



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 16

Friday, 24 March 1995

---

### • [Issue 01 \(2 May 1994\)](#)

- [Vandalism disrupts service at UK University \(Peter Ladkin\)](#)
- [Subjectively, it's eerie \(Phil Agre\)](#)
- [Miniature cameras on Sacramento-area alarm systems \(Dan Zerkle\)](#)
- [DIA delays due to programmers, mayor implies \(Bear Giles \[2\]\)](#)
- [Re: DMV Computer upgrade goes awry... \(Shel Kaphan\)](#)
- [Re: Unusual Newspaper Error \(Stewart Rowe, David Wittenberg, Daniel Dobkin\)](#)
- [Re: MIT student arrested for BBS ... \( Fredrick B. Cohen\)](#)
- ["The Streetwise Guide to PCs" by Jerome/Taylor \(Rob Slade\)](#)
- [Computer-Aided Verification 94 Conference Announcement \(David Dill\)](#)

### • [Issue 02 \(3 May 1994\)](#)

- [NEW YORKER article on library automation \(Jon Jacky\)](#)
- [Information Warfare: GM vs VW \(Mich Kabay\)](#)
- [TechWar: Cell Phone Jamming \(Mich Kabay\)](#)
- [Green Card Con Artists Exposed! \(Bonnie L. Mahon via D.R. Hilton\)\)](#)
- [New firewalls book - a great risk reducer \(Ray Kaplan\)](#)
- [Re: Drunk in charge \(John Simutis, Andy Ashworth, Dan Astoorian\)](#)
- [Boot Prom commits Denial of Service Attack \(Butch Deal\)](#)
- [Staying Informed of Security & Privacy Issues \(David Johnson\)](#)

### • [Issue 03 \(5 May 1994\)](#)

- [Spelling correction \(Phil Agre\)](#)
- [Sigh -- security through obscurity is NOT security \(Alan Wexelblat\)](#)
- [Bellcore cracks 129-digit RSA encryption code \(Steven Tepper\)](#)
- [Risk of Non-Computerization? \(Klaus Brunnstein\)](#)
- [Computers Blamed For FAA Woes \(Mark Thorson\)](#)
- [Brief note re DIA fiasco \(Paul Green\)](#)
- [Followup on credit card policies \(re: "Streetwise Guide ..."\) \(Rob Slade\)](#)
- [ABC Nightline re LaMacchia \(Mich Kabay\)](#)
- [Risks of electronic door locks for automobiles \(Paul Wallich\)](#)

### • [Issue 04 \(10 May 1994\)](#)

- [Secret elevator codes baffle Metro Toronto government \(Dave Leibold\)](#)

- [Smoke or Malaria - Lesser of the two evils \(Hiranmay Ghosh\)](#)
- [Dartmouth prof spoofed \(Mich Kabay\)](#)
- [11-digit ZIP code \(Christine Harbs\)](#)
- [Frozen computer scientist \(David Honig\)](#)
- [Re: Bellcore cracks 129-digit RSA \(Paul C Leyland, Dik Winter, Paul Buder\)](#)
- [Re: Streetwise Guide \[Risks ... credit-card laws\] \(Robert Slade\)](#)
- [Future of US health care? \(Mark Stalzer\)](#)
- [White House May Issue National ID Cards \(Mitch Ratcliffe via W.C. Daugherty\)](#)
- [Canadian long-distance service reseller blunders \(Mich Kabay\)](#)
- [Cheers to two companies \(Michael J. Zehr\)](#)
- [Re: MIT student arrested \(David desJardins\)](#)

• [Issue 05 \(11 May 1994\)](#)

- [Are we betting on horses or computers? \(off-track betting\) \(Reva Freedman\)](#)
- [Amusing computer-related anecdote about local cable service \(H Morrow Long\)](#)
- [MTV Sues Curry \(Adam Curry\)](#)
- [China Airlines A300 Crash \(Mark Stalzer\)](#)
- [Re: Elevators, Car bumpers and Cryptography... \(Peter Wayner\)](#)
- [Re: Bellcore cracks 129-digit RSA encryption code \(Fred Cohen, Amos Shapir\)](#)
- [Re: ACM Nightline \(Robert Morris\)](#)
- [Don't always believe those E-Mail addresses \(A. Padgett Peterson\)](#)
- [EFF's Kapor announces new cyberspace TV show \(Kapor via Stanton McCandlish\)](#)
- [Automation: request for input \(Ken Funk\)](#)

• [Issue 06 \(12 May 1994\)](#)

- [Plane accidentally ejects pilot into sea \(Frank E Carey\)](#)
- [Tax preparation programs; IRS privacy; IRS computerization \(PGN and COOVEN\)](#)
- [Digital Defamation in the UK \(Brian Randell\)](#)
- [We spy harder! \(Mich Kabay\)](#)
- [Killers sue over phone taps \(Mich Kabay\)](#)
- [Journalists attack credit card account \(Mich Kabay\)](#)
- [Fragmenting of the News \(Mich Kabay\)](#)
- [Software piracy vexes industry \(Mich Kabay\)](#)
- [Ultra-high dependability and the Channel Tunnel \(R.J. Stroud\)](#)
- [Re: Future of US health care? \(Amy McNulty\)](#)
- [Re: China Air A300 Crash \(David Wittenberg\)](#)
- [Re: Copyright/patent owners: quick correction \(Mark Seecof\)](#)
- [Re: Amusing computer-related anecdote about cable \(Ry Jones, Paul N Hrisiko\)](#)
- [Re: 11-digit ZIP code \(Ed Ravin\)](#)

• [Issue 07 \(17 May 1994\)](#)

- [Crossover of Diagnosis and Procedure Code creates risk \(Paul Stoufflet\)](#)
- [The Italian Crackdown? \(Fabrizio Sala via Stanton McCandlish\)](#)
- [Umass/Amherst Suffers From Week-long Service Degradation \(Randy Sailer via Jonathan Welch and Sullivan\)](#)
- [More on the A300 crash at Nagoya on 26 April 1994 \(Peter Ladkin\)](#)
- [Palm-reading and immigration \(John Oram\)](#)
- [Computer-based Notice Boards and Emergency Information \(John R. Gersh\)](#)
- [Re: Killers sue over phone taps \(Adam Shostack\)](#)
- [Revision to the Secure Hash Standard \(NIST message via Paul Carl Kocher\)](#)
- [Automated address changes \(Linus Sherrill\)](#)
- [Re: Tandem and California DMV \(Scott Hazen Mueller\)](#)
- [Tracking \(Phil Agre\)](#)

- [Secret... not so secret \[NYNEX PINs\] \(Alan Wexelblat\)](#)

• [Issue 08 \(18 May 1994\)](#)

- [Phone system crash at San Jose airport \(Tarun Soni\)](#)
- [Logging on as root is easy! \(Eddy\)](#)
- [Computer Crime on Wall Street \(Sanford Sherizen\)](#)
- [Going by the Book \[air accidents\] \(Richard Johnson\)](#)
- [Editor functionality mutates code \(Kevin Lentin\)](#)
- [UK ATM Spoof \(Mich Kabay\)](#)
- [The RISKS of complex procedures \(Ry Jones\)](#)
- [Tactical research \(Phil Agre\)](#)
- [FIPS to be tied... \[hashing hashed, Capstone\] \(Peter Wayner\)](#)
- [Re: INS recordkeeping \(Jonathan Corbet\)](#)
- [Re: killers sue over phone taps \(Robert Morrell Jr.\)](#)
- [Re: Secret... not so secret \(Tony Harminc\)](#)
- [Novel risk of medical records \(David Honig\)](#)
- [Crossover of Diagnosis and Procedure Code ... \(Carl Ellison\)](#)

• [Issue 09 \(25 May 1994\)](#)

- [Call Your OPERATER! \(Martin Minow\)](#)
- [Bank goof creates millionaire \(Andy Fuller\)](#)
- [Two risk-related articles from Edupage 5/24/94 \(Terry Alford\)](#)
- [Dell monitors too hot to handle \(Mich Kabay\)](#)
- [Canada, The Internet, and the Homolka trial \[anonymous\]](#)
- [Risks of setting up awful puns \(Aaron Barnhart\)](#)
- [Re: China Airlines A300 Crash \(John Yesberg\)](#)
- [Re: Computer Crime on Wall Street \(Mike Rosenberg, Marc Horowitz\)](#)
- [Cable / Closed Circuit TV Info Display Risks and 911 \(Bob Richardson\)](#)
- [Re: Logging on as root is easy! \(Dan Franklin, Eddy\)](#)
- [Re: UK ATM Spoof \(Gary Preckshot\)](#)
- [Privacy Digests \(reminder\)](#)

• [Issue 10 \(31 May 1994\)](#)

- [Closed Doors in Glasgow](#)
- [Human.risks-- Scapegoats and Puddlejumpers... \(Peter Wayner\)](#)
- [Man charged with E-mail stalking \(John C. Rivard\)](#)
- [Police BBS in Silver Spring, MD \(Mich Kabay\)](#)
- [Re: alt fan karla homolka \(Phil Overy\)](#)
- [Eavesdropping hits NSA \(Peter Wayner\)](#)
- [Risks of too-simple responses \(Jerry Leichter\)](#)
- ["Zap!" by Sellers \(Rob Slade\)](#)

• [Issue 11 \(3 June 1994\)](#)

- [Flaw in Clipper detected \(Jim Huggins\)](#)
- [Re: Solo midair collisions \(Martyn Thomas\)](#)
- [Donuts with Ears, Part II \(Peter Wayner, David Wright\)](#)
- [Ollie North on the high seas...Big toys, big egos, E-trails \(David Honig\)](#)
- [Nonexistent Risks \(Re: Call Your OPERATER!\) \(Gregory B. Sorkin\)](#)
- [Risks of faxing \(Adam Shostack\)](#)
- [The Ghost in the Modem \(Loka Alert 1:6 via Phil Agre\)](#)
- [Zimmermann statement on PGP 2.6 \(Philip Zimmermann\)](#)
- ["The Hacker Crackdown" by Bruce Sterling \(Rob Slade\)](#)

• [Issue 12 \(8 June 1994\)](#)

- [RISKS OF RISKS again \(PGN\)](#)
- [Hazards of the real-time switchover of a prison system \(Ray T. Stevens\)](#)
- [Campaigns and Elections \(Phil Agre\)](#)
- [Library fines unstoppable after earthquake \(Geoff Kuenning\)](#)
- [Flames and viruses in e-mail - article in the New Yorker \(Martin Minow\)](#)
- [Tetris addiction? \(Mich Kabay\)](#)
- [Re: Closed Doors in Glasgow - Trapped Guard Dies in Fire \(John Vilkaitis\)](#)
- [Re: Risks of too-simple responses \(UK ATM Spoof\) \(Henry J. Cobb, Mathew Lodge, Jerry Leichter\)](#)
- [Re: Clipper \(Gene Spafford, Sidney Markowitz \[2\], A. Padgett Peterson, Paul Carl Kocher\)](#)

• [Issue 13 \(9 June 1994\)](#)

- [RISKS summer slowdown \(PGN\)](#)
- [False alarm in Channel Tunnel \(John Colville\)](#)
- [Apathy toward computer errors \(Chip Seymour\)](#)
- [Mailing-list software security problem \(Jim Patterson\)](#)
- [GIF contains more than just a picture \(Matthew David Aldous\)](#)
- [Re: "The Ghost in the Modem" \(Scott Dickson\)](#)
- [Re: China Airlines A300 Crash \(Mark Terribile\)](#)
- [Re: Flaw ? in Clipper \(A. Padgett Peterson, Robert I. Eachus\)](#)
- [WWW Virtual Library page on safety-critical systems \(Jonathan Bowen\)](#)
- ["Network Security Secrets" by Stang \(Rob Slade\)](#)
- [Re: "The Hacker Crackdown" by Bruce Sterling, via WWW \(John Oram\)](#)

• [Issue 14 \(13 June 1994\)](#)

- [Unconventional Telephones \(Mike Hoffberg\)](#)
- [Ex-deputy police chief charged over Computer Records \(Mich Kabay\)](#)
- [RISKS in UK Election Voting Process \(Thomas Rushton\)](#)
- [Big brother wants the shirt off your back \(Lynn R Grant\)](#)
- [Re: GIF contains more than just a picture \(Castor Fu\)](#)
- [Re: How to feel safer in an Airbus \(Peter Ladkin\)](#)
- [Airbus A3\(0?\)0 deductions \(Phil Overy\)](#)
- [Correction for address of Clipper paper \(Sidney Markowitz\)](#)
- [Chunnel vision \(David Honig\)](#)
- [RISKS of real-time image processing \(Andy Cunningham\)](#)
- [Re: Women and Tetris addiction \(Hilarie Orman\)](#)
- [Re: Campaigns and Elections \(Robert J. Burkhart\)](#)
- [Re: Apathy toward computer errors \(Tom Yurkiw\)](#)
- [Security? Maybe.... \(Neill Clift\)](#)
- [Re: Call Your OPERATER \(Hardwire\)](#)
- [Re: Risks of too-simple responses \(Ross Anderson\)](#)

• [Issue 15 \(15 June 1994\)](#)

- [Privacy: Your Secrets For Sale \(Les Earnest\)](#)
- [Life imitates Bart Simpson \(Jeffrey S. Sorensen\)](#)
- ["Computer Ethics" by Deborah Johnson \(Rob Slade\)](#)
- [Re: More Chunnel vision \(Philip H. Smith III\)](#)
- [Re: Airbus \(Mary Shafer, Robert Dorsett, Phil Overy, Wesley Kaplow\)](#)
- [Re: Risks of speed enforcement \(Jonathan Clark, Clive D.W. Feather\)](#)
- [Re: RISKS in UK Election Voting Process \(Doug Tooley, Kent J Quirk, John C Sager, Sean Matthews, Peter Robinson, John Gray\)](#)

• [Issue 16 \(15 June 1994\)](#)

- [Congressman Jack Brooks' Statement on Crypto \(David Banisar\)](#)
- [WSJ article: RFI hoses medical equipment \(Robert Allen\)](#)
- [Summary of safety-critical computers in transport aircraft \(Peter Ladkin\)](#)
- [More on Airbuses \(Robert Dorsett, Peter Ladkin, Wesley Kaplow, Pete Mellor, Kaplow again, Bob Niland\)](#)

• [Issue 17 \(17 June 1994\)](#)

- [Poulsen guilty of L.A. charges \(Mich Kabay\)](#)
- [Counterfeit graduation tickets \(Mich Kabay\)](#)
- ["Virtual Billboard" on TV \(R. Peter Jackson\)](#)
- [Misdirected Mail \(Jeffrey Austen\)](#)
- [Revenue Canada database allows birthday change \(John Howard\)](#)
- [NIST Response to Blaze Attack on Clipper \(Ed Roback\)](#)
- [ROLM phones and "Do Not Disturb": how to lose calls \(Rob Levandowski\)](#)
- [A320 hull losses: Lies, damned lies and statistics \(Pete Mellor\)](#)

• [Issue 18 \(21 June 1994\)](#)

- [Physical Location via Cell Phone \(Derek Atkins\)](#)
- [RF Interference \(unattributed alt.shenanigans item via Elana\)](#)
- [EDI mail storm \(Cheryl Berthelsen via Brian D. Renaud\)](#)
- [Re: Campaigns and Elections \(Peter J. Denning\)](#)
- [Re: Airframe Safety \(Bill Murray, Mark Staler, Andy Dingley, Tom Lane\)](#)
- [Shopping Risks... \(Philip R. Banks\)](#)

• [Issue 19 \(5 July 1994\)](#)

- [A330 crash: Press Release \(Pete Mellor\)](#)
- [States crack down on "cyberfraud" \(Mark Seecof\)](#)
- [AI to screen bad from good cops in Chicago \(Christopher Maag\)](#)
- [Going to a Computer Conference? Don't use your real name! \(Steve L. Rhoades\)](#)
- [Fraud on the Internet \(Mich Kabay\)](#)
- [ACM Releases Crypto Study \(US ACM, DC Office\)](#)
- [USACM Calls for Clipper Withdrawal \(US ACM, DC Office\)](#)
- [Re: Physical Location via Cell Phone \(Lauren Weinstein, Willis H. Ware, Robert Morrell Jr.\)](#)
- [Cellular Confusion \(Bob Frankston\)](#)

• [Issue 20 \(6 July 1994\)](#)

- [EM RF RISK turns into life-saver \(Ralph Moonen\)](#)
- [Mosaic risks \(Faisal Nameer Jawdat\)](#)
- [Airbus \(Robert Morrell Jr.\)](#)
- [ACM crypto policy panel chairman's statement \(Steve Kent\)](#)
- [Re: Physical Location via Cell Phone \(A. Harry Williams\)](#)
- [Phone records \(Lauren Weinstein\)](#)
- [Video cameras in City Centres \(Scott A. McIntyre\)](#)
- [Re: AI to screen bad from good cops in Chicago \(Piers Thompson\)](#)
- [Re: Scary \(Jim Horning\)](#)
- [Environmentally Aware Computing \(JAN Lee\)](#)
- ["Repetitive Strain Injury" by Pascarelli \(Reviewed by Rob Slade\)](#)
- ["Computer Ethics" by Forester/Morrison \(Reviewed by Rob Slade\)](#)
- ["A Short Course on Computer Viruses" by Fred Cohen \(Reviewed by Rob Slade\)](#)
- [Re: Rob Slade's review of "The Hacker Crackdown" \(Richard Schroepfel\)](#)

• [Issue 21 \(7 July 1994\)](#)

- [Risks of REDIAL \(via Lance Hoffman and others\)](#)
- [Online services taking big hits \(Alan Wexelblat\)](#)
- [Tax Software to Avoid: CA Simply Tax \(Smith Craig\)](#)
- [IRS SSN risks may abate \(Michael Gerlek\)](#)
- [Re: Fraud on the Internet \(Jeff Barber\)](#)
- [Signatures in electronic commerce \(Mich Kabay\)](#)
- [Re: Scary \(Peter J. Denning\)](#)
- [Just the Facts, Ma'am \(AI to screen bad from good cops\) \(David Honig\)](#)
- [Re: Video cameras in City Centres \(Robert Allen\)](#)
- [Digitized CC Signatures \(Eric Richards\)](#)
- [Re: Shopping Risks... \(Jane Anna LANGLEY\)](#)

• [Issue 22 \(9 July 1994\)](#)

- [Roller coaster accident -- computer blamed \(Jonathan Moffett, Marcus Marr\)](#)
- [Re: Tax Software to Avoid: CA Simply Tax \(Rick Smith, Barry Margolin\)](#)
- [Re: Risks of vote fraud \(Lawrence Kestenbaum\)](#)
- [Literary treatment of street-corner cameras \(Mark Seecof\)](#)
- [Re: Just the Facts, Ma'am \(Bob Frankston\)](#)
- [Re: Mosaic risks \(John R Levine\)](#)
- [Any data of Bill Gates's Info-highway book? \(Richard Botting\)](#)
- [Re: A330 crash \(Curtis Jackson, Peter Ladkin\)](#)
- [Re: ACM Crypto Policy Statement \(Nap & Erik van Zuuren\)](#)
- [Re: Fraud on the Internet \(D. Owen Rowley\)](#)
- [EMI of 'VW'? NOT! \(Chris Norloff\)](#)

• [Issue 23 \(13 July 1994\)](#)

- [Inmates con jail computer \(Peter Ilieve\)](#)
- [White House Buys Off EES Patent Holder \(Brock N. Meeks v. Stanton McCandlish\)](#)
- [New National ID Card Proposal \(David Banisar\)](#)
- [SimCity \(Phil Agre\)](#)
- [Teletext run amok \(Michael J. Stern\)](#)
- ["Glyphs" may track your demographics \(Walter C. Daugherty\)](#)
- [EMI of 'VW'? YES \(Rick Cook\)](#)
- [Correction to A330 report \(Peter Ladkin\)](#)
- [Re: Promises and "Scary" \(Phil Agre\)](#)
- [Laptop Danger for Airplanes \(Dan Arias via Martin Howard\)](#)
- ["If Ajax had a good computer system, Peter would still be alive." \(Daniel P. B. Smith\)](#)
- [Re: Roller coaster accident -- computer blamed \(Clive D.W. Feather\)](#)
- [Re: ACM Crypto Policy Statement \(Dave Golber\)](#)
- [Re: Phone records \(S. E. Grove\)](#)
- [Re: Signatures in electronic commerce \(Robin Kenny\)](#)
- [Re: Digitized CC Signatures \(Mark Brader\)](#)

• [Issue 24 \(14 July 1994\)](#)

- [Quoth the Maven, Livermore! \(porno repository\) \(PGN\)](#)
  - ["DUMB FROGS AHEAD" \(Tom Zmudzinski\)](#)
  - [Digital display boards on highways \(Jason Hanson\)](#)
  - [Mailers that add "Company Confidential" \(Paul Szabo\)](#)
  - [Scams \(Phil Agre\)](#)
  - [Re: Secure use of Internet \(Tom Patterson\)](#)
-

[Re: Shopping Risks...](#) (Philip H. Smith III)

- [Re: Brock Meeks article on Clipper](#) (Jerry Leichter)
- [Cellular phone risks/privacy](#) (Phillip Brown)
- [Literary treatment of street-corner cameras](#) (Scott Dorsey)
- [Teletext](#) (Bob Richardson, Clive D.W. Feather, Bob Frankston)
- [Re: Laptop Danger](#) (Bob Frankston, Joe Chew, Lars-Henrik Eriksson, Tony Abo)

• [Issue 25 \(19 July 1994\)](#)

- [NASDAQ computers crash](#) (PGN abstracting)
- [An Irish Sting Operation](#) (Brian Randell)
- [TCAS story on NBC Dateline 7/14/94](#) (Andres Zellweger)
- [Vindication](#) (Winn Schwartau)
- [Re: Risks of electronics on aircraft](#) (Phil Overy, F. Barry Mulligan, Chris Norloff)
- [Re: Digital Display Boards on Highways](#) (Don Root)
- [EDCC-1, Final Program \[European Dependable Computing Conf.\]](#) (Erik Maehle)

• [Issue 26 \(20 July 1994\)](#)

- [IRS](#) (Phil Agre)
- [Crashed bank teller](#) (Kees Goossens)
- [HERF Vindication II](#) (Winn Schwartau)
- [The digital individual](#) (Phil Agre)
- [Victim on the infobahn](#) (Bill Donahue)
- [Benefits Agency Smart Payment Card](#) (Shaggy)
- [Risks of confusing "headlines" with "in depth news"](#) (Bob Estell)
- [Re: Aircraft Avionic Vulnerabilities](#) (A. Padgett Peterson)
- [Re: Inmates con jail computer](#) (Amos Shapir)
- ["Firewalls and Internet Security" by Cheswick/Bellovin](#) (review by Rob Slade)
- ["The Fool's Run" by Camp](#) (review by Rob Slade)
- [InfoWar II--First Call for Participation](#) (Mich Kabay)

