision was laid out in a March 2004 memorandum."

<http://www.latimes.com/news/local/la-fi-toyota-recall8-2009nov08,0,2472257,full.story>

Now, it sounds to me that the NHTSA believes (i.e., its official position) that the brakes should stop the car, but it does not sound like an edict, regulation or that it is even tested.

Well, that is why I buy a manual transmission. When that clutch is in, I KNOW I can stop the car...

Patients' data used as Packing

"Robert (Bob) Waixel" <r.waixel@bcs.org.uk>

Sat, 21 Nov 2009 22:37:59 +0000

Jeweler finds hospital records sent in packaging for gift boxes; Confidential records from "solicitor's office acting for patients" were shredded (but not enough) and then used as gift box packing.

Jeweler had ordered gift boxes for her Jewelry products, and the boxes came with the shreadings as packing. Patients' data came from Papworth Hospital, Cambridge, England, 'who were horrified' and 'were investigating'.

"I could clearly make out the name and address and the name of the hospital and solicitors" said the finder. The solicitors said " we don't shred paper here and we will be having a chat with our suppliers". Papworth Hospital described the secure shredding service it used onsite to make sure that all confidential paperwork was completely unidentifiable. "In certain circumstances a patient will request that their notes are given to a third party, such as a solicitor. In these circumstances we would expect that extreme care is taken in the disposal of these documents by this third party."

Reported by Raymond Brown <raymond.brown@cambridge-news.uk>

[Abridged summary by R Waixel from Cambridge Evening News Fri 20 Nov 09 Pp 1, 5]

Bob's Comments

- * Clear breach of UK Data Protection Act 1998 and Principle 7 (Security) by the solicitors... Wonder whether the hospital has any written procedures for handing personal data over to solicitors. Presumably not as such professionals have their own clear professional duty of care as well as legal (Data Protection) one.
- * How easily the Hospital can be tarnished by the Solicitor's carelessness (Hospital data lost not Solicitor's!) Page 1 headline.
- * Solicitor possibly had the data because of potential litigation against Hospital? (mere speculation by me)
- * The solicitors seem to be remarkably relaxed over the matter - perhaps it could invest in (several) cross cut shredders?
- * Pity the solicitor [who was] not identified.
- * There for the grace of God goes many another organisation too...

Robert (Bob) Waixel, MBCS, MCIInstM, FHEA, RW Systems, Cambridge, UK
Chartered Information Technology Professional (CITP) <r.waixel@bcs.org.uk>

Re: Apostrophe in Your Name? You Can't Fly!

Andy Behrens <andy@behrens.net>

Wed, 25 Nov 2009 23:01:54 -0500

I would call this a bureaucratic problem rather than a technological one. It is well known that airline computer systems drop apostrophes, remove accents from letters, and truncate long names. The insanity lies in the fact that someone wrote a regulation which requires an exact match, even though it should be clear that such a match is frequently not possible.

At least there are no signs posted saying "No Irish Need A-fly".

✉ Re: Apostrophe in Your Name? You Can't Fly! (Brady, [RISKS-25.84](#))

*"JosephKK" <quiettechblue@yahoo.com>
Fri, 27 Nov 2009 18:49:38 -0800*

And the next (or as likely at the same time) problem will be hyphenated names. I have seen this way too much already. And current programming (CS) courses do not help. I have met people with names like O'Hara-Mgabe and O'Rourke-Hollins.

[Not to mention multiple hyphens, and multipart middle names such as Charles Henry Anthony Richard. PGN]

✉ Re: Apostrophe in Your Name? You Can't Fly! (Brady, [RISKS-25.84](#))

*Dag-Erling_Smørgrav <des@des.no>
Thu, 26 Nov 2009 12:54:19 +0100*

They can't print accented letters either, or in fact any character not used in English, such as in German, Scandinavian, Icelandic, Finnish, Sami, etc.

[And my mailer has trouble with them also!]

✉ Re: Apostrophe in Your Name? You Can't Fly! (Brady, [RISKS-25.84](#))

*"Bob Frankston" <bob2-39@bobf.frankston.com>
Fri, 27 Nov 2009 00:50:01 -0500*

We'll have to see what happens in practice as there are too many such examples because the airlines are stuck with 1960's US 6 bit character sets. No hyphens, accents or other markings. I suspect special characters will be simply ignored. Though optional spaces may be an issue..

More problematic will be ambiguous translations into English characters and name variations like Bob vs. Robert or insisting on matching my middle name.

When flying from SFO on Virgin America a two weeks ago where I am Bob I did ask the security people and was told it would be no problem. 100% strictness won't work in practice but I do worry about depending on the security

people's willingness to be flexible.

Re: Warren Buffett cell phone skills: did they doom Lehman?

Curt Sampson <cjs@cynic.net>

Thu, 26 Nov 2009 14:42:06 +0900

For the record, here's are the final two paragraphs of the above misleadingly titled article:

> It makes a great story - but as Michael Corkery of the Wall Street
> Journal wrote last night: "If the Oracle from Omaha really thought he
> could profit from insuring Lehman's assets, he would have followed up
> with Diamond. Likewise, if Diamond thought he had a realistic chance
> of closing a deal with Buffett, don't you think he would have likely
> lobbed a follow up call?"

>
> Here's the truth according to Corkery: "Buffett may not know how
> to use a cell phone, but he's pretty savvy about avoiding terrible
> investments. That was one call he has to be glad he never answered."

In other words, there was a system in place to deal with the risk of failure, it it simply wasn't activated because he wasn't interested in the deal.

Curt Sampson <cjs@starling-software.com> +81 90 7737 2974

Re: Warren Buffett cell phone skills: did they doom Lehman?

Henry Baker <hbaker1@pipeline.com>

Thu, 26 Nov 2009 05:21:49 -0800

Oh, and you've never used the old "your cellphone signal is fading, I'll have to call you back" excuse to get out of a call ?

Buffet is nothing, if not polite.

Re: Teleportation via Skyhook ([RISKS-25.84](#))

Charles Wood <j.charles.wood@gmail.com>

Fri, 27 Nov 2009 12:01:13 +0800

Checking on the Skyhook wireless site they describe their location methodology in <http://www.skyhookwireless.com/howitworks/privacypolicy.php>

As part of the location process all available information is collected by

the mobile device and sent to the server system for location calculation. A result is then sent back. From the wording it appears that only phone tower and wireless network information is sent; though there is an option to manually enter a street address.

What seems odd to me is why they don't collect and transmit GPS information at the same time. It would make a lot more sense to have a host of end users doing their mapping for them rather than having to pay for expensive vans to go around and do the mapping.

The fairly accurate location of the user is usually known already based on their database. The addition of GPS would not significantly affect the privacy of the user as they have already agreed to submit location identifying information. In fact the user's main focus is to get very precise location information as quickly as possible and has agreed to let skyhook wireless access to all data that will achieve that aim.

I also tried the service from a windows laptop. I am not in an area of the world that is especially likeley to have been mapped and so it returned an error. What surprises me is that they don't appear to have a fallback to IP geolocation. Nor do they seem to use it for verification purposes - The example in the teleportation post would very easily have been solved by use of IP geolocation and sanity checks on successive readings

Android Mythbusters (Matt Porter)

<jidanni@jidanni.org>

Sun, 15 Nov 2009 03:52:05 +0800

http://laforge.gnumonks.org/weblog/2009/11/04#20091104-android_mythbusters

Executive summary: Android is a screwed, hard-coded, non-portable abomination.

Solving the Android "Grayed Out Application" Deadlock

Lauren Weinstein <lauren@vortex.com>

Mon, 16 Nov 2009 14:40:32 -0800 (PST)

Lauren Weinstein's Blog Update: Solving the Android "Grayed Out Application" Deadlock

November 16, 2009

<http://lauren.vortex.com/archive/000636.html>

Greetings. Since I'm fairly vocal in my support of -- and enthusiasm for -- Google's Android OS, I tend to have quite a few people who send me their own Android experiences, both pro and con.

While by far most of these notes are positive, there has been a recurring theme lately of reported deadlocks involving already installed applications on Android phones. Previously installed applications suddenly wouldn't run, couldn't be uninstalled, and couldn't be reinstalled. Apparently no "official" explanation or cure for this condition has been apparent.

I wasn't in a position to investigate this myself until a few days ago, when a significant number of apps on my Android 1.6 G1 phone suddenly entered this "zombie" state, triggering my looking at the situation rather intently.

The primary symptom of these unusable apps is that not only won't they run directly, but the Android "Market" mechanism refuses to either "Open" or "Uninstall" them -- those options are grayed out. But since Market believes the apps are still installed, they cannot be reinstalled either.

Even with a rooted phone, this presents a quandary -- on a non-rooted phone, even more so.

Here are the results of my investigation into this issue, and my recommended procedure for recovery from such situations without completely resetting your phone and having to manually rebuild your entire configuration from scratch.

The basic problem appears to occur when (for whatever reason) an installed app's "apk" file has vanished from /data/app (or /data/app-private). Once this occurs the market app apparently goes out of sync, and then the affected programs won't run, can't be uninstalled, and can't be reinstalled -- via market directly, anyway.

The trick out of this dilemma is to obtain the original apk files that are missing. If you already have backups of these files, you can reinstall them via the app package manager. In my case, I used the Astro file manager to select the app apk files for which I had backups -- Astro then executes the package manager.

The affected programs will appear to already be installed -- that is, the app package manager will offer an UNINSTALL choice, not an INSTALL choice. Go ahead and tap UNINSTALL. When the uninstall finishes, go back to the package (e.g. via Astro again), then back to the package manager, and this time tap the offered INSTALL. The app should reinstall and be good to go.

It may also be possible to follow a similar sequence via the Android "adb" tool externally, but I had mixed results trying this, so I recommend working on the phone itself if possible, from backups on the sd card. The adb tool is still useful in this context for file copying operations -- see below.

If you don't have backups of the necessary apk files for the desired apps, you need to get them, but as noted above, market won't let you download them since it thinks they're already installed. Here's how to get them.

First, use Nandroid to back up the current state of the phone. I can't emphasize enough the value of Nandroid -- it's extremely useful. Once you have a Nandroid backup, do a factory data reset ("wipe") and reboot. You'll

need to re-authenticate the phone to Google (that is, login with your Google account). Now go to the market program and install the programs for which you were missing apk files earlier -- you should be able to download them successfully now.

Once they've downloaded and installed, the new apk files should be in /data/app (or in some cases, /data/app-private). Copy the files (e.g. "cp") from the /data/app or /data/app-private dirs to the sdcard (/sdcard). You can do this via a terminal console on the phone or through the "adb shell" command.

Now reboot, then restore the Nandroid backup that you made before doing the factory reset wipe.

After you're back in the previously saved system, you can navigate (e.g., with Astro) to the new apk files that you copied to the sd card, and follow the procedure above to first "uninstall" and then "install" those programs through the app package manager.

Using these techniques, I was able to completely restore all apps on my G1 that had mysteriously found themselves in the limbo of the unusable "grayed out" state. Why the apk files vanished from /data/app in the first place, triggering this entire sequence of events, remains a mystery to me at this point.

Lauren Weinstein <lauren@vortex.com> Tel: +1 (818) 225-2800
http://www.pfir.org/lauren Lauren's Blog: <http://lauren.vortex.com>
Co-Founder, NNSquad - Network Neutrality Squad - <http://www.nnsquad.org>
Co-Founder, PFIR - People For Internet Responsibility - <http://www.pfir.org>
Founder, PRIVACY Forum - <http://www.vortex.com>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 86

Monday 14 December 2009

Contents

- [Stryker Operating Room System II Surgical Navigation System recall](#)
[Richard Cook](#)
- [Northwest Flight 188](#)
[Curt Sampson](#)
- [Chase Quicken and MS Money bill pay broken for 2 weeks, no fix ETA](#)
[John Rivard](#)
- [UK Digital Economy Bill -- Blocking Illegal Downloaders](#)
[Chris D.](#)
- [Massive New UK Internet Wiretapping Plan Announced](#)
[Lauren Weinstein](#)
- [Public servant fired over leak of private info of 14,000](#)
[Gene Wirchenko](#)
- [Farmer claims GPS led him to breed clams in the wrong place](#)
[Rob McCool](#)
- [My mother regarding LED traffic lights and Wisconsin winters](#)
[Richard Cook](#)
- [Were you talkin' to me?](#)
[Jerry Leichter](#)
- [All the best efforts gone to naught...](#)
[Jeremy Epstein](#)
- [Various Internet Issues, Succinctly Put](#)
[Peter Ladkin](#)
- [Re: The Joy of satellite navigation failures](#)
[Jerry Leichter](#)
- [Info on RISKS \(comp.risks\)](#)

✉ Stryker Operating Room System II Surgical Navigation System recall

*Richard Cook <ri-cook@uchicago.edu>
Sun, 29 Nov 2009 20:09:05 -0600*

MedWatch - Stryker Operating Room System II Surgical Navigation System:
Recall due to potential for the navigation PC SPC-1 component to stop

working which could result in potential harms associated with this failure
[href="http://service.govdelivery.com/service/w3c/p3p.xml"](http://service.govdelivery.com/service/w3c/p3p.xml)

First known recall of a computer-based surgical positioning system.

Most surgical intervention takes place under direct observation. In these "open" procedures, the surgeon sees the anatomy and moves an instrument (e.g. scissors) under direct vision. The product line involved in this recall includes a positioning product that allows procedures to be performed under indirect observation. These instruments allow the surgeon to operate on deep, hidden structures in close proximity to critical points, e.g. in the sinuses close to the thin bone that separates them from the brain.

The principle of operation is straightforward. Prior to the surgical procedure, a computed scan (e.g. spiral CT) is obtained while the patient wears a locator fiducial, typically a headpiece that incorporates several easy to identify points. The patient wears the same device during surgery. The scan is imported into an operating room system that includes an array of sensors capable of detecting and triangulating the location of the fiducial, special instruments that register with the sensors, and a high quality display that shows patient anatomy and instrument location. Depending on the application, the representation may be multiple "flat" cross-sections or a 3D reconstruction. The system displays the patient anatomy along with the location of the instruments in realtime. The display is updated frequently to track the location of the instrument as it moves through the patient. This allows the surgeon to move the tip of the instrument and accomplish the surgical intervention by watching a representation rather than under direct observation.

There are a variety of such instruments available for different applications. For neurovascular procedures, the system can use a contrast enhanced computed tomogram to map the arterial vascular tree in the head and then by digital subtraction to remove the non-vascular structures to allow realtime 3D display so that aneurysms can be embolized. The advantage of such an approach is that it entirely eliminates the need for a surgical craniotomy with its attendant risks, allowing the procedure to be accomplished from "the inside".

The failure of this type of instrument would certainly get attention. The "Dear Doctor" letter (<http://www.stryker.com/en-us/139059>) notes that the system failure could result in:

``delay in surgery, reschedule of the procedure resulting in an additional surgery, risk of infection, increased morbidity, potential neurological deficits, or injury due to the surgeon operating in an area where they did not intend to operate. Depending on the type of surgery, these failures could potentially lead to serious adverse health consequences, including death. There have been no reports of injury."

Based on the description of the failure and the specific serial numbers of instruments included in the recall, it is possible that the sensors are not detecting reliably the fiducial or the instruments being used. Software faults are also possible, of course; the application, while simple in theory, is complicated in implementation.

The FDA recall notice:

MedWatch - The FDA Safety Information and Adverse Event Reporting Program
Stryker Operating Room System II Surgical Navigation System: Recall due to
potential for the navigation PC SPC-1 component to stop working...

Audience: Hospital risk managers, surgical service managers

Stryker and FDA notified healthcare professionals of a recall of 23 Operating Room System II Surgical Navigation Systems because there is a potential for the navigation PC SPC-1 component to stop working which could result in the screen freezing, the system updating at a slow rate, or not responding at all. The Navigation System II is a computer aided surgery platform that surgeons can use to perform Hip, Knee, Spine, Neuro and ENT surgical procedures and contains a computer workstation with the navigation System II software and various components necessary to run the system. The potential harms associated with this failure are: delay in surgery, reschedule of the procedure resulting in an additional surgery, risk of infection, increased morbidity, potential neurological deficits, or injury due to the surgeon operating in an area where they did not intend to operate. Depending on the type of surgery, these failures could potentially lead to serious adverse health consequences, including death. Hospitals that have product that corresponds to the catalog numbers above should immediately quarantine the product, label it as a recalled product and stop using the product.

Read the complete MedWatch 2009 Safety summary including a link to the firm press release, at:

<a class="moz-txt-link-freetext"

href="http://www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm192105.htm">http

>

Richard I. Cook, MD, Associate Professor, Department of Anesthesia and Critical Care, University of Chicago, <href="http://www.ctlab.org">

Northwest Flight 188

Curt Sampson <cjs@cynic.net>

Tue, 8 Dec 2009 02:24:07 +0900

A blogger has posted what he says are "excerpts of an e-mail I received from a fellow airline pilot. It is a summary of another pilot's conversation with Tim Cheney, the Captain of NW Flight 188, that overflew MSP."

http://thedonovan.com/archives/2009/11/about_that_nort.html

It's hard to tell the veracity of this report, given that it's a friend of a friend thing, but it sounds quite plausible. Here's a summary.

The flight had a 100 knot tailwind that appears to have shortened travel

time considerably. (Though they left San Diego 35 minutes late due to an ATC flow restriction, even after overflying their destination, they arrived only 15 minutes late.)

After passing Denver, the captain left the cockpit to go to the toilet. While he was out, the first officer (FO) received ATC instructions to move to a new frequency. However, for whatever reason, the FO changed to Winnipeg ATC rather than the correct frequency for Denver Center. Normally this would be caught quickly, but the FO apparently did not confirm communications on the new frequency. (Had he done so, and realized that he was talking to the wrong ATC, the standard procedure would be to go back to the previous frequency and confirm the new frequency he was being directed to use.)

When the captain returned, the FO neglected to inform the captain of this change. Because there was chatter on the frequency, the captain didn't realize that they were not talking to the ATC that was supposed to be controlling them. When Denver Center couldn't contact the flight, they did have the airline send an ACARS message to the flight, but on the Airbus 320 apparently there's no audible signal upon receipt of an ACARS message, just a light that turns on for thirty seconds and turns off again.

During this time, the captain mentioned that he was unhappy with the scheduling software, which was new to him, being Delta's software and he being a Northwest pilot. The FO offered to help, and they spent perhaps five minutes with laptops out dealing with this.

Then,

The F/As called the cockpit on the interphone...and asked when they will get there. They looked at their nav screens and were directly over MSP [the Minneapolis-Saint Paul International Airport].

Because they had their screens set on the max 320 nm setting, when the F/O called on the frequency, which of course was Winnipeg Center, he saw Eau Claire and Duluth on his screen. They asked where they were and the F/O told them over Eau Claire, which was not even close, but MSP had disappeared from the screen even though they were right over the city. ...

They were, as you all know, vectored all over the sky to determine if they had control of the a/c and Tim kept telling the F/O to tell them they have control, they want to land at MSP, etc. They landed with 11,000 pounds of fuel (no, they did not come in on fumes, but had 2 hours in an A320)....

✂ Chase Quicken and MS Money bill pay broken for 2 weeks, no fix ETA

*John Rivard <jcr@jcrdesign.com>
Mon, 30 Nov 2009 10:10:00 -0500*

I just got off the phone with a customer service agent at Chase online support.

I was attempting to discover why electronic payments sent via the Quicken desktop application are failing with an error code. The error message recommends trying again later, and contacting your financial institution if the problem does not go away.

The phone agent I spoke to said that since an upgrade to their system two weeks ago, both Quicken and Microsoft Money payments have been failing. Yes, you read that correctly, Chase is aware that this problem has been occurring for two weeks, but instead of notifying users of this by phone or e-mail (or even snail mail, since it has been two weeks), they have been waiting for them to call in, navigate the phone tree, and wait on hold to talk to an agent.

Perhaps they have delayed informing users directly because they have no idea how to fix the problem. The agent also stated that there was no estimate available for when this problem. I was fairly incredulous, and pressed if there was any order-of-magnitude estimate available: would it be fixed in hours, days, another two weeks? There is no estimate available at all.

UK Digital Economy Bill -- Blocking Illegal Downloaders

*"Chris D." <e767pmk@yahoo.co.uk>
Sat, 28 Nov 2009 19:51:49 +0000*

There have been reports in the news this week (late Nov 2009) about the UK Government's Digital Economy Bill which has started its course through Parliament. The main concern for RISKS readers is most likely the requirement for ISPs to throttle or suspend broadband connections for "persistent" illegal file-sharers and pass details over to copyright holders. I haven't seen anything about how such criminals are supposed to be identified or who arbitrates in the event of a dispute, but obviously it will all have to be paid for, and news reports comment that if ISPs have to start up whole departments to monitor traffic and handle violation claims then this may well increase Internet service bills. That's apart from the more-fundamental issue of ISPs moving away from just giving access to cyberspace, of course; looks like yet another case of governments legislating for the desired results. Talking of costs, the UK Government has pledged to offer everyone in the whole country (i.e. including remote rural areas) at least 2MBit/s broadband by 2012, funded by a proposed 6 pounds (\$10) a year levy on fixed-line telephone rental, so another good reason to give up the landline and just use a cellphone.

Chris Drewe, Essex County, UK, still on dial-up.

Massive New UK Internet Wiretapping Plan Announced

*Lauren Weinstein <pfir@pfir.org>
Fri, 4 Dec 2009 18:43:18 -0800*

<http://lauren.vortex.com/archive/000646.html>

Greetings. Remember the controversy over the UK's "Phorm" - "ISPs Spy on Users" Internet ad system? (<http://bit.ly/91Yvgz> [Lauren Weinstein's Blog])

Phorm was eventually beaten back, but it was small potatoes compared to what the surveillance-happy folks in Jolly Old England have got up their sleeves now.

Britain's Virgin Media ISP has announced a stunning plan to actually spy on the data content of Internet users -- using law enforcement grade equipment -- in search of illegal file sharing (<http://bit.ly/80maxP> [ZDNet]).

The scope of the plan is breathtaking. File sharing protocol packets will be opened and the contents run through music fingerprinting systems to try determine if files are licensed or not. At this stage of the plan, any positive "hits" will be anonymous, but one can imagine how long that aspect will remain in force. And of course, if this sort of system can be justified to "protect" the music and film industries, it's a small step to arguing that all traffic should be monitored for *any* Internet content considered to be suspicious, illicit, or inappropriate by Her Majesty's government -- it's basically just a matter of how much communications and processing power you're willing to throw at the task.

There is no opt-out or opt-in. All files carried by any of the three primary file-sharing protocols are subject to inspection, with initially about 40% of subscribers being included in the "lucky" test group. And remember, these are *private* user-to-user Internet connections being monitored -- not postings on public Web sites where license fingerprinting can be reasonably justified.

What Virgin has announced is essentially the same concept as monitoring telephone calls in hopes of overhearing something illegal being discussed.

The question here isn't whether or not people should inappropriately trade licensed materials -- they shouldn't. The issue is Internet users -- including innocent, law-abiding subscribers -- being subjected to having their data content searched by whim of their ISPs, when such behavior would not (we assume!) be tolerated on conventional telephone calls (but what of VoIP phone calls traversing the Internet? A fascinating question of ever increasing importance ...)

Notably, the answer to these dilemmas is contained in a single word, which you've seen me use many times before: *encrypt*! As far as I'm concerned, all Internet traffic should be routinely and pervasively encrypted, not just to protect civil rights, but to protect economic and business security as well.

In fact, a spokesman related to the new Virgin ISP spying project notes that, "encryption of the data packet would defeat us."

Sounds like good advice to me.

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org/lauren>
People For Internet Responsibility - <http://www.pfir.org>
Network Neutrality Squad - <http://www.nnsquad.org>
PRIVACY Forum - <http://www.vortex.com>

Public servant fired over leak of private info of 14,000

*Gene Wirchenko <genew@ocis.net>
Sun, 29 Nov 2009 11:52:12 -0800*

This appeared in the 2009-11-27 issue of "The Daily News" of Kamloops, British Columbia, Canada on page A7:

Second B.C. public servant fired over leak of private info on 14,000[1] people

The B.C. government says two public servants have now been fired following a leak of the private information of 1,400 [1] welfare recipients. The NDP [2] claims the first person sacked was a man and the second was his wife, but Citizen Services Minister Ben Stewart would not confirm that, saying it was a personnel issue.

The leak came to light after the personal information was found in the hands of a public servant under investigation by the RCMP's [3] commercial crime unit and the Insurance Corporation of B.C. on an unrelated matter. The NDP says that information included birth dates, social insurance numbers and other data.

The controversy came up for the second day in question period in the legislature on Thursday, where the NDP once again demanded to know why it took seven months to warn the people affected and why Stewart wasn't told earlier about the breach. Stewart promised a full investigation into the issue, adding that the RCMP doesn't believe people's information was compromised.

1. The headline is apparently the error. All other coverage that I have seen has the number as being 1,400.
2. New Democratic Party. In B.C., they are currently the official opposition party.
3. Royal Canadian Mounted Police: Canada's national police force

Farmer claims GPS led him to breed clams in the wrong place

*Rob McCool <robm@robm.com>
Thu, 10 Dec 2009 19:10:42 -0800 (PST)*

<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2009/12/10/financial/f162026S49.DTL&tsp=1>

An oyster farm in Marin County, California was fined recently for farming clams in an area designated as protected for the harbor seal. The owner of

the operation claimed that a faulty GPS device led his employees to place the clam farm in the wrong place.

✂ My mother regarding LED traffic lights and Wisconsin winters

Richard Cook <ri-cook@uchicago.edu>

Fri, 11 Dec 2009 11:20:07 -0600

Mom wrote:

"Interesting, some of the new traffic lights are LEDs and since they don't give off much heat, the snow sticks to the lights and drivers can't see the light. I was yelling at someone who drove through a red and scared me but when I came home, realized that I couldn't see the light. Now what?

Richard I. Cook, MD, Assoc.Prof., Department of Anesthesia and Critical Care, U. Chicago, 5841 S. Maryland Ave MC4028, Chicago, IL 60637 773-702-4890

✂ Were you talkin' to me?

Jerry Leichter <leichter@lrw.com>

Sun, 29 Nov 2009 12:29:14 -0500

Early last spring I received mail containing a textual date and time for an appointment. Apple's mail client implements "data detectors," which spot certain patterns in the text of messages and provide you with a pull-down to implement various natural operations. For example, the date and time in this message gave me the opportunity to either go to that date and time in iCal, the Mac calendar; or directly create a new event at that date and time. I chose the latter, and it worked as desired - even naming the appointment from the subject of the mail message.

Except that ... the sender had specified the time zone with the date and time. And he specified it as EST. But this was on a date shortly after we switched over to EDT. iCal faithfully converted the time to EDT, and made the appointment an hour too late! (There is a setting in iCal - which I don't have enabled right now - in which the originating time zone is preserved. That might well have been even **more** confusing, as I suspect the numeric time in the calendar would have agreed with the numeric time I remembered from the mail message, keeping me from spotting the problem quickly - but the alarm would still have gone off an hour too late!)

The risk: Increasingly, you really can't be sure when what you type (and, soon, say) will be interpreted by a human being or by a machine. Machines are getting better, but they remain much more literal in their interpretations than we expect humans to be. We'll need to be very careful in our use of language - as when we speak to someone from another culture - or misunderstandings will multiply.

All the best efforts gone to naught...

*Jeremy Epstein <jeremy.j.epstein@gmail.com>
Mon, 30 Nov 2009 21:54:39 -0500*

For one of my volunteer activities (anyone wanna buy Girl Scout cookies?), I have a logon to a web site. Every year we have to get renewed, which is reasonable considering that the assignment changes annually. There's always gripes about setting a password for your account.

Here's an excerpt from an e-mail I received today on using the site: "They will also have to change their password. If they want to go back to their original password, the next time they sign in they should complete the login and password but click the 3rd green bullet below the login and go back to that contact page for another password edit. This a little tricky - most people would like to keep their old password so here is what they can do - when they go to the 3rd bullet it will ask for a new password - just put in any kind of word - get out of that and go back to the login to the 3rd bullet and go through that procedure for the new password , put old password in and that way you will have your same password."

In summary, people will go to far more effort to keep the old password than to set a new one....

But I guess it beats the message we got from my daughter's school telling us that all the kids were instructed to change their password from the default of "dragon" to the new password "dragons" - kids aren't allowed to pick their own passwords, because then the teachers can't give them access, I guess. Sounds like a system that's poorly designed if the teacher can't reset the students' passwords, so they ensure that all students have the same password...

And we wonder why there are so many web account compromises?!?!?!

Various Internet Issues, Succinctly Put

*"Prof. Dr. Peter Bernard Ladkin" <ladkin@rvs.uni-bielefeld.de>
Sun, 29 Nov 2009 08:20:24 +0100*

Jeremy Clarkson is long-time host of the BBC's car-review program Top Gear, which (I find out from the link below) is the most illegally- downloaded television program from some unspecified sample.

Clarkson is known for his biting wit, the Oscar Wilde of the Morris Mini. Like Garrison Keillor, he has crossed over from broadcast to print journalism and writes entertaining pieces for The Times/Sunday Times (Murdoch's News International), amongst others.

Here is his take on a number of Internet problems. I only wish I could write so well:

http://www.timesonline.co.uk/tol/comment/columnists/jeremy_clarkson/article6936087.ece

Peter Bernard Ladkin, University of Bielefeld, 33594 Bielefeld, Germany
www.rvs.uni-bielefeld.de

Re: The Joy of satellite navigation failures

Jerry Leichter <leichter@lrw.com>

Sun, 29 Nov 2009 13:14:06 -0500

In [RISKS-25.85](#), Steve Loughran complains specifically about an ad in which a car will use GPS "to get you home" - and more generally about over-reliance on GPS.

I find myself increasingly an old curmudgeon myself, and I'm bothered by the young whippersnappers who couldn't read a map to find their way down a midwestern plains highway - dead straight and level as far as the eye can see in both directions.

But ... let's be a bit objective here. How accurate were paper maps? The period in which, even in the US and Western Europe, you could rely on maps to be more than approximations doesn't date back much more than 50 years or so. In most of the world, there have never been accurate road maps. I drove around Puerto Rico in the late 1970's. Hardly an undeveloped part of the world. And yet the maps were ... fanciful in places. Roads shown that were planned but not yet built. Roads that existed on the ground but somehow didn't make it onto the maps. Drive based just on the map - which in one spot showed a 4-lane highway - and find yourself in the middle of a sugar cane field.

Are GPS maps up to date? How about the paper maps that used to fill glove boxes?

Accurate road markers are of roughly the same vintage - and for historical reasons are often difficult to use for navigation. When I drove in England about 20 years ago, most road signs except on the largest roads (a) did **not** show you the compass direction; (b) named the next town down the road, not some larger city you might have heard of beyond that. One wrong turn and you could go many miles the wrong way without knowing it. (I did!)

Were there complaints from experienced users of compasses and rough maps showing topographical features when people stopped learning how to use them and relied on street signs? When maps were introduced and people stopped observing what was around them? When compasses disconnected people from navigation by the sun and stars? Of course. And did this lead to some people getting lost because they had an old map, when someone of a previous era would have had no problem noticing that we couldn't possibly turn **there**, the topo maps shows that we should be going uphill? Sure.

The fact is, GPS's get it right most of the time. They are much easier to use, much more reliable (when you consider the entire system, including the inexperienced map reader), much more accurate than any system we had before. People aren't going back, short of some kind of collapse that renders the systems inoperable. There's not much point in complaining.

Do **inappropriately used** or **badly designed** GPS's cause problems? Sure, but just how new are those? People blindly followed maps, too - sometimes because the maps were wrong or simply omitted some information like "low bridge" (frankly, I've never seen a **consumer** road map with that piece of information on it, any more than consumer GPS's inappropriately used by truckers show this information), sometimes because most people never learned how to read more than the basic information from a map.

We can certainly make the current systems better - and we are. But consider: Suppose you were driving somewhere unfamiliar, in a heavy thunderstorm, using your GPS - and I suddenly took it away from you and handed you some 4-year-old ratty, disintegrating map out of the glove box. Would you think I'd improved things for you?



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 87

Tuesday 15 December 2009

Contents

- [A Deluge of Data Shapes a New Era in Computing](#)
[John Markoff](#) via PGN
- [Forensics, COFEE, and Decaf](#)
PGN
- [Encryption Considered Harmful](#)
[Curt Sampson](#)
- [Toronto subway line closed for 6 hours after tunnel pierced by gas line crew](#)
[Tony Harminc](#)
- [Happy Holidays?](#)
[Zach Tudor](#)
[Jeremy Epstein](#)
- [Re: The Joy of satellite navigation failures](#)
[Michael D. Sullivan](#)
- [Re: Teleportation via Skyhook](#)
[Jonathan de Boyne Pollard](#)
- [Re: Android Mythbusters](#)
[Phil Colbourn](#)
- [Re: Toyota uncontrolled acceleration](#)
[Jeremy Epstein](#)
[Graham Reed](#)
- [Info on RISKS \(comp.risks\)](#)

A Deluge of Data Shapes a New Era in Computing

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

Tue, 15 Dec 2009 7:17:12 PST

John Markoff, Science Times, *The New York Times*, 15 Dec 2009

A superb article by John Markoff this morning pays a wonderful and well-deserved tribute to Jim Gray's notion of a "fourth paradigm" -- that computing is fundamentally transforming the practice of science. (The first three paradigms are experimental, theoretical, and computational.) "In

essence, computational power created computational science, which produced the overwhelming flow of data, which now requires a computing change. It is a positive feedback loop in which the data stream becomes the data flood and sculpts a new computing landscape."

I love the quote from John Wilbanks: "I Have Seen the Paradigm Shift, and It Is Us" (his chapter title).

Please read Markoff's pithy article. I still read *The NYT* in hardcopy, and believe in supporting the future of real news, analysis, and thoughtful writing. Thus, I try not to exceed fair use guidelines in RISKS. However, you can find the article with minimal browsing. PGN

Forensics, COFEE, and Decaf

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 15 Dec 2009 6:41:52 PST

COFEE (Computer Online Forensic Evidence Extractor) has been distributed through Interpol only to law enforcement agencies for the past 2.5 years. COFEE consists of about 150 tools used to collect digital evidence at crime scenes. ("Microsoft has been pouring free COFEE to law enforcement officers since at least mid 2007.") However, it has recently been accidentally released more widely. Perhaps not surprisingly, a subverting program called Decaf has now been released that monitors Windows systems for the presence of COFEE, and automatically executes some countermeasures that effectively dilute the benefits of COFEE (but apparently without any nasty side-effects to the system). [Source: Dan Goodin, *The Register*, 14 Dec 2009; PGN-ed, with thanks to Jeremy Epstein for spotting this item.]

http://www.theregister.co.uk/2009/12/14/microsoft_coffee_vs_decaf/

An excerpt from *The Register* article:

"We want to promote a healthy unrestricted free flow of internet traffic and show why law enforcement should not solely rely on Microsoft to automate their intelligent evidence finding," one of the two hackers behind Decaf told *The Register* in explaining the objective of the project.

Encryption Considered Harmful

Curt Sampson <cjs@cynic.net>
Tue, 15 Dec 2009 13:05:08 +0900

In [RISKS-25.86](#), under the subject "Massive New UK Internet Wiretapping Plan Announced," Lauren Weinstein <pfir@pfir.org> writes,

> [Notes on a British ISP perpetrating a man-in-the-middle attack on their
> customers.]

>

> Notably, the answer to these dilemmas is contained in a single word, which
> you've seen me use many times before: *encrypt*!

Unfortunately, this is just wrong. That single word is not the answer, and in fact is an even worse problem in disguise.

We must be careful about giving out very dangerous advice.

> In fact, a spokesman related to the new Virgin ISP spying project
> notes that, "encryption of the data packet would defeat us."

It will only do so until they get someone just a wee bit smarter to use attack methods that have been available in open source software for some time [1,2]. What they'll do is this:

Alice (the user at this ISP) will attempt to connect to Bob (some file-sharing source). But of course, Mallory (the ISP) has control of every packet flowing between them, and can decide to drop them, forward them, and even change them.