• [Issue 27 \(21 July 1994\)](#)

- [Pentagon computers cracked](#) (Mich Kabay)
- [Chemical Bank ATM's go down after snafu](#) (Josh Rivel)
- [Re: Crashed Bank Teller](#) (William Hugh Murray)
- [EPIC on Gore Letter](#) (David Sobel)
- [Re: Victim on the infobahn](#) (Marc Horowitz, Jeffrey I. Schiller, Max Hadley, Bob Rahe, John W. Burgeson, Mich Kabay, Andrew Marc Greene)

• [Issue 28 \(22 July 1994\)](#)

- [Hoods Hit the Highway](#) (Jon Loeliger)
- [Dutch police victim of phone-tapping criminals](#) (Ralph Moonen)
- [As the Worm Turns--Ant-icipating Problems](#) (Mich Kabay)
- [It's a real world out there, and the Internet is part of it.](#) (Phil Agre)
- [Automated mail listserver causes Internet "Spamming"](#) (Jean Renard Ward)
- [Leahy Statement on Gore Statement on Clipper](#) (Marc Rotenberg)
- [Privacy Journal this month](#) (Robert Ellis Smith)
- [CFP: IEEE Symposium on Security and Privacy](#) (Catherine A. Meadows)

• [Issue 29 \(26 July 1994\)](#)

- [Let me off the Information Superhighway!](#) (Nancy Leveson)
- [Risks of assuming standard interfaces](#) (Clive D.W. Feather)

[Airport codes \(Clive D.W. Feather\)](#)

- [Embezzlement at Beijing Hotel \(Mich Kabay\)](#)
- [Remote reading of gas meters \(Mich Kabay\)](#)
- [Hack FAQ \(summary\) \(Martin Minow\)](#)
- [Risks of being unable to clear records \(Marcus J Ranum\)](#)
- [More inadvertent mail list "spamming" \(Phillip Finch\)](#)
- [Two kinds of risks \(Robert Morrell Jr.\)](#)
- [Risks of hot lines \(Philip H. Smith III\)](#)

• [Issue 30 \(2 August 1994\)](#)

- [MCI inbound internet gateways choked \(Mich Kabay\)](#)
- [RISKS of electrical wiring \(Robert Rose\)](#)
- [How to clean out a checking account \(Paul Dineen\)](#)
- [FBI hunting for Agent Steal, flashy computer hacker \(Mich Kabay\)](#)
- [PCMCIA cards \(Mich Kabay\)](#)
- [Progress on RFI in aircraft \(Mich Kabay\)](#)
- [Porn Peddlers Convicted in Memphis \(Mich Kabay\)](#)
- [Re: Video Cameras \(Nap van Zuuren\)](#)
- [Computer telephony \(Phil Agre\)](#)
- [Re: Crashed bank teller \(Ted Lemon, Patrick O'Callaghan\)](#)
- [The Cult of Information by Ted Roszak \(WN Peters\)](#)
- [Report Released on Public Key Law and Policy \(Michael S Baum\)](#)

• [Issue 31 \(9 August 1994\)](#)

- [Unda\(u\)nted exploration: DANTE II \(PGN\)](#)
- [Denver "solves" hi-tech baggage handling problems \(Lauren Weinstein\)](#)
- [Re: Squirrels again bring down Nasdaq \(Joe Morris, Bob Frankston\)](#)
- [More than squirrels: Newbridge Networks \(Bob Frankston\)](#)
- [Re: RISKS of electrical wiring \(Lauren Weinstein\)](#)
- [Re: The Cult of Information \(Steven Tepper\)](#)
- [Rapid Application Development \(RAD\) \(Rebecca Mercuri\)](#)
- [Intel plant in Albuquerque \(Phil Agre\)](#)
- [Madcap world of modern banking \(Ross Anderson\)](#)
- [A330 Crash investigation: Pilot error blamed for crash \(Erik Hollnagel\)](#)
- [Workshop Announcements PDCS2 and SCSC \(Barry Hodgson\)](#)
- [CSR Software Reliability & Metrics Club - Meeting Announcement \(Pete Mellor\)](#)
- [Washington DC ACM Seminar \(John Sheckler\)](#)

• [Issue 32 \(16 August 1994\)](#)

- [Pin the tail on the Dante? \(PGN\)](#)
- [Adventures in Debugging \(Michael J. Stern\)](#)
- [Commercial identity on the Internet \(Mich Kabay\)](#)
- [Desktop check forgery \(Phil Agre\)](#)
- [Burglary suspects caught by Caller ID \(Jonathan I. Kamens\)](#)
- [National Guard payment problems \(Mich Kabay\)](#)
- [Escrowed keys vulnerable to chosen contraband attacks \(Stephen R. Savitzky\)](#)
- [The Danger of Six-Digit Dates \(Mike Sullivan\)](#)
- [A Minor Risk for Centenarians \(Bruce Scott\)](#)
- [IRC bug \(Andrew David Tinkham\)](#)
- [Privacy Conference \(Dave Banisar\)](#)
- [Intrusion Detection Workshop announcement \(Debra Anderson\)](#)



Issue 33 (23 August 1994 [misdated 22 Aug])

- [Program Information: 17th National Computer Security Conference \(long\)](#)

• [Issue 34 \(24 August 1994\)](#)

- [Bug in Microsoft Word \(Chris Norloff\)](#)
- [Report on the 1992 Gatwick near-miss \(Peter Ladkin\)](#)
- [The new Cray and Unix passwords... \(Peter Wayner\)](#)
- [Most home security alarms are false \(Mich Kabay\)](#)
- [Misconceptions about PGP 2.6 from MIT \(Philip Zimmermann\)](#)
- ["Secrets of a Super Hacker" by Fiery \(Rob Slade\)](#)
- [International Cryptography Institute \(Dorothy Denning\)](#)

• [Issue 35 \(25 August 1994\)](#)

- [Fraud and Identity \(Mich Kabay\)](#)
- [Summary of Der Spiegel interview with Airbus' Bernard Ziegler \(Peter Ladkin\)](#)
- [CORRECTION, Report on the \\*1993\\* Gatwick near-miss \(PGN\)](#)
- [Re: pi = 3 \(James Dudley, L. P. Levine\)](#)
- [Re: The new Cray and Unix passwords... \(Chris Ransom\)](#)

• [Issue 36 \(29 August 1994\)](#)

- [Vandals Cut Cable, Slow MCI Service \(Mich Kabay\)](#)
- [Mexican election computers \(John Sullivan\)](#)
- [Attack of the killer spellcheckers... \(Valdis Kletnieks\)](#)
- [U.S. Mail causes ZIP-code problem \(Al Stangenberger\)](#)
- [Re: Bug in Microsoft Word \(Dave Moore\)](#)
- [Salt in wounds \(Re: New Cray and Unix Passwords...\) \(Peter Wayner\)](#)
- [Re: Fraud and Identity -- SCI-FI \(Andrew Marchant-Shapiro\)](#)
- [Politicians Join the Internet \(Mich Kabay\)](#)
- [Re: pi = 3 \(Mark Stalzer, Rob Boudrie\)](#)
- [System makes bank check forgery easy \(Christopher Klaus\)](#)
- [CFP: 2nd ACM Conference on Computer and Communications Security \(Li Gong\)](#)

• [Issue 37 \(31 August 1994\)](#)

- [Risks of spread-spectrum cordless phones \(Don Alvarez\)](#)
- [St. Louis water mishap \(David G. Himrich\)](#)
- [Satellite imaging for targeted marketing? \(Denis Haskin\)](#)
- [Millennium goes to prison \(Henry Troup\)](#)
- [Breakdown of police emergency number \(John Colville\)](#)
- [Risks of client search tools \(the WWWorm turns, and returns, ...\) \(Rob Slade\)](#)
- [Changeable `constants' \(James Ashton\)](#)
- [Re: vandals Cut Cable, Slow MCI Service \(C. Paul Ferroni\)](#)
- [Unintended document contents \(Walter Smith\)](#)
- [Re: Bug in Microsoft Word \(Steen Hansen, Pete Ferris, Anthony E. Siegman\)](#)
- [Re: system makes bank check forgery easy \(Paul Gloger\)](#)
- [More on Real World/Cyberspace ID matching \(Paul Green\)](#)
- [Re: pi = 3 \(Mark Brader\)](#)
- [New indecency rules proposed for all online services \(Daniel J. Weitzner\)](#)

• [Issue 38 \(2 September 1994\)](#)

- [Football interference without penalty? \(PGN\)](#)
- [RFI and "winchcraft" \(Mich Kabay\)](#)

- [Drawbridge controls -- fail-safe? \(Steve Summit\)](#)
- [Chile: "Multicarrier" telephone system collapses \(Patricio Poblete\)](#)
- [Anarchist files linked to child mutilation \(Mich Kabay\)](#)
- [Poulson Pal Pinched \(Mich Kabay\)](#)
- [Barclays Bank's new computer system \(Steve Kilbane\)](#)
- [Risks of living abroad \(DelleraK\)](#)
- [Re: Changeable `constants' \(George W Dinolt, Joseph H Presley, Mark Brader, Bob Frankston, Steve Kilbane, Lars-Henrik Eriksson, James Cottrell, James Carlson, Mark Nelson\)](#)

• [Issue 39 \(6 September 1994\)](#)

- [PKZIP encryption broken \(known plaintext attack\) \(Paul Carl Kocher\)](#)
- [Some privacy notes \(Phil Agre\)](#)
- [Database Marketing \(privacy in \\*Business Week\\*\) \(Mark Stalzer\)](#)
- [Backspace Problems \(John Vilkaitis\)](#)
- [Backspace Failure \(John Vilkaitis\)](#)
- [Re: Millenium goes to prison \(Jim Hiller\)](#)
- [\\_Modern\\_ risks of call by reference \(Mike Albaugh\)](#)
- [Some comments on the A330 accident \(Peter Ladkin\)](#)
- [ESORICS 94 Program \(Yves Deswarte\)](#)

• [Issue 40 \(12 September 1994\)](#)

- [Highest Quality Company Logos for Inclusion in Software \(Dennis Lawrence\)](#)
- [German Parking Violators Accused of War Crimes \(Scott Mincey\)](#)
- [Enola Gay: Another text substitution \(from alt.folklore.urban\) \(Henry Troup\)](#)
- [More daring tales of address disasters! \(Peter Ladkin\)](#)
- [Risks of duality in electronic media \(Bob Mehlman\)](#)
- [Unique way to find bugs: be investigated for breaking the rules \[McLaren Peugeot Formula One\] \(Bjorn Freeman-Benson\)](#)
- [Neural Redlining == Plausible Deniability ? \(Fred Baube\)](#)
- [Reply to New indecency rules proposed for all online services \(Julian Meadow\)](#)
- [CPSR Annual Meeting \(Phil Agre\)](#)
- [Proceedings on Assurance and Trustworthiness \(Marshall D. Abrams\)](#)

• [Issue 41 \(22 September 1994\)](#)

- [Computer disk crash causes misprinted ballots \(Lani Teshima-Miller\)](#)
- [Internet Gets First False Ad Charge \(PGN\)](#)
- [Uninterruptable thought patterns \(Phil Agre\)](#)
- [Re: Digital Logos \(Peter J. Denning\)](#)
- [Reason 55: National Security and the FBI Wiretap Bill \(Marc Rotenberg\)](#)
- [Yet More daring tales of address disasters! \(Paul T. Keener\)](#)
- [High Security Digital Payment Systems \(Michael Waidner\)](#)
- [The Fuzzy Systems Handbook \(Rob Slade\)](#)
- [Neural redlining \(Andrew W Kowalczyk, Peter J. Denning, Fernando Pereira, Thomas E. Janzen, Jan Vorbrueggen, Bob Frankston, John Turnbull\)](#)

• [Issue 42 \(23 September 1994\)](#)

- [Power Outage in Russia? \(Bradford Wetmore\)](#)
- [The Future of the Internet is Secure: Press Conference \(Winn Schwartau\)](#)
- [Telephone background noise RISKS \(Michael P. Gerlek\)](#)
- [Re: Uninterruptable Thought Patterns \(A. Padgett Peterson\)](#)
- [Re: Computer disk crash causes misprinted ballots \(Douglas W. Jones\)](#)

- [Re: Yet More daring tales of address disasters! \(Steve Bellovin et al.\)](#)
- [Re: Address disasters \(John Cantrell, Martin Ewing\)](#)
- [Re: Highest Quality Company Logos \(Jim Prall, Gary Greene, Ray T. Stevens\)](#)
- [Call For Papers: 8th IEEE Computer Security Foundations Workshop \(Li Gong\)](#)

• [Issue 43 \(27 September 1994\)](#)

- [Pretty Bad Privacy in Top-Level Negotiations \(Charles Dunlop\)](#)
- [Re: Mexico election \(Hvard Hegna\)](#)
- [Coyote sues Acme Co. \(Luis Fernandes\)](#)
- [Reasoning 101, the FBI Telecom Bill, and EPIC \(Jerry Leichter, Marc Rotenberg\)](#)
- [Please!, let's call it the "Government Wiretap Bill" !!! \(Jim Warren\)](#)
- [The high-tech university: 500 channels, all alike \(Phil Agre\)](#)
- [Pagers and power supplies \(Laszlo Nemeth\)](#)
- [Marketing of science \(Michael Jampel\)](#)
- [Power Disasters \(Matthew D. Healy\)](#)
- [Re: Power Outage in Russia? \(Arthur D. Flatau\)](#)
- [Questions re: security of computerized medical records \(Richard Goldstein\)](#)
- [Network Security Observations \(NSO\)](#)

• [Issue 44 \(29 September 1994\)](#)

- [Re: Neural Redlining == Plausible Deniability? \(Jim Horning on Brian Randell\)](#)
- [Response to various comments on Internet Security \(Winn Schwartau\)](#)
- [Present Internet Security \(George Thornton\)](#)
- [Re: Mexico election \(Alex Lopez-Ortiz\)](#)
- [Re: Uninterruptables \(Phil Agre, Martyn Thomas\)](#)
- [Safety issues with Screen Savers \(Rich Baker\)](#)
- [Re: Phil Agre on high-tech university \(Robert Ashcroft\)](#)
- [Re: Neural networks and testing \(Fred Cohen\)](#)
- [Re: Yet More daring tales of address disasters! \(Dan Fass, Andrew Marc Greene, Steve Summit, Jan Mandel, Jonathan I. Kamens, Mike Crawford, Chris Smith, Paul Robinson, Michael Jampel\)](#)
- [Privacy & American Business conference in DC next week \(Lance J. Hoffman\)](#)

• [Issue 45 \(10 October 1994\)](#)

- [Anonymity and the Stock Markets... \(Peter Wayner\)](#)
- [ICL loses 1.3m pounds poll-tax case \(Jonathan Bowen\)](#)
- [AOL sells its subscriber list \(David L. Gehrt\)](#)
- [Twins out of luck in Brazil \(Debora Weber-Wulff\)](#)
- [Confidential information passed on \(Nik Clayton\)](#)
- [Privacy Digests -- and Digital Telephony \(PGN\)](#)
- [CFP for CFP'95 \(Computers, Freedom, and Privacy\) \(Carey Heckman\)](#)
- [CALL for PAPERS: EUROCRYPT '95 \(Jean-Jacques Quisquater\)](#)

• [Issue 46 \(19 October 1994\)](#)

- [Risks of putting out RISKS](#)
- [Software Bug Cripples Singapore Phone Lines \(Lee Lup Yuen\)](#)
- [Cellular Phone Scam \(PGN\)](#)
- [Barclays Bank Banks Big-Bang Bump-up \(a success story\) \(Brian Randell\)](#)
- [Data security in Iceland \(Haukur Hreinsson\)](#)
- [Memory Chip Theft \(R. Szczesniak\)](#)
- [Risks of not thinking about what you're stealing \(Mark Brader\)](#)
- [Calling Number ID debate \(Phil Agre\)](#)

- [Creating kidspaces on the net \(Prentiss Riddle\)](#)
- [And you thought one-letter passwords were RISKy ... \(Dan Astoorian\)](#)

• [Issue 47 \(20 October 1994\)](#)

- [Computer mess at Greyhound \(Phil Agre\)](#)
- [British Rail Journey Planner \(Marcus Reynolds via Clive D.W. Feather\)](#)
- [Spin control by computer \(Rob Hasker\)](#)
- [Tampering blamed for rebuffed candidacy in Peru \(PGN\)](#)
- [Re: Data Security in Iceland; Software Bug Cripples Singapore \(Jim Haynes\)](#)
- [Tarom Airbus: automatic mode switch escaped the commandant \(Daniel Salber\)](#)
- [Computer risk that nearly proved deadly \(Carl Maniscalco\)](#)
- [Software reuse \(Mark Gonzales\)](#)
- [Risk of seeming similar interfaces \(Monta Elkins\)](#)
- [Re: squirrelcide \(Douglas W. Jones\)](#)
- [Re: CNID \(Peter da Silva, Scott E. Preece, A. Padgett Peterson\)](#)
- [Washington DC ACM Professional Development Seminars \(John Sheckler\)](#)

• [Issue 48 \(21 October 1994\)](#)

- ["The Mother of All Utility Bills." \(F. Barry Mulligan\)](#)
- [Observed Electro-Magnetic Interference \(Henry Troup\)](#)
- [Re:Computer risk that nearly proved deadly \(Mark Thorson, Gary Koerzendorfer\)](#)
- [Cellular Phone Fraud Operator Arrested \(Paul Robinson, Chip Maguire\)](#)
- [Not enough bytes bites again \(Marc Auslander\)](#)
- [Inadvertent postal forwarding \(V. Michael Bove Jr.\)](#)
- [Computer model of Haiti \(Phil Agre\)](#)
- [Re: Risks of not thinking about what you're stealing \(Joel Finkle\)](#)
- [Re: Risk of similar interfaces \(Chris Norloff, Erann Gat, John Mainwaring\)](#)
- [Re: Software reuse \(David Honig\)](#)
- [Re: Greyhound \(Danny Burstein\)](#)
- [CNID and Don Norman -- CNID can be private \(Justin Wells\)](#)
- [Re: CNID \(Andrew Klossner, Phil Agre\)](#)

• [Issue 49 \(24 October 1994\)](#)

- ["Computer Related Risks" by Neumann \(Rob Slade\)](#)
- [Half a degree is better than none? \(Mark Brader\)](#)
- [Re: Barclays Bank Banks Big-Bang Bump-up \(Mark Brader\)](#)
- [Re: Not enough bytes bites again \(Dave Moore\)](#)
- [The FTC wades in \(Don Blumenthal via Joel K. Furr\)](#)
- [That Macintosh Power Switch \(Don Norman\)](#)
- [The Risks of Ignorant in Computer Science \(Yaron Y. Goland\)](#)
- [More on risky interfaces \(Mike Perry, Gary Page, Brad G. Parks, Jean Renard Ward, Kevin Purcell, Kent Borg, Mike Alexander\)](#)

• [Issue 50 \(25 October 1994\)](#)

- [Another way for computer failure to delay trains \(Mark Brader\)](#)
- [Bank Robber Foiled by Security Screen \(Paul Gillingwater\)](#)
- [Re: Ignorance in Computer Science \(Roy Maxion\)](#)
- [Re: Don Norman and the Power switch \(William Hugh Murray\)](#)
- [Re: deadly risk \(Scot E. Wilcoxon\)](#)
- [Re: Cell Phone Fraud Countermeasures \(Bill Hensley\)](#)
- [Re: Badly designed interface in MS Mail \(Russell Stewart\)](#)
- [Re: Inadvertent postal forwarding \(Kent J Quirk\)](#)

- [Re: Data security in Iceland \(Curtis Jackson\)](#)
- [Mailing lists risk critical-mass spamming \(Benjamin A Ostrowsky?\)](#)
- [Re: CNID \(Lauren Weinstein, Michael D. Sullivan, Tim Duncan, B.M. Cook, J. Eric Townsend, Michael Jampel, Mark Stalzer,\)](#)
- [Issue 51 \(28 October 1994\)](#)
  - [Stolen account used to send hate mail at Texas A&M \(Bruce Sterling via Prentiss Riddle\)](#)
  - [Orwell was off by 499 channels, and what to do about it \(Phil Agre\)](#)
  - [GRE Computer-Based-Testing scores reconsidered \(Carlos I McEvilly\)](#)
  - [America Online Offlines America \(PGN\)](#)
  - [More on backspace problems \(John Vilkaitis\)](#)
  - [CAPS-LOCK Considered Harmful \(Barton C. Massey\)](#)
  - [Microsoft Natural Keyboard \(Don Alvarez\)](#)
  - [Re: Mailing lists risk critical-mass spamming \(Paul Wallich\)](#)
  - [Re: CNID and screening \(Robert Ellis Smith\)](#)
  - [Drivers license as universal ID? \(John Sullivan\)](#)
- [Issue 52 \(31 October 1994\)](#)
  - [Telephone game glitch \(Julian Meadow\)](#)
  - [The Sinking of the USS Gitarro \(Mike Crawford\)](#)
  - [Re: FEC Voting "Standards" \(Rebecca Mercuri\)](#)
  - [No Real Risks of Seemingly Similar Interfaces \(Roger Carasso\)](#)
  - [There are risks and then there are risks \(Alan Wexelblat\)](#)
  - [Re: Security screen \(Bank fences, power keys, etc.\) \(Frederick B. Cohen\)](#)
  - [Re: More on backspace problems \(Esther Filderman, Russell Stewart\)](#)
  - [CAPS-LOCK \(Paul Barton-Davis, P. Kevin Parker, Rick Cook, Phil Keys, Doug Siebert\)](#)
  - [Re: AOL \(Greg Lindahl, Mike Crawford\)](#)
  - [Re: Half a degree is better than none? \(Curtis Jackson\)](#)
- [Issue 53 \(6 November 1994\)](#)
  - [UK boy cracks S.Korean system \(Mich Kabay\)](#)
  - [CMU blocks access to nasty newsgroups \(Mich Kabay\)](#)
  - [Roll-Over Date Frozen? \(Ed Ravin\)](#)
  - [Followup on Sears captures signatures \(Steve Holzworth\)](#)
  - [Minnesota driver license \(Daniel Frankowski\)](#)
  - [Re: CAPS-LOCK Considered Harmful \(Jim Griffith\)](#)
  - [RFD: sci.engr.safety \(Sethu R Rathinam\)](#)
  - [2nd Conf. on Mathematics of Dependable Systems \(Victoria Stavridou\)](#)
- [Issue 54 \(7 November 1994\)](#)
  - [Fall time change and the usual computer system havoc \(L. Scott Emmons\)](#)
  - [Ottawa Library fines people using unreliable automatic calling system \(Michael Slavitch\)](#)
  - [Tele-Phoney \(John Vilkaitis\)](#)
  - [Risks of assumption \(Tom Swiss\)](#)
  - [Re: CMU blocks access to nasty newsgroups \(Bob Frankston, Arthur Hicks, Jim Huggins, Harry Rockefeller\)](#)
- [Issue 55 \(9 November 1994\)](#)
  - [EMI and construction cranes \(Steve Summit\)](#)
  - [Postscript FAX Security Hole \(Mike Crawford\)](#)
  - [Hardware-borne Trojan Horse programs \(Chris Tate\)](#)
  - [Risks of posting warnings with the wrong time or date \(George Swan\)](#)

[Existential risks of computer systems \(Ian Horswill\)](#)

- [E-Signatures \(Benjamin Wright\)](#)
- [Re: Suitable for whom? \(Jon Green\)](#)
- [PBX at Large? \[Re: Tele-Phoney\] \(Stephen Bogner\)](#)
- [Re: Parental Responsibility \(Mich Kabay\)](#)
- [Re: Ottawa Library fines people ... \(Erik Jacobsen, Daniel P. B. Smith\)](#)

• [Issue 56 \(14 November 1994\)](#)

- [Catalogin' \(Henry Cate\)](#)
- [Worker cleared of deleted planning files \(Vinc Duran\)](#)
- ["Netsafe makes the Internet safe for K-12 schools" \(Forman\)](#)
- [Alberta vote-by-phone fiasco \(Mich Kabay\)](#)
- [Rob Slade's review of Robert Slade's book \(Rob Slade\)](#)
- [Re: EMI and construction cranes \(Michael P. Hartley, Arthur Byrnes\)](#)
- [Re: Ottawa Library fines people ... \(Peter Kaiser, Sean Donelan\)](#)
- [Re: Postscript FAX Security Hole \(Andrew Klossner, Brooks Benson, Ross Oliver, Kevin S. McCurley, Ed Taft, Barry Margolin\)](#)

• [Issue 57 \(22 November 1994\)](#)

- [Cell-phone ergonomics side-effect \(Robert Stanley\)](#)
- [Pentium FDIV bug \(Bill Broadley\)](#)
- [All's Well that Orwells? \(Peter Wayner\)](#)
- [Spell Checker Goes Berserk; Editorial Maimed \(Robert Bane\)](#)
- [Security is not privacy \(Phil Agre\)](#)
- [Authorities Still Investigating Software Theft \(Edupage 15 Nov 1994\)](#)
- [Beware the Calendars \(Pertti Malo\)](#)
- [Re: Parental Responsibility \(Daniel P. Johnson\)](#)
- [Clarifying answers to TEN QUESTIONS PARENTS SHOULD ASK THEIR CHILDREN](#)

• [Issue 58 \(26 November 1994\)](#)

- [Hacker learns intelligence secrets \(Mathew Lodge\) \[See RISKS-16.58BT\]](#)
- [Automated Weather Reports for Pilots \(Tom Keenan\)](#)
- [Extended Phone Failure in Iowa City \(Douglas W. Jones\)](#)
- [Enormous water bills - gigo strikes again \(James M. Politte\)](#)
- [Computer-generated bridge-tournament hands \(G. Gates/M. Brader/PNG\)](#)
- [The PC as a RISC \(how could I resist 8\\*\) \(A. Padgett Peterson\)](#)
- [Problem with 911 service in Philadelphia \(Paul Robinson\)](#)
- [Department store security cameras linked to computer \(David Hembrow\)](#)
- [Children on the Infobahn \(Bradley K. Sherman\)](#)
- [Re: Pentium FDIV bug \(Mike Carlton\)](#)
- [Re: Cell-phone ergonomics side-effect \(Bill Inananen, Paul Robinson\)](#)
- [Re: Anon. on "TEN Q's" \(Mark Seecof PSD x77605\)](#)

• [Issue 59 \(30 November 1994\)](#)

- [The IRS knows "everything about you that we need to know" \(John Sullivan\)](#)
- [RISKS of electronic ticketing on buses \(Rhys Weatherley\)](#)
- [Why You Need a UPS For Your Bread Machine \(Curtis Jackson\)](#)
- [Listserv Loops \(Richard Klau\)](#)
- [NYNEX touts Credit Card authorization over Cell Phones \(Paul Green\)](#)
- [Re: Iowa phone switch \(Matthew Charles Wetmore\)](#)
- [Re: Reasonably Large Water Bill \(L. P. Levine\)](#)
- [Risks on TV: Eye-to-Eye-to-RFI \(Jan I. Wolitzky\)](#)

- [British Telecom "hacker" article was a hack! \(Sidney Markowitz\)](#)
- [The risks of media hack reports \(Rob Slade\)](#)
- [Re: Pentium FDIV bug \(Wilson P. Snyder II, Peter da Silva, Ron Heiby, Dale R. Call, Andy Grove via Richard Wirt\)](#)
- [Issue 60 \(5 December 1994\)](#)
  - [Excel linked spreadsheet bug \(Michael D. Crawford\)](#)
  - [3 hits and you're out? \(SSN use\) \(Geoffrey S Knauth\)](#)
  - [The Economist and E-cash \(Mark Stalzer\)](#)
  - [RISKS of Going to the Movies \(Keith Schengili-Roberts\)](#)
  - [Providing Good Defaults \(and risks of not doing so\) \(Ry Jones\)](#)
  - [The PC as a RISC \(Michael Slavitch\)](#)
  - [HERF Rides Eye To Eye \(Winn Schwartau\)](#)
  - [Interesting product claim \(Mike Kenney\)](#)
  - [Criminals 1, Consumers 0 \(Peter J. Denning\)](#)
  - [Re: Duplicate bridge-tournament hands \(Asya Kamsky\)](#)
  - [Re: Listserv Loops \(Steve Summit, Peter da Silva, Joe A. Dellinger\)](#)
  - ["Tekroids" episode of Tekwar and the perception of viri \(Rob Slade\)](#)
- [Issue 61 \(6 December 1994\)](#)
  - [Lots of Turkeys \(Debora Weber-Wulff\)](#)
  - [Fun with your phone company \(Russell Stewart\)](#)
  - [Pentium + Spell-Checkers \(Paul Fuqua\)](#)
  - [Pentium FDIV bug \(A. Padgett Peterson\)](#)
  - [Re: Interesting product claim \(Mathew Lodge\)](#)
  - [Virus alert virus alert \(Yehuda Berlinger\)](#)
  - [Re: Mailing list problems... \(Errors-To\) \(David Barr\)](#)
  - [Mailing-list deadman switch \(Steve Losen\)](#)
  - ["Applied Cryptography" by Schneier \(Rob Slade\)](#)
- [Issue 62 \(7 December 1994\)](#)
  - [Baby-proof keyboard handling needed \(Amos Shapir\)](#)
  - [Network file race condition \(Andrew Koenig\)](#)
  - [Power failure causes airline check-in chaos \(Fernando Pereira\)](#)
  - [Pepsi promotion misfires - computer error \(John Dalbey\)](#)
  - [Formal verification of the AAMP5 Microprocessor \(John Rushby\)](#)
  - [Re: Formal methods and the Pentium FDIV \(Mark Stalzer\)](#)
  - [Re: Formal verification of INMOS T800 \(Patrick Campbell-Preston, Mathew Lodge\)](#)
  - [Re: Formal methods ... \(Steve Kilbane, Mark Lomas\)](#)
  - [Re: Slade's review of Schneier's "Applied Cryptography" \(Richard Schroepfel\)](#)
  - [Self-extracting emacs elisp code \(David Blob\)](#)
  - [Virus time \(Dwight Silverman, Zygo Blaxell, Reuven Lerner\)](#)
  - [Program Announcement - ISOC 1995 Symp. Netw. & Distr. Sys. Security \(David M. Balenson\)](#)
- [Issue 63 \(9 December 1994\)](#)
  - ["High-Tech Can Hinder Policy Work" \(PGN\)](#)
  - [Laptop proscription \(Bob Morris\)](#)
  - [Our police and media in action \[RF interference\] \(Lynn Gold\)](#)
  - [Digital cash on the web -- comments? \(Justin Wells\)](#)
  - [New printer font: Sloppy Handwriting 14pt \(Norman H. Cohen\)](#)
  - [Multicast backbone blunder \[risks of hidden transmission\] \(Alan Clegg\)](#)
  - [A Question for the Community regarding National Crypto Policy \(Herb Lin\)](#)

- [Problems with compiler optimisation \(Pentium related\) \(Martin Poole\)](#)
- [Risk of \\_not\\_ using floating point..... \(David Leshner\)](#)
- [Re: Formal methods and the Pentium FDIV \(Tim Bradshaw\)](#)
- [It's all my fault, really \[re: Good Times\] \(Martin Minow\)](#)
- [Good Times is a \\*meta\\*virus \(Joe Chew\)](#)
- [Good Times is a Meme \(Keith Henson\)](#)
- [Re: Schneier's book "Applied Cryptography" \(Y. Radai\)](#)
- [Re: Fun with your phone company \(Geoff Kuenning, Russell Stewart\)](#)
- [More on network file race condition \(Andrew Koenig\)](#)
- [Rights and Responsibilities of Participants in Networked Communities \(Herb Lin\)](#)
- [Searching RISKS et al. \(Frederick B. Cohen\)](#)

• [Issue 64 \(10 December 1994\)](#)

- [Re: Interesting product claim \(more Pentium stuff\) \(Paul N. Hilfinger\)](#)
- [Re: Formal Methods ... Intel FDIV bug and verifying FPU's \(Miriam Leeser\)](#)
- [Re: Formal verification of the AAMP5 \(Srivasa\)](#)
- [Re: Multicast backbone blunder \(Derek Atkins\)](#)
- [Re: Digital Cash \(A. Padgett Peterson\)](#)
- [Re: Cellular One roaming in NYC \(Alan Clegg\)](#)
- [Re: "Good Times" virus \(Steve Summit, Susanne Forslev\)](#)
- [Re: Fun with your phone company \(Andy K\)](#)
- [Re: Digital cash on the web \(Hal Pomeranz\)](#)
- [German Telecom: technical risks/crime \(Klaus Brunnstein\)](#)

• [Issue 65 \(15 December 1994\)](#)

- [No, I'm not Newt. \("GingrichN" alias Steve Barr\)](#)
- [Oral Hackers \(Mark Colan via John Markoff\)](#)
- [Technology Under the Weather \(Gordon Symonds\)](#)
- [Wendy's Stock \(Charles R Trew\)](#)
- [Re: Formal Methods and Exhaustive testing \(Tony Lauck\)](#)
- [Re: Mailing-list deadman switch \(John Gardiner Myers\)](#)
- [Re: Self-extracting emacs elisp code \(Morgan Jones\)](#)
- [RISKS demonstrates more RISKS in mailing list software \(Sidney Markowitz\)](#)

• [Issue 66 \(20 December 1994\)](#)

- [Microsoft has no plans to acquire Catholic Church \(from EDUPAGE\)](#)
- [Mistaken Identity \(Tom Knoedler\)](#)
- [Emergency Broadcast System Goes Automatic? \(Darrell F. Oresky\)](#)
- [Brands Burn the Bull's Behind \(Peter Wayner\)](#)
- [Followup to "No I'm not Newt" \(Ted Koppel\)](#)
- [Re: Oral Hackers \(Steve Holzworth\)](#)
- [Re: Technology Under the Weather \(Ross Oliver\)](#)
- [Intel announces new Pentium replacement policy \(Rich Kulawiec\)](#)
- [Pentium bug as data management problem \(Rob Aitken\)](#)
- [Testing the Pentium bug \(Daniel Essin\)](#)
- [Mary Payne and "Good to the last bit!" \(Paul A. Karger\)](#)
- [Pentium FDIV problem - so what's new ? \(A. Padgett Peterson\)](#)
- [Spreadsheet Errors Study \(Ray Panko\)](#)
- [The Status of Disclaimers \(Dick Nickalls\)](#)
- [CFP: New Security Paradigms Workshop \(Catherine A. Meadows\)](#)
- [CFP: Safety and Reliability of Software Based Systems \(Stella Page\)](#)



Issue 67 (23 December 1994)

- [Software glitch snares Social Security Administration \(Mike Manos\)](#)
- [Cancelbot Derails Online Promo \(WSJ via Edupage\)](#)
- [Ben & Jerry's expects first loss \(Arthur D. Flatau\)](#)
- [Proliferation of Cockpit Warning Signals \(David Walter\)](#)
- [Year 2000 date problems already happening now \(Elana\)](#)
- [Re: Prevention of Oral Hacking \(Brad G. Parks\)](#)
- [Re: Pentium FDIV problem - so what's new? \(Mark Brader\)](#)
- [Intelligent Commentator on McNeil-Lehrer \(D.P. Schneider\)](#)
- [Financial Payment Systems \(Jeff Stapleton\)](#)
- [Possible solution to the \(electronic\) meme problem \(Bob Mehlman\)](#)
- [Advertising on the Net \(Mich Kabay\)](#)
- [Risk Takers Among Management \(Tom Kaiser\)](#)
- [Re: Koppel et al. \(Peter da Silva\)](#)
- [Re: Microsoft and the Catholic Church \(John Stevenson\)](#)
- [EDUPAGE on the WWW \(Timothy Hunt\)](#)
- [Public CM WAIS Server to end operation \(WAIS Admin\)](#)
- [Call for Papers and Panels: National Information Systems Security Conference \(Jack Holleran\)](#)

• [Issue 68 \(27 December 1994\)](#)

- [Washington Post flubs stock prices \(William C. Fenner\)](#)
- [Sorcerer's Apprentice Hits Medicare \(Mich Kabay\)](#)
- [\\$25m power bungle: Automation at Australian electricity plant \(Tom Worthington\)](#)
- [Buy a country for \\$1200 \(Amos Shapir\)](#)
- [Re: Mary Payne and "Good to the Last Bit" \(Jim Haynes\)](#)
- [Rate Hike For Universal TouchTone? \(Leonard Erickson\)](#)
- [Re: Year 2000 date problems already happening now \(Scot E. Wilcoxon\)](#)
- [Re: American Scientist article on the year 2000 \(Brian Hayes\)](#)
- [RISKS of guessing at Fair Use \(Mich Kabay\) \[long\]](#)

• [Issue 69 \(3 January 1995\)](#)

- [Gov't Recommends Electronic Copyright Restrictions \(Edupage\)](#)
- [One for the GIFFer \(CompuServe-Unisys GIF Tax Protest\) \(Pat Clawson\)](#)
- [Mail repeatedly returned to sender \(Curtis Keller\)](#)
- [Dates in a 4GL \(name removed\)](#)
- [Dates and Times Not Matching in COBOL \(Fred Ballard\)](#)
- [Testing and the Sources of Dates and Times \(Fred Ballard\)](#)
- [Dates in "Ancient" Systems \(Fred Ballard\)](#)
- [COBOL's Two-Character Year Field \(Fred Ballard\)](#)
- [Last call for papers for COMPASS 95 \(John Rushby\)](#)

• [Issue 70 \(4 January 1995\)](#)

- [GIF, UNISYS, and CompuServe \(Tim Oren\)](#)
- [Datastream may be charged in Jan 1995 \(Mich Kabay\)](#)
- [Common Criteria Draft \(0.9\) on CD-ROM \(Klaus Brunnstein\)](#)
- [Computer Addiction \(Mich Kabay\)](#)
- [Virus Creation Labs \(Andy S. Lopez\)](#)
- [Don't plot murder via cordless phone \(Mich Kabay\)](#)
- [Cell phones in Israeli army \(Mich Kabay\)](#)
- [Dense ordinateurs \(Mark Stalzer\)](#)
- [Re: COBOL's Two-Character Year Field \(Mark Brader, Walter Murray, Paul Robinson\)](#)

• [Issue 71 \(5 January 1995\)](#)

- [A Whole Bunch of Date-Time Stuff \(Fred Ballard, Paul Robinson, John Cavanaugh, Dave Moore, Chuck Karish, Jerry Leichter, Richard Schroepfel, Craig Everhart, Erann Gat, Wayne Hayes, Walt Farrell, Stanley F. Quayle, Marc Horowitz, Peter Capek, Lars Wirzenius, Phil Rose, David Jones, Jonathan I. Kamens, Andrew W Kowalczyk, Barry Jaspan, Joe Morris, Lord Wodehouse\)](#)

• [Issue 72 \(6 January 1995\)](#)

- [Computing error at Fidelity's Magellan fund \(Kathy Godfrey, Arthur Flatau\)](#)
- [Phone system problems in Santa Fe \(Bruce Wampler\)](#)
- [LZW/GIF flap on RISKS \(Tim Oren\)](#)
- [Re: CompuServe-Unisys GIF Tax Protest \(Peter Bishop\)](#)
- [Software math errors \(Chris Phoenix\)](#)
- [Rutherford Effect: term for particular class of failures \(Bill Thomas\)](#)
- [Re: Cancelbot Derails Online Promo \(Andrew Haley\)](#)
- [Re: Soldiers and Cellular Telephones \(Linden B. Sisk\)](#)
- [Re: Computer Addiction \(Mary Shafer, John C. Rivard, Steven D. Brewer\)](#)
- [Re: Date and Time \(Leslie Lamport\)](#)

• [Issue 73 \(6 January 1995\)](#)

- [My life as an international arms courier \[longish, but good\] \(Matt Blaze\)](#)
- [Work monitoring \(Phil Agre\)](#)
- [GRE by computer, the sequel \(Cris Pedregal Martin\)](#)
- [More on "Cell phones in Israeli army" \(Heinz Wrobel\)](#)
- [Re: Adopting Programming Improvements \(Douglas W. Jones\)](#)
- [Re: CompuServe-Unisys GIF Tax Protest \(Kenneth Albanowski\)](#)

• [Issue 74 \(8 January 1995\)](#)

- [Software sensitive to cold? \(Karol Fruehauf\)](#)
- [Revision Level, What Does It Mean???](#) (Mark Thorson)
- [Re: Cancelmoose, WSJ word usage, and vigilantism \(Steward\)](#)
- [Re: ETS Electronic Testing \(Simson L. Garfinkel\)](#)
- [Re: Fidelity error \(Barry Margolin, Floyd Ferguson\)](#)
- [Re: My life as an International Arms Courier \(A. Padgett Peterson\)](#)
- [Re: Israeli army, cellular phones, pizza \(Michael Dahan, David Wadsworth\)](#)
- [Re: GIF \(David Winfrey, Simson L. Garfinkel, John Mainwaring, Garrett Nievin\)](#)
- [Re: Date/Time \(Steve Sapovits, Mark Brader, Erann Gat\)](#)

• [Issue 75 \(19 January 1995\)](#)

- [Airline schedules in local time \(Matthew Kwan\)](#)
- [Car-radio security code nuisance \(Daniel P. B. Smith\)](#)
- [Bugs in Digital RAID Storage Subsystems \(Andy Ram\)](#)
- [Maryland Emission testing \(Paul Peters\)](#)
- [Computers in nuclear plant \(WB Whaley via Jonathan\\_Welch\)](#)
- [Anik E2 redux \(Luis Fernandes\)](#)
- [Shaky testing \(Mark Stalzer\)](#)
- [Re: Midnight Batch Run Bites \(Paul Robinson\)](#)
- [New Risk from the WWW \(John MacInty\)](#)
- [RISKS on the World Wide Web \(Lindsay F. Marshall\)](#)
- [Criminal hacker arrested in Winnipeg \(Mich Kabay\)](#)
- [Phone Phreaking Explored \(Steve O'Keefe\)](#)

- [International Cryptography Institute 1995 \(Dorothy Denning\)](#)
- [12th Annual ISSA Conference & Exposition \(Jack Holleran\)](#)
- [Issue 76 \(24 January 1995\)](#)
  - [CERT Advisory CA-95:01.IP.spoofing.attacks.and.hijacked.terminal.connections](#)
  - [More on the new CERT advisory \(Steve Bellovin\)](#)
  - [Bouncemail \(Phil Agre\)](#)
  - [Another post office stamp machine story \(they \\*almost\\* got it right!\) \(Jonathan I. Kamens\)](#)
- [Issue 77 \(30 January 1995\)](#)
  - [UK Cabinet Secret on National ID Card Found in Surplus Store \(Li Gong\)](#)
  - [Perils of Call Forwarding \(Stephen Thomas, Quentin Fennessy\)](#)
  - [Deutsche Telekom offices searched \(Mich Kabay\)](#)
  - [My life as "uucp@aol.com" \(Uucp@aol.com\)](#)
  - [Risks of reusing accounts \(Charlie Shub\)](#)
  - [From the cat file \(Andrew Koenig\)](#)
  - [Another stamp machine story \(John Kriens\)](#)
  - [The risks of Risks \(Fritz Knabe, Haritini Kanthou\)](#)
  - [ACSAC '95 Call for Papers and Participation \(Marshall D Abrams\)](#)
- [Issue 78 \(2 February 1995\)](#)
  - [Novel form of interference \(Mich Kabay\)](#)
  - [Attack on glasfibre cables causes Lufthansa delays \(Klaus Brunnstein\)](#)
  - [Anonymous ?? Survey \(Dave Moore\)](#)
  - [Deep Faults with NYNEX default? \(Edward P Ravin\)](#)
  - [Nynex glitch lets Call ID work even if blocked \(Dick Mills\)](#)
  - ["Protect Your Privacy" by Stallings \(Rob Slade\)](#)
  - [Identification technologies \(Phil Agre\)](#)
  - [Automatic file downloads in Seyon \(Bruce E. Wampler\)](#)
  - [Announcement of new mailing list on ethical issues \(Bashir Jiwani\)](#)
  - [CFP: 3rd International Workshop on Feature Interactions \(Nancy Griffith\)](#)
- [Issue 79 \(8 February 1995\)](#)
  - [Proposed Virginia law on self-disabling software \(Jeremy Epstein\)](#)
  - [Cellular Phone Security \(Chip Seymour\)](#)
  - [Japanese bank workers steal 140 million yen by PC \(Mich Kabay\)](#)
  - [Road pricing in Singapore \(Phil Agre\)](#)
  - [InfoWar Level II in Miami \(Mich Kabay\)](#)
  - [Phone switch bug causes alarm among NM officials \(Mich Kabay\)](#)
  - [Telephone RISKS \(Ry Jones\)](#)
  - [Risks in computerized cockpits \(Rob Horn\)](#)
  - [Concatenating phrases produces confusing results in bank responses \(Daniel P. B. Smith\)](#)
  - [More from the cat file \(Phil\)](#)
  - [1996 ACM COCCS call for papers \(R.F. Graveman\)](#)
- [Issue 80 \(13 February 1995\)](#)
  - [German Railway Wage Woes \(Debora Weber-Wulff\)](#)
  - [Risks of modern newspaper article composing or editing? \(Thomas A. Russ\)](#)
  - [Portuguese E-cash \(Kent Borg\)](#)
  - [Long-Distance Debit Cards \(Len Bauer\)](#)
  - [Risks of remote printing through a network \(Skyrunner\)](#)