When Alice connects to "Bob" for the first time, she'll get a notice that Bob is using a self-signed certificate that she's never seen before, and would she like to accept it or not. She'll say yes, a little lock icon will appear, and she'll exchange sensitive material in the comfort that it's all being encrypted.

And it is. Twice. Unfortunately, it was Mallory who generated and sent her "Bob's" certificate, set up his own encrypted connection to Bob (pretending to be Alice), and who is now proxying that connection. (There's a nice little picture of this at [3].) When Alice sends an encrypted packet to "Bob," Mallory decrypts it, examines the content, changes it as he wishes, re-encrypts it, and sends it on to the real Bob.

In short, encryption without authentication is not only useless against an attacker who forwards your packets, but is in fact dangerous, because it looks as if you're safe when you're not.

This is the very reason that recent versions of Firefox have made it much more difficult to accept self-signed certificates. Johnathan Nightingale, in [4], mentions that your ISP is not the only danger here; there are open source, point-and-click tools available[1] to attackers to subvert your router or other hosts on your own network to perform this same attack.

It is ever more important, now that attackers are heading in on all sides, that we discourage as much as possible the use of encryption without authentication.

Unfortunately, this is still widespread, even amongst those who you'd think would be reasonably savvy about such things. I know far too many industry professionals who would never think about using unencrypted telnet to connect to a remote system, but who happily run SSH clients

with "StrictHostKeyChecking off" and blithely accept the credentials of any remote system for which they don't already have a public key.

1. <http://ettercap.sourceforge.net/>
2. <http://www.pburkholder.com/sysadmin/SSL-mitm/>
3. <http://www.pburkholder.com/sysadmin/SSL-mitm/webmitm.jpg>
4. <http://blog.johnath.com/2008/08/05/ssl-question-corner/>

Curt Sampson +81 90 7737 2974 <http://www.starling-software.com>

✶ Toronto subway line closed for 6 hours after tunnel pierced by gas line crew

Tony Harminc <tony@harminc.net>

Mon, 14 Dec 2009 14:18:40 -0500

The computer risks to this story are peripheral, but it strikes me that it's a classic "category error" of the sort that leads to some of the medical, aviation, and GPS misadventures we have seen. [I suppose the computerized Ontario One Call registry is as close as it gets to being computer-related.]

On November 18 2009, a work crew digging a trench for a natural gas line on Jackes Avenue discovered that they had broken through into the top of a Toronto Transit Commission (TTC) subway tunnel. Work was stopped, and the subway line -- the city's busiest -- was isolated at that point, with turnbacks splitting the line into two for a six hour period that included evening rush hour, until emergency structural repairs could be made. There were no injuries, but thousands of commuters had unplanned long walks or crowded shuttle bus rides. Permanent repairs are still ongoing, and work in progress can be seen from subway trains passing the spot.

The fundamental problem appears to be that the crew thought they were working on a road, but they were actually digging their trench on a bridge. The subway line in question was opened in 1954, and originally this midtown section was in an open cut for several blocks, with sloped grassed sides, and with minor roads carried over the line on flat bridges with low railings. Over the subsequent decades, much of the open cut has been covered over right up to the bridge edges, in some cases with parks, and tennis courts, in others with various buildings including parking structures and high rise apartments. In the case of Jackes Avenue, the original distinctive railings have been removed, though on other streets one or both remain.

While there are disagreements between the TTC and the construction company engaged by Enbridge, the gas distributor, to work on its pipes, it appears that the work crew followed accepted procedures for digging a trench on a road; they obtained a city permit for the dig, contacted Ontario One Call, the province-wide agency run by various utilities (gas, electrical, phone, etc.) to locate underground services, and cut both sides of a trench using a concrete saw. Evidently they were removing some of the sawed concrete at one end when they broke through, and realized they had a problem. The TTC is not a member of Ontario One Call, and it's not clear if large-scale objects like subway tunnels and bridges would be expected to be listed with such an agency.

I have lived in this area for a long time, and saw the covering over of the subway through the years, and so it is inconceivable to me that anyone could not know there are bridges there. But to someone not familiar with the area, there are few visual clues that there's anything different about those bits of road; perhaps the absence of large trees nearby is the biggest. Even the characteristic low green railings, while iconic to me, would doubtless have no special meaning to others, and in any case are no longer there on Jackes Avenue..

Your favourite mapping website can show you aerial and street views of the bridge in question, and some of its neighbours. Rather than include ephemeral URLs, I'm giving nearby street addresses, which I imagine will last longer. There are also various news sites with maps and diagrams of the incident, with unknown web lifespans.

* 38 Jackes Avenue, Toronto" (the site of the incident, no railing on either side)

* 26 Woodlawn Avenue East, Toronto" (the next bridge south, with an original railing on the south side only, serving no obvious purpose)

* 24 Summerhill Avenue, Toronto" (one further south, with original railings on both sides)

* 20 Roxborough Street East, Toronto" (further south, and suddenly it's quite obvious this one is a bridge)

Would you dig a hole in a road at any of these sites? Not that last one, surely. But any of the others? What would it take to change your world view, once you were thinking it was just another road, and that the locate call had come back all-clear? The sound of subway trains rumbling underneath? An unexpected layer of concrete under the paving? Breaking through and seeing a train...?

[Enbridge seems to be entrenched in its endeavors. But the risks are seemingly ENdless, so I thought it might be interesting to include this item. PGN]

🚩 Happy Holidays?

*Zach Tudor <zachary.tudor@sri.com>
Tue, 15 Dec 2009 12:47:50 -0500*

A friend is a Senior VP of risk management at Citi. I e-mailed to tell him I wouldn't click on the link in this card, especially given the amount of spear phishing that targets bank (especially Citi Bank) customers. He replied that it was the marketing folks that came up with the idea (and he joked that "you security folks" are so touchy). I was glad that he at least knew about it, and that it wasn't a hook!

Happy Holidays?

Jeremy Epstein <jeremy.epstein@sri.com>

Tue, 15 Dec 2009 13:09:47 -0500

IEEE sent out something similar for their annual salary survey. I pointed out the same thing - they said that the outsourced marketing company they use required unique URLs for each person. Amazing how one side of an organization doesn't know what the other side is doing...

Re: The Joy of satellite navigation failures (Loughran, [R-25.85](#))

"Michael D. Sullivan" <mds@camsul.com>

Sun, 29 Nov 2009 01:00:24 -0500

Steve Loughran entertainingly takes apart a BMW ad for suggesting that its GPS will guide the user home, noting issues concerning satellite coverage, map quality, etc. One difference between auto makers' built-in GPS navigators and the ones available from TomTom, Garmin, Magellan, etc., is that at least some auto makers don't rely solely on GPS satellites for their navigation systems, but incorporate dead reckoning as well. I don't know whether BMW's nav systems do this, but my VW 2005 Touareg's nav system uses dead reckoning in addition to GPS. It can correctly track my car's location to the lowest level of my office building's underground garage and follow it through underwater tunnels. It never gets thrown off in urban canyons or in heavily tree-shaded rural areas where GPS reception gets a bit dicey. So for a carmaker's built-in navigation system, the actual location of the car shouldn't be a serious issue, if the carmaker has taken advantage of the data available in the in-car electronic environment.

Maps, on the other hand, are a problem. Many mapping data suppliers have included intentional errors, usually of a harmless nature, that give their products "creativity" and thus provide copyright protection. Sometimes, these errors can be serious, however, if the driver does not exhibit appropriate skepticism. Near my home there is a road that dead-ends at a homeowner's driveway. Some online and GPS maps, however, show the road continuing through the driveway and right past the home through a forest to a public street a few hundred feet away. If somebody decided to rely on that map late at night, a serious accident could occur. Likewise, in another nearby location some online and GPS maps show a road continuing through between two other roads when in reality that lot contains only a footpath; the road restarts with the same name on the other side. I've also run into a situation where my car's nav system told me that a footbridge was a road. And, of course, even with updated discs no nav system is going to have totally current mapping data as roads expand and reroute. I just drove between DC and Philly, and the road construction on I-95 left even the August 2009 update disc behind.

The key to the BMW ad is that the GPS will "guide" you home. It will not

unerringly direct you. "Guidance" inherently needs to be evaluated as to whether it is reasonable and correct.

I don't think Steve would want nav systems to provide all of the disclaimers he amusingly asserts with respect to the ads, at least on an ongoing basis. It would be hard to pay enough attention to pick the wheat from the chaff if the nav system were to say, "Unless you are in Scotland or the Lake District or Alaska or woodlands or canyonlands or an urban area, or you don't have the latest mapping disc, or any number of situations where this system's guidance is questionable, in 400 meters, bear right," . . . and thereafter, "Take next right turn, unless you meet the criteria stated previously, in which case you are on your own."

Re: Teleportation via Skyhook (Wood, [RISKS 25.85](#))

*Jonathan de Boyne Pollard <J.deBoynePollard@Tesco.NET>
Wed, 02 Dec 2009 05:33:55 +0000*

"What surprises me is that [Skyhook Wireless doesn't] appear to have a fallback to IP geolocation." says Charles Wood. I expect that that is because the people at Skyhook Wireless read RISKS. I pointed out the problems of IP address geolocation five years ago (almost to the day), in [RISKS-23.63](#), mentioning then that they are well known, but less well known than they should be. To recap: the data are either coarse-grained, or subject to IP address churn; and in either case they eventually become dated to the point of uselessness.

To emphasize these points, I report the following: I today ran the DNS query against "clientcontinent.cr.yip.to.", that I mentioned in [RISKS-23.63](#), from a computer in Europe. Dan Bernstein's database, still based upon the 2001 IANA IPv4 address space allocation list, reports that the machine is in North America.

"The example in the teleportation post would very easily have been solved by use of IP geolocation", says Charles Wood. No, no, and no again. I strongly emphasize that IP addresses are **not** a reliable mechanism for determining the geographical location of a machine. Posit that I, with the computer in Europe mentioned above, were in the same situation as M. Wood of having no Skyhook Wireless mapping information available. Had Skyhook Wireless fallen back to IP address geolocation using (say) the same source data as Dan Bernstein, Skyhook Wireless would have placed me on entirely the wrong continent. Even if its data were more recent, the degree to which Bernstein's database is now dated, and was dated even back at the time of [RISKS-23.63](#), shows how quickly the data quality of **any** such IP address geolocation dataset erodes over time.

There's a fairly simple point here, and yet it's one that I regularly observe people missing again and again. IP addresses, postcodes, and the like, were not invented to directly encode geographical locations. That is, simply, not their purpose. IP addresses are used for routing network traffic around Internet, and postcodes are used by postal services to route

mail through a postal system. They are designed for *those* purposes. The "locations" that they do encode are locations in the topographies of Internet network connections and of postal system sorting and delivery systems, which are often *very* different to actual geography. Any correspondence that they might have to actual geographical locations should be considered fortunate, and unreliable. Don't expect postcodes to always work in navigation systems. Don't expect your computer's IP address(es) to identify what country, or even what continent, you are in. They weren't designed for that purpose, aren't maintained and updated for that purpose, and often produce highly erroneous results when (mis-)used for that purpose.

So one should not, really, be surprised at Skyhook Wireless avoiding this well-known (but still, five years on, not well-known enough, it seems) error in this instance.

Re: Android Mythbusters ([RISKS-25.85](#))

*phil colbourn <philcolbourn@gmail.com>
Sun, 29 Nov 2009 16:50:46 +1100*

> Executive summary: Android is a screwed, hard-coded, non-portable abomination.

I'm not sure the Executive summary cited in [RISKS-25.85](#) is justifiable:

1. Android is open source although Google do add closed source applications.
2. It has been ported to many devices and even PCs, laptops and netbooks.
3. In order to keep boot times low and software base minimal, it is expected that the OS be customised for the target device - it is not designed as a general purpose OS in the same way that, say, Ubuntu is. It is an embedded OS.
4. People are free to port 'normal' Linux to their device if they choose to.
5. Design choices about what aspects of the Linux kernel or GNU libraries are implemented is a design choice. I suspect that the designers wanted to reduce the attack surface.

I think the biggest issue is the lack of open source Google Apps, which includes MarketPlace.

The key point is that Android OS is Open Source - do with it as you please.

Re: Toyota uncontrolled acceleration (Leshner, [RISKS-25.82](#))

*Jeremy Epstein <jeremy.j.epstein@gmail.com>
Sat, 28 Nov 2009 20:38:09 -0500*

JC Cantrell wrote:

>Well, that is why I buy a manual transmission. When that clutch is in, I
>KNOW I can stop the car...

Well, at least so long as your clutch is a physical device, and not a "fly by wire". I don't know if such things exist, but I can think of many reasons why a fly-by-wire clutch would be a good thing - maybe software could reduce the opportunities for stalling, or switching into the wrong gear, or burning it out by riding the clutch. And once that happens, then how long before the fly-by-wire clutch decides you really shouldn't be going into neutral at highway speeds, so it refuses to engage... and silently stops the fail-safe mechanism Cantrell describes.

--Jeremy

Re: Toyota uncontrolled acceleration (Cantrell, [RISKS-25.85](#))

Graham Reed <greed@pobox.com>

Sat, 28 Nov 2009 18:47:19 -0500

On Mon, 9 Nov 2009 12:41:33 -0800 (PST) JC Cantrell <jccant@pacbell.net> wrote:

> Well, that is why I buy a manual transmission. When that clutch is in, I
> KNOW I can stop the car...

This is getting away from the computing RISKS, but I have had clutch failure on manual vehicles. This failure mode leaves the controls unable to disengage the clutch, which means the engine cannot be decoupled from the transmission.

I use generic terms because one such incident was on a motorcycle with a hydraulic clutch. I had a cooling system fault, and was approaching boil-over in a traffic jam. Deciding the hard shoulder was better than a full breakdown in the traffic lane, I began my maneuver. Only to find that the clutch lever had no resistance--the hydraulic fluid was too hot, and it had boiled. (The clutch fluid was nearly due for changing at the time, and contaminants in it were not helping the situation.)

Fortunately, I've practiced shifting gears without the clutch, and was able to gear down enough to get off the road. Getting into neutral wasn't much more difficult. I even used the kill switch to stop the motor, even though there was nothing wrong with the ignition key circuit; I was well into emergency procedures, and forgetting "normal" operating modes.

I've also had cable clutches fail to disengage due to thermal expansion.

Still, with a true manual, you can always get to neutral with the shift lever, even without a clutch.

It's the more expensive stuff, like those "flappy paddle" boxes, that adds automatic gearbox failure modes (in the control system and actuators) to the existing failure modes of a manual box (broken shift forks, dogs, splines, and so on) and clutch (hydraulic or spring failure).



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 88

Saturday 26 December 2009

Contents

- [Insurgents Hack U.S. Drones](#)
[PGN](#)
- [Another user interface fatal accident in Afghanistan](#)
[Mark Thorson](#)
- [Security in the Ether: Cloud Computing? Or "Swamp" Computing?](#)
[Lauren Weinstein](#)
- [HP's facial-recognition can't recognize black people's faces](#)
[Randall Webmail](#)
- [Alert: Twitter apparently hacked](#)
[Lauren Weinstein](#)
- [Silent Hybrid Nearly Causes Carbon Monoxide Poisoning](#)
[Bob Gezelter](#)
- [UAL: Another risk of weather for computer based systems](#)
[Jared Gottlieb](#)
- [When the human model doesn't match the system model](#)
[Sean W. Smith](#)
- [Disconnects between the Real World and Cyberspace](#)
[Bob Gezelter](#)
- [Obscure GPS problems not just in remote areas](#)
[Jeremy Epstein](#)
- [On the Road with a GPS System](#)
[Gene Wirchenko](#)
- [GPS ads for captive bus riders](#)
[jidanni](#)
- [Cruise control failed to disengage](#)
[Steve Cody](#)
- [Re: LED Traffic Lights are efficient but cannot melt away snow](#)
[John Johnson](#)
- [Info on RISKS \(comp.risks\)](#)

Insurgents Hack U.S. Drones

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

Thu, 17 Dec 2009 16:28:57 PST

Militants in Iraq have used \$25.95 off-the-shelf software to intercept live video feeds from U.S. Predator drones, potentially providing them with essence, the Predator video link to the ground station is unencrypted. Insurgents are sniffing the link and reconstructing the video. The U.S. government has known about this flaw for a decade, but ignored it, offering the usual litany of problems: encrypting the link would delay the program, cost more, and complicate operations. "But the Pentagon assumed local adversaries wouldn't know how to exploit it, the official said." The stolen video feeds also indicate that U.S. adversaries continue to find simple ways of counteracting sophisticated American military technologies. [Source: Siobhan Gorman, Yochi J. Dreazen and August Cole, \$26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected, Wall Street Journal, 17 Dec 2009, front page; PGN-ed] The myth of security by obscurity strikes again. <http://ebird.osd.mil/ebfiles/e20091217723006.html>

I've seen arguments that key management would be too difficult to manage, although some reports say that efforts are now underway to encrypt. Other arguments are that uncleared soldiers need access to the video streams, but that seems to confuse "encryption" and "classification". Don't forget that the former does not require the information to be classified for confidentiality or that it is not important for integrity! Also, the new Reaper drones cost over \$10 million each and have the same vulnerability.

Jeremy Epstein noted that *WiReD* reports that it's not just drones, but also regular combat aircraft - although it's harder to intercept the (unencrypted) signal from the regular planes. The talk I've heard today that "it's not such a big deal" seems odd - if you were an insurgent, having a few minutes warning that there's a drone coming your direction would be useful data.

<http://www.wired.com/dangerroom/2009/12/not-just-drones-militants-can-snoop-on-most-us-warplanes/>

Also, see Bruce Schneier's essay on the topic:

http://www.wired.com/politics/security/commentary/securitymatters/2009/12/securitymatters_1223

Another user interface fatal accident in Afghanistan

Mark Thorson <eee@sonic.net>

Tue, 15 Dec 2009 20:22:41 -0800

The circumstances of this incident seem very similar to the incident a few years ago in which changing batteries cleared the offset between the observer's GPS position and the target position on his Garmin.

<http://www.dailymail.co.uk/news/article-1236087>

When the target position is cleared, it would probably be better to initialize it 100 meters to the east or something, rather than right on top of the observer position.

✂ Security in the Ether: Cloud Computing? Or "Swamp" Computing?

Lauren Weinstein <lauren@vortex.com>

Thu, 24 Dec 2009 11:04:16 -0800

Security in the Ether: Cloud Computing? Or "Swamp" Computing?

[From NNSquad, Network Neutrality Squad, <http://www.nnsquad.org>]

An important article worth reading:

<http://bit.ly/4uYabf> (MIT Technology Review)

My personal "thumbnail" view on this is that:

- a) Cloud Computing" holds enormous promise.
- b) Most of the key security and other operational issues associated with cloud computing are solvable, including aspects of pervasive encryption that would protect cloud computing clients from potential snooping by theoretically postulated unscrupulous cloud service providers.
- c) The financial and intellectual resources (including basic policy analysis) required to understand and solve these problems on an *a priori* basis, rather than on an "after there's a mess" reactive basis, are in general insufficiently emphasized and deployed.
- d) Given (c), not all of the current rush to cloud computing on today's widely available platforms can necessarily be justified as wise, particularly where sensitive and/or privacy-critical data is involved.

Or in other words, Cloud Computing can be a Really Good Thing if done right, but let's not get the cart in front of the horse.

✂ HP's facial-recognition can't recognize black people's faces

Randall Webmail <rvh40@insightbb.com>

December 21, 2009 1:29:12 PM EST

[From Dave Farber's IP]

This is awkward. It appears that HP's new webcams, which have facial-tracking software, can't recognize black faces, as evidenced in the above video. HP has responded:

- > We are working with our partners to learn more. The technology we use is
- > built on standard algorithms that measure the difference in intensity of
- > contrast between the eyes and the upper cheek and nose. We believe that
- > the camera might have difficulty "seeing" contrast in conditions where
- > there is insufficient foreground lighting.

> HP Face-Tracking Webcams Don't Recognize Black People - Hp - Gizmodo

> (21 December 2009)

<http://gizmodo.com/5431190/hp-face+tracking-webcams-dont-recognize-black-people>

<http://snipurl.com/tsfli>

Archives: <https://www.listbox.com/member/archive/247/=now>

#Alert: Twitter apparently hacked

Lauren Weinstein <lauren@vortex.com>

Thu, 17 Dec 2009 22:38:41 -0800

Twitter has apparently been hacked. Invalid security certificate for wrong site on the Twitter [https: home page](https://twitter.com), Iranian Cyber Army hack page on main twitter.com. This looks much like an SQL injection exploit I've dealt with in the past, but I don't know for sure at this point if the actual Twitter infrastructure has been hacked or if this is a DNS hack.

Presumably this won't last long, but more info when available.

Date: Fri, 18 Dec 2009 09:47:59 -0800

Twitter has not officially released details on last night's hacking-related outage of their Web site, other than to state that it was (as many of us suspected) a DNS-related attack.

There are some other details floating around unofficially. Twitter's DNS services are provided by Dyn Inc.'s Dynect Platform. Dyn is insisting that their systems were not compromised and that nobody accessed Twitter's DNS data without appropriate (login) credentials.

This suggests (but again, this is **not** confirmed) that Twitter's account on Dyn was somehow itself compromised, possibly through "social engineering" or other techniques that resulted in the attackers gaining login access to the Twitter account on Dynect, allowing them to change the associated DNS data. (From Dyn's standpoint, this could still be considered to be "appropriate login credentials.")

It goes without saying that the "Iranian Cyber Army" hack page is almost certainly a fraud, and there are no indications that Iran actually had anything to do with this attack (breathless statements blaming Iran being made by some media points notwithstanding). By the way, I've seen this exact page resulting from various bot-based, non-DNS attacks in the past.

Presumably more "official" statements about what transpired will be forthcoming at some point, after the finger-pointing slows down a bit.

Of course this once again demonstrates the fragility of DNS, but that's hardly a headline news revelation at this stage of the game.

Date: Fri, 18 Dec 2009 12:14:27 -0800

Now confirming [Ref: <http://www.nnsquad.org/archives/nnsquad/msg02460.html>] that the Twitter DNS diversion last night was the result of someone using Twitter's own login credentials to change DNS data at Dyn's site, according to Dyn's CTO:

<http://bit.ly/80Ve4Y> (Wired)

So as suspected, this was not a "sophisticated" attack (e.g., DNS cache poisoning) but rather a conventional login attack.

It is interesting to consider that apparently a single username/password pair was able to take Twitter's entire Web site effectively offline globally.

At the very least one would hope that more advanced account control mechanisms (e.g., certificate-based access authentication) would be employed with critical accounts for organizations at this level.

✂ Silent Hybrid Nearly Causes Carbon Monoxide Poisoning

*Bob Gezelter <gezelter@rlgsc.com>
Sat, 26 Dec 2009 08:07:53 -0500*

The Decemeber 27, 2009 Sunday New York Times Magazine (p. 8) contains a Letter to the Editor from Liz Cantarine entitled "Artificial Car Noises".

Ms. Cantarine describes how she accidentally left her hybrid automobile running in her garage. Apparently, when returning from a shopping trip, she became preoccupied with the packages in the trunk, and forgot to turn off the car. The car continued running, filling the garage space with fumes.

It is an interesting problem. Synthetic noise generators are being required due to a hazard to visually impaired pedestrians, but this is the first report I have seen describing a danger to owners and their families from silent cars.

✂ UAL: Another risk of weather for computer based systems

*jared gottlieb <jared@netspace.net.au>
Sun, 20 Dec 2009 15:51:55 -0700*

From the United Airlines website 20 December 2009

Weather-related delays and cancellations resulted in a significantly higher volume of calls into United's reservations centers. Our voice recognition software was hampered by the volume, which in turn drove longer wait times. We sincerely regret the inconvenience faced by our guests, and are pleased to report that our voice recognition software is fully up and running and wait times have been significantly

reduced. We are still experiencing higher than normal call volume, which may result in sporadic call interruptions.

When the human model doesn't match the system model

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

Fri, 25 Dec 2009 18:31:29 -0500

The real world gives another instance of what can go wrong:

A man in Epping tried to deposit \$580 into an ATM but neglected to note the transaction had not completed and walked away without the returned cash.

The next person pocketed the cash, but of course was identified.

[Source: AP item, 25 Dec 2009]

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

Associate Professor, Department of Computer Science, Dartmouth

Disconnects between the Real World and Cyberspace

Bob Gezelter <gezelter@rlgsc.com>

Sat, 26 Dec 2009 08:19:04 -0500

Sometimes the real world and cyberspace are truly separate realms. The other day, I experienced two episodes of just such a disconnect.

I was trying to verify the hours for a branch bank in the area. Checking the bank's www site, I discovered that the branch was not listed. Calling the customer service line, I was assured that if the branch was not listed, it must have closed.

Three hours later, I visited the branch. It was quite active, with no signs of closing or relocation. A discussion with the officers revealed that I was not the first person to note the error. It had been reported to corporate, but for some reason the data had not been corrected.

The same day, I had a similar experience with a major international distributor. A local branch was not listed as one of their locations, even though it was open and active.

It is an interesting question of IT governance when a company is unable to keep its list of branches up to date.

A longer discussion of this episode can be found in "Bricks and Mortar Hidden by Cyberspace".

<http://www.rlgsc.com/blog/ruminations/bricks-and-mortar-hidden-by-cyberspace.html>

Robert "Bob" Gezelter, +1 (718) 463 1079 35-20 167th Street, Suite 215
Flushing, New York 11358-1731 <http://www.rlgsc.com>

#Obscure GPS problems not just in remote areas

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Tue, 15 Dec 2009 16:02:12 -0500

The discussion of GPS issues with BMWs reminded me of a recent GPS navigation problem I ran into using my brand-new Garmin nuvi 275T.

The Garmin maps of Washington DC have an unfortunate mistake: they don't understand that K Street runs **under** (and parallel to) the Whitehurst Expressway. The Whitehurst Expressway intersects Key Bridge (well, actually it runs into M Street a block from Key Bridge), but K Street does not except when separated by 100 vertical feet. Specifically, if you ask the GPS for directions from northwest Washington DC (I was coming from the Tenleytown neighborhood) to Fairfax VA, it tells you to take Rock Creek Parkway south, exit onto K Street west, then drive along K Street and then make a left on Key Bridge - which is 100 feet above you. Google Maps, on the other hand, gets this right.

The RISK is thinking that GPS errors only occur in out-of-the-way locations. This is in the Georgetown neighborhood of Washington DC, hardly remote!

[Alarmin' Garmin Swarmin' Harmin' not Charmin'. PGN]

#On the Road with a GPS System

Gene Wirchenko <genew@ocis.net>

Tue, 15 Dec 2009 18:46:58 -0800

[Whenever I fail to run an item you think I may have missed, please resubmit (with "notsp" in the subject line, of course. This is an instance of something I apparently missed 3.5 years ago. Sorry!!! PGN]

GPS problems have been in the news more lately, so I thought that I would resubmit this item. I have since moved back to Canada. A key point: All of the events that I describe happened on a trip to my mom's and back. This is not a collection of events over a period of, say, months.

On the Road with a GPS System

There have been previous submissions of the joys of GPS systems used in driving. They have been brief. This writeup goes into much more detail and details more than one risk. I wrote this in June of 2006, but have kept the present tense.

I am a Canadian citizen, but I live in Bellingham, WA, USA and work near it. At the beginning of April, I went to visit my mother who was then living in Greenwood, BC, Canada. At the car rental place, because neither of the cars

available was acceptable -- perfumed cleaners are a non-computer risk some face -- and because I am a frequent customer, I was upgraded at no extra cost to a SUV, a SUV with a GPS navigator: the NeverLost system. I did not get lost, but that was not entirely due to the device.

I lost little time in starting to play with this new toy.

I found it interesting all of the streets that were nearby. Unfortunately, sometimes, the names were truncated, and in at least one case, the truncated name made sense as a word. I did not see any way to adjust the magnification.

I saw that I could ask for a course to my mother's. Unfortunately, the interface was a bit confusing and rather than selecting the city of Greenwood, BC (the smallest incorporated city in Canada), I accidentally selected the then-current city and a street. There is a street named Greenwood in Bellingham. There is also one in Lynden (near to Bellingham). I found myself being directed to the south. My mother's home was north and east. The device was quite persistent: "Please proceed to the designated route." Later, it got desperate, words to the effect of "When legal, please make a U-turn." I finally shut it off.

I tried again later, and it worked, mostly. My mom lived on Kimberley Street. It is one of, if not the, longest street in Greenwood. The device did not know its name. It did know many of the other streets, including the cross-street by my mom's then-home. The cross-street is two short blocks long. I finally programmed the device for the city centre of Greenwood.

I crossed the border at Sumas. I then proceeded to Hope. While on the way, at one point I glanced at the display to see that a road was displayed to the right. This was disconcerting as that was where a cliff was. The road turned out to dead end. I think it was a deactivated road, possibly the old highway.

I usually stop at a certain gas station in Hope to buy a sandwich and drink. In that area, there are under- and over-passes. The device got confused. It got its revenge shortly. When I restarted the SUV, I looked at the display and was confused. The USA operates on the Imperial system of measure, and Canada uses the metric system. The device, recognising that it was in Canada, had switched to metric. When I looked more closely, I could see the miles display. It was rather smaller than the digits.

The gas station is on the old highway which parallels the current highway. To get onto the current highway involves a few tight turns. Some of these, the device knew and some it did not. I was directed to make turns when there was no other road, but sometimes, the curve had no instructions. This also happened when I left Keremeos, BC.

The device warns about 2 Km before a turn and then just before. The turnoff for the Hope-Princeton Highway had already diverged from the main highway by nearly one lane-width before the device announced the just before warning that I should turn. I was already in the correct lane. Had I not been in the correct lane, I could not have safely switched.

Not long after, I looked at the time display. As it was just after noon, I could not tell whether it was the time I would arrive in Greenwood or the time left before I would arrive in Greenwood. Later, I found that that detail was documented on the card that was dangling from the unit, but many other things were not.

While driving on the Hope-Princeton Highway, I found that many roads that had no names were on the display, but that some roads that had names were not present.

The Hope-Princeton Highway does run through wilderness, and in many places, there are no other roads nearby. That did not stop the device from telling me three times each way to "Proceed to the designated route." The voice is a bit startling when it is not expected.

Glancing from time to time at the time-to-go display, I got suspicious. It seemed to be assuming 80 Km/h. This is the default highway speed in BC, but the Hope-Princeton Highway is known for being rather curvy in places. It has plenty of signs suggesting slower speeds. At one place, the advisory is 20 Km/h. In the summer, one can go bombing along much of the highway. In the winter, the curves get more dangerous, and you had better slow to 20 Km/h on the worst curve. This was near the end of breakup, so conditions could vary considerably. What was the device assuming?

Princeton is at the west end of "The Regional District of Okanagan-Similkameen". The device displayed this from time to time clipped to "Okanagan-Similkameen Region". Much of this time, it displayed this next to the road on the other side of the Similkameen River. There was no differentiation of region or city names from street names. That road across the river is called "Old Hedley Road". When it finally was displayed, well, the device leaves off the road designation. The device did not display the river though earlier, it had displayed much smaller creeks.

Leaving the village of Keremeos, BC, the road winds up a hill. At the bottom of the hill, there is a curve to the right (which the device told me about), a curve to the left at the top of the hill (which the device did not tell me about), and finally a right turn to the highway I wanted (which the device told me about). The up-shot was that I was told to make a right turn followed by a right turn, and it did not make sense. It was good that I knew the road. Had I blindly followed the advice, I would have gone down a 60 (or so) degree slope.

In the hamlet of Cawston, BC, the device thought that the main street dead-ended and suggested accordingly.

I get paid in US dollars, so I prefer to spend US dollars. Therefore, rather than continuing through Canada, I cross at Nighthawk, WA, proceed to Oroville, WA, fill up with gas, and cross back into Canada at Osoyoos, BC.

The device kept trying to get me to turn around. I was wondering when it would give up. While I was wondering I saw a road displayed on the device, but there was no road there, no sign of there ever having been a road there, and no sign of anything else that the device should know about (such as a

creek). A few miles past the border crossing, there is another road, a real one. The device seems to understand the world as segments. When I got off the segment, it recalculated. The road to Oroville is a nice drive, very pretty. At least one of the roads that the device shows is actually a long driveway.

Ah, Canada. The device was displaying Imperial. Remember how the device switched measuring systems in Hope? It switched again after I restarted the SUV at the gas station in Oroville. The system in use depends not on what country you are in, but what country you were in when you started the vehicle. I found later that one can force the setting, but I did not experiment to see if that locked down the measuring system used or that it just lasted until the next vehicle startup. Imagine explaining to a border officer that you are experimenting with your GPS. Guessing is such fun.

The device also had an odd idea of which way I should go. As far as I can tell, it intended to keep me on the highways. I know of a shortcut, and I took it. The device did not handle it well. Trying to get me back "on course", it suggested some bad ideas.

1) One road to the left comes down a hill which is steep enough that the road is broken into left and right branches. The device suggested that I take the far branch. This would have necessitated a turn of approximately 150 degrees. The near branch is about thirty degrees.

2) Later, it suggested that I take a right turn -- remember that the previous suggestion was for a left turn? -- onto a narrow road with patched potholes when I was on the best road around and which led straight to the programmed route.

3) I rejoined the programmed route and prepared to turn right. The device was instructing me to turn left!

One thing that I never did solve was how to get the device to just display without having a route programmed. I wanted to see where I was without having to select a destination.

The device has a safety feature that disables most of the user interface when the vehicle is in motion. It was also mounted so that the person in the front passenger seat would not be able to see the display. I thought this was rather counterproductive.

When I set out to go home, I planned again to stop in Oroville for gas. While I did not know the exact address, I thought I could get close. For some reason, the highway was not listed. Unfortunately, the device requires you to select first what you want (nearest city centre, a particular city centre, or a particular intersection) then the city name. The other way around is much more natural to me. It also would have been much quicker as entering alphabetic was a slow process with no keyboard.

Again, I crossed the border at Nighthawk. I crossed into the US a final time. The border between Canada and the USA is at 49 degrees north latitude. For some reason, the device told me I was in the USA when it still displayed me at seven seconds of latitude north of the border.

According to my estimate, I was much closer.

I decided to let the device tell me how to get to Bellingham. Understand that I take a short route. Roughly, I go west, then I go south. The system picked a route that was much longer and windier. Among other places that I saw, the oddly appropriate Chance Road. In Osoyoos, it was trying to keep me on the highways. Here, it avoided them until the end.

I did make it home safely, and I certainly see where these devices are useful, but much salt is needed.

✶ GPS ads for captive bus riders (Re: Sullivan, [RisKS-25.87](#))

<jidanni@jidanni.org>

Fri, 18 Dec 2009 10:57:52 +0800

Like the in-bus GPS "next bus stop" LED marquee boards here in Taiwan. Between stops they have been programmed not to waste an idle moment, but instead scroll "thank you for riding XYZ Bus Co." to riders concentrating on them to learn the next stop's name. At least accompanying audio just chants the stops. Naturally everything must be repeated for each local language too.

✶ Cruise control failed to disengage

Steve Cody <steve@codygang.net>

Sun, 20 Dec 2009 13:41:37 +1100

Similar to recent reports of uncommanded acceleration, we had an incident where cruise control could not be disengaged. This link should bring up related news items..

http://news.google.com.au/news/more?um=1&cf=all&ned=au&cf=all&ncl=dilb-MX_41mrfpMRXwbgO6EixST7M

Or google news for "Cruise control Frankston"

✶ Re: LED Traffic Lights are efficient but cannot melt away snow

John Johnson <jvj@golden.net>

Wed, 16 Dec 2009 08:05:08 -0500

The problem is also evident on motor vehicles with LED signal and stop lights. Snow is not melted away by the signal and stop lights and accumulation blocks the lights.

new item:

<http://www.newser.com/story/76251/led-traffic-lights-efficient-but-cant-melt-away-snow.html>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 89

Thursday 7 January 2010

Contents

- [Y2K+10 problem 1. German contactless bank cards](#)
[Debora Weber-Wulff](#)
 - [Y2K+10 problem 2: Symantec](#)
[PGN](#)
 - [Y2K+10 problem 3: Bank of Queensland Eftpos system](#)
[Jared Gottlieb](#)
 - [Y2K+10 problem 4: SpamAssassin tags "2010" e-mail as spammish](#)
[Danny Burstein](#)
 - [Y2K+10 Bug. for those who thought that Y2K was a made up crisis](#)
[Bob Gezelter](#)
 - [Verizon: I just don't know what to say](#)
[Geoff Kuenning](#)
 - [Eurostar Risks](#)
[Anthony Thorn](#)
 - [Display: none; visibility: hidden; overflow: hidden](#)
[jidanni](#)
 - [Crumbling Crypto: RSA 768 modulus factored + security implications](#)
[PGN](#)
 - [Couple Stuck in Oregon Snow for 3 Days After GPS Leads Them Astray](#)
[Richard Grady](#)
 - [Risks of Relying on Downstream Syndication](#)
[Bob Gezelter](#)
 - [Re: Teleportation via Skyhook](#)
[Gary Bliesener](#)
 - [Toyota acceleration; is it just the gas pedal or not?](#)
[David Leshner](#)
 - [Re: Another user interface fatal accident in Afghanistan](#)
[Curt Sampson](#)
 - [Re: LED Traffic Lights are efficient ...](#)
[Dick Mills](#)
[Jerry Leichter](#)
[Amos Shapir](#)
[Rob Seaman](#)
 - [Info on RISKS \(comp.risks\)](#)
-

Y2K+10 problem 1. German contactless bank cards (3 messages)

Debora Weber-Wulff <weberwu@htw-berlin.de>

Tue, 05 Jan 2010 00:33:39 +0100

Happy New Year!

Germans now have the answer as to why they came up short at the ATMs after the New Year. Tagesschau reports online that people who were using newer cash machine cards that had new-fangled golden chips in them were told at the machine that their cards had an error because of a "software error". Not only ATM machines were affected, supermarkets and such that check cards online refused to accept the cards.

<http://www.tagesschau.de/wirtschaft/eckarte102.html>

Since I have spent the first 4 days of the year writing "20010", anyone want to speculate that this is the error? No details on the exact nature of the error as yet. It is scheduled to be fixed tonight (Jan. 4!).

Not all of the machines refused to work, only the newer ones with the "EMV-Standard" (<http://en.wikipedia.org/wiki/EMV>) which are to keep the cards from being duplicated illegally and "secure" the data.

Older cards, which store information on a magnetic strip, were not affected.

I'm glad I still have an old card and an ancient machine around the corner. I got money after New Year's.

More: Wed, 06 Jan 2010 17:36:57 +0100

It is getting curiouser and curiouser! The Tagesschau reports in <http://www.tagesschau.de/wirtschaft/eckarte108.html> and <http://www.tagesschau.de/wirtschaft/kreditkarten144.html>, which

I translate and summarize here:

It turns out that even more cards are affected, and even more people are unable to use either their EC cards or their credit cards to obtain cash or to pay in stores.

The culprit has been named: The company that produces the cards, Gemalto. Seems that the software thinks that it is the year 2016 and not 2010, so all of the cards are no longer valid. A friend pointed out to me that 2016 is 11111100000 in binary. [*]

The problem is a program stored on the chip. The banks don't want to have to exchange all of the cards (a really expensive solution), so they are looking for a workaround. One was promised for Monday evening, but it has not yet materialized. ATMs are generally now accepting the cards again [meaning they probably don't do any checking now...], but the Point of Sale terminals refuse to cooperate.

30 million cards are affected, and changing them would entail the owners all

having to learn a new code for their cards. Only German cards are affected. Many hundred thousand cards were just exchanged in November because of problems with the data of cards used in Spain having been available after a security breach.

The company Gemalto was formed 2006 in the fusion of the French company Gemplus International and the Dutch Axalto Group. The company has 10.000 employees and produces bank cards, telephone SIM cards and electronic passports. The company reports a volume of 1,68 billion euros in 2008.

Consumer organizations and the consumer minister are blasting the banks for informing the consumers only a little bit at a time.

* On a side note, customers of smartphones using Windows Mobile operating system have been noticing that incoming SMS messages also have the date 2016.

Still More: Thu, 07 Jan 2010 08:58:34 +0100

Just a bit of scotch tape, sir!

The great Y2K+10 problem in Germany continues:

The chips were put on the cards to make them more difficult to duplicate. But it turns out, they at least have a fail-safe mode. If the chip is found to be malfunctioning or not there, the card readers resort to reading the magnetic stripe.

Spiegel and others report that all it takes is a little Scotch tape over the contacts of the card, and the readers will switch to fail-safe mode. Retailers now dispense tape at the cash registers.

<http://www.spiegel.de/wirtschaft/soziales/0,1518,670433,00.html>

It is great that they have this mode, but it kind of makes you wonder how safe these expensive chips really make you, if they can so easily be defeated.

Prof. Dr. Debora Weber-Wulff, HTW Berlin, Treskowallee 8, 10313 Berlin
Tel: +49-30-5019-2320 <http://www.f4.htw-berlin.de/people/weberwu/>

Y2K+10 problem 2: Symantec

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 7 Jan 2010 11:44:54 PST

Symantec Y2K10 Date Stamp Bug Hits Endpoint Protection Manager
<http://www.eweek.com/c/a/Security/Symantec-Y2K10-Date-Stamp-Bug-Hits-Endpoint-Protection-Manager-472518/?kc=EWKNLSTE01072010STR1>

Updates after 31 Dec 2009 11:59 p.m are being labeled as "out-of-date."

#Y2K+10 problem 3: Bank of Queensland Eftpos system

jared gottlieb <jared@netspace.net.au>

Sun, 3 Jan 2010 11:22:18 -0700

Retail businesses across the country have lost thousands of dollars over the long weekend because a computer glitch left shoppers unable to use the Bank of Queensland's Eftpos terminals. BOQ's Eftpos machines skipped ahead six years when the clock ticked over to January 1 and started date stamping January 2016. BOQ staff have not been able find what caused the problem, but a temporary solution has been put in place to ease retailers' frustrations. The glitch cost businesses untold amounts as the Eftpos terminals read customers' [debit] cards as having expired and refused their transactions. [Source: *Sydney Morning Herald* 3 Jan 2010, AAP news wire]

#Y2K+10 problem 4: SpamAssassin tags "2010" e-mail as spammish

danny burstein <dannyb@panix.com>

Sat, 2 Jan 2010 10:28:38 -0500 (EST)

Spam Assassin is a pretty widely used e-mail filtering program. One of the rules it uses is checking the date on incoming e-mail. If it's wrong, then some points are added to the "is this spam?" score.

It seems that up until a rushed update the afternoon of Jan. 1st, 2010, the standard installations, using the default rule set, considered the year "2010" to be way off in the future. Accordingly they gave e-mail with that date an automatic 3.5 points. Five points gets you to the "spam threshold", so lots of material coming through on the new year got clobbered.

It seems the "year date" was hard/hand coded, as opposed to making a comparison to "today's" date.

The SpamAssassin folk have a new version which corrects this problem. Folk running SA can also modify that one rule set and bypass the issue.

Details:

http://wiki.apache.org/spamassassin/Rules/FH_DATE_PAST_20XX

https://issues.apache.org/SpamAssassin/show_bug.cgi?id=6269

[Also noted by Dave Horsfall:

"To summarise, it blocks messages with dates set too far in the future (which apparently is a common spammer trick - I read my e-mail in forward order of delivery) and 2010 was inside the range of 2010-2099."]

<https://secure.grepular.com/blog/index.php/2010/01/01/spamassassin-2010-bug/>

#Y2K+10 Bug, for those who thought that Y2K was a made up crisis

Bob Gezelter <gezelter@rlgsc.com>

Wed, 06 Jan 2010 16:52:14 -0500

Recently, I have seen several letters questioning the whether Y2K was a real hazard, or whether it was an invented crisis. Several of these letters have appeared in *The New York Times* Letters page following the publication of "It's Always the End of the World as We Know It" (Op Ed, 1 Jan 2010).

The coincidence is uncanny. Yesterday (5 Jan 2010), Network World published "Y2K all over again in 2010?" on a series of outages related to this most recent decade change.

The Network World article can be found at:

<https://www.networkworld.com/news/2010/010510-date-change-problems.html>

The New York Times Op Ed can be found at:

<http://www.nytimes.com/2010/01/01/opinion/01dutton.html>

The Letters relating to Op Ed can be found at:

<http://www.nytimes.com/2010/01/06/opinion/l06climate.html>

- Bob Gezelter, <http://www.rlgsc.com>

✂ Verizon: I just don't know what to say

Geoff Kuenning <geoff@cs.hmc.edu>

Sat, 02 Jan 2010 14:23:51 -0800

Recently, Verizon took over MCI, resulting in me getting them as my new local telephone provider. This afternoon, I used Verizon's online site to change the billing address for my account. About an hour later, I got a nice automated phone call that was intended to verify that the change was legitimate.

So far, so good. But the automated voice informed me that if I hadn't authorized the change, I should "contact us at [slight pause] between the hours of [slight pause] and [slight pause]. Thank you for choosing Verizon."

I guess I should be glad that "[slight pause]" didn't come out as "left parenthesis null pointer right parenthesis."

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

✂ Eurostar Risks

"anthony.thorn@bluewin.ch" <anthony.thorn@bluewin.ch>

Sun, 27 Dec 2009 10:09:44 +0000 (GMT)

On December 18th, 5 Eurostar passenger trains failed, in the Channel tunnel

trapping 2000 passengers. (Eurostar is the rail service through the tunnel under the English channel) The service only resumed on Tuesday 22nd.

The failure was due to inadequately "winterised" trains encountering snow and extremely cold weather: "The snow entered the locomotives' ventilation system... When the trains entered the great warmth of the tunnel, the electrical system short-circuited and the traction motors of the Eurostars cut out and would not start again."

This problem was known. It is NOT a "Black Swan" !

Apparently in contrast to the passenger trains, the car-transporter trains are sufficiently winterised.

If the failure was not already a disaster, there is no doubt at all about the evacuation.

Some passengers were trapped in the tunnel for up to 14 hours, and complained about lack of/conflicting information, as well as the heat.

Thousands of passengers waited at the railway (train) stations for a service that would not be available for days.

There was not much of an alternative: huge queues for ferries , and planes delayed by the weather.

e.g.

<http://www.independent.co.uk/news/uk/home-news/thousands-stranded-as-eurostar-service-is-suspended-1846350.html>

The risks:

1. (IMHO) an inadequately tested contingency plan.
2. We passengers assume that a rail service will be reliable -because it almost always is. Perhaps we should not/cannot and need to take our own "emergency equipment" along?

Display: none; visibility: hidden; overflow: hidden

<jidanni@jidanni.org>

Tue, 05 Jan 2010 06:37:57 +0800

I suppose it's fair game these days to hide anything you like within an HTML div style="display: none; visibility: hidden; overflow: hidden;" like they do on <http://topics.cnn.com/topics/weather> . They even store a "404 Error The page you requested cannot be found" inside that HTML div. "Who would ever browse without using (our) stylesheets?"

✂ **Crumbling Crypto: RSA 768 modulus factored + security implications**

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

Thu, 7 Jan 2010 11:40:28 PST

After an extensive multiyear collaborative effort, the RSA 768-bit challenge number has been factored, suggesting that 1024-bit prime products may be somewhat closer to approaching the end of their practical lifetimes.

<http://bit.ly/8xXSgy> (International Association for Cryptologic Research)

✂ **Couple Stuck in Oregon Snow for 3 Days After GPS Leads Them Astray**

Richard Grady <richard@richbonnie.com>

Mon, 28 Dec 2009 13:52:20 -0800

KLAMATH FALLS, Ore. A Nevada couple letting their SUV's navigation system guide them through the high desert of Eastern Oregon got stuck in snow for three days when the GPS unit sent them down a remote forest road.

<http://www.foxnews.com/story/0,2933,581303,00.html>

✂ **The Risks of Relying on Downstream Syndication**

Bob Gezelter <gezelter@rlgsc.com>

Mon, 04 Jan 2010 19:20:31 -0500

It is common to rely on downstream syndication feeds (e.g., ATOM, RSS, usenet news) for information. Unfortunately, sometimes there are "clogs" in the pipeline that result in delayed, lost, or out of sequence messages.

Those who read RISKS using Google Groups have recently experienced just such an episode. [RISKS 25.85](#), 25.86, and 25.87 are out of sequence on the archive at <http://groups.google.com/group/comp.risks> and [RISKS 25.88](#) is completely missing as of this date (4 January 2010), despite having been posted on 26 December.

Fortunately, the RISKS page at <http://www.risks.org> is up to date.

Bob Gezelter, <http://www.rlgsc.com>

✂ **Re: Teleportation via Skyhook**

Gary Bliesener <gbliesener@comcast.net>

Tue, 29 Dec 2009 10:45:31 -0500

The default browser, Polaris 6.0, on my Samsung Rant is nearly useless so I installed the Opera Mini-Browser. I ran into IP geolocation issues when responding to e-mailed employment alerts, as many websites would reject my application with a message informing me that one must be a United States resident to apply for their position, even though I am an American using the phone in the mid-Atlantic region of the United States. The Opera mini-browser evidently brings with it an IP address out of what IP geolocation types would label a "Norwegian address pool". I had to wait until my return home to apply, rather defeating the purpose of purchasing a web and e-mail enabled cellphone.

Gary Bliesener, Unix System Administrator

✂ Toyota acceleration; is it just the gas pedal or not? ([RISKS-28.85](#))

*David Leshner <wb8foz@panix.com>
Sun, 27 Dec 2009 01:35:32 -0500*

<http://www.latimes.com/business/la-fi-toyota-throttle29-2009nov29,0,5254584.story>

An *LA Times* item has lead the coverage of the issue, bringing up the accusation that the problem is not just mechanical interference between the mats and the pedals, but also more.

Eric Weiss was stopped at a busy Long Beach intersection last month when he said his 2008 Toyota Tacoma pickup unexpectedly started accelerating, forcing him to stand on the brakes to keep the bucking truck from plowing into oncoming cars. .. But Weiss is convinced his incident wasn't caused by a floor mat. He said he removed the mats in his truck months earlier on the advice of his Toyota dealer after his truck suddenly accelerated and rear-ended a BMW.

Also, I saw a mention that a previous driver of the car that crashed had complained to the dealer about the problem, but it was reissued to the victim despite that. If true, THAT would not alter the cause, but would likely change the legal liability issues.

✂ Re: Another user interface fatal accident in Afghanistan

*Curt Sampson <cjs@starling-software.com>
Sun, 27 Dec 2009 16:14:54 +0900*

Re: Mark Thorson, [RISKS-25.88](#)

> When the target position is cleared, it would probably be better to
> initialize it 100 meters to the east or something, rather than right on
> top of the observer position.

Where it might drop on your friends?

It seems to me one wants to expand the range of values to include "no target position." It can't be all that unusual sometimes not to want to drop a bomb.

Curt Sampson <cjs@cynic.net> +81 90 7737 2974

Re: LED Traffic Lights are efficient ... (R 25 88)

*Dick Mills <dickandlibbymills@gmail.com>
Sun, 27 Dec 2009 09:47:25 -0500*

John Johnson ([R 25 88](#)): "The problem is also evident on motor vehicles with LED signal and stop lights. Snow is not melted away by the signal and stop lights and accumulation blocks the lights."

Neither can incandescent stop and signal lights melt snow if they are not used often; such as long stretches of driving on the open highway. Nor could they melt snow when there was a generous air gap between the bulb and the lens cover.

I can't recall any mention of this risk in the pre LED era. What's new?

Re: LED Traffic Lights are efficient ... (R 25 88)

*Jerry Leichter <leichter@lrw.com>
Sun, 27 Dec 2009 05:38:43 -0500*

John Johnson's mention ([R 25 88](#)) of a story that LED traffic lights can be a problem if it snows because they don't generate enough heat to clear themselves brings to mind a repeated story from the NY area. Every fall, we get delays in mass transit because of wet leaves on train tracks. I never recalled hearing of such problems years back, and indeed reports have indicated that this is another side-effect (or lack of a side-effect!) of new technology.

In the old days, trains stopped by apply brake pads to the wheels. The resulting friction heated the wheels and rails and rapidly dried and burned off any leaves. Today, the trains use regenerative braking: The wheel motors are run as generators, recovering much of the kinetic energy of the train as electricity. Much more efficient - but as a result, the wheels and rails no longer hot enough to perform a leaf-clearing function.

Re: LED Traffic Lights are efficient ... (R 25 88)

*Amos Shapir <amos083@hotmail.com>
Sun, 27 Dec 2009 17:55:49 +0200*

This is actually an old problem with a new twist: the designers of traffic lights and headlights were -- probably unknowingly -- relying on an undocumented feature of incandescent light bulbs, namely their ability to generate enough heat to melt snow on cold days. Obviously it did not occur to anyone that light fixtures should be redesigned for a different type of bulbs.

✂ Re: LED Traffic Lights are efficient ... (R 25 88)

*Rob Seaman <seaman@noaa.edu>
Mon, 28 Dec 2009 00:07:47 -0700*

The general class of risk here is that of unintended consequences. It may be helpful to drill down into the specifics of what is going wrong. In both of these submissions (traffic or vehicle signals), LEDs are replacing incandescent bulbs in outdoor applications subject to varying weather conditions. The notion appears to be that nobody could have predicted that more efficient lamp technology would be subject to a failure mode in the snow.

Such a notion is mired in confusion over the difference between describing a problem and entertaining solutions to that problem. "Unintended consequences" is another way of saying "undiscovered requirements". The underlying problem is one of signaling, not of lighting technology. After all, before there were traffic lights, there were unlighted traffic semaphores. Drivers still use hand signals on occasion to supplement lighted turn signals and brake lights.

The common goal is to communicate signals (of intent, permission, and proscription) between a community of drivers, pedestrians, and other roadway users. In addition to numerous requirements relating to sequencing of interlocking signals, there are - as a matter of course - various requirements regarding weather and ambient visibility (and other sensory) conditions. For instance, presumably the LED manufacturers did not neglect to consider the effect of rain on the operation of their signals.

A complete set of top level requirements for a roadway signaling system might not even mention lighting technology at all. More likely, constraints on lighting will appear as non-functional requirements describing current practices and standards (eg., the order of the colors on a traffic signal). A statement that a signal device should continue to operate when it is snowing (presumably up to some NNN-year blizzard threshold) is very much a functional requirement inherent in the concept of operations.

A compliance audit/acceptance test should have caught this issue - almost by inspection - before deployment. LEDs are desirable because they inexpensive to operate due to their high efficiency. They are efficient because they emit far less waste heat. What happens to the snow accumulation when heat is removed from the system?

Some possible solutions have already been mentioned: a heating element (perhaps actively controlled), weather shielding, special coatings. The point is that there is one problem description ("signal must continue to operate when it is snowing"), but many different options for solutions. It is impossible to evaluate the acceptability of any solution without matching it point-by-point against the problem requirements the solution is meant to address.

Some risks are long and involved to describe. It is precisely that this issue can be characterized so succinctly that reveals a requirements failure. Whether the vendor or the customer bears a larger burden of the responsibility for the failure is a separate question.

Rob Seaman, National Optical Astronomy Observatory seaman@hanksville.org



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 90

Friday 8 January 2010

Contents

- [NIST-certified USB Flash drives with hardware encryption cracked](#)
[PGN](#)
- [Skype: the case of disappearing telephone numbers](#)
[Chris J Brady](#)
- [Libel by Twitter?](#)
[Al Stangenberger](#)
- [Risks of USB chargers for cell phones](#)
[Paul Pomes](#)
- [Y2K+10: look at the Hex](#)
[Dave Hansen](#)
- [Y2K+10: what's underlying?](#)
[Chris Smith](#)
- [Y2K+10: The problems with sticky tape](#)
[Peter Houppermans](#)
- [Weight of a Land Rover incorrectly input into UK VCA database](#)
[Matthew Wilson](#)
- [Re: Eurostar RISKS](#)
[Richard Pennington](#)
- [Leaves on Tracks](#)
[Curt Sampson](#)
- [Re: LED Traffic Lights are efficient](#)
[Dick Mills](#)
[Terrence Enger](#)
- [Re: Silent Hybrid Nearly Causes Carbon Monoxide Poisoning](#)
[Walt Strickler](#)
- [NDSS Program](#)
[Internet Society](#)
- [Info on RISKS \(comp.risks\)](#)

***N*NIST-certified USB Flash drives with hardware encryption cracked**

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

Fri, 8 Jan 2010 10:47:27 PST

Certain USB drives using AES encryption have a major flaw that allows a way to bypass the login rules: "The SySS experts wrote a small tool for the active password entry program's RAM which always made sure that the appropriate string was sent to the drive, irrespective of the password entered and as a result gained immediate access to all the data on the drive." In essence, despite the use of AES 256-bit encryption, the password checker program always put out the same bitwise-identical POSITIVE response to a successful password check, which was trivially reproducible. [Source: The H Security, 4 Jan 2010; Thanks to John Curran; PGN-ed]
<http://www.h-online.com/security/news/item/NIST-certified-USB-Flash-drives-with-hardware-encryption-cracked-895308.html>

[Misleading title; make sure you understand what is 'certified' and what that means (or doesn't mean) with respect to systems in the large. PGN]

#Skype: the case of disappearing telephone numbers

*Chris J Brady <chrisbrady@yahoo.com>
Thu, 7 Jan 2010 17:10:04 -0800 (PST)*

The latest version of Skype (partly owned by eBay) is causing major irritations amongst web designers and users. By default when downloaded and installed it also installs a small utility unbeknown to the user. This utility effectively reformats any telephone &/or fax. nos. on a web page including adding a little flag icon and also embeds a link behind these to link to Skype. Theoretically clicking on the telephone no. then initiates a Skype call to that no.

Unfortunately there are some side effects.

Web designers are especially upset that the reformatting effectively destroys the look of a web page, especially if a web site has been designed to a corporate style when Skype then reformats parts of every page to suit itself.

Secondly in many cases the telephone &/or fax nos. are simply deleted from the web page displayed never to be seen again. Even more irritating is that telephone nos. disappear when web-based emails are viewed such as when using Yahoo Mail and/or Google Mail. That is until a cure is implemented.

And the cure is to remove the embedded utility - not easy. And/or remove Skype entirely. Both are reported to be effective.

The risk of course is trusting Skype when the company (partly owned by eBay) has deliberately chosen to allow this feature to be installed by default without any user choice in the matter.

#Libel by Twitter?

Al Stangenberger <forags@nature.berkeley.edu>

Mon, 04 Jan 2010 19:31:53 -0800

Interesting legal commentary on the problem of crafting a comment within Twitter's 140-character limit for messages. The forced brevity can cause the unwary to make statements but not to qualify them as opinion due to the maximum message length.

<http://writ.news.findlaw.com/hilden/20100104.html>

✶ Risks of USB chargers for cell phones

Paul Pomes DVM <Dr.Pomes@FurryFriendsVet.com>

Wed, 30 Dec 2009 20:40:54 -0800

My wife recently purchased a no-name third-party USB charger for her Droid cell phone. When the included cable is connected to the USB port of her laptop, the phone charges normally albeit somewhat slowly. Connecting the cable to the included voltage-sensing wall transformer starts a menagerie of interesting effects: opening applications, creating garbled text messages, changing settings, etc. No doubt this is due to floating signal lines with induced voltages that is triggering this storm of activity.

It takes little imagination, however, to visualize more sinister applications. A very small amount of logic, specific for each cell phone model the charger is marketed for, could be embedded inside the plastic transformer block. After a few minutes delay the phone could be probed for sensitive information and the results sent to an electronic dead-drop. The risk is a classic trade-off of security vs convenience. Having a single charger for our Kindles, cell phones, PDAs simplifies the number of ancillary chargers we need to tote around. Mixing the mission of power supply and data conduit opens a covert channel.

Paul Pomes, DVM (formerly a network and computer security engineer until I got tired of meetings) <http://www.FurryFriendsVet.com>
<http://PaulPomes.livejournal.com> <http://www.facebook.com/Paul.Pomes>

✶ Y2K+10: look at the Hex

Dave Hansen <iddw@hotmail.com>

Fri, 8 Jan 2010 12:14:15 -0500

A lot of the problems seem to share a common characteristic -- instead of 2010, the date appears to be 2016.

Debora Weber-Wulff wrote:

> Seems that the software thinks that it is the year 2016 and not
> 2010, so all of the cards are no longer valid. A friend pointed out to me
> that 2016 is 11111100000 in binary.

It's more interesting to look at both numbers in hexadecimal: 2009 is 0x7d9 while 2016 is 0x7e0. A little BCD math, perhaps?

Y2K+10: what's underlying?

Chris Smith <smith@vex.net>

Fri, 8 Jan 2010 11:12:28 -0500 (Eastern Standard Time)

"Seems that the software thinks that it is the year 2016 and not 2010, so all of the cards are no longer valid. A friend pointed out to me that 2016 is 11111100000 in binary."

I - and I suspect many others - would be interested in knowing the underlying error behind this problem. One the best reasons to read RISKS is to expand your personal list of bugs to watch out for.

I can see at least one strong possibility. It relates to the point that chip cards - and especially contactless chip cards - are very low power, low resource, devices. The hardware and software developers optimize *everything*.

Expressing the problem as though a two-digit year were in use, the problem was that 9 was followed by 16, not 10. But in hexadecimal, \$09 was followed by \$10 - but it should have been \$0A.

Chip cards could reasonably use BCD (binary coded decimal), where a decimal number is stored in a byte as two separate digits, one per nibble. At some point, if the chip provides a current year value, it would provide it as 10 (hex \$10, binary 0001000). But if a terminal thinks this is a *binary* field, it will misinterpret it -- starting in the year 2010. Any conversion from 10 to 2010 would have been done by the terminal.

It is also worth noting that card systems in general make heavy use of BCD. The numbers on your magnetic card stripe, for example, are all BCD.

Note that this raises the possibility that the *terminal* is at fault for misunderstanding the data format, not the card. But it also makes clear - consistent with reports - that even if the card is the problem, the terminal can correct the difficulty with a customized conversion routine, as long as it can accurately identify which cards have the problem.

Note that BCD is sufficiently common in small processors that the 6502 processors actually had a 'decimal mode', where adding \$01 to \$09 resulted in \$10, and adding \$01 to \$99 both gave \$00 and set the carry flag.

Y2K+10: The problems with sticky tape ([RISKS-25.89](#))

Peter Houppermans <peter@houppermans.com>

Fri, 08 Jan 2010 09:56:19 +0100

The "German" credit card problem is interesting from a number of angles:

- * Disaster Recovery: imaging you're abroad and your cash becomes inaccessible, but this time not because your bank fails. At least the good news is that that's easier to solve, and a fallback was available. Uncomfortable idea when you're traveling.
- * Technology migration risk: I guess it's now properly publicly known that the so-called safe chip is easy to defeat by simply avoiding it. This presents an interesting issue with respect to card cloning as you actually do not need access the chip itself. Copy the magnetic strip and make sure any chip on the target card malfunctions (expect a surge in nail varnish sales). The fallback option has now reduced the level of trouble for the end user, but I suspect a surge in that method of old, magnetic strip cloning, is unavoidable.
- * Think before you report: my immediate reaction was "uh oh" when I saw the sticky tape reporting, because I knew what would happen next: tight (anti-fraud) mechanical tolerances in ATMs resulting in transfer of sticky tape from card to mechanism, thus gumming up the works (and possibly retaining the card in the process). Sure enough: in the evening those same sources reporting the "solution" were now labeling it a "problem" without the slightest hint of irony..

✶ Weight of a Land Rover incorrectly input into UK VCA database

"Matthew Wilson" <matthew@gbelectronics.com>

Fri, 8 Jan 2010 10:25:25 -0000

It appears that the UK's Driver and Vehicle Licensing Agency - DVLA - have routinely been giving older series Land Rovers a revenue weight of 3499 kgs, which puts them in the commercial class 7 bracket of vehicle. The Land Rover (apart from some specialist version of the vehicle) should be a class 4.

It seems this weight choice was done when the computer database was set up and this 'random' value chosen.

Now that the garages where you submit your vehicle to gain a MOT certificate to prove it roadworthy have been computerised, entering the chassis number/VIN (vehicle identification number) of the vehicle causes the test to be refused as the incorrect weight retrieved from the database flags a class 7 test. The vast majority of MOT garages are only equipped for class 4 vehicles, not class 7.

Lots of additional info about this here:

<http://www.glencoyne.co.uk/motclass.htm>

I think a classic case of garbage in garbage out...

Re: Eurostar RISKS (Thorn, [RISKS-25.89](#))

*"Richard Pennington" <richardhelen@ntlworld.com>
Fri, 8 Jan 2010 00:50:02 -0000*

Here are a few comments on Anthony Thorn's piece about the Eurostar failures on 18 Dec 2009.

Firstly, one of my colleagues traveled on the last Eurostar train to pass through the Channel Tunnel from France to England before the trains failed. He reports that his train was obviously losing power and finished the journey traveling very slowly.

Secondly, I have seen no public report into what the difference was between the "winterisation" applied to the Eurostar trains this year (when there was a massive common-mode failure) and in the 15 previous years of reliable operation (in all sorts of weather conditions including a very cold spell in February 2009).

Thirdly, I have seen no public report into what happened to the signaling system. In particular, why did the controllers keep sending more trains into a tunnel which was already blocked by the previous failed trains? [As a result, they ended up with five trains trapped in the tunnel, all with identical failures. There is one track in each direction, with crossovers for use in emergencies.] I can understand that a total electrical failure (which appears to have occurred in each of the five failed trains) would prevent communications between the trains and the controllers - although that in itself raises an obvious single point of failure - but what happened to the trackside signalling systems, and why did they not send a message back to the controllers? And how long did it take the controllers to realise that there were no trains coming out of the other end of the tunnel?

Leaves on Tracks (was Re: LED Traffic Lights are efficient...

*Curt Sampson <cjs@cynic.net>
Fri, 8 Jan 2010 19:57:03 +0900*

On Sun, 27 Dec 2009 05:38:43 -0500, Jerry Leichter <leichter@lrw.com> writes:

> Every fall [in the NY area], we get delays in mass transit because of wet
> leaves on train tracks. I never recalled hearing of such problems years
> back....

He goes on to say that this problem has been attributed to the change from friction braking to regenerative braking. I believe that this may not be entirely, or even substantially correct.

The problem itself is not so very new to my knowledge: I clearly recall it being reported in the UK (on Thatcher-era passenger stock), in 1991, the first year that I lived there. Further, R. A. Wood's 1999 paper "Train Detection by Track Circuit: the Effect of the Wheel/Rail Interface" discusses leaves (among other track contaminants) and blames the issue on two quite different modernisation issues.

The first is the switch from steam to diesel locomotion ("Leaves were rarely a problem in steam days, for the simple reason that flammable vegetation at the side of the track was incompatible with machines that ejected burning cinders into the air."--section 2) and better bogies ("The main factor appeared to be the greatly improved suspension systems of modern bogies. Instead of bouncing, scraping, and sliding around the track, the wheel on a modern bogie runs straight and true along the rails, with a significantly reduced scrubbing action between wheel and rail."--section 3).

So there's the correction. Additionally, I must say, I do feel a little frisson when I think about a fire hazard mitigating another risk.

Curt Sampson <cjs@cynic.net> +81 90 7737 2974

Re: LED Traffic Lights are efficient (Johnson, [R 25 88](#))

*Dick Mills <dickandlibbymills@gmail.com>
Sun, 27 Dec 2009 09:47:25 -0500*

> John Johnson ([R 25 88](#)): "The problem is also evident on motor vehicles with LED signal and stop lights. Snow is not melted away by the signal and stop lights and accumulation blocks the lights."

Neither can incandescent stop and signal lights melt snow if they are not used often; such as long stretches of driving on the open highway. Nor could they melt snow when there was a generous air gap between the bulb and the lens cover.

I can't recall any mention of this risk in the pre LED era. What's new?

Likely predates RISKS, but this old fogey recalls the introduction of the 2 filament tail-light/brakelight bulb in common use for at least 50 years. This was introduced to address the problem mentioned here. At night, when visibility is lowest, and the tail lights would be on, the heat of the tail light would defrost the lens so the brakelights were more visible.

Just as an aside - on LED lights - I saw an ad that said that LED brake lights were safer since they lit up more quickly, at least a tenth of a second. I poo-poo'd this until I thought a bit. 60 mph is 88 feet/second 1/10 second is 8.8 feet saving even half that much in a panic stop is quite significant !

P.M. Wexelblat PhD, Erst of the Dept. of Computer Science
University of Massachusetts Lowell, One University Ave, Lowell, MA 01854

Re: LED Traffic Lights are efficient (Seaman, [RISKS-25.89](#))

Terrence Enger <tenger@iseries-guru.com>

Fri, 08 Jan 2010 09:41:00 -0500

> LEDs are desirable because they inexpensive to operate due to their high efficiency.

LEDs **are** highly efficient, but I suspect that desirability comes far more from the long lifetime. It is not much work to unscrew a bulb and screw in a new one, but getting into position to do that is not so easy.

So, the cost of energy to melt the precipitation is not obviously a show-stopper for a simple-minded heater. We know from past experience that the power for one light is at least adequate. And the cost of installation can probably be brought into the same order of magnitude as the cost to ...um... change a light bulb.

Re: Silent Hybrid Nearly Causes Carbon Monoxide Poisoning ([R-25.88](#))

<waltstrickler@hotmail.com>

Fri 1 Jan 2010 07:34:44 -0700

So I have a (maybe obvious) question: Why would a car whose engine is running need synthetic engine noise? The letter to the editor even said that it was running at full throttle, but the author seems to have missed the irony.

I suspect that this is not a risk of the hybrid being silent, but of the fact that the Prius is turned off by taking the RFID (Radio Frequency Identification Device) that enables it out of range, or by performing the unintuitive (and not usually necessary) act of pushing the START button for 3 seconds. In this case, the RFID was probably left in a purse, which was left in the car, and the car was most likely in battery-charging mode when left in the garage. The 4 hours mentioned in the letter seems like a long time to charge the batteries, but perhaps this one had been converted to a plugin hybrid with much larger battery capacity.

NDSS Program

Internet Society <craemer@isoc.org>

Mon, 4 Jan 2010 14:07:25 -0500 (EST)

17th Annual Network and Distributed System Security (NDSS) Symposium
The Dana on Mission Bay, San Diego, California, 28 Feb -- 3 Mar 2010

New research on 24 topics to be presented

The NDSS '10 program committee has selected 24 original research papers for presentation in San Diego. Topic areas include:

- * Distributed Systems and Networks
- * Web Security and Privacy
- * Intrusion Detection and Attack Analysis
- * Anonymity and Cryptographic Systems
- * Security Protocols and Policies
- * Languages and Systems Security
- * Malware
- * Spam

A complete list and summaries of each paper can be found at:

www.isoc.org/isoc/conferences/ndss/10/program.shtml

Keynote by former White House counterterrorism and cyber security czar Richard A. Clarke. Special panel discussion on Ethics in Networking and Security Research.