[Risks of Third-Party-Billed Calls \(Micah Altman\)](#)

- [Re: Info War II in Miami \(Jim Huggins\)](#)
- [Re: Road pricing in Singapore \(Mats Ohlin\)](#)
- [New service for Risks Forum members \(Frederick B. Cohen\)](#)
- [Security and Privacy Program \(Catherine A. Meadows\)](#)

• [Issue 81 \(14 February 1995\)](#)

- [Stolen ATM Card nets \\$346,770 \(David Tarabar, Jerome Whittle\)](#)
- [Sweden-Pedophiles-Internet \(Mich Kabay\)](#)
- [A RISKy place on the Web \(Stephen R. Savitzky\)](#)
- [Rumors in Cyberspace \(Adam Shostack\)](#)
- [Priests told to keep cell phones out of confession \(Mich Kabay\)](#)
- [Cellular phones \(Chaim Seymour\)](#)
- [Web Page copying reader's system information \(Brian Leibowitz\)](#)
- [RISKS of posting to newsgroups \(A. Padgett Peterson\)](#)
- [Good Pentium Followup \(Martin Minow\)](#)
- [Invisible blue zone \(Jeff Jonas\)](#)
- [RISKS of third-party-billed calls not uncommon \(Tony Yip\)](#)
- [Self-disabling software \(Jerry Leichter, Bob Brown\)](#)
- [What "RISKS of Third-Party-Billed Calls"? \(Gary Beckmann, PGN, GB\)](#)
- [Re: attack scanning \(Stephen Kelley, Frederick B. Cohen\)](#)

• [Issue 82 \(17 February 1995\)](#)

- [New York Parking Meters In Violation of Federal Law \(A. Padgett Peterson\)](#)
- [Big Brother in the Big House \(Peter Wayner\)](#)
- [Computer aids in predicting death \(Lauren Wiener\)](#)
- [Hacker Mitnick arrested \(Jim Griffith\)](#)
- [Computer addiction and the 6 O'Clock News \(Rob Slade\)](#)
- [New Area Codes & PBX Programs \(Mich Kabay\)](#)
- [E-mail risks \(Vincent Gogan\)](#)
- [Re: Self-disabling software \(Bruce Johnson\)](#)
- [Re: Invisible blue zone \(David Stodolsky\)](#)
- [CERT Advisory CA-95:04.NCSA.http.daemon.for.unix.vulnerability](#)

• [Issue 83 \(21 February 1995\)](#)

- [Denver's Computerized Baggage System Finally Works \(NYT via Edupage\)](#)
- [Cyberbandits in Europe \(CommunicationsWeek via Edupage\)](#)
- [Perfect \(?\) Office Bug can cause harm \(Gary Gillard\)](#)
- [I can't help but say more about this addiction thing. \(Peter Ladkin\)](#)
- [Sparc10 keyboards and resetting the CPU \(Carlos M. Puchol\)](#)
- [Married by computer \(Scott Sterner\)](#)
- [UPS not quite so uninterruptable after all \(Mark Frank via Jerry Leichter\)](#)
- [Risks of generalized designs \(Jim Griffith\)](#)
- [Stolen ATM Card nets \\$346,770 \(Rich Wells\)](#)
- [Re: JUDGES-L \(Peter da Silva\)](#)
- ["PGP: Pretty Good Privacy" by Garfinkel \(Rob Slade\)](#)
- [The Coming Plague \(Peter Wayner\)](#)
- [Scan results \(Frederick B. Cohen\)](#)
- [Symposium on medical records \(Phil Agre\)](#)
- [NCSA Conference: Security on the I-Way \(Mich Kabay\)](#)

• [Issue 84 \(24 February 1995\)](#)

- [Old manuals, new features = security holes \(Christopher Klaus\)](#)
- [Software Firm is Victim of Virus \(Timothy Hunt\)](#)
- [National Cryptography Policy: Call for Input and Public Meeting \(Herb Lin\)](#)
- [CapAccess compromised \(Mich Kabay\)](#)
- [Major file corruptions \(Charles M. Preston\)](#)
- [Compact fluorescent lights \(Edward S Suffern\)](#)
- [EU office distributes Galicia virus \(Klaus Brunnstein\)](#)
- [Call for Papers, Risks in End-User Computing, HICSS '86 \(Ray Panko\)](#)

• [Issue 85 \(24 February 1995\)](#)

- [Another police sting based on a freebie video offer \(Clive D.W. Feather\)](#)
- [More Security Problems on the Internet \(Edupage\)](#)
- ["E-Mail Security" by Schneier \(Rob Slade\)](#)
- [\\*BUGS in Writing: \[...\] Debugging Your Prose\\*, by Lyn Dupre \(Bob Donegan\)](#)
- [Re: CERT Advisory CA-95:04.NCSA.http\[...\]vulnerability \(Timothy Hunt\)](#)
- [Re: Perfect \(?\) Office Bug can cause harm \(Keith Schengili-Roberts, \(Jerome Whittle\)](#)
- [Re: Sparc10 keyboards and resetting the CPU \(Tarl Neustaedter\)](#)
- [Re: Major file corruptions \(George C. Kaplan, George Buckner, Kenneth Albanowski\)](#)
- [Re: JUDGES-L \(David Stodolsky\)](#)

• [Issue 86 \(3 March 1995\)](#)

- [What Goes Intuit May Not Come Out the Same Taxwise \(PGN\)](#)
- [Apple Settles RSI Claim \(Edupage\)](#)
- [Apple Settlement Due to Lawyer Error \(Edupage\)](#)
- [More Security Problems on the Internet \(Edupage\)](#)
- [Encryption Lawsuit Filed in California \(Edupage\)](#)
- [Anti-Cyberporn \[Exon\] Bill Introduced \(Edupage\)](#)
- [Home Gambling Network \(Mich Kabay\)](#)
- [Losing your Marbles and your Barings \(Peter Wayner\)](#)
- [UK National Audit Office report on computer misuse in government \(Brian Randell\)](#)
- [Re: Perfect \(?\) Office Bug ... \(Matt Cockerill\)](#)
- [Blaming the victim for money stolen with lost ATM card \(Elizabeth Schwartz\)](#)
- [Sick Medicare Scanner \(Judith Seeger\)](#)
- [Interstate Panopticon \(Phil Agre\)](#)
- [Risks of living on the left side of the continent \(Rob Slade\)](#)

• [Issue 87 \(7 March 1995\)](#)

- [Authentication: \(1\) Vienna Marathon 1995; \(2\) Lotus Notes \(Li Gong\)](#)
- [Sexy photos just computer glitch \(Louis Todd Heberlein\)](#)
- [The source of semantic content \(Erann Gat\)](#)
- [Government of Singapore \(Robert Ashcroft\)](#)
- [Happy Michelangelo's Birthday \(PGN\)](#)
- [Microsoft and Lotus spreadsheet errors \(Timothy Hunt\)](#)
- [Spreadsheet Errors working paper available \(Ray Panko\)](#)
- [6-cent T-shirts \(Jeremy Stieglitz\)](#)
- [Risk system comes too late to prevent Barings' collapse \(Jeremy Stieglitz\)](#)
- [Securities \(Bob Frankston\)](#)
- [Barings: Greenspan quote \(Frank E. Carey\)](#)
- [Re: Compact Fluorescent Lights \(Mike Farringdon, Carl Maniscalco, Osma Ahvenlampi\)](#)

• [Issue 88 \(8 March 1995\)](#)

- [Caller ID Ghosts \(Jim Huggins\)](#)

- [Interesting cellular news from Pakistan \(Abhijit Dutta via Ben Burch\)](#)
- [Re: Microsoft and Lotus spreadsheet errors \(Barry Margolin\)](#)
- [Re: Confused remotes \(Philip H. Smith III\)](#)
- [Re: The source of semantic content \(Steven Tepper, A. Padgett Peterson, Barry Margolin, Jeremy Epstein, Jon Krueger, Tim Kolar, David Harpe\)](#)
- [Re: Sparc10 keyboards and resetting the CPU \(A. Harry Williams, Simson L. Garfinkel, Ed Bruce, Mark Stalzer, David Honig\)](#)
  
- [Issue 89 \(10 March 1995\)](#)
  - [Celsius-to-Fahrenheit conversion risk \(Michael Tobis\)](#)
  - [Two on net porn charges \(Jonathan Bowen\)](#)
  - [Re: 6-cent T-shirts \(Evelyn C. Leeper\)](#)
  - [Re: Remote-Control Risks \(Mike Cavanagh\)](#)
  - [Consumer electronic problems \(Les Hatton\)](#)
  - [Can Pakistan Eavesdrop in America? \(Peter Wayner\)](#)
  - [Sow's Ear from a Purse \(Joseph H Presley\)](#)
  - [Resetting BSD/OS is easy as resetting MS-DOS \(Re: Sparc10\) \(Kenji Rikitake\)](#)
  - [Re: Microsoft and Lotus spreadsheet errors \(Tony Lauck\)](#)
  - [Loss of one of the X-31 research airplanes \(Peter Ladkin\)](#)
  - [PGP Moose: moderator authentication and antispamming tools \(Greg Rose\)](#)
  
- [Issue 90 \(14 March 1995\)](#)
  - [E-Mail Apology from Prodigy \(Edupage\)](#)
  - [Kiosk prototype fails to deliver in trial run \(Bob Frankston\)](#)
  - [Automatic return fire \(Michael J Zehr\)](#)
  - [Internet providers raided \(Kevin Yeung\)](#)
  - [Internet-Finland Privacy \(Lars Arnkil via Bruce Baker\)](#)
  - [Re: Consumer Electronics Problems \(Willie Smith\)](#)
  - [Mitnick Stole "SATAN" Security Software \(Edupage\)](#)
  - [Re: PGP Moose \(Jerry Leichter\)](#)
  - [Re: Microsoft and Lotus spreadsheet errors \(Steve Bellovin, Ken Tindell\)](#)
  - [The source of semantic content: followup \(Erann Gat\)](#)
  - [Re: Can Pakistan Eavesdrop in America? \(Laurence R. Brothers, John R. Moore, Marc Horowitz, P.vanMossel\)](#)
  
- [Issue 91 \(14 March 1995\)](#)
  - [Re: PGP Moose -- Not just the headers! \(William Oswald\)](#)
  - [Re: Automatic return fire \(Joseph Chew\)](#)
  - [Scientology Blackmail Risk \(John V. Vilkaitis\)](#)
  - [Viral morality \(Rob Slade\) \[LONG\]](#)
  
- [Issue 92 \(16 March 1995\)](#)
  - [Health card rips off ATM for \\$100,000 \(Roy Beimuts\)](#)
  - [A340 shenanigans \(Les Hatton\)](#)
  - [Mistake of platform-specific instructions \(Stanton McCandlish\)](#)
  - [The Manchurian Printer \(Simson L. Garfinkel\) \[longish\]](#)
  - [Re: Scientology Blackmail Risk \(Lance A. Brown, Jon Green\)](#)
  - [Re: Internet-Finland Privacy \(Michael Jennings\)](#)
  - [Jumping to conclusions? \(Lifeguard\) \(Peter da Silva\)](#)
  - [Re: Microsoft and Lotus spreadsheet errors \(Bear Giles\)](#)
  - [Society and the Future of Computing \(Phil Agre\)](#)
  
- [Issue 93 \(20 March 1995\)](#)

- [About the "Altona Railway software glitch" \(Klaus Brunnstein\)](#)
- [Credit-Card Fraud \(NYT via Edupage\)](#)
- [Keeping buses on time plus a little eavesdropping \(Mark Kruse\)](#)
- [Does Internet threaten civilization? \(Dick Mills\)](#)
- [Latent risks of cost-benefit analysis \(Phil Brown\)](#)
- [Re: Internet-Finland Privacy \(Peter Kaiser\)](#)
- [Risks of doing date arithmetic early in the year without FP \(Peter Ludemann\)](#)
- [Phone companies with wrong 555-1212 databases \(Frederick B. Cohen\)](#)
- [Re: The Manchurian Printer & Prodigy Spies on Users \(Frank C Ferguson\)](#)
- [Software System Safety Class \(Nancy Leveson\)](#)
- [First Bank of Internet \(FBOI\) Opens \(Vinn Beigh\)](#)

• [Issue 94 \(21 March 1995\)](#)

- [Deutsche Bahnfires continue \(Debora Weber-Wulff\)](#)
- [Canadian Government Almost Spreads Virus \(Colin Perkel\)](#)
- [Too high-tech... \(Bob Wilson\)](#)
- [Reevaluating Our Trust in Computers \(Cynthia P. Klumpp\)](#)
- [Internet: Threat or menace? \(Eric Raymond\)](#)
- [Re: Latent risks of cost-benefit analysis \(Steve Smith, David Chase\)](#)
- [Re: The Prodigious Manchurian \(Rob Slade, Bear Giles\)](#)
- [Re: First "Bank" of Internet \(Steve Holzworth, Rob Slade, Willie Smith\)](#)
- [Information Security Tutorials \(Sushil Jajodia\)](#)
- [AMAST'95 Preliminary Programme available \(Pippo Scollo\)](#)

• [Issue 95 \(22 March 1995\)](#)

- [UK National Lottery \[scratch as scratch can?\] \(Pete\)](#)
- [Re: Too high-tech... \(Steven Tepper\)](#)
- [Re: Internet: Threat or menace? \(Dave Parnas\)](#)
- [Risks of one-to-many communication \(Vicki Rosenzweig\)](#)
- [Latent risks of cost-benefit analysis \(Ron Ragsdale\)](#)
- [Re: Risks of doing date arithmetic early in the year... \(Andrew Marc Greene\)](#)
- [Re: Prodigy \(Craig Dickson\)](#)
- [Re: PGP Moose \(Jerry Leichter\)](#)
- [FBOI Apology \(fwd\) \(FBOI via Willie Smith\)](#)
- [Re: FBOI \(Mike Perry, Jonathon Tidswell\)](#)
- [Re: NCSA httpd security hole \(Timothy Hunt\)](#)
- [Citizen's Advice on the Internet \(Phil Overy\)](#)
- [Re: FBOI and \\*Security Reviews\\* \(Ross Anderson\)](#)

• [Issue 96 \(22 March 1995\)](#)

- [Dan Farmer, SATAN and SGI \(PGN\)](#)
- [Triggerfish Cellular Phone Tap \(John R Henry\)](#)
- [RISKS of non-standard interfaces \(Ry Jones\)](#)
- [Pilot not informed of plane's intended destination \(Mike Crawford\)](#)
- [Snake Oil and Grantsmanship \(Douglas W. Jones\)](#)
- [Profiting from misdialed numbers \(Matt Weatherford\)](#)
- [Re: A340 incident at Heathrow \(Peter Ladkin, John Rushby\)](#)
- [Re: FBOI \(Mike Crawford\)](#)



Search RISKS using [swish-e](#)

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

# THE RISKS DIGEST

## Forum On Risks To The Public In Computers And Related Systems

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

Search RISKS using [swish-e](#)

The RISKS Forum is a moderated digest. Its USENET equivalent is [comp.risks](#). ([Google archive](#))

- [Vol 26 Issue 47 \(Monday 6 June 2011\)](#) <= Latest Issue
- [Vol 26 Issue 46 \(Saturday 4 June 2011\)](#)
- [Vol 26 Issue 45 \(Tuesday 24 May 2011\)](#)
- [News about the RISKS web pages](#)
- [Subscriptions, contributions and archives](#)

### Feeds

[RSS 1.0 \(full text\)](#)

[RSS 2.0 \(full text\)](#)

[ATOM \(full text\)](#)

[RDF feed](#)

[WAP \(latest issue\)](#)

[Simplified \(latest issue\)](#)

---

[Smartphone \(latest issue\)](#)

[Under Development!!](#)

You can also monitor RISKS at [Freshnews](#), [Daily Rotation](#) and probably other places too.

Please [report](#) any website or feed problems you find to the [website maintainer](#). Report issues with the digest content to the moderator.

### Selectors for locating a particular issue from a volume

Volume number:            Issue Number:

### Volume Index

The dates and counts do not include the index issues for each volume.

Index to the RISKS Digest

Volume Number	Date Range	Number of Issues
<a href="#">Volume 1</a>	<a href="#">1 Aug 1985 - 31 Jan 1986</a>	45 issues
<a href="#">Volume 2</a>	<a href="#">1 Feb 1986 - 30 May 1986</a>	56 issues
<a href="#">Volume 3</a>	<a href="#">4 Jun 1986 - 30 Oct 1986</a>	91 issues
<a href="#">Volume 4</a>	<a href="#">2 Nov 1986 - 6 Jun 1987</a>	96 issues
<a href="#">Volume 5</a>	<a href="#">7 Jun 1987 - 31 Dec 1987</a>	84 issues

<a href="#">Volume 6</a>	<a href="#">2 Jan 1988 - 31 May 1988</a>	94 issues
<a href="#">Volume 7</a>	<a href="#">1 Jun 1988 - 22 Dec 1988</a>	98 issues
<a href="#">Volume 8</a>	<a href="#">4 Jan 1989 - 29 Jun 1989</a>	87 issues
<a href="#">Volume 9</a>	<a href="#">6 Jul 1989 - 30 May 1990</a>	97 issues
<a href="#">Volume 10</a>	<a href="#">1 Jun 1990 - 31 Jan 1991</a>	85 issues
<a href="#">Volume 11</a>	<a href="#">4 Feb 1991 - 28 Jun 1991</a>	95 issues
<a href="#">Volume 12</a>	<a href="#">1 Jul 1991 - 24 Dec 1991</a>	71 issues
<a href="#">Volume 13</a>	<a href="#">6 Jan 1992 - 2 Nov 1992</a>	89 issues
<a href="#">Volume 14</a>	<a href="#">4 Nov 1992 - 27 Aug 1993</a>	89 issues
<a href="#">Volume 15</a>	<a href="#">2 Sep 1993 - 29 Apr 1994</a>	81 issues
<a href="#">Volume 16</a>	<a href="#">2 May 1994 - 22 Mar 1995</a>	96 issues
<a href="#">Volume 17</a>	<a href="#">27 Mar 1995 - 1 Apr 1996</a>	96 issues
<a href="#">Volume 18</a>	<a href="#">5 Apr 1996 - 31 Mar 1997</a>	96 issues
<a href="#">Volume 19</a>	<a href="#">1 Apr 1997 - 23 Sep 1998</a>	97 issues
<a href="#">Volume 20</a>	<a href="#">1 Oct 1998 - 31 Jul 2000</a>	98 issues
<a href="#">Volume 21</a>	<a href="#">15 Aug 2000 - 29 Mar 2002</a>	98 issues
<a href="#">Volume 22</a>	<a href="#">1 Apr 2002 - 27 Oct 2003</a>	98 issues
<a href="#">Volume 23</a>	<a href="#">7 Nov 2003 - 2 Aug 2005</a>	96 issues
<a href="#">Volume 24</a>	<a href="#">10 Aug 2005 - 30 Dec 2007</a>	93 issues
<a href="#">Volume 25</a>	<a href="#">7 Jan 2008 - 1 Apr 2010</a>	98 issues
<a href="#">Volume 26</a>	<a href="#">8 Apr 2010 - 6 Jun 2011</a>	47 issues



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 16: Issue 1**

**Monday 2 May 1994**

## Contents

- [Vandalism disrupts service at UK University](#)  
[Peter Ladkin](#)
- [Subjectively, it's eerie](#)  
[Phil Agre](#)
- [Miniature cameras on Sacramento-area alarm systems](#)  
[Dan Zerkle](#)
- [DIA delays due to programmers, mayor implies](#)  
[Bear Giles \[2\]](#)
- [Re: DMV Computer upgrade goes awry...](#)  
[Shel Kaphan](#)
- [Re: Unusual Newspaper Error](#)  
[Stewart Rowe](#)  
[David Wittenberg](#)  
[Daniel B. Dobkin](#)
- [Re: MIT student arrested for BBS ...](#)  
[Fredrick B. Cohen](#)
- ["The Streetwise Guide to PCs" by Jerome/Taylor](#)  
[Rob Slade](#)
- [Computer-Aided Verification 94 Conference Announcement](#)  
[David Dill](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Vandalism disrupts service at UK University

*Peter Ladkin* <[Peter.Ladkin@loria.fr](mailto:Peter.Ladkin@loria.fr)>

*Sat, 30 Apr 1994 11:35:23 +0200*

Early on Monday 18th April, a vandal exploiting a not-known security hole started disrupting services and corrupting files at Stirling University in the UK. Stirling University is a SuperJanet site, with a microwave link to Edinburgh. The entire site was affected. I was working intensively with a colleague in Stirling at the time. My experience was that the site was unreachable by Internet services for over 24 hours, and that telnet and ftp services were seriously degraded for 3-5 days. Email service was unavailable

for 2-3 days. It would be conservative to estimate that at least 6 person-weeks of expert time were required to discover and repair the damage. I cannot assess the amount of disruption, not only in terms of work time lost but in terms of reorganising one's planned work time, to users of the systems. It must be considerable, if my experience is any guide.

Someone believed to be the vandal, and a member of the University, was identified I believe on Tuesday 19th. I understand he is no longer on University premises, and the University authorities are considering what further action is required. Because of possible legal proceedings, I'll identify my sources of information and exactly what they said in an Appendix.

In a separate submission, I'll offer a few comments of my own on this incident. I had been a member of the Stirling Department of Computer Science and Mathematics for 18 months up until April 94. Knowing that it was an 'inside job', I queried a colleague as to whether more than one member of the department knew the suspect. The answer was yes. >From this information alone, I was able to identify my own suspect X, and ask whether X was any longer around, or whether anyone expected to see him back. The answer confirms to me with high probability that X is the suspect. (I note that nothing has been proved concerning X.)

If X did it, the process by which he came to it would be interesting, both for psychologists and for those who wish to secure their systems against corruption. [I'll drop the conditional and use the indicative, for stylistic not semantic reasons. Readers should reinsert it, since nothing has been proven against X.] And it provides a cautionary tale that shows how vulnerable we all are. After the fact, I can guess who X is with a bare minimum of hints. However, before the act, only X's therapist, if he had one, is likely to suspect that anything may happen. And of course, in any case if he had been able to communicate his feelings to anyone sympathetic or understanding - but otherwise uninvolved - the chances are that the incident would not have happened. It's a very self-destructive act. Playing with computers is an important part of X's life, and indications are that he was good at it and liked it. Now, no one but no one is likely to offer him a job doing it. A major part of his life is in ruins. Despite all else, I can feel some sympathy for what must be his current plight. It isn't even zero-sum. Everyone has lost in a big way. [And it must be far, far worse for him if he's not the culprit!]