Registration Information: www.isoc.org/ndss10

Organized by the Internet Society



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 91

Tuesday 19 January 2010

Contents

- [New Massachusetts unemployment insurance employer website crashes and burns upon launch](#)
[Jonathan Kamens](#)
- [Moscow grinds to a halt: spoofed traffic signs?](#)
[PGN](#)
- [Despite Risks, Internet Creeps Onto Car Dashboards](#)
[Matthew Kruk](#)
- [Software Firms Fear Hackers Who Leave No Trace](#)
[Markoff/Vance via PGN](#)
- ["--b" parsed as a double-negation](#)
[jidanni](#)
- [Network flaw connects Facebook users to wrong accounts](#)
[Steven J Klein](#)
- [Fraudulent Facebook group leads to malware scam](#)
[Matthew Kruk](#)
- [A5/3 attack](#)
[Alexander Klimov](#)
- [S&P loses 8.5%](#)
[Daniel P.B. Smith](#)
- [Dangerously wrong trailer weight in Web tool](#)
[Rex Sanders](#)
- [Australian man dies after being crushed by computers](#)
[Darryl Smith](#)
- [Update Your XYZZY Web Site Password](#)
[Dale E. Coy](#)
- [Offensive shutting down of botnets](#)
[Kelly Jackson Higgins via PGN](#)
- [Y2K+10 problem 1910 in BPCS 8.1 ERP](#)
[Al MacIntyre](#)
- [Y2K+10: Windows Mobile has 2010 problems too](#)
[Jeremy Epstein](#)
- [Y2K? Taiwan, N. Korea calendars facing Y1C in 2011!](#)
[jidanni](#)
- [Re: Couple Stuck in Oregon Snow for 3 Days After GPS Leads Them Astray](#)
[Al Stangenberger](#)
- [Other Traffic Risks](#)

[Gene Wirchenko](#)

• [REVIEW: "Into the Breach", Michael J. Santarcangelo](#)

[Rob Slade](#)

• [Info on RISKS \(comp.risks\)](#)

✂ New Massachusetts unemployment insurance employer website

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

Thu, 14 Jan 2010 21:52:41 -0500

crashes and burns upon launch

The Commonwealth of Massachusetts has a convoluted(*) unemployment insurance system, under which employers are required to make various quarterly and annual filings and quarterly payments involving at least two different state agencies.

This system is administered by the Department of Unemployment Assistance (DUA), who decided to replace their old, paper-based system with a Web-based system called QUEST ("Quality Unemployment System Transformation"). The DUA promised QUEST would bring countless improvements: one-stop shopping, filings for all agencies in one place, faster filings, less wasted paper, reduced printing and postage costs, reduced data entry costs, no more data transcription errors, etc., etc. You've no doubt heard it all before.

QUEST went live at the beginning of 2010. As of the go-live date, the usage of QUEST for all employer unemployment insurance transactions was mandatory; paper filings were no longer permitted. I.e., the DUA went straight from paper filings only to on-line filings only, with no transition period or overlap.(**)

It would be an understatement to say that QUEST is having some problems. It would probably be more accurate to say that it is a disaster. Some examples of the issues I've experienced trying to use the new system today to do my filing for the last quarter of 2009:

* I received an e-mail message informing me that there was correspondence in my QUEST inbox, and I should log into QUEST to read it. When I log into QUEST and click on the link for the correspondence in question, I get a .NET error page.

* When I attempted to enter my quarterly filing numbers, I was asked to fill in the fields "UI gross wages", "UI taxable wages", and "UHI taxable wages", with no explanation on the form or anywhere else on the site of what these terms mean or how to determine the correct amounts. A DUA employee with whom I spoke today informed me that those words were supposed to be links that I could click on for definitions, but for some reason the links were missing from the page.

* The two DUA employees with whom I spoke today both said that the new system is having innumerable problems across the board.

* The first phone number I called today in an attempt to get help with QUEST was so swamped that I was not even given the option of waiting on hold -- a recording told me they were too busy to help me and I should call back later, and then I was disconnected.

* A little while ago I tried to click on the QUEST login link on the DUA Web page and instead reached a DUA Web site error page indicating that the page I was trying to access had moved or was temporarily unavailable, or some such thing.

* Some time after that, I tried again, and this time I actually got into the QUEST application, at which point I was greeted with a different error: "Error: You have reached the Commonwealth of Massachusetts Department of Unemployment Assistance. The Quest Unemployment System is temporarily unavailable due to scheduled maintenance in order to better serve you. Please try your request again later. We appreciate your understanding." Given everything else that's going on, it seems highly unlikely to me that it is any way accurate to claim that this outage was "scheduled".

* Earlier today, a new message showed up on the DUA Web site: *Additional Time for 4th Quarter Filing and Account Activation* Two-week grace period for filing 4th Quarter Employment and Wage Detail Report. New deadline: *February 16, 2010*. Penalties apply after deadline. ... Although the January 8th deadline has passed, you can still activate your account without a late penalty. Please activate your account as soon as possible to avoid the expected high volume of calls and Web traffic near the filing deadline.

More.

http://www.mass.gov/Elwd/docs/dua/quest/empl_%26_wage_detail_filing_1st_reminder.pdf

As is typical in government bureaucracies facing epic disasters, there has been no public disclosure of the fact that there is a problem, or of what is being done to fix it, or of the ETA for when it will be fixed. It remains to be seen whether anything will be disclosed later, or whether any heads will roll at the DUA in recognition of this monumental cock-up.

1. Perhaps the system does not seem so convoluted to businesses, but it does to me, a "household employer" who is required to participate in it only because I've made the seemingly naive decision of attempting to abide by the law while employing a babysitter for six hours per week.

2. At least, requiring QUEST filing as of 1/1/2010 seems to have been their original plan. However, a letter sent to employers January 14 encourages the use QUEST for filing 4Q2009 reports, which would seem to imply that not using QUEST is in fact an option. If so, it's a difficult option to exercise, since all instructions and forms for filing on paper appear to have been removed from website, or at least cunningly hidden.

<http://www.mass.gov/Elwd/docs/dua/quest/empl_%26_wage_detail_filing_1st_reminder.pdf>

🚧 Moscow grinds to a halt: spoofed traffic signs?

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

Tue, 19 Jan 2010 13:45:06 PST

The long URL tells the story nicely. Two downtown billboard video screens caused traffic to "jerk.. to a standstill" for 20 minutes, until Panno.ru removed the content. They claim it was the result of either "hooligan hackers" or "advertising competitors". [Thanks to Herb Lin and Steve Bellovin for this one. PGN]

<http://www.switched.com/2010/01/16/russian-commuters-treated-to-free-roadside-pornography/>

Steve Bellovin has noted various sign-hacking events.

<http://www.foxnews.com/story/0,2933,484326,00.html> (see [RISKS-25.53](#))

<http://www.i-hacked.com/content/view/274/48/> (ADDCO)

<http://www.nytimes.com/2006/05/08/business/media/08sign.html>

("Stephen Harper Eats Babies")

and a very amusing official posted sign ("Do not take any risks.")

http://www.woostercollective.com/2009/06/culture_jamming_on_the_london_tube.html

RISKS has noted other cases of spoofed signs in the past, notably dating back to the 1984 Rose Bowl scoreboard (Caltech vs MIT). PGN]

✂ **Despite Risks, Internet Creeps Onto Car Dashboards**

"Matthew Kruk" <mkruk@gmail.com>

Sat, 9 Jan 2010 16:58:33 -0700

As if we didn't have enough bad drivers out there ...

To the dismay of safety advocates already worried about driver distraction, automakers and high-tech companies have found a new place to put sophisticated Internet-connected computers: the front seat. [Source: Ashlee Vance and Matt Richtel, *The New York Times*, 7 Jan 2010.]

<http://www.nytimes.com/2010/01/07/technology/07distracted.html>

✂ **Software Firms Fear Hackers Who Leave No Trace**

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

Tue, 19 Jan 2010 13:48:18 PST

The title of this article gives you a strong clue as to its content. The Web page includes many readers' comments, so I won't try to capture the entire discussion -- which should be very familiar to RISKS readers.

John Markoff and Ashlee Vance, Fearing Hackers Who Leave No Trace, *The New York Times*, dated 19 Jan 2010

<http://www.nytimes.com/2010/01/20/technology/20code.html>

✂ "--b" parsed as a double-negation

<jidanni@jidanni.org>

Tue, 12 Jan 2010 10:22:51 +0800

POSIX says support for ++ and -- is "not required", but doesn't say how to deal with ++b and --b when they aren't supported.

So we end up with

```
$ bash -c 'b=5; echo $((-b)); echo $((-b))'
```

4

3

```
$ dash -c 'b=5; echo $((-b)); echo $((-b))'
```

5

5

--b is being parsed here as a double-negation!

<http://bugs.debian.org/508602>

✂ Network flaw connects Facebook users to wrong accounts

Steven J Klein <steven@klein.us>

Sun, 17 Jan 2010 13:30:02 -0500

Source: <http://www.washingtontimes.com/news/2010/jan/16/network-flaw-causes-scary-web-error/>

2010 Network flaw causes scary Web error

A woman in Georgia using a Nokia phone connected to facebook.com, and found herself logged in to a stranger's account, without ever having been prompted to log in. She asked her mother & sister, both with the same model phone to try it, and both also ended up in the accounts of other unknown parties. They sent an e-mail from Facebook as evidence that what they described really happened.

I want to emphasize that the error isn't specifically a Facebook problem, but an AT&T network issue. Facebook could fix the problem by using a secure connection.

Excerpt:

The glitch -- the result of a routing problem at the family's wireless carrier, AT&T -- revealed a little known security flaw... In each case, the Internet lost track of who was who, putting the women into the wrong accounts... It's not clear whether such episodes are rare or simply not reported... The women, who live together in East Point, Ga., outside Atlanta, had recently upgraded to the same model of phone and all used the same carrier, AT&T... AT&T spokesman Michael Coe said its wireless customers have landed in the wrong Facebook pages in "a limited number of instances" and that a network problem behind those episodes is being fixed.

This is, of course, a serious problem. But it's not clear to me that there's any way for bad guys to intentionally exploit it.

Steven J Klein, A+ and Apple Certified, Your Mac & PC Expert (248) YOUR-MAC

✶ Fraudulent Facebook group leads to malware scam

"Matthew Kruk" <mkruk@gmail.com>

Sat, 9 Jan 2010 23:42:15 -0700

If you happen to be on Facebook today and spot a group that is called, "WE'RE AGAINST THE 4.99 A MONTH CHARGE FOR FACEBOOK FROM JUNE 30TH 2010," be sure to keep away from it. If you don't - instead of finding a friendly group of people that are there to discuss ideas or similar interests, a user could potentially end up with loads of malware garbage on their computer.

<http://www.geek.com/articles/news/fraudulent-facebook-group-leads-to-malware-scam-20091229/>

✶ A5/3 attack

Alexander Klimov <alserkli@inbox.ru>

Tue, 12 Jan 2010 12:46:25 +0200

As you may already know, GSM phone conversations are encrypted with the 20+ years old A5/1 and A5/2 stream ciphers. The ciphers were repeatedly shown to be weak, but in absence of a publicly available decryption tools the GSM Association was able to claim that the attacks are not practical. Last December the completion of tables needed for breaking A5/1 was announced and now the GSM Association intends to speed up the transition to A5/3.

This A5/3 block cipher is KASUMI, which is a modified version of the MISTY cryptosystem. Recently (2010-01-10) it was publicly shown that it is possible to derive the complete 128-bit key of the full KASUMI by using only 4 related keys, 2^{26} data, 2^{30} bytes of memory, and 2^{32} time (two hours on a single PC). <<http://eprint.iacr.org/2010/013.pdf>>

Authors of the attack note:

neither our technique nor any other published attack can break MISTY in less than the 2^{128} complexity of exhaustive search, which indicates that the changes made by the GSM Association in moving from MISTY to KASUMI resulted in a much weaker cryptosystem.

Never attribute to malice that which can be adequately explained by stupidity.

✶ S&P loses 8.5%

"Daniel P.B. Smith" <usenet2006@dpbsmith.com>
Tue, 12 Jan 2010 09:13:04 -0500

As noted in the Bogleheads investing forum, the S&P 500 index plummeted 97.7 points or 8.53% in the last instant of trading on Monday, January 11th, 2010... as shown by Google Finance and other online charts.

An actual 8.53% drop would of course have generated screaming headlines, but perfunctory Googling suggests that this glitch has escaped the notice of the financial press.

The obvious RISK is that an investor might take action on erroneously reported information, especially when that information could be "confirmed" by more than one source. This particular glitch is obvious enough to make such a thing unlikely, but it does place into question the reliability of our financial reporting channels.

Why does such a thing ever happen? How difficult is it to calculate the average of 500 numbers... and to omit reporting the result if any of them are missing?

Here is a screenshot of the glitch as shown by Google Finance. The glitch was not limited to Google, however.

<http://img31.imageshack.us/img31/6914/sp8.png>

The arrow points to the plummet. The chart displays a dynamic readout when you point to places on the curve, and the circled number is the readout for the right end of the curve. Fortunately, all of the summary numbers are displayed correctly, showing that it was a gratifyingly dull day.

Bogleheads discussion:

Bogleheads link: <http://www.bogleheads.org/forum/viewtopic.php?t=48592&mrr=1263297139>

Dangerously wrong trailer weight in Web tool

Rex Sanders <rsanders@usgs.gov>
Tue, 12 Jan 2010 17:22:21 -0800

A good friend wanted to rent a trailer to haul heavy stuff about 1,000 miles. The website of a reputable company had a tool for matching vehicle towing capacity, trailer weights, and trailer cargo capacity. He found a trailer that just met all his requirements, and reserved the trailer online.

Except it seemed a little too good to be true. A couple days before leaving, he dug deeper on that company's website. Under the specifications for that trailer, he found the trailer weight listed at 1,000 pounds higher!

He called customer service. The first agent tried to convince him through

some dubious logic that the extra weight would not be a problem.

He called again to get a second agent, who confirmed an error in the Web tool, and promised to get it fixed. My friend rented a truck instead.

If he had trusted the Web tool, or the first agent, he could have suffered a serious crash through overloading.

Lessons: A trailer rental database error could have killed people. And some customer service agents are more trustworthy than others.

✂ Australian man dies after being crushed by computers

"Darryl Smith" <Darryl@radio-active.net.au>

Tue, 12 Jan 2010 22:15:20 +1100

An Australian man has died after computer equipment fell on him as it was being unloaded from a truck according to a local paper... "It appears the man was helping others unload a large computer server from the back of a truck," ambulance clinical support officer Mark Lamb said.

<http://www.news.com.au/breaking-news/man-dies-after-being-crushed-by-computer-in-melbourne/story-e6frku0-1225818578320>

Darryl Smith, VK2TDS POBox 169 Ingleburn NSW 2565 Australia
www.radio-active.net.au/blog/ - www.radio-active.net.au/web/tracking/

✂ Update Your XYZZY Web Site Password

"Dale E. Coy" <dale@thecoys.net>

Sat, 16 Jan 2010 11:53:11 -0600

For many years I've been a member of an organization that has a website that has negligible risk, but requires a login for some purposes. The organization (let's call it XYZZY) has always used the members' surname as a password. On January 16th, I received the following e-mail (slightly altered to obscure the organization [and the sender! PGN]).

Dear Mr. Coy,

Due to website maintenance, the "member/guest only" sections of the XYZZY website will not be available until after Jan. 26. As part of this maintenance, we are increasing security measures. Passwords now must be at least five characters in length. Your current password does not meet this security requirement and you will be unable to log in. Please call XYZZY's Member Service Center at (800) 555-1212 from 8 a.m. to 6 p.m. EST or e-mail webmaster@xyzy.org to update your password. We apologize for this inconvenience.

I. Mostly Clueless, Deputy Director/Web Manager

Of course, I've sent e-mail requesting that they change my password. I'm anticipating that they will send my new password by email.

[PGN says, not so Coyly, you should request a password of "Coyote" as in "Don Coyote", Or you could change your name. That would certainly increase your security! But they will probably change your NAME and PASSWORD for you. I remember the 1108 operating system password, which was also the same as your user name. If you attempted to change your password, as I recall it would tell you that your desired password change was already in use if it belonged to another user. Now that's what we mean by REAL security!]

Offensive shutting down of botnets

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

Tue, 12 Jan 2010 9:37:02 -0800

<http://www.darkreading.com/insiderthreat/security/vulnerabilities/showArticle.jhtml?articleID=222300408>

Kelly Jackson Higgins, DarkReading, 11 Jan 2010

Yet another botnet has been shut down as of today as researchers joined forces with ISPs to cut communications to the prolific Lethic spamming botnet -- a development that illustrates how botnet hunters increasingly are going on the offensive to stop cybercriminals, mainly by disrupting their valuable bot infrastructures.

For the most part researchers monitor and study botnets with honeypots and other more passive methods. Then security vendors come up with malware signatures to help their customers scan for these threats. But some researchers are turning up the heat on the bad guys' botnet infrastructures by taking the lead in killing some botnets: Aside from last weekend's takedown by Neustar of Lethic, which is responsible for about 10 percent of all spam, FireEye last November helped shut down the MegaD botnet. And researchers at the University of California at Santa Barbara in May revealed they had taken the offensive strategy one step further by infiltrating the Torpig botnet, a bold and controversial move that stirred debate about just how far researchers should go to disrupt a botnet.

Back in 2008 after two major ISPs halted traffic to malicious hosting provider McColo, spam worldwide dropped around 70 percent because McColo had been the main home to most botnet command and control (C&C) servers.

But deploying more offensive tactics to stop botnets and bad guys is not so straightforward: Researchers walk a fine line as to how far they can go legally and ethically, and sometimes taking down a botnet actually backfires, either with the bad guys returning the favor with a denial-of-service (DoS) attack, or learning how to better evade investigators next time. There's the danger that getting inside a botnet will just give its operators more tools and insight into how to strengthen

their operations; botnet operators are notorious for reinventing themselves with stealthier botnets and new forms of malware. [...]

#Y2K+10 problem 1910 in BPCS 8.1 ERP

Al MacIntyre <macwheel99@wowway.com>

Fri, 8 Jan 2010 20:51:20 -0600

<http://archive.midrange.com/bpcs-l/201001/msg00012.html>

BPCS-L discussion group has found out about a Y2K+10 problem in Business Planning and Control System (BPCS) version 8.1.00 where Trusted Link Enterprise (TLE) version 3.2.01 substitutes 1910 for 2010 in Electronic Data Interchange (EDI). The vendor (Infor) knows about it, and is working on a fix.

#Y2K+10: Windows Mobile has 2010 problems too

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Thu, 14 Jan 2010 13:49:34 -0500

Should be no surprise, given [RISKS 25.89](#) and 25.90, but.... according to Cnet, there's reports of a glitch on Windows Mobile that some devices are putting the wrong date on incoming SMS messages - using 2016 rather than 2010. Microsoft has acknowledged the problem, but I haven't seen any reports of fixes.

Source: http://news.cnet.com/8301-13860_3-10425455-56.html

#Y2K? Taiwan, N. Korea calendars facing Y1C in 2011!

<jidanni@jidanni.org>

Sun, 10 Jan 2010 05:47:49 +0800

"This [everything-begins-again-with-us] dating system -- which reflects the habits of the imperial dynasties, isn't just a quaint local custom, its continued use is heading Taiwan toward its very own type of Y2K problem on 2011/1/1, when Taiwan's calendar reaches the age of 100 and has to jump to three-digit years, Taiwan will likely experience what I like to call the Y1C problem. (Yes, I know: I'm mixing systems in that C represents hundred in a system that uses M, not K, for 'thousand.' But that's the best I could come up with. I'm open to suggestions for catchy but correct names.)" North Korea too, the very same day.

<http://pcofftherails101.blogspot.com/2010/01/is-there-y1c-computer-glitch-in-taiwans.html>
<http://pinyin.info/news/2006/taiwans-y1c-problem>

http://en.wikipedia.org/wiki/Y1C_Problem
http://en.wikipedia.org/wiki/Minguo_calendar
<http://en.wikipedia.org/wiki/Juche#Calendar>

Re: Couple Stuck in Oregon Snow for 3 Days After GPS Leads

Al Stangenberger <forags@nature.berkeley.edu>
Fri, 08 Jan 2010 11:48:39 -0800

Them Astray (Grady: Risks 25:89)

Part of this problem can be caused by poor-quality data in the underlying map database used by the GPS.

I found a similar error while reviewing a web page which has a link to Google Maps to give directions from Berkeley to the University of California's forestry camp in Plumas County. The printed map directed users to take a Forest Service road as the shortest route; the road is dirt and not suitable for passenger cars. I contacted Tele Atlas (the firm which supplies the basic road data used by Google Maps), and found that they did not know that the road was dirt. They have updated the database, which fixed the problem.

But all of these incidents (remember the Stolpa family in 1993?) just point out that all the technology and maps in the world are no substitute for common sense...

Other Traffic Risks

Gene Wirchenko <genew@ocis.net>
Fri, 08 Jan 2010 21:23:34 -0800

While these traffic risks are not computer-related, they do help point out how hard it can be to get it right. So how difficult is it to construct a good road sign?

1) Snow can stick to signs. I recall driving near Penticton, British Columbia, Canada one night and being very thankful that I knew the road. The highway has some switchbacks as it descends into the Okanagan Valley from Keremeos. The turns are signed. They are very visible three seasons of the year. In snow, the signs can be barely visible and not readable at all. *I* knew to slow down. What about someone else?

Heated signs anyone?

2) In the same area and in others, it can be very windy. I have seen signs mounted so that they turn in the wind. I would not have thought that necessary.

I wonder if anyone has been injured by a sign that broke loose in the wind.

REVIEW: "Into the Breach", Michael J. Santarcangelo

Rob Slade <rmslade@shaw.ca>

Mon, 11 Jan 2010 11:45:04 -0800

BKINTBRE.RVW 20091012

"Into the Breach", Michael J. Santarcangelo, 2008, 978-0-9816363-0-6

%A Michael J. Santarcangelo michael@securitycatalyst.com

%C New York, USA

%D 2008

%G 978-0-9816363-0-6 0-9816363-0-6

%I Catalyst Media

%O www.intothebreach.com

%O <http://www.amazon.com/exec/obidos/ASIN/0981636306/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0981636306/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0981636306/robsladesin03-20>

%O Audience i+ Tech 1 Writing 2 (see revfaq.htm for explanation)

%P 110 p.

%T "Into the Breach"

The introduction states that security (which seems to be limited to disclosure or breaches) is a "people" problem, and therefore requires social solutions. This addresses a common problem: security professionals, and even non-technical managers, concentrate on breaches in systems and thus miss the real heart of the matter: people.

Although not overtly stated, part one seems to be related to the first stage in the Strategy to Protect Information, understanding information. Chapter one repeats the position that breaches are a human problem. Security awareness is promoted in chapter two. In chapter three an analogy is drawn between faddish security and crash dieting, noting that neither works. Chapter four addresses risk management.

Part two suggests managing people. Chapter five outlines the aforementioned Strategy to Protect Information: understand your information assets, manage and communicate with your people, and optimize your processes and systems. Implementing this strategy is seen, in chapter six, as a five step process: learn the jobs, gather information, prioritize, plan, and communicate. Steps seem to be missing, such as dividing your data or systems into elements for the process. Guidance for planning is limited. Chapter seven suggests making a trial run with a pilot project, which is a good idea. Measurement of the success of the project is discussed in chapter eight.

Part three deals with improvement. Chapter nine notes that the strategy benefits overall management, which is unsurprising, since it is basically a general management process. Costs of compliance with regulations or standards are also partially covered, as is mentioned in chapter ten, since a significant portion of the initial cost of compliance relies on the type of research and analysis demanded by the strategy. (However, a great deal

of the content simply emphasizes the importance of compliance.) The advice about outsourcing, in chapter eleven, seems to be to audit the vendor. Chapter twelve closes off the book with an exhortation to act.

Although generic, the strategy proposed is sound and likely useful. This slim volume would help a significant number of managers and security practitioners who are caught up in the latest security fad or device, to the detriment of actual business (and personnel) needs.

copyright Robert M. Slade, 2009 BKINTBRE.RVW 20091012
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
victoria.tc.ca/techrev/rms.htm blog.isc2.org/isc2_blog/slade/index.html
<http://blogs.securiteam.com/index.php/archives/author/p1/>
<http://twitter.com/NoticeBored> <http://twitter.com/rslade>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 92

Tuesday 26 January 2010

Contents

- [*NY Times* expose on medical radiation overexposure](#)
[Jeremy Epstein](#)
- [Air-traffic control glitch due to the installation of new software](#)
[Chiaki Ishikawa](#)
- [Extending TCP/IP into space](#)
[Randall Webmail](#)
- [Y2K+10 and SMS](#)
[Richard Gadsden](#)
- [Body scanners that don't work](#)
[Peter Houppermans](#)
- [Corporate espionage in the news: Hilton and the Oil industry](#)
[Gadi Evron](#)
- [Have the Chinese Really Hacked into MSN's DB?](#)
[Chris J Brady](#)
- [Cyberattacks on Google in China](#)
[PGN](#)
- [Unsearchable stores](#)
[Mark Brader](#)
- [ICSI claims "effectively perfect" spam blocking method](#)
[Lauren Weinstein](#)
- [LORAN being retired](#)
[David Magda](#)
- [PROVINCE OF CHI](#)
[jidanni](#)
- [Google Maps won't be taking my address for a ride](#)
[jidanni](#)
- [Upgrading a World of Warcraft account ends in tears](#)
[Turgut Kalfaoglu](#)
- [Unique PINs](#)
[Dag-Erling Smørgrav](#)
- [Re: Offensive shutting down of botnets](#)
[Dick Mills](#)
- [Cloud Computing Security](#)
[Ivan Arce](#)
- [Info on RISKS \(comp.risks\)](#)

NY Times expose on medical radiation overexposure

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Sat, 23 Jan 2010 23:25:21 -0500

There's nothing here that's akin to the infamous Therac disasters where interactions of hardware and software caused unexpected results, but more examples of how wrong configurations lead to dramatic radiation overexposures. "The Times found that on 133 occasions, devices used to shape or modulate radiation beams [...] were left out, wrongly positioned or otherwise misused." But there were also software errors - crashes that lost portions of the programming for the radiation beams. "as [the medical physicist] was trying to save her work, the computer began seizing up, displaying an error message. The hospital would later say that similar system crashes 'are not uncommon with the Varian software, and these issues have been communicated to Varian on numerous occasions.' [...] At 12:57 p.m. -- six minutes after yet another computer crash -- the first of several radioactive beams was turned on." In another case, "One therapist mistakenly programmed the computer for 'wedge out' rather than 'wedge in,' as the plan required. Another therapist failed to catch the error. And the physics staff repeatedly failed to notice it during their weekly checks of treatment records. Even worse, therapists failed to notice that during treatment, their computer screen clearly showed that the wedge was missing. Only weeks earlier, state health officials had sent a notice, reminding hospitals that therapists 'must closely monitor' their computer screens."

The problem was lack of fail-safe processes. "The software required that three essential programming instructions be saved in sequence: first, the quantity or dose of radiation in the beam; then a digital image of the treatment area; and finally, instructions that guide the multileaf collimator. When the computer kept crashing, [...] the medical physicist, did not realize that her instructions for the collimator had not been saved, state records show. She proceeded as though the problem had been fixed. "

It's a pretty frightening article.

<http://www.nytimes.com/2010/01/24/health/24radiation.html?hp>

[The article spans the middle of the front page and three inside pages. It's well worth reading in its entirety. I also received comments on this from Jared Gottlieb, Harry Hochheiser, Matthew Kruk, Nancy Leveson, Martyn Thomas, and others. See recent harbingers ([RISKS-25.81,82](#)) of the current round of events, as well as the earlier items on the Therac-25 problems ([RISKS-8.5](#), 12.50, 14.04). PGN]

Air-traffic control glitch due to the installation of new software

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

Thu, 21 Jan 2010 18:19:59 +0900

<http://www.airportbusiness.com/online/article.jsp?siteSection=1&id=33648>

Air-traffic control glitch due to the installation of new software

Air-traffic control software problem (airplane positions could not be identified in a timely manner) caused the disruption of air flights in Japan on 14 Jan 2010.

This happened after the installation of new software that consolidated the air-traffic control operations of two large and busy airports, Haneda and Narita. The program controls the radar screen displays for the controllers. Due to a software problem, the display on the screen got sluggish to the point that the operators switched to a backup system and operators diverted to traffic to other airports and such.

On 15 Jan 2010, the official announcement was made by the Ministry of Land, Transport, Infrastructure and Tourism that the climate information, especially bad weather, was mistakenly fed to the module of the control program that display the positions of airplanes in this new software setup. This caused overload of processing, and thus the failure to keep track of the airplanes timely.

This incorporation of the bad weather is a new feature according to the short announcement made by the minister in charge.

Usual risk. But I really wonder why this was not caught in advance testing.

The unwanted climate data by the position display module was silently thrown away without no logging? If the bad weather was properly reflected on the screen by the feed to the proper module (assuming the testing was done for the display of bad weather condition on radar), then the data was duplicated by mistake and fed to the airplane position display module, also? Why and how?

Inquiring minds want to know more.

I really wish that there is a public database of software bugs that caused social glitches like this one and that record details for posterity for the benefit of future programmers, etc. I suspect such a database will be a loath to parties in the legal tangling as the result of such bugs, but the society needs such a database, I think. We need better foundation and not try to build sand castles from scratch again and again with similar mistakes in the foundation.

(This incident has nothing to do with the bankruptcy filing of Japan Air Lines recently.)

✶ Extending TCP/IP into space (From Dave Farber's IP)

Randall Webmail <rvh40@insightbb.com>

January 22, 2010 11:16:07 AM EST

NASA EXTENDS THE WORLD WIDE WEB OUT INTO SPACE

Astronauts aboard the International Space Station received a special software upgrade this week - personal access to the Internet and the World Wide Web via the ultimate wireless connection.

Expedition 22 Flight Engineer T.J. Creamer made first use of the new system [on 22 Jan 2010], when he posted the first unassisted update to his Twitter account, @Astro_TJ, from the space station. Previous tweets from space had to be e-mailed to the ground where support personnel posted them to the astronaut's Twitter account.

"Hello Twitterverse! We r now LIVE tweeting from the International Space Station -- the 1st live tweet from Space! :) More soon, send your ?s"

This personal Web access, called the Crew Support LAN, takes advantage of existing communication links to and from the station and gives astronauts the ability to browse and use the Web. The system will provide astronauts with direct private communications to enhance their quality of life during long-duration missions by helping to ease the isolation associated with life in a closed environment.

During periods when the station is actively communicating with the ground using high-speed Ku-band communications, the crew will have remote access to the Internet via a ground computer. The crew will view the desktop of the ground computer using an onboard laptop and interact remotely with their keyboard touchpad.

Astronauts will be subject to the same computer use guidelines as government employees on Earth. In addition to this new capability, the crew will continue to have official e-mail, Internet Protocol telephone and limited videoconferencing capabilities.

To follow Twitter updates from Creamer and two of his crewmates, ISS Commander Jeff Williams and Soichi Noguchi, visit:

http://twitter.com/NASA_Astronauts

For more information about the space station, visit:

<http://www.nasa.gov/station>

Archives: <https://www.listbox.com/member/archive/247/=now>

[Well, that may be just a little more secure than an early desire for the space station that I heard when I visited Johnson Space Center long ago, which was that researchers should be able to uplink over the Internet to the Space Station control computer and monitor and guide their own experiments in real time. PGN]

#Y2K+10 and SMS

Richard Gadsden <richard@gadsden.name>

Thu, 21 Jan 2010 14:21:01 +0000

The timestamp on SMS messages (known as TP-SCTS) stores the year in two nibbles in a binary-coded decimal representation with the nibbles swapped.

Aside from the known risks of using a two-digit year, this is about as bad a representation as can be imagined. 2009 is represented as 1001 0000 in BCD swapped-nibble (i.e., as 09, decimal). 2010 (decimal) is represented as 0000 0001.

A number of telephone SMS programs, generally those that don't inherit a code-base from pre-Y2K systems, have misread the spec, and are interpreting it as swapped-nibble binary, rather than BCD, so are interpreting 0000 0001 as 00010000, i.e., as 0x10 or 16 instead of 10. This is why some phones (notably Windows Mobiles) are displaying text messages as having been sent in 2016, rather than 2010.

It's worthy of note that these systems would not have worked correctly in 1999 either - they would have interpreted 0x99 as 153 (decimal) - and may have displayed either 19153 or 2053.

In the specific case of Windows Mobile, the text message database stores two dates, the TP-SCTS date and an internal datestamp applied to the text when received by the phone. There is a setting in the firmware that allows the internal datestamp to be shown in preference to the TP-SCTS date, so some phones are showing the correct information and some are not. This setting is set by the firmware programmer, normally being either the manufacturer or the network operator.

RISKS:

Date code written after 2000 may display Y2K-like bugs, by making assumptions that all dates are post-2000.

Programs installed in firmware are much more difficult to correct for bugs, so code quality for firmware is much more important.

Systems are frequently coded to a small set of sample data, rather than to the actual specification. Checking against the specification rather than unit testing with sample data is harder, but may be necessary, especially for systems that are difficult to correct.

Richard Gadsden richard@gadsden.name

[The authors of the post-Y2K phone software have obviously never heard The Ring of the Nibble-Young-un (Wagner). It's worthy of a Ring-Tone-Poem (Strauss). PGN]

Bodyscanners that don't work

Peter Houppermans <peter@houppermans.com>

Sun, 24 Jan 2010 14:22:55 +0100

Interesting article in The Register about a full body scanner demo on German live TV demo. You guessed: it would not be news unless the thing had failed to detect some Very Bad Stuff.

You may want to watch the video, it's in German but I think you will be able to see that the key message is that the man scanned was carrying more than what he originally mentioned:

http://www.theregister.co.uk/2010/01/24/body_scanner_fail/

Keep watching - he will use the stuff that wasn't picked up, just to prove the point (notice that he almost ruins a camera when he stirs the remains). I hope these scanners won't lure security staff into a false sense of security, and wonder how the use of these expensive devices will pan out in real life use. We'll soon see.

Speaking of pan - no idea of correlation between frying pan material and what is used for a plane hull..

Corporate espionage in the news: Hilton and the Oil industry

Gadi Evron <ge@linuxbox.org>

Tue, 26 Jan 2010 08:53:07 +0200

Corporate espionage in the news, and not just because of Google: Hilton and the Oil industry. Is anyone calling espionage by means of computers cyber-espionage yet? I hope not. At least they shouldn't call it cyber war.

Two news stories of computerized espionage reached me today.

The first, regarding the Oil industry, was sent by Marc Sachs to a SCADA security mailing list we both read. The second, about the hotel industry, was sent by Deb Geisler to science fiction convention runners (SMOFS) mailing list we both read.

US oil industry hit by cyberattacks: Was China involved?

<http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved>

"At least three US oil companies were the target of a series of previously undisclosed cyberattacks that may have originated in China and that experts say highlight a new level of sophistication in the growing global war of Internet espionage."

Starwood Charges That Top Hilton Execs Abetted Espionage

http://www.meetings-conventions.com/article_ektid31918.aspx

"Starwood's claim points to a "mountain of undisputed evidence," including e-mails among Hilton senior management, that Klein and Lavani worked with others within Starwood to steal sensitive documents by sending them via personal e-mail accounts, among other methods, and that such information was shared and used by all of Hilton's luxury and lifestyle brands, as well as in the development of Hilton's now-shelved Denizen brand. In the new filing, Starwood says, "This case is extraordinary, and presents the clearest imaginable case of corporate espionage, theft of trade secrets, unfair competition and computer fraud...Hilton's conduct is outrageous.""

As to whether China is involved, maybe. But the automatic blaming has got to stop. Many other countries have been known to be conducting corporate espionage, such as France, and as the second story above shows, so do corporations themselves.

[Source on naming France: <http://samvak.tripod.com/pp144.html>]

But.. here are a few questions:

- My dog barked, was China involved?
- The traffic light turned red, was China involved?
- I am tired. Is China involved?

Have the Chinese Really Hacked into MSN's DB?

*Chris J Brady <chrisjbrady@yahoo.com>
Wed, 20 Jan 2010 06:04:14 -0800 (PST)*

Seen in a forum on LoveMoney.com:

"There is a new scam today offering cheap goods from China. They probably don't exist and they have hacked accounts, it appears they are in the MSN database. Anyone with hotmail or live.com accounts should change their passwords. This may be in the wrong thread. We are trying to figure out what they are doing. It looks like a major operation hacking from China."

Is the risk believing that there is a risk here, or is there more of a risk in ignoring it? Hmm ... but the Chinese do seem to be gaining a reputation for hacking.

Cyberattacks on Google in China

*"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 19 Jan 2010 16:21:02 PST*

Google has uncovered a "highly sophisticated and targeted attack" coming from China on its infrastructure that resulted in some of its intellectual property being stolen. The cited article suggests that at least 20

technology companies were similarly targeted (and more than 30, according to other reports).

<http://www.computerworld.com/s/article/9145679/>

In addition, *The Jewish Chronicle* website (thejc.com) was recently defaced.

http://www.theregister.co.uk/2010/01/18/jc_defaced/

See also John Markoff, David E. Sanger, Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent, *The New York Times*, 26 Jan 2010, A1/A6 today's National Edition.

✂ Unsearchable stores

Mark Brader

Sun, 24 Jan 2010 17:06:43 -0500 (EST)

Tangentially to recent thread in alt.usage.english, Cheryl Perkins made a comment about how programmers dealing with addresses "don't like apostrophes" and "don't allow for their existence". John Varela then wrote this (quoted by permission) about his TomTom One 130:

| I ran into that today when I wanted the GPS to take me to a store
| called "Lowe's". There's no way to enter an apostrophe on the GPS.
| A search for "Lowe" found nothing and a search for "Lowe's" found a
| store called "Lowest Price something-or-other". I had to find the
| place on my own. Doing so gave me a real feeling of independence
| and of superiority to technology.

Mark Brader, Toronto, msb@vex.net | "Fast, cheap, good: choose any two."

[Lowe's common denominator? PGN]

✂ ICSI claims "effectively perfect" spam blocking method

Lauren Weinstein <lauren@vortex.com>

January 25, 2010 6:51:19 PM EST

``Researchers have now come up with a system that deciphers the templates a botnet is using to create spam. These templates are then used to teach spam filters what to look for."

[Maybe "effectively perfect" against that specific type of attack *at this point in the development of spam*. Just ask Darwin.]

<http://bit.ly/7GwsVx> (New Scientist)

[From the Network Neutrality Squad, <http://www.nnsquad.org>]

#LORAN being retired

David Magda <dmagda@ee.ryerson.ca>

Thu, 21 Jan 2010 09:00:27 -0500

The U.S. Coast Guard has announced that it will begin turning off the Loran-C navigation system on February 8, 2010, with a full decommissioning by October 1, 2010:

http://www.access.gpo.gov/su_docs/fedreg/a100107c.html#Coast%20Guard

<http://yro.slashdot.org/article.pl?sid=10/01/12/223241>

While some people have said that GPS has made it redundant, critics of the decision have said that having redundancy / backups is entirely the point. The "Federal Register" statement implies that this concern is not very pressing:

- > The Loran-C system was not established as, nor was it intended to be, a
- > viable systemic backup for GPS. Backups to GPS for safety-of-life
- > navigation applications, or other critical applications, can be other
- > radio-navigation systems, or operational procedures, or a combination of
- > these systems and procedures. Backups to GPS for timing applications can
- > be a highly accurate crystal oscillator or atomic clock and a
- > communications link to a timing source that is traceable to Coordinated
- > Universal Time.

<http://edocket.access.gpo.gov/2010/2010-83.htm>

Not sure what these other navigation systems would be (e.g., WAAS "augments" GPS, not replaces it). For time a least, WWVB is available in large portion of the continental U.S.

http://en.wikipedia.org/wiki/Wide_Area_Augmentation_System

Other countries have their own LORAN towers, and it remains to be seen how this will affect them:

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

#PROVINCE OF CHI

<jidanni@jidanni.org>

Mon, 11 Jan 2010 02:18:46 +0800

Fidelity.com is where I keep my retirement millions. A few days after a cordial address update I double checked to find it had become a mangled DONGSHI 42351 PROV-INCE OF CHI TAIWAN behind both my and staff's backs.

In order to please neighboring China, their run a batch job that alters all Taiwan addresses. It then took much staff effort whack mine back into shape.

Jackson.com is where I keep my other millions. Foreign customers have a pseudo-state of "OT" appended to their addresses. It used to be "OC" but that probably landed mail into an even darker hole at the post office.

Google Maps won't be taking my address for a ride

<jidanni@jidanni.org>

Tue, 26 Jan 2010 07:30:24 +0800

Ah, the amazing ability of <http://maps.google.com/> to pinpoint anything one tosses into its search box.

Let's just change this search string from house number 21, to e.g., 22:

[http://maps.google.com/maps?](http://maps.google.com/maps?f=q&hl=en&q=21+DaGuan+RD+%E5%A4%A7%E8%A7%80%E8%B7%AF21%E8%99%9F%2C+Taichung%2C+Taiwan)

[f=q&hl=en&q=21+DaGuan+RD+%E5%A4%A7%E8%A7%80%E8%B7%AF21%E8%99%9F%2C+Taichung%2C+Taiwan](http://maps.google.com/maps?f=q&hl=en&q=21+DaGuan+RD+%E5%A4%A7%E8%A7%80%E8%B7%AF21%E8%99%9F%2C+Taichung%2C+Taiwan)

[http://maps.google.com/maps?](http://maps.google.com/maps?f=q&hl=en&q=22+DaGuan+RD+%E5%A4%A7%E8%A7%80%E8%B7%AF22%E8%99%9F%2C+Taichung%2C+Taiwan)

[f=q&hl=en&q=22+DaGuan+RD+%E5%A4%A7%E8%A7%80%E8%B7%AF22%E8%99%9F%2C+Taichung%2C+Taiwan](http://maps.google.com/maps?f=q&hl=en&q=22+DaGuan+RD+%E5%A4%A7%E8%A7%80%E8%B7%AF22%E8%99%9F%2C+Taichung%2C+Taiwan)

Whammo... for #21 all along Google was merely matching a text string attached to a story associated with a point in their database. For #22 etc. Google Maps says "We could not understand the location."

If one has a Facebook account, here I am telling the business owner their new address finds a point (stuck to their old address (mentioning their new address.))

http://www.facebook.com/permalink.php?story_fbid=253295461155&id=12619981155

Me? I'm at <http://maps.google.com/maps?ll=24.181699,120.866261>.

No text strings to get hijacked by pagerank.

Upgrading a World of Warcraft account ends in tears

Turgut Kalfaoglu <turgut@kalfaoglu.com>

Wed, 20 Jan 2010 11:04:54 +0200

My son and I have something in common: We love the online game Warcraft. We are separated by a continent as he lives with his mother, but we still meet online through this game.

For those who are not familiar, it consists of a 5GB game download, followed by numerous similarly-sized updates, and finally being able to play (and pay monthly) online.

We recently attempted to upgrade our gaming accounts to their new "Wrath of Leech King" expansion - it was suppose to be a Christmas present for him. So I entered their web site, gave my credit card details, clicked upgrade. It promptly said congratulations, and that the account was upgraded.

A day later, we got another e-mail saying that the purchase was "undone" and the game upgrade was rolled back. No details were given, but we were given a hint that we should phone them. That simple task of phoning them took three days of non-stop phoning from overseas: Their UK help desk was so swamped/understaffed that I could not get in their waiting queue. When I did, I was dropped off after waiting 9 minutes on the phone. It eventually turned out that my security-conscious son had not entered his correct name and address when signing up to the service some years back, and apparently only during the upgrade that Blizzard bothers to check these things.

After a successful phone call to their help desk, we were sent a questionnaire to fill out to correct the details. However, even after the details were entered into their system, we were STILL denied the upgrade. Reason? As far as I can tell, it was their security system again: It will not let you "upgrade" twice from the same IP address!

Since according to their records, we had one "successfully" upgraded, we were now denied an upgrade!

After numerous fruitless e-mails, I finally re-re-re-did the registration from a work computer, and it went through, and it became a late new year present for my son instead.

Moral of the story:

- 1) You must reveal your complete identity if you want to play games,
- 2) Your request must not look like it's coming from a sweatshop in China.

And you thought playing online games was all fun and games?

Turgut Kalfaoglu, Msc. Computer Engineering, Izmir Institute of Technology

✂ Unique PINs

*Dag-Erling Smørgrav <des@des.no>
Wed, 20 Jan 2010 11:51:22 +0100*

A number of municipal cinemas in larger Norwegian cities have a common fidelity program called Kinosonen ("the cinema zone"). Amongst other benefits, members get a card they can use to prepay tickets (at a discount, of course).

A few days ago, two e-mails were sent out to program members. The first e-mail enjoined all members to change their PIN as quickly as possible "for security reasons". All well and good. The second... The second said, loosely translated:

We have been notified of a flaw in our procedures, and have asked all our members to change their PIN. Several members have been issued the same PIN for their membership cards. As many as 1200 cards may be affected. This only applies to cards issued after 2007-11-25. We are in the process

of changing the PIN for those 1200 members. You will receive a new PIN by e-mail.

So... am I to conclude that the security of their system depends on each member's PIN being unique? The mind boggles. If so, why do they ask members to select their own PIN? What happens if a member selects a PIN that is already in use - does she get a message to that effect? So now she knows that somebody else uses that PIN, can she take advantage of that knowledge? If not, why are duplicate PINs a problem in the first place?

I'm not sure how long the PIN is, by the way, but my guess is four or five digits. The total population of these cities and their suburbs is around two million people. Even with conservative estimates of their membership base, latecomers are going to have a hell of a time trying to find an unused PIN. Even with six digits, the odds are that a lot of people are going to use either their birth date or the last six digits of their 12-digit card number...

Re: Offensive shutting down of botnets

Dick Mills <dickandlibbymills@gmail.com>

Thu, 21 Jan 2010 09:14:38 -0500

It seems foreseeable that someday a mass cutoff of botnet infected computers will trigger some kind of disastrous side effect.

Of course, mission critical or life critical applications should never be allowed to exist on unprotected net connected computers, especially those infected by malware. Nevertheless, it would be foolish to presume that nobody else is ever foolish.

Here's the risk. We may know that a mass collection of computers are hosting malware, but we have no way of knowing what good and vital services they may also be providing. Is it not true therefore, that any action to remotely cut off a class of nodes is somewhat reckless by nature.

[Old wine in new bot-tles? PGN]

Cloud Computing Security

Ivan Arce <ivan.arce@CORESECURITY.COM>

Sat, 23 Jan 2010 18:24:12 -0200

We have a special issue on Security in Cloud Computing scheduled for publication in Nov/Dec 2010. The final date for submissions is approaching (5 Mar 2010). and The Call for Papers is here:

<http://www.computer.org/portal/web/computingnow/spcftp6>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 93

Friday 29 January 2010

Contents

- [Doug Maughan's CACM article & Roadmap for Cybersecurity Research](#)
PGN
- [UI fix freezes NYSE, affects 975 stocks](#)
T Byfield
- [False positives galore in SARs](#)
Geoff Kuening
- [DC Metro - only kills average of 1 customer each 3 years](#)
Paul Robinson
- [GPS Control Software Glitch: NANU Issued](#)
PGN
- [How Not to Design Authentication](#)
Alexander Klimov
- [Radiation Offers New Cures, and Ways to Do Harm](#)
David Hollman
- [Warning: Your Cell Phone May Be Hazardous to Your Health](#)
Christopher Ketcham via PGN
- [Driver watching laptop movie kills woman](#)
Walter Roberson
- [It depends on which bus you take](#)
Paul Robinson
- [Driving and walking through buildings](#)
Pete Kaiser
- [Re: Teleportation via Skyhook](#)
Tony Lima
- [Re: Extending TCP/IP into space](#)
Mark Jackson
- [Info on RISKS \(comp.risks\)](#)

✉ Doug Maughan's CACM article & Roadmap for Cybersecurity Research

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

Thu, 28 Jan 2010 16:19:18 PST

Doug Maughan's Inside Risks column on the Cybersecurity Roadmap and the underlying security issues will appear in the Feb 2010 *CACM*. An html version is now up on my Inside Risks website:

Douglas Maughan,
The Need for a National Cybersecurity Research and Development Agenda
Communications of the ACM, February 2010
<http://www.csl.sri.com/neumann/insiderisks08.html#220>

It includes hotlinks to the roadmap and various other relevant documents on the Department of Homeland Security Science and Technology cybersecurity website. (The roadmap document is currently the first item in the list.)

<http://www.cyber.st.dhs.gov/documents.html>

UI fix freezes NYSE, affects 975 stocks

*t byfield <tbyfield@panix.com>
Thu, 28 Jan 2010 01:11:45 -0500*

Ars Technica reports (Jon Stokes, "How a stray mouse click choked the NYSE & cost a bank \$150K," 27 Jan 2010):

On November 14, 2007 at 3:20pm one of Credit Suisse's trading algorithms suddenly went haywire, and, in a few moments, sent hundreds of thousands of bogus requests to the exchange. This sudden surge of requests, which were cancellations for a large batch of orders that the machine had never actually sent out, acted like a denial-of-service attack on some parts of the New York Stock Exchange. The messages clogged the tubes and caused parts of the exchange to freeze up, affecting trading in 975 stocks.

The article goes on to blame "a programmer [who] took it upon himself to unilaterally improve [the Credit Suisse program] by adding a new user input feature," which lacked "feedback and 'forgiveness'" and a lack of testing.

On November 14, a few seconds after 3:20, a trader put a number in the box and then double-clicked the "up" arrow. This double-click was interpreted by SmartWB as two separate clicks, so the system dutifully sent out a second batch of cancel/replace orders in addition to the batch that was intended by the trader. This sudden flood of cancel/replace orders, half of which were requesting cancellation of orders that had never been sent, overwhelmed the system and backed up five of the posts on the NYSE trading floor.

Without endorsing the programmer's impromptu improvement, it's fair to ask why a "flood" of bogus orders from a single bank would overwhelm the system.

<http://arstechnica.com/business/news/2010/01/how-a-stray-mouse-click-choked-the-nyse-cost-a-bank-150k.ars>

✂ False positives galore in SARs

Geoff Kuenning <geoff@cs.hmc.edu>

Thu, 28 Jan 2010 23:05:14 -0800

I went to a talk today by a rather clueless Los Angeles company who is partnering with the Washington, DC, police in a number of efforts, many based on web-scraping. One of the things they're proud of is a (non-scraping) system that automatically delivers SARs ("Suspicious Activity Reports") to interested parties. For example, if an SAR has a location that's within 1000 feet of a university, they send a text to everybody's cellphone. They're at least a little bit clever; for example, for a big school they'll only contact the students living in the dorm(s) nearest the incident.

OK, what's an SAR? Just about anything. If a little old lady sees a "suspicious man on the corner" (e.g., waiting for a taxi) and calls it in, that's an SAR. Obviously, in these fear-everything days, any forgotten package becomes an SAR-worthy possible bomb. About 300-400 SARs go out per day, though to be fair not every SAR goes to every person.

When queried, they informed us that of course most SARs are bogus, but "three or four per year" are valid. Hmmm... $300 * 365 / 4 = 27,375$. That's a pretty impressive false-positive rate. They don't seem to see a problem with crying "wolf" that often. And one of their examples of a "true" positive was a political protest by Greenpeace, involving a not-very-dangerous stuffed polar bear.

Nor do they seem to have thought about security and privacy issues. How do they protect their database of who lives in which dorm? Questions were cut off before I got a chance to ask that one, but I'm not optimistic.

The RISK here is that everybody (developers and police) is so in love with the shiny technology that nobody stops to notice that the emperor has no clothes.

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

[If you **can't** measure it, it's not science.
Robert A. Heinlein, "The Door Into Summer"]

[If you think you **can** measure it, something is probably wrong anyway.
Peter G. Neumann, The ACM Risks Forum
(Check your model and your assumptions at the door, eat a Heisenburger, and beware of many other risky challenges.)]

✂ DC Metro - only kills average of 1 customer each 3 years

Paul Robinson <rhc1394@yahoo.com>

Fri, 22 Jan 2010 00:18:27 -0800 (PST)

The Washington Metropolitan Transportation Authority, which runs the metrorail system in Washington, DC, has had exactly two accidents that killed customers in the 34 years it has been operating. From the system's opening in 1976 until 1982, there were no passenger fatalities.

The first accident occurred when a derailed train was backed up, but the other half of the train had also derailed, crashing it into a tunnel abutment and killing 3 passengers. The accident happened on January 13, 1982, at the same time as the Air Florida Flight 90 crashed into the 14th Street Bridge.

The second accident where 9 people were killed was in June, so if you average this, chances are either Metro won't kill someone until 2012, or, since each time they do have an accident, they kill 3 times as many, we could expect that since it was 6 years for the first accident, then 17 more for the second, that sometime around 2055, another Metrorail accident will kill 22 people!

And it's this sort of estimation that actuaries use to figure out insurance rates. Given enough incidents you can do a pretty good job of figuring out how often you'll have claims.

Actually, you're more likely to be killed on Metro if you're an employee than a customer, based on the number of employee deaths they've had. This also brings up a question: is the low number of customer deaths and long times between accidents a result of luck or some factors such as the equipment as designed being relatively safe?

GPS Control Software Glitch: NANU Issued

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

Thu, 28 Jan 2010 16:06:38 PST

Mostly affects military users, but also implications for some civilians. [TNX to Paul Saffo for spotting this one. (Robin Williams' Nanu-Nanu references probably unfamiliar to many readers.) PGN-ed]

``Moving Three GPS Satellites into New Orbits will have a profound effect on GPS capabilities for all civil, commercial, and military users worldwide." The GPS AEP Command and Control operational software update enables new capabilities ... but requires absolute compliance with the published GPS Interface Control Document (ICD). Some of the new features that are incorporated work only with authorized military receivers that have successfully passed security tests. However the live introduction of the new functions is causing problems wherein some of these receivers are intermittently not tracking Y-code, and non-compliant civilian receivers are also reporting continuing problems. Corrective action could encompass either the Air Force rolling back the update or revising its software, or the manufacturers modifying GPS software within the receivers to be totally compliant with the ICD.

January 21, 2010

<http://www.gpsworld.com/gnss-system/news/gps-control-software-glitch-nanu-issued-9414>

<http://www.gpsworld.com/gnss-system/news/new-243-gps-configuration-will-increase-accuracy-9368>

✂ How Not to Design Authentication

Alexander Klimov <alserkli@inbox.ru>

Wed, 27 Jan 2010 11:32:06 +0200

"Verified by Visa and MasterCard SecureCode:

or, How Not to Design Authentication"

by Steven J. Murdoch and Ross Anderson

<<http://www.cl.cam.ac.uk/~rja14/Papers/fc10vbvsecurecode.pdf>>:

Banks worldwide are starting to authenticate online card transactions using the '3-D Secure' protocol, which is branded as Verified by Visa and MasterCard SecureCode. This has been partly driven by the sharp increase in online fraud that followed the deployment of EMV smart cards for cardholder-present payments in Europe and elsewhere. 3-D Secure has so far escaped academic scrutiny; yet it might be a textbook example of how not to design an authentication protocol. It ignores good design principles and has significant vulnerabilities, some of which are already being exploited. Also, it provides a fascinating lesson in security economics. While other single sign-on schemes such as OpenID, InfoCard and Liberty came up with decent technology they got the economics wrong, and their schemes have not been adopted. 3-D Secure has lousy technology, but got the economics right (at least for banks and merchants); it now boasts hundreds of millions of accounts. We suggest a path towards more robust authentication that is technologically sound and where the economics would work for banks, merchants and customers -- given a gentle regulatory nudge.

✂ Radiation Offers New Cures, and Ways to Do Harm

David Hollman <dah8@cornell.edu>

Wed, 27 Jan 2010 09:47:25 +0000

Radiation Offers New Cures, and Ways to Do Harm

The New York Times, January 23, 2010

<http://www.nytimes.com/2010/01/24/health/24radiation.html>

This article goes into some detail about several failures in radiation treatments which lead to severe injury and deaths in patients. Although there was substantial human error involved, it seems that in some cases computer crashes and lack of failsafe functionality were at least contributing causes.

In one example, a crash of the controlling computer led a technician to mistakenly believe that instructions to properly restrict the amount of radiation received were saved, when in fact they were not. This was then compounded by additional error as operators failed to manually check whether the settings were correct. The patient was then massively over-radiated on several occasions.

I wonder if the general flakiness in personal computers that we are all used to results in an attitude that accepts such things as normal and acceptable, even in people who should have been trained to know better, and possibly even product designers and managers. In this example, such an attitude would probably have worse consequences than the actual technical fault in the equipment.

Warning: Your Cell Phone May Be Hazardous to Your Health

*"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 28 Jan 2010 16:15:45 PST*

Ever worry that that gadget you spend hours holding next to your head might be damaging your brain? Well, the evidence is starting to pour in, and it's not pretty. So why isn't anyone in America doing anything about it?

[Source: Christopher Ketcham, February 2010 issue of *GQ*, PGN-ed]
<http://www.gq.com/cars-gear/gear-and-gadgets/201002/warning-cell-phone-radiation>

Driver watching laptop movie kills woman

*"Walter Roberson" <roberson@hushmail.com>
Thu, 28 Jan 2010 13:05:22 -0600*

[The article emphasizes that it was a porn movie being watched, but it seems to me that the result could easily have been the same for many other genres -- WDR]

State police say a truck driver was watching pornographic movies on his laptop computer when his rig struck a disabled car on the New York State Thruway near Buffalo last month, killing the driver. Thomas Wallace of Ohio was arrested Tuesday. He's been charged with second-degree manslaughter in the death of 33-year-old Julie Stratton, a mother of two from a Buffalo suburb. [...] Investigators say Wallace also violated federal trucking rules by sleeping no more than four of 27 hours before the crash.

<http://cnews.canoe.ca/CNEWS/World/2010/01/27/12640006-ap.html>

It depends on which bus you take

*Paul Robinson <rfc1394@yahoo.com>
Fri, 22 Jan 2010 03:06:23 -0800 (PST)*

To go home from the Washington DC Metro I take either the 83 or 86 Metrobus into Maryland. The difference between the two routes is that the #86 takes a detour into the Prince George's Plaza station.

There is a street that crosses both routes. On the #86, the bus turns off Baltimore Ave and eventually reaches 40th Avenue, turns onto Oglethorpe street, where it turns on 42nd Ave. On the 83, it continues on Baltimore Ave and simply crosses Oglethorpe.

However, on board every bus running on the 83 and 86 lines is a display that shows to the passengers every street where the bus is making. It is consistent, in that on every #86 bus, it indicates when it is at *Oglethorpe Street*. On every #83 bus, it indicates when it is at *Ogelthorpe Street*.

Maybe it's just a GSP, err I mean GPS error...

✂ Driving and walking through buildings

*Pete Kaiser <djc@resiak.org>
Wed, 27 Jan 2010 12:15:48 +0100*

Near where I live in Zurich, Friedackerstrasse meets Friedheimstrasse in a T intersection. But Google Maps and the street map overlay in Google Earth show Friedackerstrasse making a 45-degree angle there.

The canopy of a tree at that intersection overhangs the entire actual meeting point of the two streets, something perfectly evident to the human eye in the aerial photograph. I hazard the guess that software used to detect roads on aerial photographs simply lost the streets there because of the tree, leaving the algorithm to do something -- anything -- about that, using some additional GIS data indicating that the streets really do intersect. And the algorithm routed (the mapping of) Friedackerstrasse through the house on the northeast corner. (It also routes a nearby pedestrian walk squarely through the apartment building it abuts.)

In practice this one case isn't a large risk because you can't really get lost because of it, but it provides some insight into how the software works, and how it fails when it fails. Where else are streets re-routed, nonexistent segments added, or existing ones omitted? And other features? It's not hard to imagine how this might be important.

This error, combined with the (here well known) principle "there's never just one bug", must give us pause.

✂ Re: Teleportation via Skyhook (Bliesener, [RISKS-25.89](#))

*Tony Lima <tony@tonylimaassociates.com>
Wed, 27 Jan 2010 16:59:18 -0800*

Actually this is a user error. Opera Mini uses transcoding to present the web page on mobile devices. That means every single bit transmitted and received is processed through Opera's computers. That's the reason for the Norwegian IP address.

Gary should have paid a few bucks for Opera Mobile which does not use transcoding, relying on more traditional on-device html interpretation.

I spent quite a bit of time testing both versions. Opera Mini is, indeed, very fast, but it always struck me that users were giving up way too much privacy.

Tony Lima Associates, Los Altos, CA, USA, 650-243-1286

Re: Extending TCP/IP into space (Randall, [RISKS-25.92](#))

*Mark Jackson <mjackson@alumni.caltech.edu>
Wed, 27 Jan 2010 15:12:21 -0500*

When the Shuttle overflies the runway when returning from the next ISS mission, we'll know why.

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



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 94

Sunday 14 February 2010

Contents

- [Electronic Systems That Make Modern Cars Go](#)
[Jim Motavalli](#)
- [Toyota Braking Problem Link](#)
[Gene Wirchenko](#)
- [How computers took over our cars](#)
[Amos Shapir](#)
- [Ex-Toyota lawyer points to electronic throttle control](#)
[PGN](#)
- [Motor racing solution to Toyota runaway](#)
[Dave Crooke](#)
- [Mercedes Benz E Class Commercial](#)
[Richard S. Russell](#)
- [Medical privacy: They never, ever learn](#)
[Geoff Kuenning](#)
- [Who Owns Your PC?](#)
[Lauren Weinstein](#)
- [EMV busted](#)
[David Magda](#)
- [Website glitch drives up parking penalty](#)
[Nick Rothwell](#)
- [The Century Bug will repeat ...](#)
[Jonathan de Boyne Pollard](#)
- [Making the grade or changing the grade?](#)
[Jeremy Epstein](#)
- [Phishing Scam Cripples European Emissions Trading](#)
[Danny Burstein](#)
- [Meta-spearphishing](#)
[Jeremy Epstein](#)
- [CAPTCHA with the answer in the ALT text](#)
[jidanni](#)
- [Re: GPS Control Software Glitch: NANU Issued](#)
[Andy Piper](#)
- [Re: Unsearchable Stores](#)
[Bob Bramwell](#)
- [Info on RISKS \(comp.risks\)](#)

✂ Electronic Systems That Make Modern Cars Go (Jim Motavalli)

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

Sat, 6 Feb 2010 14:41:34 PST

Source: Jim Motavalli, *The New York Times*, 4 Feb 2010

<http://nytimes.com/2010/02/05/technology/05electronics.html>

The electronic systems in modern cars and trucks -- under new scrutiny as regulators continue to raise concerns about Toyota vehicles -- are packed with up to 100 million lines of computer code, more than in some jet fighters. "It would be easy to say the modern car is a computer on wheels, but it's more like 30 or more computers on wheels," said Bruce Emaus, the chairman of SAE International's embedded software standards committee. Even basic vehicles have at least 30 of these microprocessor-controlled devices, known as electronic control units, and some luxury cars have as many as 100.

[Nice article on "throttle-by-wire" cars, eschewing physical linkages. PGN]

✂ Toyota Braking Problem Link

Gene Wirchenko <genew@ocis.net>

Thu, 11 Feb 2010 12:09:57 -0800

It appears that the problem was software:

Toyota to recall 400,000 Prius cars over software glitch. Following driver complaints about poor braking performance, Toyota plans to recall around 400,000 Prius hybrid cars to replace software controlling the antilock braking system.

<http://www.itbusiness.ca/it/client/en/home/news.asp?id=56365>

✂ How computers took over our cars

Amos Shapir <amos083@hotmail.com>

Thu, 11 Feb 2010 17:56:55 +0200

Increasingly, computers are in control of our cars, says Paul Horrell, and that is changing our relationship with the open road

<http://news.bbc.co.uk/1/hi/magazine/8510228.stm>

✂ Ex-Toyota lawyer points to electronic throttle control (USATODAY.com)

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

Thu, 11 Feb 2010 7:33:14 PST

Nancy Leveson commented to me, "When is the auto industry (and everyone else) going to learn that you cannot 'exhaustively test' software and introduce modern safety engineering techniques that are appropriate for digital systems and not just use those developed for the electro-mechanical systems of the past?"

Motor racing solution to Toyota runaway

Dave Crooke <dcrooke@gmail.com>

Sun, 31 Jan 2010 13:38:00 -0600

It occurred to me that I've had a throttle stuck wide open twice in the past[*], and neither incident was at all dramatic; the recent Toyota problem is only deadly due to the misapplication of the PC-style "soft power button" concept to a safety critical system. This is compounded by the use of a non-standard control interface in an environment that is otherwise highly standardized - that very standardization is a "key" safety feature.

Home-made dashboards with non-standard layouts and pushbutton ignition switches are common in motor racing, and a simple, robust solution was implemented decades ago - all race cars are required to have a *mechanical* switch which cuts power to all drive-train systems, with standard color, labeling and placement.

Perhaps in future cars with ignition buttons like this Toyota, or software controlled drive-trains like in a hybrid, there could be a mandatory standard requiring a hard-wired engine cutoff knob on the right hand side of the steering column, thus implementing the UI everyone (who doesn't drive a Saab) is familiar with?

Also ... I would have expected that the US federal "PRND21" standard for automatic transmission controls would require that a car could always be freely shifted from D or R to N to guard against just this circumstance ... any US auto engineers available to comment?

* For Lindsay Marshall's amusement: one in Tyne Tunnel at rush hour, when it was used by the A1.

Mercedes Benz E Class Commercial

"Richard S. Russell" <richardsrussell@tds.net>

Thu, 4 Feb 2010 23:27:06 -0600

An ad for the Mercedes Benz E Class touts its "safety" features, among which is that it can "even stop itself if [the driver] becomes distracted".

<http://www.youtube.com/watch?v=3DgjzHY5-2sM>

Right. Because nothing could EVER go wrong with THAT.

Richard S. Russell, 2642 Kendall Av. #2, Madison WI 53705-3736
608+233-5640 RichardSRussell@tds.net <http://richardsrussell.livejournal.com/>

Any idiot, upon seeing the first automobile, could easily predict that it would revolutionize transportation. Only someone with exceptionally keen insight could have foreseen that it would also revolutionize the sex lives of teenagers. Isaac Asimov

✂ Medical privacy: They never, ever learn

*Geoff Kuenning <geoff@cs.hmc.edu>
Mon, 08 Feb 2010 10:55:58 -0800*

I've been buying some medications through an online pharmacy run by my health plan. They seem to have added a new feature: when it's refill time, an automated system calls you and walks you through reordering. All in all, I found it to be a pretty convenient system.

Of course, Federal law requires them to protect my privacy; as I understand it, they can't legally reveal my prescriptions even to a family member. So when they got to the point of telling me what was available for refill, the automated voice kindly told me that they needed to verify my identity, then asked me to enter my birthdate and one other super-secret piece of information... my ZIP code.

Um, yeah. My wife **definitely** isn't going to know that one.

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

Keep trying, and keep the best.

✂ Who Owns Your PC?

*Lauren Weinstein <lauren@vortex.com>
Thu, 11 Feb 2010 17:21:19 -0800*

Who Owns Your PC? New Anti-Piracy Windows 7 Update
"Phones Home" to Microsoft Every 90 Days

(<http://lauren.vortex.com/archive/000681.html>)
(<http://lauren.vortex.com/WAT-KB971033.jpg>)

Greetings. Sometimes a seemingly small software update can usher in a whole new world. When Microsoft shortly pushes out a Windows 7 update with the reportedly innocuous title "Update for Microsoft Windows (KB971033)" -- it will be taking your Windows 7 system where it has never been before.

And it may not be a place where you want to go.

[Very long but worthy item TRUNCATED for RISKS. Check out the original.
PGN]

✂EMV busted

David Magda <dmagda@ee.ryerson.ca>

Thu, 11 Feb 2010 18:29:12 -0500

Seems that the EMV standard has been compromised:

- > "Chip and PIN is fundamentally broken," Professor Ross Anderson of
- > Cambridge University told ZDNet UK. "Banks and merchants rely on the words
- > 'Verified by PIN' on receipts, but they don't mean anything."

<http://news.zdnet.co.uk/security/0,1000000189,40022674,00.htm>

More reports:

<http://resources.zdnet.co.uk/articles/0,1000001991,40022669,00.htm>

<http://www.telegraph.co.uk/science/science-news/7215920/>

<http://www.physorg.com/news185118205.html>

Anderson's paper is available:

<http://www.lightbluetouchpaper.org/2010/02/11/chip-and-pin-is-broken/>

EMV is called often called "Chip and PIN", as well as "Chip Card" in Canada.

Some financial institutions put a lot of stock in the security of this:

- > You are responsible for the full amount of all authorized activity or
- > other Transactions resulting from use of the Card or Connect ID and PIN or
- > Password by any person, including any entry error or fraudulent or
- > worthless deposit at an ABM or other machine. You are responsible for the
- > full amount of all unauthorized activity or other Transactions which occur
- > before we receive notification that your PIN, Password or Card was lost or
- > stolen or that your Connect ID, PIN or Password may have become known to
- > an unauthorized person. On receiving such notice from you we will block
- > the Card's, PIN's or Connect ID's ability to access our services and/or
- > the use of a Card or the Account.

<https://www.tdcanadatrust.com/tdvisa/pdf/select.pdf> (column 9)

In many cases, the banks' (now no longer trust-worthy) logs are the definitive record:

- > Our records will be conclusive proof of use of a Card or the Account or
- > electronic services and will be considered your written request to perform

> the Transaction. Even though you may be provided with a Transaction
> receipt, verification or confirmation number, or interim statement by or
> through an ABM or other machine, the following applies to all Transactions
> or other activity on the Account:

> * our acceptance, count and verification of Transactions or deposits
> will be considered correct and binding unless there is an obvious error
> [...]

(Ibid.)

Some are a bit more reasonable, but if your card has been cloned (and put
back in your wallet/purse), you may not notice the problem until too late:

> If someone uses your Visa Card and your PIN or your Visa Account number
> with any other security code to make unauthorized purchases or otherwise
> obtain the benefits of your Visa Card, you will not be responsible for
> those charges provided that you (i) are able to establish to our
> reasonable satisfaction that you have taken reasonable steps to protect
> your Visa Card [...] and (ii) cooperate fully with our
> investigation. [...]

> You are not responsible for unauthorized use of your Visa Card or your
> Visa Account number in transactions in which neither a PIN nor a security
> code is used as the cardholder verification method.

<http://www.rbcroyalbank.com/cards/documentation/pdf/ch-agreement.pdf>

Website glitch drives up parking penalty

Nick Rothwell <nick@cassiel.com>

Fri, 12 Feb 2010 12:49:30 +0000

A driver's parking penalty fee escalates after the council payment web site
repeatedly reports that she has nothing to pay - because she entered her car
registration number in lower case.

<http://www.guardian.co.uk/money/2010/feb/12/southwark-council-car-registration>

The Century Bug will repeat every hundred years, sometimes

Jonathan de Boyne Pollard <J.deBoynePollard-newsgroups@NTLWorld.COM>

Sun, 24 Jan 2010 19:00:03 +0000

every ten years, because we forget or ignore what we should have learned.

In [RISKS-25.89](#) ("Y2K+10 problem 4: SpamAssassin tags '2010' e-mail as
spammish") M. Burstein wrote that the problem was that "It seems the 'year
date' was hard/hand coded, as opposed to making a comparison to 'today's'
date." and observed that "The SpamAssassin folk have a new version which

corrects this problem." In fact, they do not. The replacement rule incorporates the same problem as before, scheduled to occur simply ten years further into the future, in January 2020. This mistake has not been learned from, let alone corrected.

This is a core problem. The human race forgets or ignores problems that it has already solved. Back in the 1990s I was quietly predicting that by the year 2010 people would have forgotten all of the issues that had to be dealt with for the 1999-to-2000 transition, and would have gone back to (say) using two-digit year numbers. In part this would have been because people were erroneously calling it a "Millennium Bug", causing the erroneous inference that it was something that only ever arose every thousand years and could be forgotten once the year 2000 was past. Michael C. Battilana (www.cloanto.com/usrs/mcb), D. R. Ladd (writing in the letters page of *New Scientist* on 1998-03-14), J. R. Stockton, and others besides, all more loudly than I pointed out that the bug was due every century, and that the foolish name "Millennium Bug" tended to disguise that. But in part it would also have been because we won't have turned to people making the same mistakes all over again, saying "What you are doing is a bad idea, that cost the world a lot of time, effort, and money the last time we had to clean up the mess made. Don't repeat it."

And here we are, in 2010, showing that the world has not only not learned from the mistakes of 10 (and more) years ago, but is even making mistakes of the same type but with shorter periods than a century. The developers of SpamAssassin hit a problem caused by, in effect, ONE-digit year numbers (with regular expressions that fix the first three digits of the year at "200"), and rather than learn from the world's experience with the problems of two-digit year numbers of a mere ten years ago, they simply put the bug off for another ten years. It's "Rollover Year" every ten years with SpamAssassin.