Peter Ladkin

Appendix: Sources of Information.

I talked to the Senior Computer Officer of the Department of Computing Science and Mathematics by phone on Tuesday 19th. He confirmed that the Stirling site was off the Internet on Monday, that disruption started early Monday morning, luckily just after Computer Science had made backups of their subnetwork of systems. He confirmed an estimate of at least 3 person-weeks of the DCSM staff, and suggested at least an equal number for Computing Services staff, to identify damage and effect some repair. He said that the disruption was caused by someone exploiting a not-unknown system weakness, and that a suspect who was a member of the University had been identified and removed from the site. He identified the gender of the suspect by his choice of pronoun. He gave no

further information, citing administrative and legal responsibility.

I talked to one member of the Department of Computing Science and Mathematics, who confirmed that a suspect was known to more than one member of the Department, and that he (male) was identified through a piece of 'luck'.

Peter Ladkin, CRIN-CNRS & INRIA Lorraine BP 239 54506 VANDOEUVRE-LES-NANCY FRANCE (+33) 83 59 20 14 (Msgs 20 00) Peter.Ladkin@loria.fr

---

## Subjectively, it's eerie

*Phil Agre <pagre@weber.ucsd.edu>  
Sun, 1 May 1994 13:05:12 -0700*

,In the 5/1/94 Sunday New York Times, the Business section includes one of those nice experiential articles about new technology, in this case a Ford with DSP circuitry in it that makes the inside of the car sound like a cathedral (concert hall, night club, opera house, stadium, etc). The full reference is:

Hans Fantel, A recital hall on wheels, New York Times, 1 May 1994, Business section page 7.

Here is a brief quotation:

"Subjectively it's eerie. Sitting inside this hologram, I felt bathed in music, virtually forgetting where I was. Engine and traffic noises faded from awareness. The car somehow seemed like a space capsule. I was gliding along, swathed in Puccini, while outside the harried scenes of Manhattan rolled by like a silent movie."

On the same page is another article about plans by the US government and Rockwell International for "intelligent vehicle highway systems".

Phil Agre, UCSD

---

## Miniature cameras on Sacramento-area alarm systems

*Dan Zerkle <zerkle@cs.ucdavis.edu>  
Sun, 1 May 94 00:35:54 PDT*

The April 24 edition of the Sacramento Bee (page B5, staff writer) publishes a story about a miniature camera that will "revolutionize" the Sacramento area security alarm industry.

Some important points of the article:

A miniature "camera on a chip," about the size of a postage stamp, is attached to an alarm system. When the alarm is tripped, the camera sends four pictures back to the the alarm monitoring service. Presumably, the pictures are digitally encoded and sent through some sort of modem.

The first picture arrives twenty seconds after the alarm is tripped.

Police are particularly excited about this because it will let them use the pictures to detect false alarms.

The system is intended to be used in a wide variety of businesses, and also residencies.

The photographs will be usable as evidence in court against robbers and burglars.

The camera is so small that it can be easily hidden anywhere. It is also inexpensive -- one third to one half the cost of a closed-circuit video camera.

"The pictures come out pretty clear," according to a police communications supervisor.

The device was developed by Automated Security Holdings in England, licensed to TVX Inc. of Broomfield, Colorado, and test-marketed by Roseville Telephone (near Sacramento).

.....

The risks? Many. Here are a few:

It only takes four pictures, which are presumably freeze-frames. A burglar may trip the alarm yet not be photographed (perhaps going by the camera between pictures). The alarm agency or police may see that the pictures don't show anything, and thus believe that it is a false alarm. They may then decline to respond or may respond inappropriately.

This is a perfect spy device, and will be easily available at a price less than a simple video camera. The potential abuses of such a device are many, but employee monitoring is one. Your boss could point one at your work area to watch you, and you'd never know. A hidden security camera is really a spy camera, equivalent to an audio bug. In fact, the article mentions that it could be used against internal thefts.

If someone says the pictures are "pretty" clear, that means that they aren't entirely clear. If police trust pictures too much, the potential is there for police to misidentify a suspect (based on a picture), but firmly believe that they are right. This is especially likely if the pictures are monochrome. As the first picture arrives in twenty seconds, they are certainly low resolution (consider connection time for the modems).

A camera in my residence? What if it starts sending pictures back to the alarm company at random? What if some voyeur at the alarm company figures out how to get pictures whenever he wants? Most people who have these alarm systems will not know how they work, so they won't be aware of these risks.

A remote digital camera would be useful in some situations. For instance, it

could send pictures of a bank robber holding a gun, so that the police could more easily identify a suspect. The main risk here is (again) too much trust in the technology. Also, there's not a great need to hide a security camera. You generally want potential crooks to know they're being monitored.

Dan Zerkle zerkle@cs.ucdavis.edu

---

## DIA delays due to programmers, mayor implies

*Bear Giles <bear@tiger.cs.Colorado.EDU>  
Sat, 30 Apr 1994 11:21:16 -0600*

The Saturday, 30 April 1994 issue of the *\_Rocky Mountain News\_* (and probably every other paper within 500 miles) had a massive front page story on the utter failure of the luggage system during tests at Pena International. (IMHO these design failures have reached the point where the current Secretary of Transportation needs to answer some questions.)

Apparently, Mayor Webb is considering an *\*indefinite\** delay, at the request of the hub airlines United and Continental.

Of interest to comp.risks readers are the following paragraphs from the article:

Webb, who has regretted setting -- and missing -- other airport deadlines during his three years in office, said other one isn't a good idea.

Although deadlines motivate some people, they don't work well for computer programmers who must fix what is wrong at DIA, he said.

Strictly speaking, this is probably true. The incredible design flaws (e.g., designing the airport to use an untested luggage transportation system with *\*no\** fallback capability) and construction snafus (e.g., the "messy" power system despite contractual agreements to provide a "clean" power feed, leading to significant delays while BAE scrambled to find power filtering equipment) leave software as the only practical way of getting out of this mess.

And very few experienced programmers would tolerate the same people who have screwed up things to this extent trying to impose an unrealistic deadline on them now...

... but Joan Q Public will undoubtedly read this as yet another example of computer software screwing up the system. It's the 90's -- your dog didn't eat your homework; the software garbled it!

It's almost enough for me to move 30 miles so I can vote against Webb in the next election. :-)

Bear Giles bear@cs.colorado.edu/fsl.noaa.gov

---

## More on DIA fiasco

*Bear Giles <bear@tiger.cs.Colorado.EDU>*

*Sat, 30 Apr 1994 15:33:11 -0600*

Reading later articles (there were several pages of DIA coverage today, not just Mayor Webb's flamebait), it appears the scapegoat du jour for the DIA delay is the "buggy software" that reads the bar codes in the luggage and determines where to send the cart.

A fascinating (for the wrong reasons) newspaper article included such interesting factoids as:

Software -- essentially the brains of a computer system -- is so complex that a misplaced comma or an omitted semicolon can crash entire computer systems.

Even the smallest error can cause a ripple effect that turns into a tidal wave of the kind that swamped AT&T's main switching system several years ago and shut down nearly 90% of the phone company's domestic long-distance operations for hours.

Strange how us computer types have never figured out how to check for syntax errors like this. (Compilers can't catch all such errors, but that's why we set up human checks like coding standards and code walkthroughs.)

The BAE system employs laser scanners that read bar-coded labels placed on baggage. Experts say that means the BAE computer system probably employs real-time, numerical-control software.

Hmm... doesn't "numerical control" refer to machining equipment?

At Louisville-based Storage Technology Corp., such software is a key feature of the company's robotic tape library storage systems.

"What they are probably seeing, and I saw it many times, is that you fix one problem and you're just peeling back a layer of the onion," said Mark Hopkins, an engineering manager for StorageTek.

Which explains why Iceberg has been such a successful product.

Strangely absent from the article is the reason Denver (or BAE) decided to build a system which reads tags on luggage (which can be oriented in an arbitrary direction) instead of reading permanent tags on the cart itself. The latter case would require keeping track of what luggage is in which cart, but eliminates all of the headaches of reading the tags on the luggage itself. (Hmm, the wording of a newspaper graphic implies that a copy of the luggage tag may be placed on the cart as well, but its alignment may not be perfect.)

Even stranger was an item in another article which identified "gaps" in the tracks as a biggest problem right now (the software being

a bigger long-term problem). It seems the wheels on the cart are falling into gaps between sections of track, causing jams or derailments. (Failing luggage is a serious construction worker hazard.)

This is truly bizarre since the luggage system is in a protected environment, located in underground tunnels. For the tracks to be damaged by "vibration" caused by a couple limited tests implies that this infrastructure was \*seriously\* underdesigned.

Bear Giles bear@cs.colorado.edu/fsl.noaa.gov

[Various articles also noted by greg@imsl.com (Greg Holling), who also contributed similar analyses. Greg, thanks. PGN]

---

### Re: DMV Computer upgrade goes awry...

Shel Kaphan <sjk@netcom.com>  
Fri, 29 Apr 1994 21:11:15 -0700

SACRAMENTO - The California Department of Motor Vehicles has informed a flabbergasted legislative committee that it has spent \$44.3 million on a computer modernization program that will never work.

...

Note that this amount of money is approximately equal to the \$50M per year in highway funding that the federal government has been withholding from California because we have not yet instituted the rule that anyone caught in possession of any amount of any illegal drugs or prescription drugs without a prescription will have their driver's license suspended for six months. That's whether you're driving at the time or not. According to the SJ Mercury News a week or two ago, the CA state legislature is most unlikely to put off adoption of this rule any longer, presumably at least in part because of the effect of recent disasters on highway construction budget requirements.

Even without the DMV debacle the state might have decided to do this, but perhaps one can hold them partially responsible for the declining quality of legislation these days.

Shel Kaphan sjk@netcom.com

---

### Re: Unusual Newspaper Error

"Stewart Rowe" <usr2210a@tso.uc.edu>  
Thu, 28 Apr 1994 13:47:28 -0400

In [Risks 15.79](#) I asked:

>Perhaps one of your readers can explain how the Midwest edition of \*The New  
>York Times\* today had a photo on the front page with the caption. "Joseph P.  
>Kennedy Jr. being arrested at the White House yesterday", with no further  
>explanation or story anywhere in the paper?

Several respondents have reported that, in the Metro edition, the explanation was found in three paragraphs at the end of the adjacent story about Haitian refugees. Apparently these paragraphs were cut by the person who made up the continuation page in the Midwest edition, leaving Joe Jr. hanging there on page 1. (Yes, I checked back and they are not there in my copy).

Stewart Rowe [usr2210a@tso.uc.edu](mailto:usr2210a@tso.uc.edu)

---

### **Re: Kennedy arrest**

*David Wittenberg <[dkw@cs.brandeis.edu](mailto:dkw@cs.brandeis.edu)>*

*Wed, 27 Apr 1994 10:31:19 -0500 (EDT)*

According to the "Boston Globe", Congressman Kennedy and several other colleagues (7 or 8?) were arrested for demonstrating in protest of the US government's policy on Haiti. The arrests were made by the Park Service police. My guess is that the congressmen had every intention of getting arrested as a way of increasing publicity.

The error was in a correct, but misleading caption. We usually assume that when a politician is arrested it is unintentional.

--David Wittenberg      [dkw@cs.brandeis.edu](mailto:dkw@cs.brandeis.edu)

---

### **Re: Unusual Paper Error (Rowe, [RISKS 15.79](#))**

*"Daniel B. Dobkin" <[dbd@ans.net](mailto:dbd@ans.net)>*

*Thu, 28 Apr 94 16:51:23 EDT*

For what it's worth, my wife asked the same question, and she was looking at the New York Metro/Suburban edition. While I can't speak with any real authority about the Midwest (national) edition, I will say that in my experience the first page doesn't change much; the big difference is in the metro section: the national editions don't carry the local stories.

The picture with the caption ("Joseph P. Kennedy Jr. being arrested at the White House yesterday") accompanied the story about the Administration's policy on Haiti. While there was no mention of Rep. Kennedy anywhere in the story, it did state that (quoting from memory) "four members of the House of Representatives were arrested during a protest at the White House." To my eye, this is sloppy copy editing, not a bona fide technology blunder.... The technology does seem to encourage such sloppiness, though, a fact to which our moderator (and the RISKS archives) will bear witness.

\dbd

---

### **Re: MIT student arrested for BBS ... (Cohen, [RISKS-15.76](#))**

*Fredrick B. Cohen <[fc@Jupiter.SAIC.Com](mailto:fc@Jupiter.SAIC.Com)>*

Tue, 26 Apr 94 16:16:01 PDT

Sorry - I was mistaken when I claimed that LaMacchia was arrested. The correction noted by Tim Shepard and Douglas Rand in [RISKS-15.79](#) was accurate.

As to the issue of his intent to pirate software, that was not the charge against him. It was wire fraud! I have read the copy of the indictment and commentary and I find this awfully strange. Furthermore, I find little if any substantive evidence of intent to pirate software in my reading of the quotes from the indictment. If you assume he is innocent and ask yourself if these comments could have been innocently made by a person of that age in that environment, you may find that the assertion of guilt is not warranted.

FC

---

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">  
Mon, 02 May 1994 12:50:25 -0600 (MDT)

Subject: "The Streetwise Guide to PCs" by Jerome/Taylor

BKSTRTPC.RVW 940118

Addison-Wesley Publishing Company

Heather Rignanesi, Marketing, x340, 73171.657@Compuserve.com

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

telephone 416-447-5101, fax: 416-443-0948

or

Tiffany Moore, Publicity tiffanym@aw.com

Bob Donegon bobd@aw.com

John Wait, Editor, Corporate and Professional Publishing johnw@aw.com

Tom Stone, Editor, Higher Education Division tomsto@aw.com

Philip Sutherland, Schulman Series 74640.2405@compuserve.com

1 Jacob Way, Reading, MA 01867-9984

800-822-6339 or 617-944-3700, Fax: (617) 944-7273

5851 Guion Road, Indianapolis, IN 46254, 800-447-2226

"The Streetwise Guide to PCs", Jerome/Taylor, 1993, 0-201-60839-1, U\$14.95

Those of us who have been around the computer world for any length of time have seen a great many "How to Buy a PC" seminars, articles and user group meeting talks. They generally offer a lot of helpful advice and useful information for the novice. I have, however, often noted personal bias being delivered with the same force and weight as known and tested fact. The neophyte generally comes away with a much better knowledge of the computer market--but also with a number of unsubstantiated prejudices.

Here, then, is a book on the same topic. Containing far more material than any one-hour talk or magazine article, it nevertheless has some of the same tone. Those wise in the ways of computer purchasing will many times breathe an "Amen!" to much of what is here. There are also, however, personal biases and blind spots that the newcomer will have difficulty recognising.

Chapter one is a general diatribe against the industry as a whole. As vitriolic as it may sound to the newcomer, the authors may, in fact, be \*under\*stating the case. Chapter two states that software is central to the whole process, and gives tips for evaluating the major applications. The remaining eight chapters are devoted to hardware.

There are some easily identifiable oddities. The statement that Windows' management of resources makes things easier obviously comes from someone who has never had to check the five completely different print menus under Windows to find out why nothing is coming off the printer. Some items seem to be subject to time lag, as with the insistence that 386 and 486 CPUs are maker-independent. (This might have been true earlier, but the 486 market is now an utter shambles.) The authors still cling to their claim that all surge protectors are created equal. I found the section on virus protection to be fairly reasonable--except that they still get the Stoned message wrong, think all scanners are equally effective, and don't know about shareware scanners. In fact, shareware doesn't get much of a shake in spite of the railing against overpricing and software bloat.

In addition, some of the recommendations for protection may give a false sense of security. The authors frequently repeat the refrain that one should never buy anything with cash or cheque: put it on a credit card so that you will have some fallback. The use of a credit card, however, does \*not\* necessarily protect you. Once you sign the charge slip, you are committed to honour that debt. The credit card company \*may\* choose to reverse the charge and not pay the merchant, but that is at \*their\* discretion, and they are not automatically on your side. (The credit card company may take several months even to decide whether or not to reverse the charge: the representatives I talked to, at the credit card service office, the local bank, the head office complaint department and the head office PR office refused to give any upper bound or time limit for a decision. The PR department initially stated that paying by card was the same as paying by cash, but refused to answer when asked to comment specifically about the case of defective equipment.)

You really are alone out there: I recently checked up on the Better Business Bureau, and found that while the technology the BBB is using for phone access to reports is impressive, the reports themselves are less so. A company which has had several disputes in the past, and has a current dispute outstanding, is listed as being in "satisfactory" standing, and the BBB had "received no complaints" during its existence. The BBB also had a chance to respond to this and indicated that it was because of their "standard reporting language" imposed from head office. (BBB is a franchise.) Complaints are not entered into the automated system until proven, beyond doubt, to be "valid": the consumer is not allowed an opportunity to respond to the final offer from the merchant. Decisions on validity are made by the BBB. The BBB is paid by the vendor. The conclusion is left as an exercise to the reader. (The General Manager of the local BBB stated that more detailed information is available from the counselors, although this is not made at all clear from the automated system. I checked this out later, and it turns out not to be the case. She also stated that most people deal with the counsellors rather than the automated system, which doesn't surprise me in the least.)

In the absence of any better, though, this book is to be recommended for

beginners \*before\* they buy a computer. One of the particularly nice features is a sample advertisement introducing every chapter and dissected for "lies". Get some street smarts before you go buy a PC. And never buy anything on the spot.

copyright Robert M. Slade, 1994 BKSTRTPC.RVW 940118

DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733  
DECUS Symposium '95, Toronto, ON, February 13-17, 1995, contact: rulag@decus.ca

---

## Computer-Aided Verification 94 Conference Announcement

David Dill <dill@hohum.stanford.edu>

Mon, 2 May 94 11:42:09 PDT

CONFERENCE ANNOUNCEMENT  
Conference on Computer-Aided Verification  
CAV 1994

Stanford University, June 21-23, 1994

The Sixth Conference on Computer-Aided Verification will be held June 21-23 at Stanford University. The conference will be followed on June 24th by a one-day workshop on practical aspects of computer-aided formal verification.

CAV 94 is sponsored by a group of companies with a strong interest in the topic area: AT&T, IBM, Intel, Motorola, Redwood Design Automation and Sun Microsystems. [...]

FURTHER INFORMATION: You can send electronic mail to "cav@hohum.stanford.edu" if you want registration information, a copy of the program, or further information about the conference.



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 16: Issue 2**

**Tuesday 3 May 1994**

## Contents

- [NEW YORKER article on library automation](#)  
[Jon Jacky](#)
- [Information Warfare: GM vs VW](#)  
[Mich Kabay](#)
- [TechWar: Cell Phone Jamming](#)  
[Mich Kabay](#)
- [Green Card Con Artists Exposed!](#)  
[Bonnie L. Mahon via D.R. Hilton](#)
- [New firewalls book - a great risk reducer](#)  
[Ray Kaplan](#)
- [Re: Drunk in charge](#)  
[John Simutis](#)  
[Andy Ashworth](#)  
[Dan Astoorian](#)
- [Boot Prom commits Denial of Service Attack](#)  
[Butch Deal](#)
- [Staying Informed of Security & Privacy Issues](#)  
[David Johnson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### NEW YORKER article on library automation

*Jon Jacky <[jon@violin1.radonc.washington.edu](mailto:jon@violin1.radonc.washington.edu)>  
Mon, 2 May 1994 21:10:10 -0700*

The April 4, 1994 issue of the NEW YORKER had a long article by Nicholson Baker on library automation: "ANNALS OF SCHOLARSHIP: Discards". It runs from pages 64 through 87. My issue also came with a flyer stapled to the cover with the headline, "THE TRASHING OF AMERICA'S GREAT LIBRARIES."

Baker reports that when most libraries replace their paper card catalogs with on-line systems, they simply discard the card catalogs. Baker argues that the card catalogs are an irreplaceable resource, and contain much scholarly content which is not carried over into the new systems. Baker also argues

that the on-line systems often suffer from poor data quality, and make some kinds of searches (particularly subject searches) more difficult.

RISKS readers will find much of interest about the difficulties of maintaining integrity and consistency in very large databases. Baker reports one instance where all instances of "Madonna" were replaced with "Mary, Blessed Virgin, Saint," causing reclassification of recent works by Ms. Ciccone.

Some letters responding to the article appear in the May 2, 1994 NEW YORKER.

- Jon Jacky, jon@radonc.washington.edu, University of Washington, Seattle

---

### **Information Warfare: GM vs VW (cont'd)**

*"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>  
03 May 94 09:19:36 EDT*

>From the Reuter newswire via Executive News Service on CompuServe (GO ENS):

"BONN, April 30 (Reuter) - The German car manufacturer Volkswagen, accused by rival Opel of industrial espionage, on Saturday denied a magazine report that incriminating material had been found in the office of an employee.

Der Spiegel magazine said on Saturday prosecutors found a computer disc containing plans for a high-tech small car factory in the office of Jaero Arthur Wicker, office manager of production head Jose Ignacio Lopez de Arriortua."

The article continues with the following key points:

- o Lopez used to work for General motors; he's accused of having stolen confidential files when he was hired by VW.
- o VW claims the disk has plans submitted to both GM and VW and rejected by both companies.
- o The situation is under investigation by both German and US authorities.
- o The newest scuttlebutt is that GM has asked German prosecutors to investigate daughter Begona Lopez, whom they accuse of having stolen a disk containing information on cost reductions at GM.

[Comments by MK: sounds like a tabloid newspaper's version of a rivalry between movie stars.]

Michel E. Kabay, Director of Education, National Computer Security Assn

[That would be a REALLY SMALL car factory if it were to fit into the office of Jaero Arthur Wicker, Jaerodynamically at least. PGN]

---

## TechWar: Cell Phone Jamming

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>

03 May 94 09:19:40 EDT

>From the Reuter newswire via Executive News Service on CompuServe (GO ENS):

"KINSHASA, April 30 (Reuter) - Zaire's main cellular telephone company, at loggerheads with a rival firm trying to muscle in on its territory, said on Saturday its signals were being deliberately jammed.

Jim Galan, head of coordination at Telecel, said five or six microwaves had been trained on its main antenna for the last four days, drowning out many calls made from central Kinshasa."