And it's "Rollover Year" every century with others. It's sad to note that not only have some parts of the world forgotten the lessons of two-digit year rollover of a mere ten years ago, and gone back to using two-digit years, but other parts of the world never really even fixed the problem in the first place.

Here's one example from personal experience. Recently, I wrote an NNTP server and updated an NNTP client. Following RFC 3977, section 7.3.2, I made the client use 4-digit years in all "NEWNEWS" commands that it sends. I also made the server outright reject "NEWNEWS" commands that used 2-digit years, on the grounds that the RFC 3977 semantics for 2-digit years differed from the RFC 977 semantics, differed from the Single Unix Specification semantics, and were quite silly (requiring, as they did, the inference of year numbers that pre-date by several decades the very existence of NetNews); and that surely everyone had long since switched to 4-digit years, it being more than a decade since the specification for 4-digit years in NNTP (which has been around since IETF draft specifications of the 1990s) was invented and (supposedly, given that IETF standardization is supposed to follow practice) put into practice.

I was quite saddened to discover in testing that the world of NNTP simply ignored the Century Bug completely, and largely ignores RFC 3977 too. I

have yet to find in production use (albeit that I've not finished testing) an NNTP client that sends anything other than 2-digit years with the "NEWNEWS" (and "NEWGROUPS") command, despite the strong recommendation in RFC 3977 to the contrary, and I have yet to find an NNTP server (other than my own) that actually recognizes 4-digit year numbers when sent, despite the outright requirement in RFC 3977 for supporting this.

I haven't tested, but I strongly suspect that no-one even implements the RFC 3977 semantics for inferring four-digit years from two-digit ones, and the world still implements the RFC 977 semantics, which date from 1986 and mandate (for example) protocol commands as daft as asking for the NetNews articles from the year 1961. (The RFC 3977 changes to those semantics make things yet dafter, mandating protocol commands as daft as asking for the NetNews articles from the year 1912, and which introduce a new problem of jitter resulting from poor implementations on the 31st of December and the 1st of January every year.)

I'm sure that RISKS readers can produce similar experiences in other fields. So WHY haven't we learned the lessons here? Why are people, only a mere ten years on, forgetting the problem entirely and going back to employing two-digit years? Why are people even creating and perpetuating new ONE-digit year rollover problems, that they then had to deal with this year, and will even have to deal with again a few years from now?

JosephKK, in [RISKS 25.85](#), on a different subject, touched upon one of what is almost certainly many reasons. Xe is right. Current computer programming courses are inadequate in several areas which are perennial RISKS staple topics: bad handling of personal names; bad handling of dates, times, and timezones; and bad handling of geographic locations. I did a quick review of a couple of IT textbooks at the time of [RISKS 25.85](#) but didn't turn up anything that explained the common IT errors to avoid with personal names. It would be interesting to hear from RISKS' resident book reviewer, M. Slade, or anyone else, how many IT textbooks he has encountered that explain, for example, how it doesn't match reality to design database schemata (or laws!) specifying "Christian name" and "Surname" fields that hold one, capitalized, word each; how many books explain that there is an inherent ambiguity in a timestamp that doesn't include, or have implicit in its specification, a timezone; and how many books explain that there are practices that the world discovered, from the 1999-to-2000 transition, to be bad, and that it is simple foolishness to repeat them. How much of the experience that we've gained with doing simple, everyday, things with computers in the wrong ways, over and over again (as past issues of RISKS will attest), have we written down, published, and taught, for the benefits of those who will come after us?

On the subject of not learning lessons from situations that we've already experienced years before, here's a final something to think about in relation to the recent RISKS discussion of synthetic engine noise for otherwise nearly-silent cars (Gezelter, [RISKS 25.88](#); Strickler, [RISKS 25.90](#); and others): Look up and consider the decades-long legal battle in the U.K. (and elsewhere) over the requirement for and use of the humble bicycle bell.

Making the grade or changing the grade?

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Thu, 4 Feb 2010 14:43:08 -0500

Montgomery County Maryland public schools have learned that students apparently installed keyloggers on teachers' computers, then used the passwords they captured to log in and change their grades. Besides disciplining the students, they've given teachers two (ineffective) instructions: to check grades, and to change their passwords. The first is ineffective because most teachers enter grades directly into the system, and don't have hardcopies of the assigned grades to compare against. (According to the reports, there's an audit log, but no indication whether teachers are being sent copies of their portions of the log to examine for anomalies.) Changing the passwords is ineffective, of course, unless they're confidence the keyloggers are cleaned up....

Source:

<http://www.washingtonpost.com/wp-dyn/content/article/2010/01/28/AR2010012803494.html>

<http://www.washingtonpost.com/wp-dyn/content/article/2010/01/29/AR2010012902352.html>

<http://voices.washingtonpost.com/answer-sheet/montgomery-county-public-school/mcps-orders-password-changes-a.html?hpid=newswell>

The RISK is quite similar to many other types of systems -- if there's no way to cross-check data, then data attacks are much harder or even impossible to detect. That's true if you have a bank account and don't balance your checkbook, a grading system if the teacher believes everything on the screen, or an electronically cast vote.

Phishing Scam Cripples European Emissions Trading

danny burstein <dannyb@panix.com>

Thu, 4 Feb 2010 23:36:24 -0500 (EST)

(putting aside the whole issue of whether "cap and trade" and AGW is good, bad, or indifferent...)

[Speigel Online]

Phishing Scam Cripples European Emissions Trading

Sneaky cyber-thieves have made millions by fraudulently obtaining European greenhouse gas emissions allowances and reselling them. The scam has hampered trading of the credits, which are seen as an important tool in curbing climate change, in several European countries. According to a report in the Wednesday edition of the Financial Times Deutschland, hackers sent e-mails last Thursday to several companies in Europe, Japan and New Zealand which appeared to originate from the Potsdam-based German Emissions Trading Authority (DEHSt), part of the EU's Emission Trading System (EU

ETS). Ironically, the e-mail said that the recipient needed to re-register on the agency's Web site to counter the threat of hacker attacks.

The cyber-thieves then exploited the user data that was entered into their spoof Web site to transfer emissions allowances to other accounts, mainly in Denmark and Britain, from which they were quickly resold. The new owners of the allowances would have assumed that they had acquired them legally. ... The crime has hampered the registering of trades in allowances across a wide swath of the European Union.

rest:

<http://www.spiegel.de/international/europe/0,1518,675725,00.html>

✂ Meta-spearphishing

*Jeremy Epstein <jeremy.j.epstein@gmail.com>
Wed, 10 Feb 2010 12:33:22 -0500*

I received the following message today (links removed for obvious reasons) with a subject line "Russian spear phishing attack against .mil and .gov employees". What's interesting is that it's carefully written (good grammar), explains the real issue with Zeus, references a real project ("2020 project" which is at DNI) and then provides links to innocent (but presumably compromised) sites to download a "fix". In fact, the first paragraph is taken from a legitimate site: <http://intelfusion.net/wordpress/2010/02/08/russian-spear-phishing-attack-against-mil-and-gov-employees/> and the signature at the bottom is a legitimate researcher/company - but of course the email didn't come from him, as shown by the email headers.

This is definitely the best example I've seen of a phish....

>Russian spear phishing attack against .mil and .gov employees
>
>A `relatively large' number of U.S. government and military employees
>are being taken in by a spear phishing attack which delivers a variant
>of the Zeus trojan. The email address is spoofed to appear to be from
>the NSA or IntelLink concerning a report by the National Intelligence
>Council named the `2020 Project'. It's purpose is to collect passwords
>and obtain remote access to the infected hosts.
>
>Security Update for Windows 2000/XP/Vista/7 (KB823988)
>
>About this download: A security issue has been identified that could
>allow an attacker to remotely compromise a computer running Microsoft®
>Windows® and gain complete control over it. You can help protect your
>computer by installing this update from Microsoft. After you install this
>item, you may have to restart your computer.
>
>Download:
><http://REMOVEDTHEDOMAIN.org/downloads/winupdate.zip>

>or

><http://www.REMOVEDTHEDOMAIN.com/file/tj373l>

>

>_____

>Jeffrey Carr is the CEO of GreyLogic, the Founder and Principal Investigator

>of Project Grey Goose, and the author of "Inside Cyber Warfare".

>EMAILREMOVED@greylogic.us

✂ CAPTCHA with the answer in the ALT text

<jidanni@jidanni.org>

Wed, 03 Feb 2010 08:01:13 +0800

Hmmm, a accessible CAPTCHA

<http://en.wikipedia.org/wiki/CAPTCHA#Accessibility>

with ALT text for each letter,

...

(Seen on http://www.mofnpb.gov.tw/PubOpinionMail.php?cat_id=99)

Well I suppose they aren't giving away the store by putting them

all in one string, but it is still nice for we text browser users.

✂ Re: GPS Control Software Glitch: NANU Issued (PGN, [RISKS-25.93](#))

Andy Piper <andy@xemacs.org>

Mon, 01 Feb 2010 10:53:57 +0000

> Mostly affects military users, but also implications for some civilians.

Good old RISKS!

My old TomTom Go 300 has been having trouble telling which road I am on for the last couple of weeks. Usually it's out by about 20 yards - enough that sometimes it gets the road right and sometimes wrong. I thought maybe it was a hardware fault, but now I am not so sure.

How long until we have a flurry of new SatNav-got-it-wrong related posts?

✂ Re: Unsearchable Stores (Brader, [RISKS-25.92](#))

Bob Bramwell <bob@copenhagen.cuug.ab.ca>

Sat, 13 Feb 2010 16:57:07 -0400

There's no way to enter an apostrophe on the GPS. (quoting John Varela)

Equally irritating is the inability to search for names which contain digits on my iPod Classic. Since I have a large number of classical

music tracks with titles along the lines of:

BWV 198: Lass Fürstin, Lass Noch Einen Strahl
this makes life unnecessary awkward.

The risk, I suppose, is that next time I'll look for a product that provides
a better user interface - assuming such a thing exists.

Bob Bramwell +1 902 531 2289



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 95

Sunday 28 February 2010

Contents

- [Growing Threat to GPS Systems From Jammers](#)
[Jerry Leichter](#)
- [Sat-nav systems under growing threat from 'jammers'](#)
[Amos Shapir](#)
- [More on Risks of EMV Legacy Compatibility](#)
[Anthony Thorn](#)
- [Self-Signed Certificates Strike Again?](#)
[Bob Gezelter](#)
- [Facebook friended, boyfriend offended, tragically ended](#)
[John Linwood Griffin](#)
- [Google: Serious threat to the web in Italy](#)
[Monty Solomon](#)
- [Fault-Tolerance as a Risk](#)
[Gene Wirchenko](#)
- [School District Spying on Students at Home?](#)
[Gene Wirchenko](#)
- [A Message from Ric Edelman about data lost](#)
[fjohn reinke](#)
- [Nationwide Technetium shortage: coinciding reactor failure/maintenance](#)
[Richard I. Cook](#)
- [IEEE Symposium on Security and Privacy: 30th anniversary](#)
[David Evans](#)
- [FOSE 2010](#)
[Kalin Tyler](#)
- [Info on RISKS \(comp.risks\)](#)

✉ Growing Threat to GPS Systems From Jammers

Jerry Leichter <leichter@lrw.com>

Thu, 25 Feb 2010 20:44:03 -0500

The BBC reports (<http://news.bbc.co.uk/2/hi/science/nature/8533157.stm>) on the growing threat of jamming to satellite navigation systems. The

fundamental vulnerability of all the systems - GPS, the Russian Glonass, and the European Galileo - is the very low power of the transmissions. (Nice analogy: A satellite puts out less power than a car headlight, illuminating more than a third of the Earth's surface from 20,000 kilometers.) Jammers - which simply overwhelm the satellite signal - are increasingly available on-line. According to the article, low-powered hand-held versions cost less than £100, run for hours on a battery, and can confuse receivers tens of kilometers away.

The newer threat is from spoofers, which can project a false location. This still costs "thousands", but the price will inevitably come down.

A test done in 2008 showed that it was easy to badly spoof ships of the English coast, causing them to read locations anywhere from Ireland to Scandinavia.

Beyond simple hacking - someone is quoted saying "You can consider GPS a little like computers before the first virus - if I had stood here before then and cried about the risks, you would've asked 'why would anyone bother?'" - among the possible vulnerabilities are to high-value cargo, armored cars, and rental cars tracked by GPS. As we build more and more "location-aware" services, we are inherently building more "false-location-vulnerable" services at the same time. -- Jerry

✂ Sat-nav systems under growing threat from 'jammers'

*Amos Shapir <amos083@hotmail.com>
Wed, 24 Feb 2010 17:54:47 +0200*

"While "jamming" sat-nav equipment with noise signals is on the rise, more sophisticated methods allow hackers even to program what receivers display. At risk are not only sat-nav users, but also critical national infrastructure."

Full story at: <http://news.bbc.co.uk/1/hi/sci/tech/8533157.stm>

[This risk noted by several others as well.]

✂ More on Risks of EMV Legacy Compatibility (Magda, [RISKS-25.94](#))

*Anthony Thorn <anthony.thorn@atss.ch>
Tue, 23 Feb 2010 09:27:28 +0100*

Recently Ross Anderson's group has published a new and very serious vulnerability in the "Chip & Pin" (EMV) authentication used by many -probably most- credit and debit card issuers world wide.

Very briefly: "The attack uses an electronic device as a "man-in-the-middle" the terminal thinks that the PIN was entered correctly, and the

card assumes that a signature was used to authenticate the transaction."

The paper:

<http://www.cl.cam.ac.uk/research/security/projects/banking/nopin/oakland10chipbroken.pdf>

The FAQ

<http://www.cl.cam.ac.uk/research/security/projects/banking/nopin/>

The BBC Video

http://www.bbc.co.uk/blogs/newsnight/susanwatts/2010/02/new_flaws_in_chip_and_pin_syst.html

The risk: Providing "legacy compatibility", in this case with signature based authentication, always involves additional risk and requires special attention.

(Acknowledgment to Bruce Schneier's blog)

✂ Self-Signed Certificates Strike Again?

Bob Gezelter <gezelter@rlgsc.com>

Tue, 23 Feb 2010 07:03:33 -0500

CNN has posted an item: "Elvis Presley passport exposes security flaw" (Atika Shubert, 2010-02-23) relating an interview with Adam Laurie and Jeroen Van Beek, two self-described "ethical hackers" who created a forged passport in the name of Elvis Presley from a non-existent country.

According to the article, the passport was accepted by an automated scanning machine, even though it was signed by what amounted to a self-signed certificate. Laurie is quoted as saying that many countries do not share sufficient information for others to authenticate the digital signatures.

The article can be found at:

<http://www.cnn.com/2010/TECH/02/19/passport.security/index.html>

The need for commonly accepted higher level certification authority or authorities is a well-understood part of such digital signature authentication schemes. It is disturbing that such a registration or acceptance feature, common to all web browser security implementations, has not been internationally accepted, despite the fact that the infra-structure is already in place in a number of international organizations (e.g., IPU, ITU-T [formerly CCITT], and others).

- Bob Gezelter, <http://www.rlgsc.com>

✂ Facebook friended, boyfriend offended, tragically ended

John Linwood Griffin <griffin2@ece.cmu.edu>

Thu, 25 Feb 2010 14:49:21 -0500 (EST)

The independent newspaper **City Paper** runs a weekly column, "Murder Ink", that provides coverage of homicides here in Baltimore City, Maryland.

A computer-related murder on February 17, 2010, caught my eye:

> Two men got into an argument with Couther's aunt over a Facebook page.
> Couther went into the living room to help his aunt and ended up arguing
> and then fighting with one of the men [resulting in Couther's throat being
> slashed] [...] Couther died at a local hospital an hour later. Montaize
> Alford [was] arrested and charged with Couther's murder. According to
> [Stephen Janis of investigativevoice.com], the aunt was being beaten by
> her boyfriend because a man "friended" her on Facebook.

<http://www.citypaper.com/news/story.asp?id=19818> (Anna Ditkoff writing in **City Paper** volume 34 number 8, page 8, February 23, 2010)

Peter Hermann of **The Baltimore Sun** corroborates the Facebook angle on his blog, citing police detective Michael Moran's charging documents:

> [Couther's aunt] Begett had returned from work and was sleeping on her
> sofa when Alford called her on her cell phone at about 2 a.m. and started
> arguing with her about a male friend on her Facebook page [...] Begett
> hung up on Alford and moments later he showed up at her home and entered
> using a key. He began assaulting her [then] Couther and Alford began
> fighting [resulting in] a large laceration to [Couther's] neck which was
> bleeding profusely.

http://weblogs.baltimoresun.com/news/crime/blog/2010/02/slew_of_homicide_arrests_inclu.html

Since this is the RISKS Forum, I felt at first compelled to come up with a piquant observation about the erosion of privacy inherent in social network computing. But then I realized I'm missing the broader issue. It's not our role as scientists and practitioners to complain about how "the times they are a-changin'" -- it's to ask questions like "was Begett aware when she accepted the friending request that the action would be visible to her boyfriend, and if she was not aware then how could that consequence have been conveyed better by Facebook or other entities?" The RISK to me (whom a student called "tragically uncool" due to my apparent underuse of social networking media) is missing an opportunity to do something about a problem simply because I don't like the problem.

Google: Serious threat to the web in Italy

Monty Solomon <monty@roscom.com>
Wed, 24 Feb 2010 09:30:43 -0500

Serious threat to the web in Italy, 24 Feb 2010

In late 2006, students at a school in Turin, Italy filmed and then uploaded a video to Google Video that showed them bullying an autistic schoolmate. The video was totally reprehensible and we took it down within hours of being notified by the Italian police. We also worked with the local police to help identify the person responsible for uploading it and she was subsequently sentenced to 10 months community service by a court in Turin, as were several other classmates who were also involved. In these rare but unpleasant cases, that's where our involvement would normally end.

But in this instance, a public prosecutor in Milan decided to indict four Google employees -David Drummond, Arvind Desikan, Peter Fleischer and George Reyes (who left the company in 2008). The charges brought against them were criminal defamation and a failure to comply with the Italian privacy code. To be clear, none of the four Googlers charged had anything to do with this video. They did not appear in it, film it, upload it or review it. None of them know the people involved or were even aware of the video's existence until after it was removed.

Nevertheless, a judge in Milan today convicted 3 of the 4 defendants - David Drummond, Peter Fleischer and George Reyes - for failure to comply with the Italian privacy code. All 4 were found not guilty of criminal defamation. In essence this ruling means that employees of hosting platforms like Google Video are criminally responsible for content that users upload. We will appeal this astonishing decision because the Google employees on trial had nothing to do with the video in question. Throughout this long process, they have displayed admirable grace and fortitude. It is outrageous that they have been subjected to a trial at all. ...

<http://googleblog.blogspot.com/2010/02/serious-threat-to-web-in-italy.html>

✶ Fault-Tolerance as a Risk

*Gene Wirchenko <genew@ocis.net>
Mon, 22 Feb 2010 12:44:10 -0800*

Tim Greene, *IT Business*, 22 Feb 2010

Kneber botnet -- a multi-headed hydra that's wreaking havoc

The most sinister aspect of the Kneber botnet is its interaction with other malware networks, suggesting a symbiotic relationship that ultimately makes each bot more resistant to being dismantled.

<http://www.itbusiness.ca/it/client/en/home/news.asp?id=56499>

At the bottom of the first page of the article are these two paragraphs:

'What he found is that more than half the 74,000 compromised computers -- bots -- within Kneber were also found infected with other malware that uses a different command-and-control structure. If one of the criminal networks were disabled, the other could be used to build it up again,

"At the very least, two separate botnet families with different [command-and-control] infrastructures can provide fault tolerance and

recoverability in the event that one [command-and-control] mechanism is taken down by security efforts," he says in his written analysis of the Kneber botnet.'

✂ School District Spying on Students at Home?

Gene Wirchenko <genew@ocis.net>

Mon, 22 Feb 2010 13:37:37 -0800

http://news.cnet.com/8301-30977_3-10457077-10347072.html

Students'-eye view of Webcam spy case

The first two paragraphs:

'Students at Herriton High School in Lower Merion School District near Philadelphia are given Apple MacBook laptops to use both at school and at home. Like all MacBooks, the ones issued to the students have a Webcam. And, in addition to the students' ability to use the Webcam to take pictures or video, the school district can also use it to take photographs of whomever is using the computer.

In a civil complaint (PDF) filed in federal court, a student at the school, Blake Robbins, said he received a notice from an assistant principal informing him that "the school district was of the belief that minor plaintiff was engaged in improper behavior in his home, and cited as evidence a photograph from the Webcam."

It is apparently worse than that:

http://www.infoworld.com/d/adventures-in-it/when-schools-spy-their-students-bad-things-happen-474?source=IFWNLE_nlt_notes_2010-02-22

InfoWorld Home / Adventures in IT / Robert X. Cringely Notes from the Field
February 22, 2010

When schools spy on their students, bad things happen Pennsylvania's Lower Merion School District thought it was clever to use webcams to track its students' MacBooks -- boy, were they mistaken

Savanna Williams, a statuesque sophomore at Harriton, appeared on CBS's "The Early Show" with her mother, talking about how she takes her school-supplied notebook everywhere -- including the bathroom when she showers. If that doesn't give you a strong mental image of the potential for abuse, nothing will.

For a thoroughly creepy demonstration of how another school, the Bronx's IS 339, spies on its students using webcams, check out this video. Assistant Principal Dan Ackerman cheerfully shows how he watches sixth and seventh graders in real time without their knowing it while they preen in front of an app called Photo Booth.

Photo Booth is always fun... a lot of kids are just on it to check their

hair, do their makeup, the girls, you know. They just use it like it's a mirror... They don't even realize that we're watching...I always like to mess with them and take a picture.

At least he's doing it on school grounds and not in their bathrooms."

A Message from Ric Edelman about data lost

*fjohn reinke <fjohn@reinke.cc>
Tue, 23 Feb 2010 17:54:09 -0500*

Begin forwarded message:

> From: "Edelman Financial" <client@ricedelman.com>
> Date: February 23, 2010 4:58:14 PM EST
> Subject: A Message from Ric Edelman

Dear fjohn and Evlynn:

For the past two years we have been distributing news, reviews and other important information to you via email. By bypassing the postal service we are able to contact you more easily, quickly and cheaply --- which improves speed and helps us control expenses. Email also allows you to respond to us more easily and quickly, too, resulting in faster and better service.

The vendor we use for sending you my updates and other non account-related communications is iContact. We have just been informed that email addresses have been stolen from iContact's system, possibly by one of their former employees. iContact is working with law enforcement officials on the matter and has not yet determined the extent of the theft. At this time, your email address may or may not have been involved. Because we do not provide iContact with anything other than email addresses and names, your personal information remains safe. It was not possible for the thief to obtain addresses, account numbers or any personal financial data. The worst case is that you might notice an increase in the amount of spam that you receive. [...]

My best regards, Ric Edelman, Chairman & CEO, 888-752-6742

[I invite you to read my blog "Reinke Faces Life", visit my sites (all listed at <http://krunchd.com/reinkefj>), and use whatever you need. Join me (reinkefj) on LinkedIn, Facebook, Plaxo, and / or follow me on Twitter. Remember the adage "first seek to help; then be helped".]

Nationwide Technetium shortage: coinciding reactor failure/maintenance

*"Richard I. Cook, MD" <rcook@airway2.bsd.uchicago.edu>
Tue, 23 Feb 2010 15:45:28 -0600*

> Subject: Clinical Update: Nationwide Technetium shortage memo..[]

> Date: Tue, 23 Feb 2010 ##:##:## -####
> From: Big University Hospital

On 14 May 2009 the NRU Reactor in Canada was shut down due to a heavy water leak for repairs. This has impacted approximately 40% of the world's supply of Mo-99. Consequently, this has created a nationwide shortage of Tc99 which is used in 80% of nuclear medicine imaging procedures.

On 19 Feb 2010 the High Flux Petten Reactor in the Netherlands will be shut down for approximately 6 months for repairs further exasperating the already acute shortage. In the coming weeks it may be necessary to adjust schedules to cope with the cyclical nature of the remaining supply of Tc99 from our commercial radiopharmaceutical providers. Typically, our providers will have a more ample supply in the beginning and end of the week, with seriously depleted availability Tuesdays and Wednesdays as a result.

Even further complicating the matters, all five major medical isotope reactors will be off-line for approximately two weeks in mid-March for routine maintenance. There is a strong possibility there may be no product available during certain days during those two weeks.

We will be doing everything we can to minimize the impact of this shortage to our patients including reducing our normal radioactive doses, switching to protocols that can conserve our supply of Tc99 and possibly using alternative radioisotopes when clinically applicable. We hope to continue to serve our faculty and our patients as efficiently as possible during this crisis.

If you have any questions, please feel free to contact...

We appreciate your understanding during this shortage.

Technetium-99m is a short half-life gamma emitter that is used extensively in nuclear imaging, especially in nuclear cardiology where is the mainstay of stress-test imaging. It's short half-life makes it ideal for diagnostic studies; a small dose of Tc-99m containing tracer can be given to a patient for a high-quality imaging study with the radioactivity falling to virtually nothing within a day. The isotope is produced continually as a decay product of Molybdenum-99 which has a half-life about 10x as long.

The great benefit of the short half-life of the metal imposes a hard physical limit on its use: it is essential that newly isolated TC-99 be used within a few hours of its production -- there is no way to store it. The radiation exposure from a routine TC-99m heart exam is 250 to 500 x that from a routine chest x-ray. As many as 4 million people undergo such testing in the U.S. each year.

The present trouble is the result of a long and complex chain of events. The main Mo-99 production reactor, located in Canada and operated by Atomic Energy of Canada Limited (AECL), was shut down in early 2009 after a containment vessel leak was discovered. Repairs are proceeding slowly. Two replacement reactors were constructed and commissioned but have never used

for production because of technical problems and because AECL determined in early 2008 that they would have been too expensive to run. Unrelated to the Canadian outage, a major European source in Holland as shut down in 2008 because of corrosion problems. It was expected to restart this month but this has been pushed back to "the second half" of August 2010. Several news sources are reporting that the Maria Polish reactor will be used to produce medical isotopes, although there are obstacles that may delay availability further.

A combination of factors have generated the high degree of dependency on a few, old reactors. The cost of designing, certifying, building, and commissioning a new reactor is high and operating them has proven far more expensive than was expected. Concerns about the security for reactors have increased greatly in the wake of 9/11. Radiopharmaceutical production is not a growth industry -- indeed advances in non-radioactive imaging show great promise and may replace the older methods within a decade. No one wants to spend the huge amount of money needed to build a new reactor to serve a declining market share. The use of the Maria reactor, which was constructed in 1970 and renewed in 1986, for this purpose makes sense on a marginal cost basis: you have a reactor than can do this and no one else does, why not take advantage of the brief window of opportunity afforded by fate?

A spin-off of the shortage is that it creates an incentive for the quick use of available Tc-99m. Rather than allowing substantial amounts of Tc-99m to simply decay before use, look for nuclear medicine programs to seek rigid control of exam timing and to book patients "standby" to assure that all of the available material gets used each day.

What does this have to do with RISKS? Not a thing. For once, the problem is not related to the computers for these reactors, many of which are ancient devices that only augment the manual and conventional automation that controls the reactors!

R.I.Cook, MD

IEEE Symposium on Security and Privacy: 30th anniversary

David Evans <evans@cs.virginia.edu>

Fri, 19 Feb 2010 21:04:19 -0500

31st IEEE Symposium on Security and Privacy, 16-19 May 2010
The Claremont Resort, Berkeley/Oakland, California

Advance Program

Sunday, 16 May 2010

4-7pm Registration and Welcome Reception

Monday, 17 May 2010

8:30-8:45 Opening Remarks

Ulf Lindqvist, David Evans, Giovanni Vigna

8:45-10:00 Session 1: Malware Analysis

Chair: Jon Giffin, Georgia Institute of Technology

Inspector Gadget: Automated Extraction of Proprietary Gadgets from Malware Binaries

Clemens Kolbitsch (Vienna University of Technology),
Thorsten Holz (Vienna University of Technology),
Christopher Kruegel (University of California, Santa Barbara),
Engin Kirda (Institute Eurecom)

Synthesizing Near-Optimal Malware Specifications from Suspicious Behaviors

Matt Fredrikson (University of Wisconsin),
Mihai Christodorescu (IBM Research),
Somesh Jha (University of Wisconsin),
Reiner Sailer (IBM Research),
Xifeng Yan (University of California, Santa Barbara)

Identifying Dormant Functionality in Malware Programs

Paolo Milani Comparetti (Technical University Vienna),
Guido Salvaneschi (Politecnico di Milano),
Clemens Kolbitsch (Technical University Vienna),
Engin Kirda (Institut Eurecom),
Christopher Kruegel (University of California, Santa Barbara),
Stefano Zanero (Politecnico di Milano)

10:20-noon Session 2: Information Flow

Chair: David Molnar, Microsoft Research Redmond

Reconciling Belief and Vulnerability in Information Flow

Sardaouna Hamadou (University of Southampton),
Vladimiro Sassone (University of Southampton),
Catuscia Palamidessi (École Polytechnique)

Towards Static Flow-based Declassification for Legacy and Untrusted Programs

Bruno P.S. Rocha (Eindhoven University of Technology),
Sruthi Bandhakavi (University of Illinois at Urbana Champaign),
Jerry I. den Hartog (Eindhoven University of Technology),
William H. Winsborough (University of Texas at San Antonio),
Sandro Etalle (Eindhoven University of Technology)

Non-Interference Through Secure Multi-Execution

Dominique Devriese, Frank Piessens (K. U. Leuven)

Object Capabilities and Isolation of Untrusted Web Applications

Sergio Maffei (Imperial College London),
John C. Mitchell (Stanford University),
Ankur Taly (Stanford University)

1:30-2:45 Session 3: Root of Trust

Chair: Radu Sion, Stony Brook University

TrustVisor: Efficient TCB Reduction and Attestation

Jonathan McCune (Carnegie Mellon University),
Yanlin Li (Carnegie Mellon University), Ning Qu (Nvidia),
Zongwei Zhou (Carnegie Mellon University),
Anupam Datta (Carnegie Mellon University),
Virgil Gligor (Carnegie Mellon University),
Adrian Perrig (Carnegie Mellon University)

Overcoming an Untrusted Computing Base: Detecting and Removing
Malicious Hardware Automatically

Matthew Hicks (University of Illinois),
Murph Finnicum (University of Illinois),
Samuel T. King (University of Illinois),
Milo M. K. Martin (University of Pennsylvania),
Jonathan M. Smith (University of Pennsylvania)

Tamper Evident Microprocessors

Adam Waksman, Simha Sethumadhavan (Columbia University)

3:15-4:55 Session 4: Information Abuse

Chair: Patrick Traynor, Georgia Institute of Technology

Side-Channel Leaks in Web Applications: a Reality Today, a Challenge
Tomorrow

Shuo Chen (Microsoft Research),
Rui Wang (Indiana University Bloomington),
XiaoFeng Wang (Indiana University Bloomington),
Kehuan Zhang (Indiana University Bloomington)

Investigation of Triangular Spamming: a Stealthy and Efficient
Spamming Technique

Zhiyun Qian (University of Michigan),
Z. Morley Mao (University of Michigan),
Yinglian Xie (Microsoft Research Silicon Valley),
Fang Yu (Microsoft Research Silicon Valley)

A Practical Attack to De-Anonymize Social Network Users

Gilbert Wondracek (Vienna University of Technology),
Thorsten Holz (Vienna University of Technology),
Engin Kirda (Institute Eurecom),
Christopher Kruegel (University of California, Santa Barbara)

SCiFI - A System for Secure Face Identification

Margarita Osadchy, Benny Pinkas, Ayman Jarrous,
Boaz Moszkovich (University of Haifa)

6:30pm Special Gala Event

Celebrating the 30th Anniversary of Security and Privacy
Master of Ceremonies: Peter G. Neumann

Tuesday, 18 May 2010

9-10:15am Session 5: Network Security

Chair: Cristina Nita-Rotaru, Purdue University

Round-Efficient Broadcast Authentication Protocols for Fixed Topology
Classes

Haowen Chan, Adrian Perrig (Carnegie Mellon University)

Revocation Systems with Very Small Private Keys

Allison Lewko (University of Texas at Austin),
Amit Sahai (University of California, Los Angeles),
Brent Waters (University of Texas at Austin)

Authenticating Primary Users' Signals in Cognitive Radio Networks via
Integrated Cryptographic and Wireless Link Signatures

Yao Liu, Peng Ning, Huaiyu Dai (North Carolina State University)

10:15-10:45 Session 6: Systematization of Knowledge I

Chair: Z. Morley Mao, University of Michigan

Outside the Closed World: On Using Machine Learning For Network
Intrusion Detection

Robin Sommer (ICSI/Lawrence Berkeley National Laboratory),
Vern Paxson (ICSI/University of California, Berkeley)

All You Ever Wanted to Know about Dynamic Taint Analysis and Forward
Symbolic Execution (but might have been afraid to ask)

Thanassis Avgerinos, Edward Schwartz,
David Brumley (Carnegie Mellon University)

State of the Art: Automated Black-Box Web Application Vulnerability
Testing

Jason Bau, Elie Bursztein, Divij Gupta,
John Mitchell (Stanford University)

1:45-3:00 Session 7: Secure Systems

Chair: Jonathan McCune, Carnegie Mellon University

A Proof-Carrying File System

Deepak Garg, Frank Pfening (Carnegie Mellon University)

Scalable Parametric Verification of Secure Systems: How to Verify
Reference Monitors without Worrying about Data Structure Size

Jason Franklin (Carnegie Mellon University),
Sagar Chaki (Carnegie Mellon University),
Anupam Datta (Carnegie Mellon University),
Arvind Seshadri (IBM Research)

HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor
Control-Flow Integrity

Zhi Wang, Xuxian Jiang (North Carolina State University)

3:20-4:10 Session 8: Systematization of Knowledge II

Chair: Ed Suh, Cornell University

How Good are Humans at Solving CAPTCHAs? A Large Scale Evaluation

Elie Bursztein, Steven Bethard, John C. Mitchell,
Dan Jurafsky (Stanford University), Céline Fabry

Bootstrapping Trust in Commodity Computers

Bryan Parno, Jonathan M. McCune,
Adrian Perrig (Carnegie Mellon University)

4:30-5:30 Short Talks

Short Talks Chair: Angelos Stavrou, George Mason University

5:45-7:30pm Reception and Poster Session

Poster Session Chair: Carrie Gates (CA Labs)

Wednesday, 19 May 2010

9-10:15am Session 9: Analyzing Deployed Systems

Chair: J. Alex Halderman, University of Michigan

Chip and PIN is Broken

Steven J. Murdoch, Saar Drimer, Ross Anderson,
Mike Bond (University of Cambridge)

Experimental Security Analysis of a Modern Automobile

Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel,
Tadayoshi Kohno (University of Washington), Stephen Checkoway,
Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham,
Stefan Savage (University of California, San Diego)

On the Incoherencies in Web Browser Access Control Policies

Kapil Singh (Georgia Institute of Technology),
Alexander Moshchuk (Microsoft Research),
Helen J. Wang (Microsoft Research),
Wenke Lee (Georgia Institute of Technology)

10:45-noon Session 10: Language-Based Security

Chair: David Brumley, Carnegie Mellon University

ConScript: Specifying and Enforcing Fine-Grained Security Policies
for JavaScript in the Browser

Leo Meyerovich (University of California, Berkeley),
Benjamin Livshits (Microsoft Research)

TaintScope: A Checksum-Aware Directed Fuzzing Tool for Automatic
Software Vulnerability Detection

Tiefei Wang (Peking University), Tao Wei (Peking University),
Guofei Gu (Texas A & M University), Wei Zou (Peking University)

A Symbolic Execution Framework for JavaScript

Prateek Saxena, Devdatta Akhawe, Steve Hanna, Stephen McCamant,
Dawn Song, Feng Mao (University of California, Berkeley)

noon-12:15 Closing, Ulf Lindqvist, David Evans, Giovanni Vigna

Thursday, 20 May 2010

Workshops (separate registration required):

- * Systematic Approaches to Digital Forensic Engineering
- * Workshop on Security and Privacy in Social Networks
- * W2SP 2010: Web 2.0 Security & Privacy

FOSE 2010

"Kalin Tyler" <ktyler@1105media.com>

Thu, 18 Feb 2010 23:42:37 -0800

You are well aware of the challenges we as a CyberSecurity community face from rapid changes in the technology landscape. FOSE 2010 is the place to discover opportunities and solutions along with changing expectations for government IT professionals.

Register today for the FOSE 2010 experience <http://www.fose.com>. If you sign up now you also get a 10% discount on a conference pass. You can redeem this discount here <http://cli.gs/FOSE10>.

You can expect:

- 3 days of IT resources helping you navigate today's shifting tech landscape
- 2 full conference days packed with education on emerging technologies, trends, and new improvements to existing solutions
- Thousands of products on the FREE* EXPO floor allowing you to gain one-on-one insight into the capabilities of our exhibitors through demos, theater presentations and FREE Education.
- Attend the Accenture CyberSecurity Pavilion or Focus on Digital Forensics.

*FOSE is a must-attend free show for government, military, and government contractors.

It's time to register and reserve your place at FOSE today! Visit <http://www.fose.com> to learn more about what FOSE has to offer, or redeem your 10% discount by registering here: <http://cli.gs/FOSE10>.

Kalin Tyler, ktyler@1105media.com, FOSE Team/Tuvel Communications

Connect with FOSE

Twitter: <http://twitter.com/FOSE>

Facebook: <http://cli.gs/85RgD5>

LinkedIn: <http://cli.gs/Vn8mMQ>

GovLoop: <http://www.govloop.com/group/fose>



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 96

Saturday 13 March 2010

Contents

- [Silly season: DST is approaching](#)
[David Magda](#)
- [Sony PS3: Yet Another leap year folly](#)
[Steve Summit](#)
- [Sony thinks 2010 is a leap year](#)
[Debora Weber-Wulff](#)
- [Old models of PS3 failed to connect to network due to leap-year miscalculation](#)
[Chiaki Ishikawa](#)
- [Re: The Century Bug Will Repeat](#)
[Jerry Leichter](#)
- [Death in the Atlantic: The Last 4 Minutes of Air France Flight 447](#)
[F John Reinke](#)
- [Software flaws may be at the root of Toyota's woes](#)
[Gene Wirchenko](#)
- [Risk: Toyota secretive on 'black box' data](#)
[AP via Gabe Goldberg](#)
- [Breakthrough in Electron Spin Control Brings Quantum Computers Closer to Reality](#)
[NSE](#)
- [German Data Retention Law Overturned](#)
[Bob Gezelter](#)
- [USGov rescinds 'leave Internet alone' policy](#)
[Richard Forno](#)
- [Man posts "wanted" poster of himself on own Facebook page](#)
[Mark Brader](#)
- [Car insurance bug](#)
[Clive D.W. Feather](#)
- [Daily cyber attacks on the UK](#)
[Martyn Thomas](#)
- ["Traffic analysis" from data](#)
[David Magda](#)
- [Paranoia 101](#)
[Paul Wexelblat](#)
- [Risks of having friends with computers](#)
[Rob McCool](#)
- [Computer core risks](#)

[Robert Schaefer](#)

- [4th International Conference on Network and System Security](#)
[NSS 2010](#)
 - [IEEE Symposium on Security and Privacy](#)
[Ulf Lindqvist](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ **Silly season: DST is approaching**

David Magda <dmagda@ee.ryerson.ca>

Mon, 1 Mar 2010 08:06:58 -0500

[This one was stuck in my queueueueue. But it's more appropriate tonight anyway, on the eve of U.S. DST. PGN]

Everyone gird your loins as it's March, so that means we're now entering "silly season": the bi-annual event of adjusting our time pieces by one hour. North America will be making the great leap forward on 14 Mar, while in Europe it's 28 Mar.

Anyone want to start a pool on how many time incidents will make the news this time around?

✂ **Sony PS3: Yet Another leap year folly**

Steve Summit

Mon, 01 Mar 2010 23:18:10 -0500

It's been widely reported that some models of Sony's PS3 game console malfunctioned today, evidently because they thought the date was 29 Feb. Hard to believe that in this 21st century, programmers are still having trouble with this algorithm...

http://news.cnet.com/8301-17938_105-10461881-1.html

[PGN notes Mark Brader commented on this one:

Well, maybe it's not the *same* programmers who had trouble with it in the 20th century...]

✂ **Sony thinks 2010 is a leap year**

Debora Weber-Wulff <weberwu@htw-berlin.de>

Sat, 06 Mar 2010 01:37:08 +0100

As noted on

<http://scitech.blogs.cnn.com/2010/03/01/playstation-network-down/> Sony's Playstation 3 was convinced that 2010 was a leap year and attempted to use Feb. 29, 2010. This kept gamers from connecting to the Playstation Network

[\(http://blog.us.playstation.com/2010/03/playstation-network-service-restored/\)](http://blog.us.playstation.com/2010/03/playstation-network-service-restored/)

It seems that the clock is a necessary part of the DRM scheme that Sony uses to make sure that people don't use bootleg copies of their games.

It rather incensed some users to be locked out of using their perfectly legal copies because the programmers had a little trouble dividing by 4.

Prof. Dr. Debora Weber-Wulff, Treskowallee 8, 10313 Berlin +49-30-5019-2320
weberwu@htw-berlin.de <http://www.f4.htw-berlin.de/people/weberwu/>

✂ Old models of PS3 failed to connect to network due to leap-year miscalculation

*"ishikawa,chiaki" <ishikawa@yk.rim.or.jp>
Wed, 03 Mar 2010 02:43:58 +0900*

Japan may have experienced the problem due to timezone differences earlier than others.

Sony Computer Entertainment announced on 2 Mar 2010 (and many users have complained on blogs and twitters) that old models of PS3 popular game console experienced failures such as failing to connect to network since its software miscalculated the year 2010 to be a leap year and its internal date was set to bogus 29 Feb on 1 Mar.

The model sold after September of 2009 didn't experience this bug.

As the date rolled to March 2nd (UCT), the problem disappeared.

Every now and then I noticed this leap-year miscalculation occur in OS and other basic software, but please note 2010 is not even a multiple of four. I wonder what faulty calculation was done in the software.

It could be a classic example that should be put in software engineering textbook if the faulty line is made public.

✂ Re: The Century Bug Will Repeat (Pollard, [RISKS-25.94](#))

*Jerry Leichter <leichter@lrw.com>
Sun, 14 Feb 2010 19:44:11 -0500*

Jonathan de Boyne Pollard discusses software that ignores even quite recent experience and continues to use techniques - like 2-digit years - that have quite recently caused us much grief and expense. He asks why we don't seem to learn from this experience.

I really hate to point this out but ... there are two reasons that, in other engineering and technological fields, we *do* manage to avoid repeating at least the reasonably common mistakes:

1. We develop standards and practices that have the force of law. Electrical circuitry in houses is subject to a variety of such standards. So is plumbing. You can't sell a house if it fails to meet code. In some cases, you'll be required to make modifications to come up to code even to remain in your own nose. If you're an electrician or a plumber and you do work that doesn't meet code, you'll lose your license and no longer be allowed to work in the field. You may be subject to criminal penalties. You can certainly be sued if someone is injured or property is damaged because you didn't follow the rules.
2. We require training and passing of exams *on those standards and practices*. We enforce this requirement by requiring licenses to work in many fields - and those licenses depend on passing the exams.

Now, I know all the downsides of this approach - the technology that's frozen in place for years, the use of licensing to limit competition, the pointlessness of much of what's on those exams. But the fact is that we have indoor plumbing that (usually) doesn't leak water on us, and that only very rarely causes disease even as it pumps gallons of pure stuff we eat and drink right near gallons of contaminated stuff. And we have electrical systems in our houses that don't (usually) start fires or electrocute us. We're so used to this latter feature that we've forgotten that this doesn't happen automatically. At least 12 US soldiers died in Iraq - not due to battles, but electrocuted due to incorrect wiring, like improperly grounded pumps that killed several soldiers in their showers.

We in the software industry have been leading charmed lives for many years. We've managed to avoid liability, avoid serious training in good practices, avoid any kind of standards - all by arguing that this would cramp our style and keep us from continuing to innovate. Maybe that's true - but we've been building up a massive debt side by side with all that innovation. Eventually, that debt's going to come due. If we don't clean up our own mess, the greater society will come along and do it for us - and the results won't be pleasant.

✂ Death in the Atlantic: The Last 4 Minutes of Air France Flight 447

*fjohn reinke <fjohn@reinke.cc>
Mon, 1 Mar 2010 09:15:30 -0500*

A lot of people are dead because they depended upon obsolete testing to keep them safe. While there is probably a lot of blame to go around, the failure of knowledgeable experts to make bureaucrats and bean-counters do the "right thing" seems to be obvious all throughout this story. I submit any risk reader will find this fascinating, educational, and, if you fly, scared! What else is hidden, overlooked, or just lazily ignored. There is a hint of corruption as well (i.e., failure to come down hard on a local business); the possibility of politics or payoffs can't be overlooked. Even if unprovable, suspicion is warranted. Argh!

In fact, the problem with the airspeed indicators lies far deeper. To this day, the relevant licensing bodies still only test pitot tubes down to temperatures of minus 40 degrees Celsius (minus 40 degrees Fahrenheit) and an altitude of about 9,000 meters (30,000 feet). These completely antiquated specifications date back to 1947 -- before the introduction of jet planes.

What's more, most of the incidents of recent years, including that involving the ill-fated flight AF 447, occurred at altitudes above 10,000 meters (33,000 feet). (SPIEGEL ONLINE - News - International)
<http://www.spiegel.de/international/world/0,1518,679980-2,00.html>

Blog "Reinke Faces Life", <http://krunchd.com/reinkefj>

✂ Software flaws may be at the root of Toyota's woes

*Gene Wirchenko <genew@ocis.net>
Thu, 04 Mar 2010 11:21:50 -0800*

While Toyota CEO President Akio Toyoda insists that neither electronics nor software can be blamed for the rash of runaway Toyotas, others aren't so sure. [Source: Joab Jackson, *IT Business*, 4 Mar 2010]
<http://www.itbusiness.ca/it/client/en/home/news.asp?id=56648>

Page 2 has discussion of an electronic control module (ECM) that supposedly has fail-safe, but "David Gilbert, a professor of automotive technology at Southern Illinois University Carbondale, found that the ETC is not foolproof, despite Toyota's claims. In tests, which he later described before last week's Congressional hearings, he found that the ETC did not detect certain types of short-circuit malfunctions that could occur with the pedal sensors. If the ETC did not detect the complete possible range of errors, then it could not enter into a fail-safe mode, he argued."

✂ Risk: Toyota secretive on 'black box' data (AP)

*Gabe Goldberg <gabe@gabegold.com>
Fri, 05 Mar 2010 17:06:18 -0500*

Toyota has for years blocked access to data stored in devices similar to airline "black boxes" that could explain crashes blamed on sudden unintended acceleration, according to an Associated Press review of lawsuits nationwide and interviews with auto crash experts. The AP investigation found that Toyota has been inconsistent -- and sometimes even contradictory -- in revealing exactly what the devices record and don't record, including critical data about whether the brake or accelerator pedals were depressed at the time of a crash.

By contrast, most other automakers routinely allow much more open access to information from their event data recorders, commonly known as EDRs.

AP also found that Toyota:

- * Has frequently refused to provide key information sought by crash victims and survivors.

- * Uses proprietary software in its EDRs. Until this week, there was only a single laptop in the U.S. containing the software needed to read the data following a crash.

- * In some lawsuits, when pressed to provide recorder information Toyota either settled or provided printouts with the key columns blank.

[Source: Curt Anderson and Danny Robbins, Associated Press Writers, 4 Mar 2010]

<http://finance.yahoo.com/news/AP-IMPACT-Toyota-secretive-on-apf-1294427692.html?x=0&sec=topStories&pos=1&asset=&ccode=>

Gabriel Goldberg, 3401 Silver Maple Place, Falls Church, VA 22042 703-204-0433

✶ Breakthrough in Electron Spin Control Brings Quantum Computers Closer to Reality

National Science Foundation Update <nsf-update@nsf.gov>

Fri, 26 Feb 2010 14:29:33 -0600 (CST)

[Noted by Bob Rosenberg in Dave Farber's IP distribution. PGN]

Illustration showing optical beam splitter method and new method of controlling electron spin. Research allows control of a single electron without disturbing other nearby electrons.

More:

http://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=116456&WT.mc_id=USNSF_1

✶ German Data Retention Law Overturned

Bob Gezelter <gezelter@rlgsc.com>

Wed, 03 Mar 2010 10:26:31 -0500

The New York Times (pp A6) 3 Mar 2010

"The country's highest court ruled Tuesday that a security law requiring the mass storage of telephone, e-mail, and Internet data violated a constitution provision on privacy and must be revised. The 2008 law required telecommunications carriers to retain customer usage data for six months so authorities could use it to track criminal networks."

The citation to the actual law was not given in the small article. Mass retention of data without specific cause is a challenge. The retained data can be used for its intended purpose, but its mere existence presents a hazard for inappropriate use.

I addressed similar issues in an item entitled "Will Long Term Dynamic Address Allocation Record Retention Help or Hurt?" in the context of the "Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act of 2009" (S.436) introduced by Senator John Cornyn (R-Texas).
<http://www.rlgsc.com/blog/ruminations/retain-dynamic-address-allocation-logs.html>

Bob Gezelter, <http://www.rlgsc.com>

✂ USGov rescinds 'leave Internet alone' policy

Richard Forno <rforno@infowarrior.org>

February 26, 2010 9:06:56 PM EST

[From Dave Farber's IP list. PGN]

US government rescinds 'leave Internet alone' policy

Kieren McCarthy, Networks, 27 Feb 2010>

http://www.theregister.co.uk/2010/02/27/internet_3_dot_0_policy/

The US government's policy of leaving the Internet alone is over, according to Obama's top official at the Department of Commerce. Instead, an Internet Policy 3.0 approach will see policy discussions between government agencies, foreign governments, and key Internet constituencies, according to Assistant Secretary Larry Strickling, with those discussions covering issues such as privacy, child protection, cybersecurity, copyright protection, and Internet governance.

The outcomes of such discussions will be *flexible* but may result in recommendations for legislation or regulation, Strickling said in a speech at the Media Institute in Washington this week.

(http://www.ntia.doc.gov/presentations/2010/MediaInstitute_02242010.html)

The new approach is a far cry from a US government that consciously decided not to intrude into the Internet's functioning and growth and in so doing allowed an academic network to turn into a global communications phenomenon.

Strickling referred to these roots arguing that it was "the right policy for the United States in the early stages of the Internet, and the right message to send to the rest of the world." But, he continued, "that was then and this is now. As we at NTIA approach a wide range of Internet policy issues, we take the view that we are now in the third generation of Internet policy making."

Outlining three decades of Internet evolution - from transition to commercialization, from the garage to Main Street, and now, starting in 2010, the Policy 3.0 approach - Strickling argued that with the Internet is now a social network as well a business network. We must take rules more seriously.

He cited a number of examples where this new approach was needed: end users worried about credit card transactions, content providers who want to

prevent their copyright, companies concerned about hacking, network neutrality, and foreign governments worried about Internet governance systems.

The decision to effectively end the policy that made the Internet what it is today is part of a wider global trend of governments looking to impose rules on use of the network by its citizens.

In the UK, the Digital Economy Bill currently making its way through Parliament has been the subject of significant controversy for advocating strict rules on copyright infringement and threatening to ban people from the Internet if they are found to do so. The bill includes a wide variety of other measures, including giving regulator Ofcom a wider remit, forcing ISPs to monitor their customers' behavior, and allowing the government to take over the dot-uk registry.

In New Zealand, a similar measure to the UK's cut-off provision has been proposed by revising the Copyright Act to allow a tribunal to fine those found guilty of infringing copyright online as well as suspend their Internet accounts for up to six months. And in Italy this week, three Google executives were sentenced to jail for allowing a video that was subsequently pulled down to be posted onto its YouTube video site.

Internationally, the Internet Governance Forum -- set up by under a United Nations banner to deal with global governance issues -- is due to end its experimental run this year and become an acknowledged institution. However, there are signs that governments are increasingly dominating the IGF, with civil society and the Internet community sidelined in the decision-making process.

In this broader context, the US government's newly stated policy more in line with the traditional *laissez-faire* Internet approach. Internet Policy 3.0 also offers a more global perspective than the isolationist approach taken by the previous Bush administration.

In explicitly stating that foreign governments will be a part of the upcoming discussions, Strickling recognizes the United States' unique position as the country that gives final approval for changes made to the Internet's Croot zone. Currently the global Internet is dependent on an address book whose contents are changed through a contract that the US government has granted to the Internet Corporation for Assigned Names and Number (ICANN), based in Los Angeles. [long item truncated for RISKS, with considerable subsequent discussion in IP. PGN]

[Dan Lynch added: It was good while it lasted. The cat is out of the bag and now all the watchdogs of our morals are descending for good reasons. We have foisted communications anarchy on the world quite successfully. Let's see how they route around their paranoia.]

IP Archives: <https://www.listbox.com/member/archive/247/>

Man posts "wanted" poster of himself on own Facebook page

Mark Brader

Fri, 5 Mar 2010 03:17:01 -0500 (EST)

Chris Crego, of Lockport, New York, pleaded guilty to assault but fled the state before sentencing. However, he then put up Facebook and MySpace pages under his real name, showing his photo, his place and hours of employment, and -- in case there was any doubt -- the police "wanted" poster of him. He was arrested and returned to Lockport, and police posted a "thank you" notice on his page.

<http://www.cbsnews.com/blogs/2010/02/08/crimesider/entry6186573.shtml>

<http://www.buffalonews.com/2010/03/02/974619/crego-back-in-lockport-held-on.html>

Car insurance bug

"Clive D.W. Feather" <clive@davros.org>

Sat, 6 Mar 2010 09:33:46 +0000

I bought a new car a couple of weeks ago, though for obvious reasons [1] I didn't collect it until Monday.

As soon as I knew the new registration number, I contacted my insurance company to alter the details. The paperwork finally arrived yesterday. At one point it reads:

It has been owned by, and registered to you or your partner,
for approximately - 1 year(s) 11 month(s).

This puzzled me, so I phoned them, to be told "it always does that for new cars". Then I realized what had happened; the clue was that the previous paperwork did **not** have the dash in this text.

The computer must have done something like "now = Feb 2010, bought Mar 2010, therefore owned for -1 months". Then it converted months to years by dividing by 12 and determining the remainder. There are two sensible answers for "-1 div/rem 12" (0 remainder -1 and -1 remainder 11) and which gets used depends on what properties you want to preserve. Or, in this case, because nobody had thought about negative inputs!

The only remaining problem: how on earth do I get this information past the call centre and to the people who actually maintain this code? Perhaps they read RISKS.

[1] Well, obvious to UK readers - it gives the car a "10" registration rather than a "59" one, affecting the resale value.

Clive D.W. Feather <clive@davros.org> <http://www.davros.org> +44 7973 377646

#Daily cyber attacks on the UK

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

Sun, 07 Mar 2010 09:39:41 +0000

Foreign states and terrorist groups are regularly launching cyber-attacks on the UK's computer systems with the potential to cause widespread damage, according to the government's security tsar. Lord West of Spithead, who is parliamentary under-secretary for security and counter-terrorism, told the *Observer* that the UK was under daily cyber attack, often from agencies working on behalf of foreign governments. He said there had been "300 significant attacks" on the government's core computer networks in the last year and warned of chaotic scenes if one successfully targeted infrastructure such as the UK's communications systems...

<http://www.guardian.co.uk/technology/2010/mar/07/britain-fends-off-cyber-attacks>

#"Traffic analysis" from data

"David Magda" <dmagda@ee.ryerson.ca>

Fri, 12 Mar 2010 09:09:50 -0500 (EST)

A little while ago the Ontario Privacy Commissioner released a report on the privacy implication of electrical smart grids ([RISKS-25.84](#): "Your smart meter is watching"). Well, it turns out water pressure is another way that "traffic analysis" can be done on people's activities:

> The water utility in Edmonton, EPCOR, published the most incredible graph
> of water consumption last week. By now you've probably heard that up to
> 80% of Canadians were watching last Sunday's gold medal Olympic hockey
> game. So I guess it stands to reason that they'd all go pee between
> periods.

<http://tinyurl.com/yedz5jt>

http://www.patspapers.com/blog/item/what_if_everybody_flushed_at_once_Edmonton_water_gold_medal_hockey_game/

Via: <http://www.boingboing.net/2010/03/11/the-effects-of-gold-.html>

Not so much a technological RISK, but more of a reminder that as chips and sensors are placed in more places, we get more data. The more data we have, the more it can be linked with other data, and that can lead to unforeseen consequences.

#Paranoia 101

Paul Wexelblat <wex@cs.uml.edu>

Mon, 1 Mar 2010 09:07:23 -0500

Are they tracking us (a/k/a Paranoia 101) - Or,

What I'd do if I was "one of 'them'".

OK, Let's do an update

1. How many "Smart Cards" are you carrying?
 2. How about your "New, Improved" Passport?
 3. EZ Pass (or equivalent)?
 4. How about those Tire Pressure things in your tires (4 and the spare!)- they're RFID's
 5. Y'know, that "keyless entry" thingie in your pocket/key - RFID, again.
 6. Oh, that ON-Star like thing in your car, can you turn it off? (Are you sure?)
 7. About that cellphone,
You want Paranoia -
 8. Um, about the remote diagnostic capability of my Mom's pacemaker
 9. The implanted ID chip in your pet
 10. Do those "security" bags really protect RFID's from concerted reading devices?
 11. "They" could easily record the serial numbers of the cash you get from the ATM
 12. While they're doing facial recognition of everyone within range of the camera.
- How many of these things can be read from how far away? [Quite a few. PGN]

✂ Risks of having friends with computers

Rob McCool <robm@robm.com>

Fri, 12 Mar 2010 12:21:59 -0800 (PST)

http://www.mpi-sws.org/~gummadi/papers/inferring_profiles.pdf

This paper discusses an interesting phenomenon for privacy. If a user has turned on privacy in either LinkedIn or Facebook such that their friends list is accessible but nothing else, the researchers were able to infer with 80% accuracy the values of the hidden attributes based solely upon 20% of those friends revealing their own value for those attributes. The article states that 95% of Facebook users expose their friends list to strangers, which means that for most people their privacy may be effectively compromised by a relatively small percentage of their friends.

To me, this is a difficult tradeoff for Facebook users. Hiding your friends list means that people you know but with whom you have not connected will have difficulty deciding if that's really you, or another John Smith. The "N mutual friends" link is an incredibly useful one for finding people you might want to reconnect with.

✂ Computer core risks

Robert Schaefer <rps@haystack.mit.edu>

Wed, 10 Mar 2010 14:47:06 -0500

This came through via slashdot:

http://www.gearlog.com/2010/03/hands_on_fake_intel_core_i7-92_1.php

Apparently the computer core you thought you were purchasing is now the risk.

Robert Schaefer, Atmospheric Sciences Group, MIT Haystack Observatory
Westford MA 01886 781-981-5767 <http://www.haystack.mit.edu> rps@haystack.mit.edu

4th International Conference on Network and System Security

"NSS 2010" <ieee.nss@gmail.com>

Wed, 3 Mar 2010 23:29:33 +1000

4th International Conference on Network and System Security (NSS 2010)

September 1-3, 2010, Melbourne, Australia

<http://www.anss.org.au/nss2010>

In technical co-sponsorship with the IEEE and the IEEE Computer Society

Technical Committee on Scalable Computing

Workshop proposal due: March 31, 2010

Paper submission due: March 31, 2010

IEEE Symposium on Security and Privacy

Ulf Lindqvist <ulf.lindqvist@sri.com>

Thu, 11 Mar 2010 08:41:27 -0800

IEEE Symposium on Security and Privacy, May 16-19, 2010

The Claremont Resort, Oakland, California, USA

Sponsored by the IEEE Computer Society Technical Committee on Security and Privacy, in cooperation with the International Association for Cryptologic Research (IACR)

It is my pleasure to announce the 2010 IEEE Symposium on Security and Privacy, to be held at the Claremont Resort 30 years after the very first symposium in this series. Please visit <http://oakland31.cs.virginia.edu/> for information about the symposium and the co-located workshops. [The SSP 2010 program is also in [RISKS-25.95](#). PGN]

Important Highlights:

* Register <<http://www.regonline.com/Checkin.asp?EventId=810837>> before April 18 to take advantage of the early registration rates

* Reserve your hotel room <<http://oakland31.cs.virginia.edu/travel.html>> early, especially if you require and qualify for the government rate

* The 30th anniversary of Security and Privacy welcomes all in the

security research community to a light-hearted *awards dinner* on May 17. Registered symposium attendees and registered guests are welcome at this retrospective event with Master of Ceremonies Peter G. Neumann. The ceremonies will include the presentation of the National Computer Systems Security Award for 2010 by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

* The advance program

<<http://oakland31.cs.virginia.edu/program.html>> is available

* Student travel grants

<<http://oakland31.cs.virginia.edu/grants.html>> are available, and applications are due by April 2

* The Call for Posters

<<http://oakland31.cs.virginia.edu/posters.html>> is now open, and poster abstracts are due by April 8

* Three co-located workshops

<<http://oakland31.cs.virginia.edu/workshops.html>> will be held in conjunction with the symposium on May 20:

- o Systematic Approaches to Digital Forensic Engineering (SADFE)
- o Web 2.0 Security and Privacy (W2SP)
- o Workshop on Security and Privacy in Social Networks

I hope to see you at the symposium on May 16-19!

Ulf Lindqvist, General Chair



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 97

Friday 26 March 2010

Contents

- [Unmanned goods train crash in Norway](#)
[Martyn Thomas](#)
- [NRC to VA: you endangered patients, you owe us \\$227k](#)
[Danny Burstein](#)
- [FBI Faces New Setback in Computer Overhaul](#)
[Eric Lichtblau](#) via [David Lesher](#)
- [IRS systems can't be trusted](#)
[Randall Webmail](#)
- [Risks to the power grid](#)
[Gary McGraw](#)
- [Pwn2Own 2010: iPhone hacked, SMS database hijacked](#)
[Ryab Naraine](#) via [Monty Solomon](#)
- [Warnings about Wifi-enabled air travel](#)
[David Strom](#) via [Gabe Gold](#)
- [Cops inadvertently harass couple: real address used as test data](#)
[Mark Brader](#)
- [Police raid wrong address 50+ times](#)
[David Lesher](#)
- [UK SAS base "exposed" through Google Streetview](#)
[Peter Baker](#)
- [Netflix Data Deanonymized](#)
[Bob Gezelter](#)
- [Hacked "miss a payment, brick your car" system](#)
[Jeremy Epstein](#)
- [Colombian vote count delayed](#)
[PGN](#)
- [Surveillance via bogus SSL certificates](#)
[Matt Blaze](#)
- [More on School Webcam Scandal](#)
[Gene Wirchenko](#)
- [Couldn't logout from Facebook Mobile](#)
[jidanni](#)
- [Re: Old models of PS3 failed to connect to network](#)
[DoN Nichols](#)
- [Info on RISKS \(comp.risks\)](#)

✂ Unmanned goods train crash in Norway

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

Wed, 24 Mar 2010 15:15:27 +0000

Several railway cars in a 16-car train broke loose, sped at 100km/h, derailed, smashed into a building, killed three people, injured three others, and wound up in a fjord.

<http://news.bbc.co.uk/1/hi/world/europe/8585315.stm>

✂ NRC to VA: you endangered patients, you owe us \$227k

danny burstein <dannyb@panix.com>

Thu, 18 Mar 2010 11:55:34 -0400 (EDT)

The Nuclear Regulatory Commission has proposed a \$227,500 fine against the Department of Veterans Affairs (DVA) for violations of NRC regulations associated with an unprecedented number of medical errors identified at the Veterans Affairs Medical Center in Philadelphia (VA Philadelphia). Medical errors at VA Philadelphia involved the incorrect placement of iodine-125 seeds to treat prostate cancer. Out of 116 procedures performed between 2002 and 2008, 97 were executed incorrectly. ... [NRC press release]

<http://www.nrc.gov/reading-rm/doc-collections/news/2010/10-005.iii.html>

[I'm not entirely comfortable with their use of the term "executed" in this context...]

✂ FBI Faces New Setback in Computer Overhaul (Eric Lichtblau)

David Leshner <wb8foz@panix.com>

Fri, 19 Mar 2010 09:20:50 -0400

[Source: Eric Lichtblau, *The New York Times*, 18 Mar 2010]

<http://www.nytimes.com/2010/03/19/us/19fbi.html?hp=&pagewanted=print>

The Federal Bureau of Investigation has suspended work on parts of its huge computer overhaul, dealing the agency the latest costly setback in a decade-long effort to develop a modernized information system to combat crime and terrorism. The overhaul was supposed to be completed this fall, but now will not be done until next year at the earliest. The delay could mean at least \$30 million in cost overruns on a project considered vital to national security, Congressional officials said. FBI officials said that design changes and "minor" technical problems prompted the suspension of parts of the third and fourth phases of the work, which is intended to allow agents to better navigate investigative files, search databases and

communicate with one another. The decision to suspend work on the \$305 million program is particularly striking because the current contractor, Lockheed Martin, was announced to great fanfare in 2006 after the collapse of an earlier incarnation of the project with the Science Applications International Corporation.

So after both classified and unclassified reviews, Congressional scrutiny, and "we'll do better next time" promises...

Esther Dyson: "Always make new mistakes."

✂ IRS systems can't be trusted

Randall Webmail <rvh40@insightbb.com>

March 23, 2010 5:41:53 PM EDT

According to a new Government Accountability Office report, the Internal Revenue Service has failed to fix almost 70 percent of control weaknesses and program deficiencies identified a year ago. The report concludes that the IRS's failure to use strong passwords, install patches quickly, and adequately control access to computer systems and information makes the system vulnerable to insider threats and attacks from outside.

http://news.cnet.com/8301-27080_3-20000987-245.html?part=rss&subj=news&tag=2547-1_3-0-20

<http://tinyurl.com/yapnjb2>

✂ Risks to the power grid

Gary McGraw <gem@cigital.com>

Fri, 26 Mar 2010 08:18:56 -0400

We have known for years that the power grid system is a fragile engineering kludge. Adopting Internet technology to bring it kicking and screaming into this Millennium may not help. Some of the RISKS described in

A keynote talk I gave for the NRECA (video)

<http://www.cigital.com/justiceleague/2010/03/22/smart-grid-equals-dumb-security/>

My colleague Sammy's talk

<http://www.cigital.com/justiceleague/2010/03/24/at-the-nreca-conference/>

An informIT article I just wrote about the subject:

The Smart (Electric) Grid and Dumb Cybersecurity

<http://www.informit.com/articles/article.aspx?p=1577441>

<http://www.cigital.com/~gem>

✂ Pwn2Own 2010: iPhone hacked, SMS database hijacked (Ryan Naraine)

Monty Solomon <monty@roscom.com>

Thu, 25 Mar 2010 23:25:39 -0400

A pair of European researchers used the spotlight of the CanSecWest Pwn2Own hacking contest [in about two weeks] to break into a fully patched iPhone and hijack the entire SMS database, including text messages that had already been deleted. Using an exploit against a previously unknown vulnerability, the duo -- Vincenzo Iozzo (Zynamics) and Ralf Philipp Weinmann (University of Luxembourg) -- lured the target iPhone to a rigged Web site and exfiltrated the SMS database in about 20 seconds. The exploit crashed the iPhone's browser session, but Weinmann said that, with some additional effort, he could have a successful attack with the browser running.

"Basically, every page that the user visits on our [rigged] site will grab the SMS database and upload it to a server we control," Weinmann explained. Iozzo, who had flight problems, was not on hand to enjoy the glory of being the first to hijack an iPhone at the Pwn2Own challenge.

[Source: Ryan Naraine, zdnet, datelined Vancouver BC, 24 Mar 2010; PGN-ed]

<http://blogs.zdnet.com/security/?p=5836>

✂ Warnings about Wifi-enabled air travel

<gabe@gabegold.com>

Mon, 15 Mar 2010 12:40:07 -0400

-- ----- Original Message -----

Date: Mon, 15 Mar 2010 08:06:49 -0500

From: David Strom <david@strom.com>

To: webinformant@list.webinformant.tv

Web Informant 15 March 2010: Warnings about Wifi-enabled air travel

I have been on a few planes in the past couple of weeks that are Wifi-enabled. American has created an entirely new opportunity for identity thieves here, and while the opportunity to surf and e-mail at 30,000 feet is tempting, count me out for those that will become frequent users.

The problem is that most people get lost in the wonderfulness of the Web and tend to forget that their seatmates can watch every move, see every keystroke (it doesn't take much to follow along, especially at the speed that many people type), and collect all sorts of information. By the end of one flight I was on, I had Larry (not his real name) the HP sales rep's Amazon account, read several of his e-mails, got to see his new sales presentations that HP corporate sales office had sent him, figured out that he was a recent hire as he was checking HP's Intranet to understand some corporate travel policies, found out who his clients that he had just visited were, and more.

Now, I wasn't really paying that much attention. I was tired, and just

wanted to be left by myself for the trip. And I think we exchanged maybe ten words between us all told. But if I really wanted to do some damage, I could be all over Larry's accounts by now (he had some nice taste from what I could see he was looking for on Amazon, too).

Yes, people have been using laptops on planes for years. I used to do it all the time, back when the middle seat was rarely occupied and you didn't have to almost disrobe to get to the gate. But those days are almost as much part of history as calling the people that worked on planes stewards. The difference is now that we have Internet piped directly to the seat, people are free to go anywhere and everywhere, and where they go are places that are critical to their life. I wouldn't be surprised if someone was doing their online banking in-flight.

So people (and HP, you might want to consider this a corporate-wide purchase) if you are going online up in the air, get a privacy filter for your laptop so that no one else can see your screen. They cost about \$30. This isn't complex technology: it has been available almost as long as Windows has been around. And while you are at it, dim your screens to save on power anyway (Larry had one of those nifty power-packs to boost his battery, too). Or better yet: don't work on anything important on a crowded plane -- and these days, what other kinds of planes are there? Bring a book or watch a movie if you must be immersed in your electronic cocoon.

I am reminded of a story from my early days as a reporter for PC Week, back in the late 1980s. We were very scoop-oriented, and would always try to get information from the vendors through all sorts of means, some of them probably unethical or at least uncomfortable in the light of the present day. One of our reporters was having dinner with her boyfriend (now husband) at a quaint and cozy Cambridge Mass. restaurant, and overhead two businessmen at the next table gossiping about work. What was unusual was they were speaking rapid German, and both were working for Lotus Development, at the time a powerhouse spreadsheet player. They were in town to discuss the company's future product plans. Trouble was, my colleague spoke German fluently, and got a couple of scoops that were published the next week in the paper. No one knew who the source of the leak was.

Remember loose lips sink ships, the World War 2 posters put up by the government? We need something similar on Wifi-enabled planes. Be careful out there people. You never know whom you are sitting next to.

Cops inadvertently harass couple: real address used as test data

Mark Brader

Sun, 21 Mar 2010 01:42:00 -0400 (EDT)

http://www.theregister.co.uk/2010/03/19/police_raid_glitch/

Note especially the last paragraph in this one.

In 2002 the New York Police Department was testing a new computer system and put in "random material" as test data. This included the real address of

Walter and Rose Martin -- which inadvertently ended up in the system as live data. The result was that the Martins' address appeared in police computers as the address of a variety of crime suspects and victims; so police were repeatedly banging on the door demanding the suspects appear, as well as sending them mail.

In 2007 the Martins finally complained to the police commissioner, but the problems remained unresolved. By now the Martins are 82 and 83 years old, police have come to their house 50 times, and the story has reached the news media. Both the mayor, Michael Bloomberg, and the police commissioner, Ray Kelly, have apologized to the couple, and the problem is now supposed to have been fixed.