The article explains that the jamming is making cellular phone use impossible for Telecel's 4000 Kinshasa users. It is generally believed that a new company, Comcell, which is supported by the Zairian government, is using the frequencies originally assigned to Telecel by that same government.

Legal action is in the works.

[MK comments: RISKS of doing high-tech business where the rule of law is weak. Example of Information Warfare a la Winn Schwartau.]

Michel E. Kabay, Director of Education, National Computer Security Assn

---

## Disbarrable under Tenn. Code (Canter/Seigel)

J Doe <rosidivi@rintintin.Colorado.EDU>

Mon, 2 May 1994 20:02:25 GMT

Reply-To: drhilton@kaiwan.com

Subject: Green Card Con Artists Exposed!

Keywords: green card canter lawyers

For Immediate Release  
October 13,1988  
Contact: Bonnie L Mahon  
The Florida Bar  
Tampa Office  
Telephone: 813/875-9821

## SUPREME COURT GRANTS ATTORNEY'S PETITION TO RESIGN PERMANENTLY

TALLAHASSEE, Oct.13-- The Florida Supreme Court has granted attorney Laurence A. Canter's petition to resign permanently, effective November 7, 1988.

Canter, of 240 North Washington Boulevard, Sarasota, was charged with numerous violations of the attorney disciplinary rules including neglect, misrepresentation, misappropriation of client funds and perjury.

Several of the complaints against Canter involved his failure to file the necessary or appropriate documents with the United States Immigration and Naturalization Services in matters of permanent residency and work visas. In addition, Canter refused to refund clients' funds and neglected to notify his clients that he has been suspended from the practice of law as a result of a previous discipline.

The Florida Bar further alleges that Canter committed perjury by filing a false affidavit with the Bar and while testifying under oath in a deposition. These charges resulted after an audit of Canter's trust account by the Bar showed that trust funds were held in Canter's account during the time period when he denied any funds were present.

Canter was born in 1953 and admitted to The Florida Bar in 1980.

The resignation without leave to apply is not final until time expires to file motion for rehearing and if filed, determined. The filling of a motion for rehearing shall not alter the effective date of this resignation.

As an official agency of the Supreme Court of Florida, The Florida Bar and its Department of Lawyer Regulation are charged with the administration of a statewide disciplinary system to enforce Supreme Court rules of professional conduct for all lawyers.

---

## **New firewalls book - a great risk reducer**

*RayK <KAPLAN@BPA.ARIZONA.EDU>*

*Mon, 2 May 1994 23:51:07 -0700 (MST)*

Cross post to RISKS (via mail submission), comp.security.announce and comp.protocols.tcp-ip news groups, and a few other various places. Sorry if you see this more than once.

Re: Firewalls and Internet Security - Repelling the Wily Hacker.  
Ray Kaplan - May 2, 1994

Buy this book!

Gentle folk,

Here is a risk reducer. With the wholesale rush to Internet connectivity, it's about time someone sat down and wrote a good book about how to do this exercise safely! And, sure enough, Cheswick and Bellovin have done just that,

Heaping superlatives on something of which you are enamored is always problematic - the possibility of overstatement looms large. Accordingly I'll cut to the chase. Buy this book! I do not get any money for saying this - I just believe you are well justified in getting it on your reading list - today. In May of this year, Addison Wesley is releasing an excellent new book

by Bill Cheswick and Steve Bellovin: Firewalls and Internet Security - Repelling the Wily Hacker. ISBN 0-201-63357-4. It will retail for \$26.95. Bulk purchases: 800- 238-9682, individual orders: 800-824-7799 (FAX 617-944-7273). Email orders over the Internet from [bexpress@aw.com](mailto:bexpress@aw.com) (no they don't take plastic via Email). For those that are net-challenged, U.S. snailmail orders from Addison-Wesley, c/o Arlene Morgan, 1 Jacob Way, Reading, MA 01867 USA.

Rumors loom large that at least one of the authors (Ches?) will be at Interop with copious quantities of this work of art. As dues of superlative authorship that is destined to be popular, I hope they both get writer's cramp autographing!

#### Details

While worthwhile, well written, pace-setting, technically astute works of art are rare - this is certainly one of them. I am always hard pressed to identify any one thing as unique in its decade (especially when the decade is still in progress). Suffice it to say that this work is the most complete treatment of firewall technology and experience that is available. The availability of this work is exciting news for security firewall builders - including Internet security firewall builders - and, for the great number of people that seem to be befuddled by the complexity and the general issues of interconnecting networks.

#### The book

While my review copy (well dog-eared, now) is a bit dated (March 7, 1994), I think you can expect that it is close to the book's final form: a standard (w=7.5in, h=9in) Addison-Wesley Professional Computing Series book like the ones that should already dot your shelves. (I don't get any money for my obvious favorable bias toward this series. My bias is born out of the fact that the series (Brian Kernighan is the consulting editor for it) contains great authors and titles like Radia Pealman's Interconnections - Bridges and Routers and Richard Stevens' TCP/IP Illustrated, Volume I - The Protocols.)

305 pages in 14 chapters, appendices, a bibliography, a list of "bombs" (security holes) and an index.

Out of the box, the authors set the tone for their work by quoting F.T. Gramp and R.H. Morris: "It is easy to run a secure computer system. You merely have to disconnect all dial-up connections and permit only direct-wired terminals, put the machine and the terminals in a shielded room, and post a guard at the door." This is followed by a detailed discussion of the art and science of building a firewall. There is so much good stuff here, that all I can do is list the book's contents - lest I write a tome which distracts you from picking up a copy of it ASAP.

Chapters and content - from the table of contents.

#### Getting started

##### Introduction

- Why security?
- Picking a security policy

- Strategies for a secure network
- The ethics of computer security
- Warning

#### Overview of TCP/IP

- The different layers
- Routers and routing protocols
- The Domain name service
- Standard services
- RPC-based protocols
- The "r" commands
- Information services
- The X-11 service
- Patterns of trust

#### Building your own firewall

##### Firewalls and gateways

- Firewall philosophy
- Situating firewalls
- Packet-filtering gateways
- Application-level gateways
- Circuit-level gateways
- Supporting inbound services
- Tunnels - good and bad
- Joint Ventures
- What firewalls can't do

##### How to build an application-level gateway

- Policy
- Hardware configuration options
- Initial installation
- Gateway tools
- Installing services
- Protecting the protectors
- Gateway administration
- Safety analysis - why our setup is secure and fail-safe
- Performance
- The TIS firewall toolkit
- Evaluating firewalls
- Living without a firewall

##### Authentication

- User authentication
- Host-to-host authentication

##### Gateway tools

- Proxylib
- Syslog
- Watching the network: Tcpcdump and friends
- Adding logging to standard demons

##### Traps, lures and honey pots

- What to log
- Dummy accounts
- Tracing the connection

##### The hacker's workbench

- Introduction
- Discovery

- Probing hosts
- Connection tools
- Routing games
- network monitors
- Metastasis
- Tiger teams
- Further reading

A look back

Classes of attacks

- Stealing passwords
- Social engineering
- Bugs and backdoors
- Authorization failures
- Protocol failures
- Information leakage
- Denial-of-service

An evening with Berferd

- Introduction
- Unfriendly acts
- An evening with Berferd
- The day after
- The jail
- Tracing Berferd
- Berferd comes home

Where the wild things are: a look at the logs

- A year of hacking

Proxy use

- Attack sources
- Noise on the line

Odds and ends

Legal considerations

- Computer crime statutes
- Log files as evidence
- Is monitoring legal?
- Tort liability considerations

Secure communications over insecure networks

- An introduction to cryptography
- The Kerberos authentication system
- Link-level encryption
- Network- and transport-level encryption
- Application-level encryption

Where do we go from here?

Appendices

Useful free stuff

- Building firewalls
- Network management and monitoring tools
- Auditing packages
- Cryptographic software
- Information sources

TCP and UDP ports - Fixed ports

- MBone usage

Recommendations to vendors

- Everyone

- Hosts

- Routers

- Protocols

- Firewalls

Bibliography - List of bombs - Index

I have criticisms, complaints and suggestions. However, considering that this is such a darn fine piece of work - I hasten to get my recommendation that you buy this book out ASAP.

Meantime, to whet your appetite:

- Index - (a well done, 26 pages worth - you can actually find pointers to what you want to know! What a concept.

- TCP ports discussion - a Comprehensive list and reasonable advice on what to do with them.

- Bombs - a summarized list of the 43 major security holes that they identify.

- Bibliography - Ahhhh. 19 pages of the best firewalls-related bibliography that I've seen.

- Where to from here - excellent advice for techies and managers who don't want to keep working at the job of firewalling or who simply want to spend a bit of resources on it only once.

Kudos to the authors - buy this book.

Of course - these are my own views, and they don't necessarily reflect those of anyone - including my employer. However, in this case, they probably do.

Ray Kaplan            CyberSAFE, Corporation  
rayk@ocsg.com        Formerly Open Computing Security Group (OCSG)  
                          (206) 883-8721  
                          FAX at (206) 883-6951  
                          2443 152nd Ave NE  
                          Redmond, WA 98052

Better living through authentication

---

**Re: Drunk in charge ([RISKS-15.80](#))**

*John Simutis <simutis@ingres.com>*

*Fri, 29 Apr 94 15:12:34 PDT*

While I was a contract programmer at GM/EDS, there was an explicitly stated policy: it was permissible to drink alcohol, as having a beer with lunch, but ONLY if one did not plan to return to work that day. It was stated further that we were obligated to give the customer our best work, and alcohol was not consistent with that effort.

John Simutis, simutis@ingres.com Alameda, California, USA

---

**Re: drunk in charge..... ([RISKS-15.80](#))**

*Andy Ashworth <tcsaca@aie.lreg.co.uk>*

*Fri, 29 Apr 94 09:10:21 BST*

I understand that British Rail have a policy that no personnel who can affect the safety of others is allowed to have alcohol in their bloodstream during working hours - the penalty for violating this rule is, I think, dismissal. This grouping includes engineering staff involved in the R&D of systems such as signaling.

This is more than just "drunk in charge of a computer", this is, sensibly IMHO, "being under the influence of alcohol while capable of influencing the safety of others". I hope that the next time I fly in a fly-by-wire aircraft or drive my systems heavy car I can have confidence that the developers of the systems that could affect my safety applied a similar abstemious regime.

Andy Ashworth, Lloyd's Register, 29, Wellesley Road, Croydon CR0 2AJ  
+44 (0)81 681 4723 Fax: +44 (0)81 681 4839 tcsaca@uk.co.lreg.aie

---

**drunk in charge... ([RISKS-15.80](#))**

*Dan Astoorian <djust@utopia.druid.com>*

*Sun, 1 May 1994 11:31:00 -0400*

Driving requires quick response time; electric work requires manual dexterity. Alcohol impairs both these things, and as noted, the dangers are obvious, immediate, and tragic.

Software engineering requires very little in the way of fast responses or manual dexterity, unless one considers an inordinate number of typos a serious RISK.

Moreover, the skills which *are* required to write software tend to be more of the problem-solving variety. I don't dispute that alcohol dulls these; however, when you take away one's problem solving skills, the result is that the problem doesn't get solved.

I seem to vaguely recall an old study in which a group of people, some of which had been given a couple of drinks, were called upon to solve arithmetic problems of moderate difficulty, with no time limit. I believe the outcome was that those who had had the drinks took much longer to finish the problems, but their responses were *more* accurate

than the teetotalers, presumably due to their awareness that they were prone to make errors.

(I would therefore advise project managers to take Friday pub lunches into account when setting deadlines.)

Incidentally, I'm not sure how one would distinguish between mistakes due to being under-the-influence and those due to being under stress (perhaps due to looming deadlines), or simple inexperience or incompetence, or even honest-to-God oversights. If the QA system for critical systems doesn't catch all such types of mistake, there's already a serious problem. Obviously this is not intended as an argument against reducing the number of errors to be found by QA, but still... a bug is a bug.

(I'm reminded of a phrase a colleague used to repeat: "Sure, alcohol kills brain cells. But only the weak ones.")

Dan Astoorian, Mississauga, Ontario, Canada [djast@utopia.druid.com](mailto:djast@utopia.druid.com)

---

## Boot Prom commits Denial of Service Attack

*Butch Deal NRL <[butch@keep.blackmagic.com](mailto:butch@keep.blackmagic.com)>*

*Fri, 29 Apr 1994 20:00:45 -0400*

What is the risk here? People like to put blame one other systems all the time. I see this as only a matter of misconfiguration and miscommunication among the different system admins. What do the DEC stations need to run tftp for? Shouldn't they be logging in to a non-critical partition? Shouldn't the Suns have a similar tcpwrapper installed? Maybe they should all log to some central machine, with syslog maybe. There could be several machines that can serve a diskless station. The broadcast allows them to find the right one on the local network and come on up. I do not think it is at all fair to try to blame a hardware manufacturer because the equipment worked exactly as documented, but that happens not to be the way you want it to work.

[butch@keep.blackmagic.com](mailto:butch@keep.blackmagic.com) Butch Deal

---

## Staying Informed of Security & Privacy Issues

*David Johnson <[worldwid@uunet.uu.net](mailto:worldwid@uunet.uu.net)>*

*Mon May 02 10:23:44 1994*

STAYING INFORMED: Resources for Privacy Seekers & Computer Security Buffs  
by David Johnson

(Copyright 1994 under the International & Pan-American Copyright Conventions)

Having conducted various types of security and investigative work that has taken me to ten Asian countries, I am quite familiar with various obstacles one must hurdle to obtain hard-to-find and elusive data.

Even though our computers are valuable tools, adopting a multi-faceted approach to information gathering is the most effective way to cover all the angles.

Use this listing to build your own private intelligence network.

COMPUTER SECURITY PUBLICATIONS

PRIVACY-RELATED PUBLICATIONS

Auerbach Data Security Management      Full Disclosure Magazine  
Information Systems Security      Box 244

Lowell, MI 49331 USA

210 South St.      Voice: (800) 633-3274

Boston, MA 02111 USA      Voice: (616) 897-7222

Voice: (800) 950-1218      Fax: (515) 897-0705

Voice: (212) 971-5000

Fax: (617) 423-2026      International Privacy Bulletin

666 Pennsylvania Ave., S.E.

Computer Security, Auditing & Controls      Washington, DC 20003 USA

57 Greylock Rd.

Box 81151

Wellesley Hills, MA 02181 USA      Privacy and Security 2001

Voice: (617) 235-2895      504 Shaw Rd., #222

Sterling, VA 20166 USA

Voice: (800) US-DEBUG

Computer Audit Update      Voice: (703) 318-8600

Computer Fraud & Security Update      Fax: (703) 318-8223

Computer Law & Security Report

Computers & Security

Crown House, Linton Rd., Barking      Privacy Journal

Essex I611 8JU, England      Box 28577

Voice: (44) 81-5945942      Providence, RI 02908 USA

Fax: (44) 81-5945942      Voice: (401) 274-7861

Telex: 896950 APPSCI G

(North American distributor)

Box 882      Privacy Laws and Business

New York, NY 10159 USA      Box 23

Voice: (212) 989-5800      7400 GA, Deventer, Netherlands

Voice: (31) 57-0033155

Fax: (31) 57-0022244

Telex: 49295 KLUDV NL

Computer Control Quarterly

1 Southbank Blvd., Level 8      (North American Distributor)

S. Melbourne, Vic. 3205, Australia      6 Bigelow St.

Voice: (03) 6121666      Cambridge, MA 02139 USA

Fax: (03) 6295609      Voice: (617) 354-0140

Computer Security Alert

Computer Security Journal      Privacy Times

Box 21501

600 Harrison St.      Washington, DC 20009 USA

San Francisco, CA 94107 USA      Voice: (202) 829-3660

Voice: (415) 905-2370  
Fax: (415) 905-2234

Fax: (202) 829-3653

#### COMPUTER SECURITY ORGANIZATIONS

##### Computer Security Digest

150 N. Main St.  
Plymouth, MI 48170 USA

Voice: (313) 459-8787  
Fax: (313) 459-2720

Center for Computer Law  
1112 Ocean Dr.  
Manhattan Beach, CA 90266 USA  
Voice: (213) 372-0198

Computing & Communications  
(Law & Protection Report)  
Box 5323  
Madison, WI 53705 USA  
Voice: (608) 271-6768

Computer Security Institute  
360 Church St.  
Northborough, MA 01532 USA  
Voice: (617) 393-2600

##### Info Systems Security Assn.

Data Security Manual  
Box 322  
3300 AA Dordrecht, Netherlands  
Voice: (31) 78-524400  
Voice: (31) 78-334911

Box 71926  
Los Angeles, CA 90071 USA

Fax: (31) 78-334254  
Telex: 29245 KAPG

Nat'l Center for Computer  
Crime Data

##### 4053 JFK Library - CSULA

(North American Distributor)  
Box 358  
Hingham, MA 02018 USA  
Voice: (617) 871-6600

5151 State University Drive  
Los Angeles, CA 90032 USA  
Voice: (213) 225-1364

#### PRIVACY-RELATED RESOURCES

##### Information Systems Security Monitor

U.S. Department of Treasury  
Bureau of the Public Debt  
AIS Security Branch  
200 3rd St.  
Parkersburg, WV 26101 USA  
Voice: (304) 480-6355  
BBS: (304) 480-6083

F.E.C., Inc.  
P.O. Box 959  
Centro Colon 1007-91/12-0695  
San Jose, Costa Rica  
(financial & personal privacy)

##### Eden Press Box 8410

InfoSecurity News  
498 Concord St.  
Framingham, MA 01701 USA  
Fax: (508) 872-1153

Fountain Valley, CA 92728 USA  
Voice: (714) 556-2023  
Fax: (714) 556-0721  
(various books on privacy)

Journal of Computer Security  
Van Diemenstraat 94  
1013 CN Amsterdam, Netherlands  
Voice: (31) 20-6382189  
Fax: (31) 20-6203419

Consumertronics  
Drawer 537, Alamagordo, NM 88310 USA  
Voice: (505)434-1778  
Fax: (505) 434-0234  
(technical invasion manuals)

(North American distributor)  
Box 10558

Burke, VA 22009 USA  
Voice: (703) 323-5554

Privacy Hotline (800) 773-7748  
(California only) 10am-3pm, M-F

\*\*\*\*\*

David Johnson                      2421 W. Pratt Boulevard, Suite 971  
President, Worldwide Consultants      Chicago, Illinois 60645  
Editor, Information Gatherer Newsletter      U.S.A.  
International Investigator              Tel: (800) 316-0801 (24 hrs.)  
Security Consultant                      Fax (c/o World-Con): (908) 542-1266  
Privacy Strategist                      E-mail: worldwid@uunet.uu.net



 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 16: Issue 3**

**Thursday 5 May 1994**

## Contents

- [Spelling correction](#)  
[Phil Agre](#)
- [Sigh -- security through obscurity is NOT security](#)  
[Alan Wexelblat](#)
- [Bellcore cracks 129-digit RSA encryption code](#)  
[Steven Tepper](#)
- [Risk of Non-Computerization?](#)  
[Klaus Brunnstein](#)
- [Computers Blamed For FAA Woes](#)  
[Mark Thorson](#)
- [Brief note re DIA fiasco](#)  
[Paul Green](#)
- [Followup on credit card policies \(re: "Streetwise Guide ..."\)](#)  
[Rob Slade](#)
- [ABC Nightline re LaMacchia](#)  
[Mich Kabay](#)
- [Risks of electronic door locks for automobiles](#)  
[Paul Wallich](#)
- [Info on RISKS \(comp.risks\)](#)

---

### spelling correction

*Phil Agre <pagre@weber.ucsd.edu>  
Tue, 3 May 1994 15:10:22 -0700*

We've had plenty of notes about spelling correctors, but I find this one particularly interesting. The otherwise excellent April 1994 issue of Z Magazine contained a particularly horrible editing error in an article by Sara Diamond about the "American Center for Law and Justice" (ACLJ). The ACLJ was created by conservative Christians in order to oppose the American Civil Liberties Union (ACLU) in court cases over issues like school prayer. Everyone has assumed that the similarity of acronyms is deliberate; ACLJ seems part of a fairly systematic conservative strategy of positioning public-interest groups as "liberal" by creating conservative mirror images of

them. Well, as the Z editors explained in their May issue, their spelling correction program included ACLU but not ACLJ, with the result that every instance of "ACLJ" in Diamond's article got changed to "ACLU" except, somehow, for the very first one, which occurred (much as it does above) in parentheses after the first mention of "American Center for Law and Justice". Apparently there was an uproar, with some Z readers calling up the ACLU to ask why it had suddenly reversed its positions. The risk is subtle: in politics, things are often designed to outwardly resemble their opposites, or to invite confusion or sharply defined contrast (or both) with their opposites. As a result, it becomes impossible to define "close enough" in (for example) a spelling corrector without a great deal of specific background knowledge.

Phil Agre, UCSD

---

### Sigh -- security through obscurity is NOT security

*"Alan (Miburi-san) Wexelblat" <wex@media.mit.edu>  
Tue, 3 May 94 17:26:46 -0400*

Peter Ladkin introduces his post with the polite phrase:

> a vandal exploiting a not-unknown security hole

or, in American English:

Some lazy person at the target site failed to plug a known hole, probably reasoning along the lines of "Oh, no one will know about this hole so I don't have to deal with it."

There is no excuse for vandalism, including failure by sysops to plug known holes. However, if I was a user at that site I'd be more pissed at the person who failed to prevent the vandalism when such prevention was possible.

--Alan Wexelblat, Reality Hacker, Author, and Cyberspace Bard, Media Lab -  
Advanced Human Interface Group wex@media.mit.edu 617-258-9168

---

### Bellcore cracks 129-digit RSA encryption code

*Steven Tepper <greep@datatools.com>  
Tue, 3 May 94 18:46:36 PDT*

[Old news to some of us. Oddly no one reported it to RISKS until now, and I did not get around to entering anything on it. PGN]

Excerpts from an article on page 14 of the May 2 issue of Network World:

A team led by Bell Communications Research last week announced it has cracked a 129-digit encryption code, which scientists had predicted would take "40 quadrillion years" to break. ...

Breaking the RSA-129 public key required that the team find the two prime numbers that, when multiplied by each other, resulted in the 129-digit key number. ...

This mathematically arduous task was accomplished in eight months by 600 volunteers in 24 countries who used their organizations' spare computing capacity. ...

---

## Risk of Non-Computerization?

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.d400.de>  
Wed, 4 May 1994 11:16:34 +0200*

In a TV report (magazine *FRONTAL*, 2nd German TV channel ZDF, Tuesday May 3, 1994), recent motorsport accidents (3rd World Championship, formula 1 racing cars, Imola/San Marino) were discussed and analysed by experts (e.g. former World champion Niki Lauda/Austria). Besides general questions about deficiencies in safety and protective measures, the question was discussed whether the recent decision to forbid the computerized ground distance control may have contributed to the strange behaviour of both racing cars which after a curve went straight into a concrete wall, without visible signs of steering. In both cases (Austrian driver Hackenberger, in training for his 2nd race, and Brazilian driver Ayrton Senna, 3-times world champion), the cars crashed at almost 300 kilometers per hour, with both drivers dying upon impact.

Until end-of-1993, formula 1 racing cars were equipped with a computerized control system aimed at maintaining a fixed but very small distance between the car's bottom and the track's surface, to allow for maximum contact and therefore maximum transfer of power on the wheels. Following arguments that a defect in the computer system may lead to serious crashes, the international authority for this sport forbidded this computer system from 1994. This decision may now have caused the problem on the very high speed track of Imola, where the cars reach maximum velocities over 300 km/h. According to the discussion quoted, the hydraulic steering support may be affected when the car's bottom contacts, at high speed, an uneven part of the track; in such a situation, the driver would no longer be able to steer the car and may even loose the ability to brake. Evidently, the decision to forbid the computer system was neither accompanied by an adequate risk analysis nor were any additional measures taken to diminish the risks e.g. by reducing the car's speed or by enlarging the minimum distance between car's bottom and track ground. Only now, discussions take place to reduce the speed in certain parts of the track.

Klaus Brunnstein (May 4, 1994)

---

## Computers Blamed For FAA Woes

*<mmm@cup.portal.com>  
Wed, 4 May 94 01:06:17 PDT*

This morning (3 May 1994), Transportation Secretary Federico Pena appeared on

at least one morning TV show in addition the MacNeil-Lehrer show to inform the public about the shocking state of the nation's air-traffic control technology. On both appearances that I saw, Pena said that the FAA needed to be a private corporation so it could acquire technology more quickly, outside of federal regulations.

He used as an example the humble vacuum tube. He said that the FAA is the world's largest buyer of vacuum tubes. That I can believe. But then by way of comparison, he held up a vacuum tube and a computer chip. The tube was a big one, about the size of a #30, which is much bigger than the tubes used on any tube computer like ENIAC, whose tubes were about the size of a 5U4. He compared it against a computer chip (something packaged like an Intel 486), and claimed the latter could replace 3.5 million vacuum tubes!

Apparently, Secretary Pena either: a) believes the FAA is running enormous, obsolete vacuum tube computers containing millions of tubes, or b) doesn't mind telling bald-faced lies to the American public to get support for his objectives. I'm not sure which is worse.

Mark Thorson (mmm@cup.portal.com)

---

### **Brief note re DIA fiasco**

*Paul Green <Paul\_Green@vos.stratus.com>  
Wed, 4 May 1994 21:14:59 GMT*

As someone who has been involved in fixing a number of terrible situations involving computers, and as someone who has not been involved in the DIA fiasco, other than as a fascinated observer, I'm sure that when the book is written on this, we'll find that there is ample blame for all of the parties involved in the project. Small groups of people make small messes. To get a really large mess, you need a large group of people working for many organizations. Anyone, or any reporter, claiming to know the source of the problems at this stage, is either quite naive or has an axe to grind.

I think Bear Giles misses the point (in [RISKS 16.01](#)) about simple software errors leading to massive, unintended consequences. The issue is not (just) syntax checkers. Sure, we've got 'em...So what? The issue is that in a mechanical or analog system a small error in the input or operation generally leads to a small **and traceable** error in the output. But in a digital system, especially a software-based digital system that can experience memory or data corruption, a small error in the input or operation can have huge **and virtually untraceable** errors in the output. I seem to recall that it was indeed a small error that brought down the AT&T long-distance switching system. I have to agree with the writer on this one.

Finally, judging by the number of bar-coded labels that I have to rip off my luggage, many airports must use bar-code readers. I have to believe that this piece of airport technology is reasonably mature. Finally, common sense says it has got to be more reliable to bar-code the luggage than the carts.

Paul Green, Sr. Technical Consultant, Stratus Computer, Inc., Marlboro, MA

01752 Paul\_Green@vos.stratus.com, PaulGreen@aol.com (508) 460-2557

---

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">  
Thu, 05 May 1994 15:21:10 -0600 (MDT)

Subject: Followup on credit card policies (re: "Streetwise Guide ...")

PGN asked me to summarise the responses to my comments in the review of "The Streetwise Guide to PCs" by Jerome/Taylor. I had suspected that it might be a bit controversial, but I was surprised that the only substantive comments I received were in regard to the difference between Canadian and American law regarding credit card purchases. The most apposite information was from Bear Giles <bear@tigger.cs.Colorado.EDU> who wrote:

=====

I don't remember the exact language, but in the U.S. consumers have the right to refuse charges made more than 50(?) miles from their home address. The refusal must be in writing, within 30 days, possibly with an explanation, etc. The bank must complete its actions within 60 days of receipt of this letter, cannot charge interest or late fees on the disputed amount, etc. (I would imagine the exact details are in the FAQ of various consumer advocacy groups.)

The presumption is that the purchase was made over the phone or while on a trip, either situation making it difficult to impossible for the consumer to evaluate the quality of the merchandise prior to purchase.

There is no corresponding law applying to purchases "near home"; this distinction is often lost on people. And of course the existence of an American law has no significance to a Canadian making a domestic purchase.

BTW, another restriction (either U.S. law or merchant agreement) which is often overlooked is a requirement that charges not be placed against your account until the merchandise is actually shipped. I believe companies can still "reserve" credit, but the only effect the customer sees from this is a reduced available credit -- she does not have to make payments against it.

=====

Much the same was said by Andrew Klossner <andrew@frip.wv.tek.com> who added:

=====

Holders of U.S. credit cards can find these procedures detailed on the back of each monthly account statement.

=====

So check the back of your statements for further details.

(As I said, I suspected there would be some controversy: I expected it, however, to be in regard to my statements about the Better Business Bureau. I guess that most people have such low expectations on that score that they simply couldn't be bothered to comment :-)

Vancouver Institute for Research into Security Vancouver Canada V7K 2G6  
ROBERTS@decus.ca Robert\_Slade@sfu.ca rslade@cue.bc.ca p1@CyberStore.ca

---

## ABC Nightline re LaMacchia

*"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>  
04 May 94 06:20:39 EDT*

On 02 May 1994, ABC News \_Nightline\_ aired a program entitled, "Law and Order on the Information Superhighway\_", which focused on the case of David LaMacchia, an MIT student accused of wire fraud for allegedly having run a BBS which permitted traffic in stolen software.

The host was Chris Wallace, substituting for Ted Koppel.

I ordered a transcript of the program from Journal Graphics, Inc. / 1535 Grant Street / Denver, CO 80203 / phone 303-831-9000 / fax 303-831-8901.

The transcript is copyright (c) 1994 American Broadcasting Companies, Inc. and therefore I can provide only an abstract.

[I received the entire abstract from Mich, who also provided me with an annotated version, which is included here. My apologies if I omitted anything necessary for understanding. However, because Mich included chunks of the abstract before each of his annotations, I could not run both the full abstract and the annotated version. PGN]

U.S. Attorney Donald Stern accuses David LaMacchia of having tolerated the exchange of stolen software worth more than \$1 million. Prof. Laurence Tribe of Harvard University Law School questions the implications of such an accusation; he argues that LaMacchia's BBS should be accorded the legal status of a common carrier, thus exculpating the owner of crimes committed through his communications channel.

Analysis of the Nightline program about David LaMacchia and the software exchange BBS:

[set flame = on]

<<LaMacchia's attorney, Harvey Silverglate, argues that providing a venue for the commission of a crime is not a crime: "The question is whether someone who activates the system should be liable for what anyone else does, or do you look to punish the person who actually commits the wrong, who actually copies, steals the software?">>

Silvergate's legalistic attitude is understandable (he is a lawyer, after all) but fails to address the question of values. Many BBS operators exercise control over content of communications or files on their systems--not out of fear of legal prosecution, but because they don't want to be tacit or active supporters of bad things. As Sysop in the NCSA's security forum on CompuServe, I have removed abusive messages and written to their authors with reminders of the standards of decorum my fellow Sysops and I expect on the forum. Free speech doesn't enter into it: CompuServe is a privately owned network and Sysops have a responsibility to maintain an environment in which participants address the issues without descending to abusive, ad hominem attacks. We do these things because they fit our values. We do not assume that if something is not illegal it must be right.

....

<<Silvergate claimed that Congress does not want to penalize BBS operators for criminal acts carried out with their systems, "... because nobody would then operate these systems, and the communications highway, the information highway would grind to a halt.">

These predictions are wrong. Many people, including the Sysops on CompuServe and many moderators in Internet news groups, regularly impose restrictions on content on moral grounds and out of respect for possible legal entanglements. For example, although I regularly post extracts of the RISKS FORUM DIGEST on the NCSA Forum, I don't post what appear to be entire copyrighted articles.

....

<<Corley replied, "...On the Internet there are no tangibles. You can ... steal something and they no longer have it, or you can go on the computer system or computer network and copy something, but it's a copy. It's not the same as stealing. I think that's the first thing we have to get over. We can't use the same analogies that exist in the real world, because this is no longer the real world.">

Corley exemplifies an attitude prevalent among criminal hackers: dehumanization of cyberspace. It seems to them that there are no people on the other end of the communications channel, only things. Stealing software in this context seems victimless; in reality, companies are losing money, and people are suffering monetary losses. Some small companies can go out of business entirely if they cannot get sufficient revenue to cover the months of grinding, often poorly-paid work by their employees. Human beings have smaller salaries or even lose their jobs because of software theft. Cyberspace is as much a part of the real world as speech, books, and telephones. No one would argue that stealing a book is a victimless crime--or would they? Some unscrupulous bookstores rip the covers off books, return the covers to the publisher for a credit, and then sell the mutilated books--with not a penny going to the people who wrote, edited, printed, bound, and marketed the book.

....

<<Wallace protested, "... what's the difference between copying a program which I'm then going to appropriate and use, and stealing?"

Corley continued, "It's not stealing, because you're not depriving somebody of it.... we're presuming that people are not selling this material. This is something that someone is simply copying to either examine, to analyze, what have you. There's different reasons why somebody would legitimately copy something."<>

Criminal hackers and software thieves miss the key point about intellectual property or confidential information. It isn't the copying that causes harm, it's the owner's loss of control over a valuable resource. Software companies sell a license to use a product, not the product itself. Software thieves steal the ability to enter into a contract with a user; it is the lost revenue that is in question, not the extra copy itself.

....

<<Jim Settle, retired member of the FBI Computer Crime Squad, argued that it is the software creator which determines whether software shall be freeware, shareware, or commercial software.

Corley said, "The problem with that is, though, that somebody can put a particular value on a piece of software and say, 'This costs \$10,000,' and then somebody copies it with a single keystroke and they're charged with stealing \$10,000...."<>

Corley implies that it is illegitimate to apply whatever price the creator wishes to a product or service. But a producer normally charges what the market will bear: a price which maximizes profit. Too high for perceived value and the market chooses alternatives--or they develop by less greedy competitors. Too low, and the producer risks going out of business.

The other peculiar (wrong) suggestion in this passage is the idea that the ease with which an act is performed somehow mitigates responsibility. So a single-keystroke copy is more of an excuse for stealing software than a 20-character command? If a vandal demolishes a building by attacking it with an ice pick over a 5 year period, are we expected to perceive his act as worse than if he had blown it up by pressing a button to explode a nuclear bomb? Once again, Corley confuses technology with morality.

....

<<In a discussion on the extent of copyright violation, Corley explained his view of why programs get copied: "... computer programs are designed to be copied, so naturally people are going to copy them. If we don't want people to copy them, then we make them so that they are uncopyable, or so that people want the original."<>

Ah, the familiar fallacy of moral possibility. This error consists of believing that if something is easy it must be right. The corollary is that the victim is to blame for being victimized. Thus if a bank robber uses a howitzer to blow a hole in the wall of a bank, it serves the bank properly for having failed to encase its building in three-foot thick titanium beryllium alloy. So software manufacturers should impose the endless nuisances of copy

protection on their products--even though these methods increase costs, enrage consumers, and don't work anyway because little creeps find ways of countering every single programmatic technique invented to date.

Just because it's possible to steal doesn't make it right.

<<Corley explained that many people tape record albums illegally; "from the band's point of view, though, it's a good thing that their music is being distributed, you see. And that's how I think we should look at copywritten software. The software is getting out. I don't think Microsoft is going to go out of business, and they're probably the company that is copied the most.">

Here we have Corley taking up the unpaid position of marketing director for musicians as well as software companies. Decisions on how to market a product or service are rightfully the responsibility of the owners of that product or service. Criminal hackers have no moral justification for interfering with those decisions.

<<Settle reminded Corley that Microsoft doesn't offer DOS for free distribution. Corley replied, "Well, they know that there are people that will pay for it, and there lots of people that will pay for any particular program, there are companies that will pay the corporate rate.">

So Corley recognizes that honest people either agree to abide by the software license agreement or they don't use the product. So what are we supposed to do about the creeps who jack our price up by stealing the same products? Corley's attitude reminds me of the idiots who race by traffic jams by using the emergency lanes; these people are contemptuous of the rest of us, sitting in orderly lines, waiting to take our turn past the obstruction causing the holdup. But no, the scoff-laws, like Corley, feel that they don't have to abide by such rules.

<<Settle repeated his point: "But they're not saying, 'Do you choose to pay or not pay?' They saying, 'You owe me X number of dollars for this product.'"

Corley replied, "Right, but that's not very realistic. There are college students that want to use computers, and according to organizations like SPA, they cannot have access if they cannot afford whatever price the software company says they have to pay, and the same thing for people in other countries." He then made an analogy between programs and books, saying that we encourage literacy with libraries but don't encourage computer literacy.>

Ah, a new right. Many criminal hackers espouse the view that they have a right to use any software they please without paying for it. The reasoning, such as it is, seems to be "I wannit--so it's mine." No one on this planet has a right to use the database I have designed to track my projects. I wrote it, I debugged it, I refined it. It's mine and mine alone. If I choose to let Albert use it and not Bob, that's my choice. If I choose to sell it only if the buyer agrees not to shoot sparrows, this eccentric term in the license agreement can be accepted or rejected by a prospective buyer, but they have no right to use the product without that contractual agreement. Can't afford MS-Word? Use another word processor. Don't like the terms of a license that doesn't let you make a copy for your portable computer? Buy

another product or do without. But wanting to use somebody else's tool is not moral justification for stealing it.

[set flame = off]

Michel E. Kabay, Ph.D. / Dir Education / National Computer Security Assn

---

## Risks of electronic door locks for automobiles

*Paul Wallich <pw@panix.com>*

*Wed, 4 May 1994 21:56:20 -0400 (EDT)*

The underlying risk of electronic car door locks is that the state of the lock depends on what a microprocessor believes rather than whether someone has turned a key or pushed a latch button. In addition to the obvious failure modes (do you need a working battery to unlock the car?) the manufacturer can also program in more complex lock behavior. Drivers and passengers may find out the full range of lock states only when bitten by a previously unknown "feature".

For example, last week I drove a two-door Chevy Cavalier that unlocks both doors when the ignition is turned off. Makes it harder to lock keys in the car, but could also pose a risk of theft if you don't notice. Compared to the Buick Century I was driving for a few days prior to that (and you'll understand why shortly), the Cavalier's behavior is positively benign.

During a sudden spring blizzard at 2,500 meters in Northwest New Mexico, I discovered the Buick's quirk. I went onto the shoulder to avoid a pickup and trailer that had decided to stop in the middle of the road during a brief zero-visibility whiteout, and found myself stuck in a newly-minted snowbank. So I turned on the hazard flashers and went to see how hard it would be to dig out. Since I had left the engine running, the doors locked automatically behind me (I later verified that this is a "well-known" behavior to the rental agents in Albuquerque). The risks of standing outside a locked car in driving snow on a lightly-traveled mountain road (wearing clothing more suitable for low-altitude desert) should be obvious. Without the timely passage of two other tourists (bound from a monastery near Abiquiu to a commune at Taos) this posting might not have been possible.

I was somewhat taken aback to note that it took the tow-truck operator less than a minute to unlock the car, equipped only with a small pry bar and a bent steel rod. So the electronic locking mechanism does not seem to add security.

During the mechanical era, auto manufacturers figured out various way to make it difficult or impossible to lock your keys in a car; it's not a good sign that they seem to be relearning those lessons from scratch.



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 16: Issue 4**

**Tuesday 10 May 1994**

## Contents

- [Secret elevator codes baffle Metro Toronto government](#)  
[Dave Leibold](#)
- [Smoke or Malaria - Lesser of the two evils](#)  
[Hiranmay Ghosh](#)
- [Dartmouth prof spoofed](#)  
[Mich Kabay](#)
- [11-digit ZIP code](#)  
[Christine Harbs](#)
- [Frozen computer scientist](#)  
[David Honig](#)
- [Re: Bellcore cracks 129-digit RSA ...](#)  
[Paul C Leyland](#)  
[Dik Winter](#)  
[Paul Buder](#)
- [Re: Streetwise Guide \[Risks of following up on credit-card laws\]](#)  
[Robert Slade](#)
- [Future of US health care?](#)  
[Mark Stalzer](#)
- [White House May Issue National ID Cards](#)  
[Mitch Ratcliffe via W.C. Daugherty](#)
- [Canadian long-distance service reseller blunders](#)  
[Mich Kabay](#)
- [Cheers to two companies](#)  
[Michael J. Zehr](#)
- [Re: MIT student arrested](#)  
[David desJardins](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Secret elevator codes baffle Metro Toronto government

*Dave Leibold* <[Dave.Leibold@f730.n250.z1.fidonet.org](mailto:Dave.Leibold@f730.n250.z1.fidonet.org)>  
06 May 94 00:06:10 -0500

An article in [\\_The\\_Toronto\\_Star\\_](#) on 5 May 1994 described secret codes which

are necessary to maintain elevators at Metro Hall, the building which houses Metro Toronto municipal council and services. The elevators, made and maintained by Schindler Elevator Corp., require secret password codes in order to maintain them. This means that only Schindler staff can maintain the Metro Hall lifts, and as such forced Metro Council to award a 10 year contract of \$3.5 million to Schindler. Meanwhile, Metro is also suing the building's developer, Marathon Realty, to try to get the codes. Without the passwords, elevator maintenance contracts cannot be given to a competing firm.

Metro Councillor Howard Moscoe wanted the Council to issue a \$10 000 reward to the first person to successfully crack Schindler's Code. This motion probably didn't get approval.

David Leibold    Fidonet 1:250/730   dave.leibold@f730.n250.z1.fidonet.org

---

## Smoke or Malaria - Lesser of the two evils

*Hiranmay Ghosh <ghosh@cdotd.ernet.in>*

*Mon, 9 May 94 09:07:35 IST*

RISKS usually features risks in high technology area, especially with computers. I am tempted to site one example for risks in a relatively low technology area encountered in a developing country like ours!

In the '50s or early '60s, there had been a massive drive to eradicate malaria (a disease characterized by high fever and spread through mosquito bites) from India. The attack was primarily on the mosquitos; their lot were killed by pesticides and their hideouts destroyed. The operation was considered to be successful and a case of malaria was rare for about twenty years to come!

Unfortunately, in late '80s, mosquitos came back with renewed a vigour and brought malaria back. How did the mosquitos come back? Some 'experts' assign the following reason:

In '60s or '70s, most of the Indian household used hearths (coal-fire) to prepare the food. At that time, a popular sight at the dusk at an Indian town was the smoke coming out of every dwelling unit to mark the ignition of the hearth for preparation of the evening meals. In a city, where the population density had been high, the volume of smoke was significant and caused concern about pollution! But, that was the time, when the mosquitos invading the households (dusk is the peak activity hour for the mosquitos!) were repelled by the smoke.

In the '80s, the hearths were replaced by 'modern' 'non-polluting' gas stoves. The coal-lit hearth was even banned in many cities in an attempt to curb pollution. So, now there is nothing to prevent the mosquitos to come and join us for dinner and spread malaria in the process!

I am not sure, if the reason cited is a valid one, but the concern about the re-advent of malaria in India is beyond any doubt!

[Next time, lease a collection of mutant boll weevils to eat the

mosquitos and you will be confronted with a lessor of weevils. PGN]

---

## Dartmouth prof spoofed

*"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>  
09 May 94 06:31:56 EDT*

Here is some old news that was new to me:

According to the *\_Dartmouth Life\_* newsletter (Feb 1994--I'm just clearing up my in basket today), an article appeared in *\_The New York Times\_* on 94.01.05 entitled "Confronting changing ethics of the computer age."

The unsigned article begins, "Hanover, N.H. -- Somebody in Prof. David Becker's course on Latin American politics did not want to take the midterm exam, so he or she used Dartmouth's innovative electronic mail network to impersonate a department secretary and cancel the test.

"At 11 o'clock on the night before the test in the Government 49 class, a message flashed on students' computer screens. Because of a family emergency, the message said, Professor Becker would be unable to administer the midterm."

The article explains that half the class understandably failed to show up for the test. No one has been identified yet as the culprit.

The rest of the article talks about the extensive electronic mail system on campus. One of the key concerns of the unregulated network is the rapid spread of rumours: "Late in August computer flashed an account of a woman being raped while jogging near campus. The message was intended as a warning, but there had been no rape."

The Hanover police department were swamped with calls. The Chief of Police now has his own electronic mail account to try to squelch rumours.

M. E. Kabay, Ph.D. (Dartmouth '76) / Dir Educn / Natl Computer Security Assn.

---

## 11-digit ZIP code

*Christine Harbs <charbs@teetot.acusd.edu>  
Mon, 9 May 1994 14:28:30 -0700 (PDT)*

According to the *\_Friday Report\_* <April 29, 1994>, Gene Del Polito, Exec. Dir. of the Advertising Mail Marketing Assn. is urging the Postal Service to adopt an 11 digit ZIP code. The 11 digits would consist of the original five + four, and the last two will be the last two numbers of YOUR house address.

<<Developing and using an 11-digit code, called a delivery point ZIP Code, is a way to 'purge the costs out of the postal system... and add value to mail as a communications medium,' said Del Polito.>> Translation? Better targeted junk mail.

This means that, with only a ZIP code, marketers and harassers will darn near

be able to pick out my house. Marketers do a lot of demographic research based on ZIP code. This could lead to extremely targeted marketing. Although not everyone would consider this a risk...

Another concern arises for people who are being stalked or harassed. Again, with just the ZIP code, the stalker could pinpoint, at the very least, the victim's street. Systems which claim to protect privacy and confidentiality because it just uses a ZIP code for identifiers, may have to be redesigned.