<http://news.bbc.co.uk/2/hi/americas/8577579.stm>

[http://www.nydailynews.com/news/2010/03/18/2010-03-](http://www.nydailynews.com/news/2010/03/18/2010-03-18_six_examples_of_cops_mistakenly_visiting_elderly_brooklyn_couples_home.html)

[18_six_examples_of_cops_mistakenly_visiting_elderly_brooklyn_couples_home.html](http://www.nydailynews.com/news/2010/03/18/2010-03-18_six_examples_of_cops_mistakenly_visiting_elderly_brooklyn_couples_home.html)

[http://www.nydailynews.com/news/ny_crime/2010/03/19/2010-03-](http://www.nydailynews.com/news/ny_crime/2010/03/19/2010-03-19_bloomberg_apologizes_to_couple_mistakenly_raided_by_nypd_over_50_times.html)

[19_bloomberg_apologizes_to_couple_mistakenly_raided_by_nypd_over_50_times.html](http://www.nydailynews.com/news/ny_crime/2010/03/19/2010-03-19_bloomberg_apologizes_to_couple_mistakenly_raided_by_nypd_over_50_times.html)

<http://www.washingtonpost.com/wp-dyn/content/article/2010/03/19/AR2010031900906.html>

Police raid wrong address 50+ times

"David Leshner" <wb8foz@panix.com>

Fri, 19 Mar 2010 08:58:49 -0400 (EDT)

[Also noted here:]

http://www.nypost.com/p/news/local/brooklyn/computer_glitch_blamed_home_years_mHUCrXCM&vhEyVGJolFIPK

Maybe they need a special doorbell "For police raids..."

Once again, the lack of sanity checks at multiple levels rears its head.

a) Did each raid have a valid warrant? If so, who obtained the warrants?
Who signed the affidavits? What judge approved them? [Is this process just rubber-stamps?]

b) After fifty raids, the NYPD has not yet figured out it is worth a moment's thought before kicking their way in?

[Harald Hanche-Olsen added: New York's police chief has delivered a cheesecake to an elderly couple in Brooklyn, to apologise for dozens of mistaken police visits to their home. PGN]

<http://news.bbc.co.uk/2/hi/americas/8577579.stm>

UK SAS base "exposed" through Google Streetview

Peter Baker <peter.baker@safe-mail.net>

Sat, 20 Mar 2010 14:18:33 +0100

A UK newspaper reports "fury" as Google Streetview was found to display detailed pictures of the SAS headquarters

<<http://www.dailymail.co.uk/news/article-1259162/Google-Street-View-shows-secret-SAS-base-major-security-breach.html>>.

I would personally wonder about perimeter security if a vehicle that is very obviously taking pictures can drive past without a discussion with either the driver in question or the organisation behind it. However, it made me curious if that other "off the map" place was featured, and yes, ECHELON is available in Streetview too <<http://bit.ly/GoogleEchelon>> (well, for the moment). The RISK is obvious: if you don't want your perimeter in the news, patrol it. If you want to remove such pictures, have a *quiet* word or expect the Streisand effect to strike with a vengeance.

It wasn't Google Streetview exposing the base, it was the resulting publicity. Duh..

✂ Netflix Data De-anonymized

Bob Gezelter <gezelter@rlgsc.com>

Sun, 14 Mar 2010 11:30:50 -0500

The movies you rent may tell a lot about you, perhaps more than you may want. This collation hazard, collating anonymized data with other data to de-anonymize the data has serious implications. This hazard was noted in RISKS many years ago, with regards to pharmacy data (which was not protected) and medical files (which were protected) [to Editor: I do not have the reference at hand, it may be pre-online RISKS, perhaps you recall when?]

In The New York Times Bits blog, Steve Lohr published an article noting the latest round of the Netflix competition has been canceled. [see <http://bits.blogs.nytimes.com/2010/03/12/netflix-cancels-contest-plans-and-settles-suit/>]

Apparently, researchers at the University of Texas were able to unmask the data. [see http://arxiv.org/PS_cache/cs/pdf/0610/0610105v2.pdf].

This is only the latest in a series of episodes involving "collation", a hazard that was included in "Security on the Internet" (Chapter 23, Computer Security Handbook (1995), section 23.4, pp 23-6) and its 2002 sequel (outline available at <http://www.computersecurityhandbook.com/csh4/chapter22.html>).

The mass adoption of micro-blogging and applications that reveal ones physical location only make this hazard more severe. I daresay this will not be the last we see of anonymized data becoming uncloaked through collation.

- Bob Gezelter, <http://www.rlgsc.com>

✂ Hacked "miss a payment, brick your car" system

Jeremy Epstein <jeremy.j.epstein@gmail.com>

Wed, 17 Mar 2010 19:16:24 -0400

A vendor offers a black box system that will remotely disable a car's ignition or start the horn honking, to allow easy recovery if the owner doesn't make the car payments. A laid-off auto dealership worker took advantage of the system and got his revenge for being laid off by logging into the system using a (former) co-worker's credentials, and going through one-by-one and disabling all of the cars sold by his former employer equipped with the device. The vendor of the remote control device says this is the first time it's ever happened. (I'd guess it's not the last!)

The Risk? Any time you have a remote control device, you've opened a new attack surface. While this attack was essentially an insider (since the person knew a co-worker's password), what's the odds that someone can guess passwords, or find them posted on monitors in the car dealership, or find a vulnerability in the web application, or There are also potential attacks going directly against the devices, completely bypassing the web-based control system.

I'd bet that the dealerships were assured the system is completely secure, because it uses SSL.

<http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/>

[Also noted by Steven J Klein, and Steve Summit, who commented: The Risks?

The usual: An unsuspected, perhaps too-powerful system, which although it had some safeguards, perhaps didn't have enough... David Leshner noted a UPI item, and remarked: Gee, shades of the Greek Wiretapping Saga, and multiple other cases. When you build Big Brother in, you can expect misuse. PGN]

✂ Colombian vote count delayed

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

Wed, 17 Mar 2010 18:02:02 PDT

Unidentified attackers reportedly struck the computerized system used to transmit voting data in Colombia's legislative elections, disrupting the vote count just as the polls closed and continuing. Three days after the polls, final results still had not been released. (AFP, 17 Mar 2010)

<http://www.google.com/hostednews/afp/article/ALeqM5iqkRi-yQWVJ6Dp3CcsKr8k9AQEw>

✂ Surveillance via bogus SSL certificates

Matt Blaze <mab@crypto.com>

March 24, 2010 3:09:19 PM EDT

[From Dave Farber's IP list]

Over a decade ago, I observed that commercial certificate authorities protect you from anyone from whom they are unwilling to take money. That turns out to be wrong; they don't even do that.

Chris Soghoian and Sid Stamm published a paper today that describes a simple "appliance"-type box, marketed to law enforcement and intelligence agencies in the US and elsewhere, that uses bogus certificates issued by *any* cooperative certificate authority to act as a "man-in-the-middle" for encrypted web traffic.

Their paper is available at <http://files.cloudprivacy.net/ssl-mitm.pdf>

What I found most interesting (and surprising) is that this sort of surveillance is widespread enough to support fairly mature, turnkey commercial products. It carries some significant disadvantages for law enforcement -- most particularly it can be potentially can be detected.

I briefly discuss the implications of this kind of surveillance at <http://www.crypto.com/blog/spycerts/>

Also, Wired has a story here: <http://www.wired.com/threatlevel/2010/03/packet-forensics/>

[IP Archives: <https://www.listbox.com/member/archive/247/=now>

✂ More on School Webcam Scandal

*Gene Wirchenko <genew@ocis.net>
Mon, 22 Mar 2010 13:44:51 -0700*

http://www.infoworld.com/d/adventures-in-it/high-school-web-cam-follies-part-ii-dumb-and-dumber-371?source=IFWNLE_nlt_notes_2010-03-22

InfoWorld Home / Adventures in IT / Notes from the Field / Robert X. Cringely

March 22, 2010

High school Webcam follies, part II: Dumb and dumber

The Lower Merion School District's 'Webcamgate' scandal continues.

Cringely updates us on the latest twists and turns

Though it's not getting quite the 24/7 cable news treatment as it garnered when it first hit the wires, the Webcam scandal in Southeastern Pennsylvania (aka "Webcamgate") is still twisting and turning in unpredictable ways. We still don't know exactly what happened, but we do know there are lessons here for everyone concerned about IT security and personal privacy.

✂ Couldn't logout from Facebook Mobile

<jidanni@jidanni.org>

Mon, 22 Mar 2010 05:48:56 +0800

There I was at a certain university library who had blocked access to facebook.com. However I found I could still get through to Facebook Moblie: m.facebook.com. All was hunky-dory until I tried to logout, a link which surprise, surprise, depends on accessing the main facebook.com site! So I was forced to rid the cookies and close the browser.

Old models of PS3 failed to connect to network due to

"DoN. Nichols" <dnichols@d-and-d.com>

Fri, 19 Mar 2010 21:12:00 -0500

leap-year miscalculation (Ishikawa, [RISKS-25.96](#))

I think that the problem was more a miscalculation of the year, as apparently occurred in some cell-phones and was reported here at the beginning of the year.

I encountered it in my watch -- a Citizen "Eco" solar-powered watch which updates itself nightly from whatever time station is most reachable. (For the USA, it is WWVB.) There is one station in Europe, and two in Japan which it also knows about.

Anyway -- I first became aware of the problem after the rollover from February 2010 to March 2010. It started displaying the day of the month one lower than it should have been.

On going into the setting mode to correct this, I discovered that it thought that the year was 2016. Apparently, this had been since the beginning of 2010, but since the year is only displayed in setting mode, it was not obvious until the rollover. Since 2010 is not a leap year, but 2016 **is**, it started calculating the day of the month incorrectly -- presumably from an internal count of days since the start of the year.

I fixed the date, and it recurred after the nighttime contact with WWVB -- every night, so I just turned off the automatic updates while tracing down the proper way to get it fixed.

The problem seems to be in the conversion of the BCD coded information from WWVB to the binary data within the watch. What it was doing was converting the bottom four bits to a decimal digit and setting that, then taking the next four bits and adding it shifted up by four bits -- thus adding a value of 16 to the total, instead of multiplying the next to LSD by ten and adding it to the binary value.

Since the upper two digits of the year are correct, I presume that it is simply using the two lowest digits and adding to 2000 internally. So -- I wonder what happens when we reach 2100? Not likely to be a problem for me, unless there are some miraculous advances in longevity medicine. :-) And I

have doubts that the battery will last that long, even with proper sun exposure to keep it charged. And I also doubt that the battery will remain in production that long. So it will probably become non-functional long before the 2100 date arrives.

To their credit -- once I got in touch with the right part of the Citizen repair organization (no simple task, given the layout of their web page) they instantly recognized the problem, told *me* the model of the watch, and started processing to get me a free shipping via UPS to their site. (I have about three years of the five year warranty left, but they did not even ask about that.)

They have just received the watch, and I am now awaiting its return in an updated state.

Subsequent e-mail with them determined that they had discovered the problem and sent information to the dealers to send the watches back for a firmware update (which they are calling a software update). Some did, and some did not.

I purchased mine about the time that they discovered the problem and issued the notice, so I don't know whether it should have been sent back at the time I got it or not.

The dealer was totally puzzled by the problem, and their own contact with the repair organization suggested that it was a problem of the battery dying (and the indicator showed a perfectly good charge on it). So -- they have a similarly difficult information channel. All watches made after the early part of 2008 were shipped with the firmware fixed. (I tested one at the store to make sure of this before I was told that they were fixed by the repair facility.)

<http://www.d-and-d.com/dnichols/DoN.html> Voice: (703) 938-4564



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 25: Issue 98

Thursday 1 April 2010

Contents

- [The 2010 Census as of April 1](#)
[Rebecca Mercuri](#)
- [Silver Iodide Can Seed Cloud Computing](#)
[PGN](#)
- [Clouding Men's Minds](#)
[Cecelia Kang via PGN](#)
- [CalJOBS Security is a Mess](#)
[Tony Lima](#)
- [Why Won't USPS Let Me File This Complaint?](#)
[Jim Reisert](#)
- [Incorrect software change to emergency ambulance call-handling system may have resulted in hundreds of deaths](#)
[Bruce Horrocks](#)
- [Ohioans are dunned for long-paid fines \(](#)
[Peter Zilahy Ingerman](#)
- [User-friendly speed cameras in Belgium](#)
[Peter Houppermans](#)
- [Academic Paper in China Sets Off Alarms in U.S.](#)
[Markoff/Barboza](#)
- [Water-treatment computer: No, not the Three Stooges, but close](#)
[Jeremy Epstein](#)
- [3.3 million student-loan records pilfered](#)
[Gene Wirchenko](#)
- [Old-fashioned computer risks, Re: 3.3 million student-loan data](#)
[Jeremy Epstein](#)
- [High-tech copy machines a gold mine for data thieves](#)
[David Hollman](#)
- [Survey: Millions of users open spam e-mails, click on links](#)
[Dancho Danchev via Monty Solomon](#)
- [Plain Dealer sparks ethical debate by unmasking anonymous poster](#)
[Ferdinand Reinke](#)
- [In Bid to Sway Sales, Cameras Track Shoppers](#)
[Stephanie Rosenbloom via Monty Solomon](#)
- [TJX Hacker Sentenced](#)
[Gene Wirchenko](#)
- [USENIX Health Security and Privacy Workshop due 9 Apr 2010](#)

[Kevin Fu](#)

• [GameSec 2010: Conference on Decision and Game Theory for Security](#)

[Albert Levi](#)

• [Info on RISKS \(comp.risks\)](#)

✂ The 2010 Census as of April 1

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

Thu, 1 Apr 2010 00:31:56 -0500

[Rebecca suggested this in response to Thomas Friedman's article supporting IRV in *The New York Times*, 24 Mar 2010. PGN]

<http://www.nytimes.com/2010/03/24/opinion/24friedman.html>

I was recently reading the FairVote (an Instant Runoff Voting advocacy group) newsletter where the Census is mentioned, and OF COURSE, one should note (though the author didn't) that it is STILL done on PAPER, not on the Internet. I sure hope that continues.

Anyway, it caused me to try to think of an IRV analogy to the Census -- perhaps filers would instead list the number of people they'd LIKE to have living in their homes on April 1, rather than the actual number of people that ARE living there. So people who are getting divorced would say 1, and people who are on the verge of giving birth would say 2 (or 9 if they are an octomom), and people who are about to die would say 0, and so on. It would be really interesting trying to figure out how to count that up accurately. And of course, since the computers would be doing advanced fuzzy math to determine the population for the subsequent gerrymandering, the software algorithms would be far too complex for anyone to ever check (also because they'd be written by some contractor who would decide that the code is a proprietary trade secret). After the results come out, we'd miraculously discover that Omaha Nebraska (gee, I wonder why it's *that* particular city) would be entitled to 25 members of Congress.

Hmmm....maybe that *is* what's going on (or if not, I'm sure some folks with deep pockets of cash would love to make it happen).

Rebecca Mercuri

✂ Silver Iodide Can Seed Cloud Computing

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

Thu, 1 Apr 2010 01:23:45 GMT

At a rump session at the annual meeting of the American Chemical Society in San Francisco last week, A. Poulter Geist, a physical chemist with a remarkably strong background in both mathematics and computer science, claimed that silver iodide (which has been used for many years to seed potential rain clouds, albeit with considerable dispute as to its actual effectiveness) could also be used to seed random-number generators used in

cryptographic key generation and hash coding, to provide better security in cloud computing and cloud data-storage. Perhaps somewhat simplistically, he also suggested that the literal string "silver iodide" might even be used as a public key in identity-based and attribute-based encryption, greatly simplifying key management. However, he rather explicitly ceded responsibility for the clouds in cloud computing itself.

[Poulter may be a distant relative of Tom "Doc" Poulter, director of the eponymous lab at SRI that still exists today. On the other hand, I note that a "poltergeist" is known for unexplained rappings, and cloud computing is likely to need wrappers in the sky -- which thus far have been easily compromised. PGN]

✂ Clouding Men's Minds (Cecelia Kang)

"Peter G. Neumann" <neumann@csl.sri.com>
Sat, 27 Mar 2010 14:00:06 PDT

Behind Facebook, Gmail, and the Bing search engine is a multibillion-dollar shift in technology that users don't see and Washington doesn't quite know how to handle: cloud computing, the hosting of data on remote servers that can be tapped from any computer connected to the Web. ... [Source: Cecelia Kang, Washington debates Cloud Computing, *The Washington Post*, 26 Mar 2010; PGN-ed. For you old-timers, the subject line refers to The Shadow.]

<http://voices.washingtonpost.com/posttech/2010/03/what.html>
<http://bit.ly/av3CRy>

✂ CalJOBS Security is a Mess

Tony Lima <tony@tonylimaassociates.com>
Tue, 30 Mar 2010 15:12:41 -0700

There are major problems with the CalJOBS website, specifically the security system. Quite a bit of this will sound all too familiar to RISKS readers.

The Employment Development Department (EDD) of the state of California runs a website for job seekers and employers called CalJOBS. A recent security upgrade, however, has made it impossible for at least one user (me) to log in at all.

The new website requires a user name and password. There are restrictions on both the name and password. The user name must be 6 to 11 alphanumeric characters. So far so good. The password must be 6 to 8 characters. Only after you enter the password (twice) and the answers to your two security questions (see below) do you see this:

**Password must contain 3 of the following 4 items:

1) capital letters A-Z,

- 2) lowercase letters a-z,
- 3) numbers 0-9,
- 4) special characters ! # \$ % ? + - _ @ **

Then you are asked for the answers to two security questions. I have no idea who made up these questions, but they are just plain bizarre. Two examples: "What was your childhood nickname?" and "On what street is your favorite restaurant located?" (The complete lists, as well as other screen shots, are available at my blog <http://TonyLimaAssociates.posterous.com>.)

Even worse, as you fill in the answers to the questions, they are blacked out. You can't see any of the characters you type, but you do have to answer each security question twice. You're out of luck if you manage to make the same typo twice. (Screen capture available on blog.)

If you make a mistake, you're really out of luck. The website instructs you to call EDD at (800) 758-0398. If there are any human beings behind the voicemail, I haven't found them yet.

To top it all off, when I tried to submit a bug report on the EDD website, I consistently got a message saying my message included illegal characters. I swear, all the characters were legal.

No wonder the state unemployment rate is still in double digits.

Tony Lima Associates, Los Altos, CA, USA 1-650-243-1286

✂ Why Won't USPS Let Me File This Complaint?

*Jim Reisert AD1C <jjreisert@alum.mit.edu>
Tue, 30 Mar 2010 15:59:43 -0600*

<http://consumerist.com/2010/03/why-wont-usps-let-me-file-this-complaint.html>

"According to Sarah, she attempted to file the below note using USPS.com's complaint form, but was told it could not be accepted because it contains a prohibited word. But neither she nor we can figure out what that word may be."

I'd like to say the risk here is being forced to complain to the USPS using a snail-mail (i.e. USPS) method instead of their website.

Jim Reisert AD1C <jjreisert@alum.mit.edu>, <http://www.ad1c.us>

✂ Incorrect software change to emergency ambulance call-handling

*Bruce Horrocks <bruce@scorecrow.com>
Tue, 30 Mar 2010 01:00:01 +0100*

system may have resulted in hundreds of deaths

UK call centers dealing with emergency ambulance calls use software to automate the prioritization of calls. Over a decade ago, a change was requested to downgrade the severity of incidents involving a fall of 10ft or more. The change was 'literally' implemented with the consequence that all incidents involving a fall were downgraded, irrespective of the severity of other symptoms.

The error came to light when a woman who had fallen 12ft, was unconscious and had breathing difficulties died after being left to wait because priority was given to a drunk who had collapsed on the street.

<http://www.telegraph.co.uk/health/healthnews/7489663/Hundreds-may-have-died-in-999-ambulance-blunder.html>

It's not clear from the article whether the change was incorrectly implemented or exactly as requested.

The risk is that requirements used to generate safety related software must be as rigorously checked as the software.

Ohioans are dunned for long-paid fines

*Peter Zilahy Ingerman <pzi@ingerman.org>
Wed, 31 Mar 2010 14:48:27 -0400*

Some motorists are complaining that old traffic fines they already paid to one Ohio county are coming back to haunt them. About 1,000 people have contacted officials in southeast Ohio's Hocking County this week to say they've heard from a collection agency about tickets already resolved, in some cases as far back as 20 years ago. Municipal Court Clerk Michele Bell said Tuesday that a glitch that occurred in 1999, when the court changed data systems. The problem surfaced amid the county's ongoing efforts to recover outstanding debts and bolster its budget. About 10,000 debt-collection letters went out last week. Bell says she's not sure how many were sent by mistake and how many went to people who still owe money.

<http://apnews.excite.com/article/20100331/D9EPNS7G0.html>

User-friendly speed cameras in Belgium

*Peter Houppermans <peter@houppermans.com>
Sun, 28 Mar 2010 15:29:16 +0200*

A Belgian Flemish MP (Jurgen Verstrepen) opened an interesting can of worms: he publicly asked why speed cameras weren't better protected. It turns out that every camera has the electricity supply cabinet right next to it, which is totally standard - and that standardisation includes the key (which you can buy legally for about EUR 14).

It gets better: opening the cabinet and killing the power to the camera does

not get you in trouble with the law as there is no actual damage. It so also won't signal the police, which it would do in case of damage.

All of this was reported in the Belgian press today. Given the popularity of speed cameras in general I suspect Monday will start with a run on those keys, and end with not a single static camera left operational. I'm not entirely sure that was the original intention..

<http://www.autokanaal.be/nieuws/guid/3905ffc1-f11b-4ac2-a123-484bb84b0807.aspx>

✂ Academic Paper in China Sets Off Alarms in U.S.

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

Sun, 28 Mar 2010 9:55:04 PDT

Larry M. Wortzel, in a hearing of the U.S. House Foreign Affairs Committee on 10 Mar 2010: "Chinese researchers at the Institute of Systems Engineering of Dalian University of Technology published a paper on how to attack a small U.S. power grid sub-network in a way that would cause a cascading failure of the entire U.S."

[Source: John Markoff and David Barboza, *The New York Times*, 20 Mar 2010. The NYTimes article is nicely nuanced, and discusses a very complex issue. It deserves your reading. The graduate-student Chinese author, Wang Jianwei, claims he was trying to find ways to enhance the stability of power grids, not trying to bring down the grid. But it should be no surprise to RISKS readers that vulnerabilities exist! PGN]

<http://www.nytimes.com/2010/03/21/world/asia/21grid.html>

✂ Water-treatment computer: No, not the Three Stooges, but close

Jeremy Epstein <jeremy.epstein@sri.com>

Mon, 29 Mar 2010 12:26:27 -0400

The theft of a computer from the Molalla Oregon water treatment facility is being considered a federal crime by authorities. Someone broke into the water plant on 27 Mar 2010 through a back window and stole the computer, which was what kept the plant working on auto pilot, with remote monitoring of water pumps and reservoir and chlorine levels. Water service was not affected, as the plant could still be operated manually. The next day, the computer was found in a nearby pond. City officials said it's destroyed, but a technician is trying to salvage the hard drive and the costly programming on it. [Source: Fox 12, KPTV.com, 26 Mar2010; PGN-ed]

<http://www.kptv.com/news/22964989/detail.html>

[So let's see, the single computer that controls their water system is in a loosely controlled building, and there's no real-time or offline backup system. Certainly a less scary attack from the cyber perspective, and hard to do from China or on a large scale, but no less effective! JE]

Jeremy Epstein, Senior Computer Scientist, SRI International
1100 Wilson Blvd, Suite 2800, Arlington VA 22209, 703-247-8708

#3.3 million student-loan records pilfered (Jeremy Kirk)

*Gene Wirchenko <genew@ocis.net>
Tue, 30 Mar 2010 12:37:33 -0700*

Confidential data on students applying for loans including names, addresses, birth dates and Social Security numbers has been stolen, according to a non-profit company that helps with student loan financing. [Source: Jeremy Kirk, *IT Business*, 30 Mar 2010.]

<http://www.itbusiness.ca/it/client/en/home/News.asp?id=56987>

Selected quotes:

"Data on 3.3 million borrowers was stolen from a nonprofit company that helps with student loan financing.

The theft occurred on 20 or 21 Mar 2010 from the headquarters of Educational Credit Management Corp. (ECMC), which services loans when student borrowers enter bankruptcy. The data was contained on portable media, said the organization, which is a dedicated guaranty agency for Virginia, Oregon and Connecticut.

The data included names, addresses, birth dates and Social Security numbers but no financial information such as credit card numbers or bank account data, ECMC said in a news release."

"ECMC didn't say whether the data taken was encrypted."

[On that last bit, why not? For that much data, should it not be a given that it would have been encrypted?]

#Old-fashioned computer risks, Re: 3.3 million student-loan data

*Jeremy Epstein <jeremy.j.epstein@gmail.com>
Sat, 27 Mar 2010 10:16:24 -0400*

In the wake of many data breaches, let's not forget the old fashioned kind. Information on 3.3 million college students with loans through ECMC was stolen in a burglary of the ECMC offices in Minnesota. It's not clear from the report whether the thieves targeted the storage device (described as "portable media with personally identifiable information"), or whether that was incidental to a theft of other equipment.

The Risk? Assuming that all data thefts are cyberthefts!

<http://www.ecmc.org/details/Announcement.html>

#High-tech copy machines a gold mine for data thieves

David Hollman <david.hollman@kcl.ac.uk>

Tue, 30 Mar 2010 13:21:42 +0100

<http://www.thestar.com/news/gta/article/781567--high-tech-copy-machines-a-gold-mine-for-data-thieves>

"..businesses are completely unaware of the potential information security breach when the office photocopier is replaced. They think the copier is just headed for a junkyard but, in most cases, when the machine goes, so does sensitive data that have been stored on the copier's hard drive for years. ... Of the dozens of multi-purpose copiers [he] has cleaned out in the past two years, he has seen hundreds of scanned documents that would be considered confidential."

Other points:

- * Many copiers are networked, allowing for another way of accessing unprotected data
- * Employees use work copiers for personal business and you'd expect to find all kinds of sensitive personal information as well as company information.

The risk seems to be the fact that many/most people wouldn't realize that a computer is part of an everyday device like a copier, coupled with the fact that said device gets to read all kinds of sensitive things.

I wonder if there are other cases where both of those things are true...? Web-enabled TV boxes perhaps? Surely there are other examples.

#Survey: Millions of users open spam e-mails, click on links

Monty Solomon <monty@roscom.com>

Thu, 25 Mar 2010 23:32:53 -0400

Dancho Danchev, Survey: Millions of users open spam e-mails, click on links, ZDNet, 25 Mar 2010

How many users access spam e-mails, click on the links found within, and open attachments intentionally? Why are they doing it, and who are they holding responsible for the spread of malware and spam in general, in between conveniently excluding themselves?

A newly released survey from the Messaging Anti-Abuse Working Group (MAAWG), summarizing the results of the group's second year survey of e-mail security practices, offers an interesting insight into the various interactions end users tend to have with spam e-mails.

Key findings of the survey:

Nearly half of those who have accessed spam (46%) have done so intentionally - to unsubscribe, out of curiosity, or out of interest in the products or services being offered.

Four in ten (43%) say that they have opened an e-mail that they suspected was spam.

Among those who have opened a suspicious e-mail, over half (57%) say they have done so because they weren't sure it was spam and one third (33%) say they have done so by accident.

Canadian users are those most likely to avoid posting their e-mail address online (46%). Those in the U.S., Canada and Germany are most likely to set up separate e-mail addresses in order to avoid receiving spam.

Many users do not typically flag or report spam or fraudulent e-mail.

When it comes to stopping the spread of viruses, fraudulent e-mail, spyware and spam, e-mail users are most likely to hold ISPs and ESPs (65%) and anti-virus software companies (54%) responsible.

Less than half of users (48%) hold themselves personally responsible for stopping these threats. ...

<http://blogs.zdnet.com/security/?p=5889>

[A fool and his password are soon parted. PGN]

Plain Dealer sparks ethical debate by unmasking anonymous poster

*reinke ferdinand <ferdinand.john.reinke@gmail.com>
Sat, 27 Mar 2010 09:18:36 -0400*

http://blog.cleveland.com/metro/2010/03/plain_dealer_sparks_ethical_de.html

Plain Dealer sparks ethical debate by unmasking anonymous Cleveland.com poster
By Henry J. Gomez, *The Plain Dealer*, 26 Mar 2010

By unmasking an anonymous poster at its companion website, The Cleveland Plain Dealer finds itself in an ethical quandary, stirring a debate that balances the public's need to know against the privacy concerns of online participants.

The newspaper traced the identity of 'lawmiss' after someone using that moniker left a comment about the mental state of a relative of reporter Jim Ewinger. The comment was removed for violating cleveland.com's community rules, which do not allow personal attacks.

Users are required to register with a valid e-mail address before posting at cleveland.com. Upon learning of the Ewinger issue Monday, an online

editor looked up lawmiss's e-mail address, which like all others, is accessible through software used to post stories to the website.

"It does raise the question of the wisdom and fairness of the newspaper using the registration system of the website for reporting purposes," Steele said in a telephone interview.

The newspaper's decisions could have a chilling effect on conversation at cleveland.com, said Rebecca Jeschke of the Electronic Frontier Foundation, an online privacy rights group.

"I would think twice before participating in a message board where I had to give my e-mail address knowing that management could access it at any time," Jeschke said. "It seems appropriate in this case, but ... it's hard not to imagine scenarios where it's abused."

Other news organizations already hide such information from their editorial staff, said Steve Yelvington, a strategist for Morris Digital Works, the online division of Morris Communications. The company runs 13 daily newspapers in Florida, Georgia, Texas and other states. "We are careful to firewall our business records from our journalists," Yelvington said.

Regardless of where one comes down on the issue of Internet privacy (IMHO there ain't none), or how much should you trust anything on the inet (IMHO zero trust), and technology in general (IMHO we give boobs the equivalent of loaded guns and they are astonished when some one gets hurt), this was completely preventable.

Use a "disposable" e-mail account!

Haven't these people ever heard of GMAIL? No invitation required now! You can even use multiple ones! Ask any "child" who wants to break free from Mom and Dad's supervision. That's without even getting "tricky" of using one of the "disposable websites that create e-mail addresses that only work for a very limited time; perfect for "e-mail validation" requirements. If Chinese bloggers can hide form their oppressive regime, then we can conclude that most of us who want "privacy" can figure out a way to do it. In this case, the technology-naive are getting a very expensive education in "technology".

And, this wasn't even the government seeking to find out who made a nasty comment. Wait till the Internet-using public says something the government doesn't like. Such as "taxes are too high", "the <insert favorite government agency> is inept, corrupt, or stupid", or quote Jefferson, Lysander Spooner, or Sam Adams. Then, the proctology exam will begin.

Replies will be considered at A953Dy7n1iLK360@gmail.com or ns9288E5T0JmV5@yahoo.com or YCiR5V5J6I3WSYR@hotmail.com.

(How long before these e-mail address get a Nigerian "offer" letter? For the totally clueless, these accounts are NOT real. Merely illustrations of the above point.)

[I hate to be an a-lawmiss-t (perhaps with a Boston accent?), but RISKS

readers certainly realize by now that privacy risks in social computing are *huge*. PGN]

✂ In Bid to Sway Sales, Cameras Track Shoppers (Stephanie Rosenbloom)

Monty Solomon <monty@roscom.com>

Sat, 20 Mar 2010 16:51:57 -0400

The curvy mannequin piqued the interest of a couple of lanky teenage boys... A father emerged from a store dragging his unruly young son by the scruff... These scenes may seem like random shopping bloopers, but they are meaningful to stores that are striving to engineer a better experience for the consumer, and ultimately, higher sales for themselves. Such clips, retailers say, can help them find solutions to problems in their stores - by installing seating and activity areas to mollify children, for instance, or by lowering shelves so merchandise is within easy reach. Privacy advocates, though, are troubled by the array of video cameras, motion detectors and other sensors monitoring the nation's shopping aisles. ...

[Stephanie Rosenbloom, *The New York Times*, 19 Mar 2010; PGN-ed]

<http://www.nytimes.com/2010/03/20/business/20surveillance.html>

✂ TJX Culprits Sentenced

Gene Wirchenko <genew@ocis.net>

Mon, 29 Mar 2010 13:42:31 -0700

Albert Gonzalez, the hacker mastermind behind the TJX credit card scam, was sentenced to two concurrent 20-year stints in prison -- as his parents and sister silently wept. [Source: Nancy Weil, Family weeps as TJX hacker gets 20 years in slammer, 29 Mar 2010]

<http://www.itbusiness.ca/it/client/en/home/news.asp?id=56970>

[Christopher Scott, who had collected credit- and debit-card numbers used by Gonzalez, was sentenced to seven years and one day, according to an item on 29 Mar 2010 by Kim Zetter in WiReD.com. The TJX saga has been ongoing for quite a while, and is well covered in previous RISKS and by what your favorite search engines can find. Too much to summarize here. PGN]

✂ USENIX Health Security and Privacy Workshop due 9 Apr 2010

Kevin Fu <kevinfu@cs.umass.edu>

Tue, 30 Mar 2010 17:34:07 -0400

[This item should be of particular interest to many RISKS readers. Perform an operation in the next week that creates two inspiring pages and

send them in to HealthSec10. Be sure to reflect on what you have learned over the years of reading RISKS! PGN]

Call for Papers

1st USENIX Workshop on Health Security and Privacy (HealthSec '10)

Submissions deadline: April 9, 2010, 11:59 p.m. PDT

<http://www.usenix.org/healthsec10/cfpb/>

HealthSec '10 is intended as a forum for lively discussion of aggressively innovative and potentially disruptive ideas on all aspects of medical and health security and privacy. A fundamental goal of the workshop is to promote cross-disciplinary interactions between fields, including, but not limited to, technology, medicine, and policy. Surprising results and thought-provoking ideas will be strongly favored; complete papers with polished results in well-explored research areas are comparatively discouraged.

Given the goals for HealthSec '10, the submission requirements are modest: 2-page papers that clearly espouse a position and that will promote discussion. Position papers will be selected for their potential to stimulate or catalyze further research and explorations of new directions, as well as for their potential to spark productive discussions at the workshop.

Workshop topics are solicited in all areas relating to healthcare information security and privacy, including:

- * Security and privacy models for healthcare information systems
- * Industrial experiences in healthcare information systems
- * Deployment of open systems for secure and private use of healthcare information technology
- * Security and privacy threats against and countermeasures for existing and future medical devices
- * Regulatory and policy issues of healthcare information systems
- * Privacy of medical records
- * Usability issues in healthcare information systems
- * Threat models for healthcare information systems

For more details on the submission process, please see the complete Call for Papers at:

<http://www.usenix.org/healthsec10/cfpb/>

We look forward to receiving your submissions!

Kevin Fu, University of Massachusetts Amherst

Tadayoshi Kohno, University of Washington

Avi Rubin, Johns Hopkins University

HealthSec '10 Program Chairs

healthsec10chairs@usenix.org

*Albert Levi <levi@sabanciuniv.edu>
Mon, 22 Mar 2010 13:33:36 +0200*

GameSec 2010, the inaugural Conference on Decision and Game Theory for Security will take place on the campus of Technical University Berlin, Germany, on November 22-23, 2010, under the sponsorships of Deutsche Telekom Laboratories, Fraunhofer HHI and IEEE Control System Society. The paper submission deadline is May 15, 2010.

GameSec conference aims to bring together researchers who aim to establish a theoretical foundation for making resource allocation decisions that balance available capabilities and perceived security risks in a principled manner. The conference focuses analytical models based on game, information, communication, optimization, decision, and control theories that are applied to diverse security topics. At the same time, the connection between theoretical models and real world security problems are emphasized to establish the important feedback loop between theory and practice. Observing the scarcity of venues for researchers who try to develop a deeper theoretical understanding of the underlying incentive and resource allocation issues in security, we believe that GameSec will fill an important void and serve as a distinguished forum of highest standards for years to come.

For more information, please visit <http://www.gamesec-conf.org/>

Albert Levi, Sabanci University, Faculty of Engineering and Natural Sciences, Orhanli, Tuzla TR-34956, Istanbul TURKEY +90 (216) 483 9563



Search RISKS using [swish-e](#)

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