<<'The reality we're stuck with is that many people in this country simply don't know what their accurate and complete address is,' said Del Polito.>> I am sure a lot of people make mistakes when addressing an envelope. I do not think the way to solve this problem is to create a system where 11 digits create a path to my doorway.

---

### Frozen computer scientist ([RISKS-16.03](#))

*David Honig <honig@binky.ICS.UCI.EDU>  
Fri, 06 May 1994 10:01:10 -0700*

In the last RISKS someone writes about the dangers of automatically-locking doors when standing in a blizzard at 2500 feet wearing light clothing. The author posits a somewhat amusing possible outcome, had he not been saved by travelling communists: a computer scientist frozen to death next to his over-clever, running but locked, vehicle.

Of course, more hardware-oriented types might have clued in to the brittleness of said vehicles' windows before hypothermia set in... :-)

---

### Re: Bellcore cracks 129-digit RSA encryption code ([RISKS-16.03](#))

*Paul C Leyland <pcl@foo.oucs.ox.ac.uk>  
Mon, 9 May 1994 18:04:54 +0100*

- > predicted would take "40 quadrillion years" to break. ...
- > This mathematically arduous task was accomplished in eight months by
- > 600 volunteers in 24 countries who used their organizations' spare
- > computing capacity. ...

There are two risks, one amusing. Ron Rivest now regrets ever making that 40 quadrillion years estimate. It was silly when he made it; his papers in the scientific literature from that era give estimates which are within an order of magnitude of how much computation we actually used. From those estimates, and the observation that way back then it wasn't feasible to hook together hundreds of computers, we can deduce that a late 70's supercomputer using the best algorithms available then would have taken a few decades, maybe a century. Certainly much less than the 40 quadrillion years. The risk is: making predictions about the runtime of computer programs can sometimes make you look silly 8-)

The other risk is more serious. RSA is widely used to protect commercially significant information. 512-bit keys are widely used for this. Most, if not all, smart-card implementations are restricted to 512-bit keys. RSA-129 has 425 bits. I estimate (taking a risk 8-) that 512-bit keys are only about 20 times harder to break than 425-bit keys. Readers are left to draw their own conclusions. However, it is not by chance that I have a 1024-bit PGP key.

Oh yes, as Arjen Lenstra had pointed out: if you had used RSA-129 as the modulus in a digital signature for a 15-year mortgage, you would have been cutting it pretty fine. It is the use of RSA for long-lived signatures which needs to be examined with a very critical eye.

Paul Leyland (one of four RSA-129 project coordinators)

### Re: Bellcore cracks 129-digit RSA encryption code

<Dik.Winter@cwil.nl>

Fri, 6 May 1994 02:45:26 +0200

Perhaps because there is no risk beyond the known ones? Bob Silverman of MITRE (well known in number factoring circles) has publicly predicted already some time ago that it would require about 5000 MIPS years to factor the number. Reasonably close to the actual figure.

That the team was led by Bell Communications Research is untrue. It is a team led by four people from Bellcore (Arjen Lenstra), MIT (Derek Atkins), Iowa State University (Michael Graff) and Oxford University (Paul Leyland).

dik t. winter, cwil, kruislaan 413, 1098 sj amsterdam, nederland, +31205924098  
home: bovenover 215, 1025 jn amsterdam, nederland; e-mail: dik@cwil.nl

### Re: Bellcore cracks 129-digit RSA encryption code ([RISKS-16.03](#))

Paul Buder <paulb@teleport.com>

Thu, 5 May 94 20:02 PDT

I've heard this 40 quadrillion years figure a couple of times now and I find it odd. Is that what the Scientific American said? I have the original document from MIT's Laboratory for Computer Science. It's titled "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" by Ronald Rivest, Adi Shamir, and Len Adleman, April 1977. I can't do superscripting with vi so 10<sup>10</sup> means 10 to the 10th power. It has the following table in it:

Digits	Number of Operations	Time
50	1.4 X 10 <sup>10</sup> th	3.9 hours
75	9.0 X 10 <sup>12</sup> th	104 days
100	2.3 X 10 <sup>15</sup> th	73 years
200	1.2 X 10 <sup>23</sup> rd	3.8 X 10 <sup>9</sup> th years

300	1.5 X 10 <sup>29</sup> th	4.8 X 10 <sup>15</sup> th years
500	1.3 X 10 <sup>39</sup> th	4.2 X 10 <sup>25</sup> th years

200 digits was supposed to take 3.8 trillion years and 100 a mere 73.  
So where does the 40 quadrillion figure come from?

paulb@teleport.COM Not affiliated with teleport.

---

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">  
Mon, 09 May 1994 12:06:09 -0600 (MDT)

Subject: Risks of following up on credit card laws (last one)

In response to my initial posting of the "Streetwise Guide" book review, and subsequent summary of the initial responses, I (and, I presume, PGN as well) am still receiving mail on the subject. Unfortunately, there is a lot of disagreement and a shortage of direct quotes from the relevant statutes. I pass along these messages, therefore, since they contain at least references to the names of specific acts.

From: avm4@crux4.cit.cornell.edu

=====

The quoted material appears to be backwards, judging from the text on the back of my credit card statement and also from the misc.credit FAQ:

Q504. Exactly which purchases qualify under the Fair Credit Billing Act?

You are protected if all of the following are true:

- The purchase was made with a credit card. (If it was a debit card, the money is already gone from your account and the bank won't get involved.)
- The amount charged is more than \$50. (The amount in dispute could be less, for example if you bought a \$90 lamp but were billed \$100. The amount in dispute is \$10.)
- You made the purchase somewhere in your home state, or within 100 miles of your mailing address. (I am not an attorney, but my understanding is that if you are having goods shipped to you by mail or phone order, the place of purchase is the address you are having them shipped to.)

If some of the above are not true, you are still protected if the credit-card company owns or operates the merchant, or the credit-card company mailed you the advertisement for what you bought. In that case your purchase is covered by the rules no matter where you bought or how much you paid.

In addition, you MAY successfully protest charges outside of these parameters, but there is no legal requirement for the credit card

company to do so.

=====

From: cramer@world.std.com (Bill Cramer)

=====

>I don't remember the exact language, but in the U.S. consumers have the  
>right to refuse charges made more than 50(?) miles from their home address.  
>The refusal must be in writing, within 30 days, possibly with an explanation,  
>etc. The bank must complete its actions within 60 days of receipt of this  
>letter, cannot charge interest or late fees on the disputed amount, etc.

This statement would seem to be in conflict with 15 USC 1666i(a), which states, in part, that a card holder can withhold payment only when the place of the transaction was **\*\*within 100 miles\*\***.

=====

There was also mention of a Consumer Credit Protection Act.

This is as far as I go, since 1) I am not a lawyer, 2) I am not an American and 3) I am part of the larger world to which my original comments still basically hold good.

---

## Future of US health care?

<stalzer@macaw.hrl.hac.com>

Fri, 6 May 1994 10:13:31 +0800

For the past few months, my baby daughter has had a large rash. My wife took her to our HMO a few times and the doctor (gatekeeper) finally authorized a blood test and a visit to a dermatologist once the blood test results were available. Last night, we received a form authorizing the visit to the specialist that contained a clearly labeled diagnosis of Lupis. We assumed that this was the result of the blood test and I logged into Prodigy to find out more about Lupis. The online encyclopedia had a detailed description and my daughter appears to have some of the symptoms. Furthermore, the disease is very serious and can lead to death. We were very worried and I immediately contacted the HMO. This was about 6:30p and the front office staff couldn't help us (the doctors were gone) even though their computer generated the form! (I expressed my displeasure as forcefully as possible without using colorful language...) I then called the dermatologist and what he had to say is very interesting. Apparently, the HMO contacted the dermatologist last week, described the symptoms, and asked for a list of possible diagnoses. He provided about half a dozen possibilities and the HMO doctor then picked the worst possible one so that it would get past the review committee! If he had put a more likely diagnosis, like an allergy or fungus, a specialist visit probably would not have been authorized. Also, the blood test results are not in, and based on my daughter's response to some medication, it looks like she has something simple that will clear up. Of course, she still gets to visit the dermatologist based on the "diagnosis" on the form.

I'm thankful that the HMO doctor "worked the system" to get the best possible care for my daughter. However, this form with a diagnosis of a serious disease

has me angry. Do health care providers really think it's okay to mail out something like that without making a personal contact? Do they tell people they have AIDS by mail now? Why didn't the front office staff at the HMO have a clue? Shouldn't doctors be spending their time helping people, not trying to figure out how to get around the system? And finally, do we really want the Clinton Administration to mandate this kind of system for all Americans?

-- Mark Stalzer (stalzer@macaw.hrl.hac.com)

---

## White House May Issue National ID Cards

Walter C. Daugherty <daugher@cs.tamu.edu>

9 May 1994 15:26:52 GMT

>From Prodigy 5/9/94:

White House May Issue National ID Cards

The Clinton administration is working on a national ID card that every American would need in order to interact with any federal agency, reports Digital Media: A Seybold Report, a computer industry newsletter based in Media, Pa.

The so-called U.S. Card would be issued to citizens by the Postal Service. It would be issued as a "smart card," with its own internal CPU, or as a plug-in "PCMCIA" card with megabytes of built-in memory.

Administration approval of the plan "could come at any time," states the newsletter.

Walter C. Daugherty daugher@cs.tamu.edu uunet!cs.tamu.edu!daugher  
Texas A & M University, College Station, TX 77843-3112 DAUGHER@TAMVENUS

[Several folks sent me Mitch's piece from EFFector Online 07.08, and Digital Media, "Ever Feel Like You're Being Watched? You Will..."

However, I cannot run it in RISKS because of its copyright notice.

Contact Mitch Ratcliffe <godsdog@netcom.com> (NOT RISKS) if you want a copy of the whole article. PGN]

---

## Canadian long-distance service reseller blunders

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>

09 May 94 17:32:49 EDT

In November 1993, I signed up with a long-distance service reseller in Canada. I won't give the name because there's no longer any reason to embarrass the company. Shortly after registering, I received a friendly welcoming letter explaining how to use their service. As expected, there was a special number to dial; when we got the dial tone, we'd punch in a 3-number PIN and our own telephone number. Then we'd get another dial tone and we would dial our destination number.

In the envelope were printed labels to stick on our phones with all of these instructions--including the PIN!

I called the company and asked to speak to the chief of security. When I finally got to speak to her, she expressed horror at the prospect of having customer PINs stuck to their phones in plain sight, where any passing dishonest person could pick up their access codes and call expensive places. It seems that no one in marketing or customer service had every discussed this brilliant plan with her or with her staff. She assured me that she would report the breach of security and effect changes.

Months passed.

In January, I spoke to the chief of security again. This time, I cheerfully told her she was running out of time. I sent her a registered letter warning her of the dangers to consumers; pointed out that although theoretically the user of a phone system is responsible for calls, there would be no way to squirm out of the irresponsibility of having sent out thousands of stickers showing the PINs of countless users; and that even if the company absorbed the costs of fraud, they'd be unable to prosecute even dishonest users who abused their own phone codes. I then added what I think was the clincher: if I didn't hear back from them within a week I'd publish a report in the RISKS FORUM DIGEST and in Computing Canada and make them a laughingstock.

I got a call from the VP to whom the security chief reports. He assured me that the problem was being solved. Indeed, a few weeks later, I received new stickers *\_without\_* a pin. The system now uses ANI to identify the client. Attempting to access the trunk from an unauthorized phone immediately causes an alert at the company switchboard; repeated attempts to abuse the system can lead to termination of service. The authorized user is informed of such attempts.

Moral: don't just ignore security breaches, fight them!

Michel E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

[Or threaten them with worldwide appearances in RISKS? PGN]

---

## Cheers to two companies

*<tada@MIT.EDU>*

*Mon, 9 May 94 12:40:52 -0400*

Although this forum is primarily for giving examples of computer problems, I'd like to give credit to two companies I recently dealt with that made an extra effort to reduce the risks in their systems.

My company recently switched to Fidelity for managing it's 401(k) retirement plans. Fidelity has a phone number one can call to check balances, transfer investments between different funds, etc. When you call for the first time, you're asked to select and enter a PIN. To identify yourself, you need the

plan number for your company, your social security number, and your birthdate. All these are easily obtained by others. To prevent misuse, the system sent confirmation by mail to the person's home address that a PIN was set up. (Allowing a PIN setup by phone worried me when I read their literature, but I felt this was a good way of minimizing the risk. Also it should be noted that one couldn't transfer money from one person to another, only transfer to different funds.)

A few days ago I stayed at a Marriott Courtyard in Landover, MD. They have an express checkout system in which a copy of the bill is printed and slipped under your door your last night there. On the bill is printed the credit card number used for billing. The copy slipped under the door had the number overwritten with a heavy black marker. It's possible that one could determine the number anyway, but it reduces the risk of casual observance, and at least demonstrates that they're thinking about the problem.

Cheers to both companies for thinking about the issues.

-michael j zehr

---

### Re: MIT student arrested (Cohen, [RISKS-16.01](#))

David desJardins <desj@ccr-p.ida.org>  
Tue, 3 May 94 13:43:20 EDT

Fredrick B. Cohen <fc@Jupiter.SAIC.Com> writes:

> As to the issue of his intent to pirate software, that was not the charge  
> against him. It was wire fraud! I have read the copy of the indictment and  
> commentary and I find this awfully strange.

According to his lawyer on Nightline (and this was not contradicted by the former FBI computer-crime head), Congress wrote the copyright law so that pirating software is not specifically criminalized unless one does it for profit. Whereas the wire fraud statute requires only a "scheme to defraud"; there need not necessarily be a profit motive.

David desJardins



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 16: Issue 5**

**Weds 11 May 1994**

## Contents

- [Are we betting on horses or computers? \(off-track betting\)](#)  
[Reva Freedman](#)
- [Amusing computer-related anecdote about local cable service](#)  
[H Morrow Long](#)
- [MTV Sues Curry](#)  
[Adam Curry](#)
- [China Airlines A300 Crash](#)  
[Mark Stalzer](#)
- [Re: Elevators, Car bumpers and Cryptography...](#)  
[Peter Wayner](#)
- [Re: Bellcore cracks 129-digit RSA encryption code](#)  
[Fred Cohen](#)  
[Amos Shapir](#)
- [Re: ACM Nightline](#)  
[Robert Morris](#)
- [Don't always believe those E-Mail addresses](#)  
[A. Padgett Peterson](#)
- [EFF's Kapor announces new cyberspace TV show](#)  
[Kapor via Stanton McCandlish](#)
- [Automation: request for input](#)  
[Ken Funk](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Are we betting on horses or computers? (Risks of off-track betting)

<[freedman@merle.acns.nwu.edu](mailto:freedman@merle.acns.nwu.edu)>

Tue, 10 May 94 15:46:02 CDT

Illinois has off-track betting on horse races. You can place your bet at one of these legalized bookie joints, then watch the race on TV and collect your winnings. If you place your bet early in the day, you don't even have to wait around for the race. You can watch the race at home and come back later to collect. That's the theory, anyway.

On Saturday, April 23, the computer system handling the betting for some of the remote sites crashed after the fourth race. People at the betting parlors were told that they couldn't place any more bets. But what about those who had placed their bets and left? When winners returned on Sunday to collect, they were surprised to learn that, from the racetrack's point of view, they had never placed a bet, and were offered only a refund of the cost of their ticket.

So were losers, if they had kept their tickets and happened to hear about the computer crash. However, the fact that refunds were available was not listed in the newspaper with the race results, mentioned on the telephone hot line, or mentioned on cable TV broadcasts of the races.

On Monday a class-action lawsuit was filed. By Tuesday, racetrack management had decided to pay up.

The system, designed by Amtote International, had only been in operation for a month. On the other hand, state officials had sued Amtote before for deficiencies in the previous system. No description was given of the original failure, but newspaper reports (Chicago Tribune, 4/26/94 and 4/27/94) said that a hardware problem caused the backup system to fail. The new system was designed to be "user-friendly." I hate to say it, but the most user-friendly component in this incident was the lawyers!

Reva Freedman freedman@merle.acns.nwu.edu

---

### **Amusing computer-related anecdote about local cable service**

*H Morrow Long <long-morrow@CS.YALE.EDU>  
9 May 1994 17:21:07 -0400*

A very interesting program was on Storer cable channel 70 last night [they call themself Comcast now, and serve the areas of West Haven, New Haven, and Hamden]. For a long time, only the following message was flashing at the top of the screen:

```
-----  
| Software Failure. Press left mouse button to continue. |  
| Error: 0000 0003 Task: 002006f0 |  
-----
```

Talk about having your software problems out where the world can see them. Didn't look like anyone was minding the store(r). I guess someone there had to press the left mouse button this morning...

H. Morrow Long, Mgr of Dev., Yale Univ., Comp Sci Dept, 011 AKW, New Haven, CT 06520-8285, (203)-432-{1248,1254} Long-Morrow@CS.Yale.EDU

[In the old days, it was not unusual for a mouse to nibble into a cable. Now we have cable nibbling at the mouse. Turn(er)about is fare prey. PGN]

---

## MTV Sues Curry

Adam Curry <curryco@panix.com>

10 May 1994 03:44:36 -0400

[IMAGE] MTV SUES CURRY

Last update: May 10 1994

\_New Jersey, May 10 1994\_

I had planned to keep the following quiet until more information was available, but since several journalists have already caught wind of it, I decided to get it out into the open so my side of the story is heard as well.

The domain I maintain and operate on the Internet, mtv.com was founded approximately one year ago. At that time I registered mtv.com with the InterNIC, purely because it was a cool address to have, and it was available. What a great "vanity plate"!

The site quickly became a frequently accessed "hangout" on the net, with an average of 35000 accesses daily from Mosaic clients alone. During the start up months I had many conversations with executives at MTV Networks about my endeavours, which btw, were all financed out of my own pocket, and vps from MTV Programming as well as Viacom New Media were aware of what I was doing on the internet, and although they stated "MTV has no interest in the internet" they gave me their blessing and supported my efforts.

This was enforced when I set up several email accounts on mtv.com for use in MTV's on-air programming. Ever since the summer of '93, popquiz@mtv.com was used for trivia quiz questions, that were then aired on MTV's "Most Wanted" a program I hosted at the time. Solicitations were made on the air, and the address was shown on the screen. For MTV's annual Valentines video dedications, viewers were offered the choice of calling in their dedications, or sending them via email to elove@mtv.com.

I never charged MTV Networks for this service, I purely saw it as a cool feature to introduce to MTV's programming, spreading the "gospel", so to speak.

Then I started to get a lot of press about mtv.com, and some people started to wake up at 1515 Broadway (MTV's HQ in New York City). And I was served with a "Cease and desist" on the use of mtv.com. MTV's attorneys claimed that there could be "confusion" for users of the internet, when connecting to *\*anything\** that had the letters mtv in the address, and then receiving music and entertainment information. I was obviously hurt by this move, but did see what point they were driving at, and asked if we could settle this matter amicably.

The situation cooled down for a couple of months, but when I resigned on-air from my job as a VJ, which MTV chose not to air btw, things started to get ugly.

Long story short, MTV Networks has filed a lawsuit against me, for copyright infringement of their "trademark", that being their "MTV" call letters, as well as having information online that was MTVN "property". In this case they

are referring to several press releases I put up on mtv.com, such an announcement about Beavis and Butthead's "experience" cd release. Understand that MTVN sent me these releases over their own internal computer network for this very purpose! Again, I was only doing this to promote the channel, not for my own personal gain..after all...mtv.com is free access for all, no charge.

Throughout all of this I have offered to maintain the site specifically for mtv, but again they said "we're not interested". Of course, I have no problem whatsoever removing all references to MTV Networks and it's projects from mtv.com, no that I don't work there anymore gives me even more reason to want to do this, but the kicker is they are moving for an injunction to make me stop using the internet address mtv.com!

This is of course totally unacceptable: I registered the domain name, and I don't plan on giving it up. Sure MTV and their parent company Viacom have a vast legal team, but david also nailed goliath, so I have faith. In the long run, everyone knows that the only \*true\* winners will be the lawyers.

There are many different viewpoints on this situation, but I feel that the use of mtv in an addressing scheme can't be seen as an infringement of intellectual property laws, and a search of the InterNIC database shows at least 15 domain names registered with mtv in the address. Irony is that I incorporated a company called ON RAMP, Inc (tm) and onramp.com was already registered to someone else, but I'm not suing them :)

It appears to me that MTV has their mind set on the address mtv.com, maybe not for now, but possibly for future use, and I feel extremely used, in that I built up quite an audience for that address, and they are basically saying "thank you very much, you may go".

A pre-motion hearing is scheduled for this thursday morning at 11am, wit the honourable Judge McKenna presiding, in an attempt to get an injunction to make me stop using the address mtv.com. I will update the situation as it unfolds.

Adam Curry, adam@mtv.com

---

## China Airlines A300 Crash

<stalzer@macaw.hrl.hac.com>

Wed, 11 May 1994 09:02:33 +0800

The L.A. Times today (May 11) published a story on the A300 crash last month at Japan's Nagoya airport. I'll quote the first paragraph and then summarize the remainder of the story.

"A terrifying battle between an inexperienced co-pilot and his airplane's super-sophisticated computer system preceded last month's crash of a Taiwanese jetliner that killed 264 people..."

The events described in the rest of the article are as follows:

1. The plane was being hand-flown on approach to landing by

- its 26-year-old copilot.
2. About 2 minutes prior to landing, the A300 went into "go-around" mode for reasons unknown.
  3. Even though the pilot warned the co-pilot 3 times in 30 seconds, as recorded by the voice recorder, the co-pilot continued to attempt to land the plane. The effect was that the auto-pilot was trying to pitch the nose up using the "horizontal stabilizer flaps" while the co-pilot was trying to pitch the nose down using the "elevator flaps" (the Times author might have this a bit confused).
  4. The crew then switched the "go-around" mode off. However, the "stabilizer flaps remained set at a sharp angle."
  5. The crew realized the plane was too high to land, so they set the "go-around" mode back on.
  6. This caused the plane to climb sharply and approach a stall. The A300 stall-prevention system automatically increased the engine thrust but this INCREASED the climb angle to 53degs.
  7. The airplane stalled.
  8. The nose dropped and the airspeed increased to 150mph at an altitude of 260 yards.
  9. At this point, the entire electrical system stopped functioning for reasons unknown, including the flight data and voice recorders.
  10. The plane crashed, killing 264 people. There were 7 survivors.

The root cause of this crash seems to be a confused co-pilot. However, the A300's automatic systems contributed in two ways. First, it continued to attempt the go-around even though the plane was still being flown by hand. Had the auto-pilot disengaged (with a suitable warning!) this whole disaster may have been averted. I think a human supplying control inputs is the "final authority" and the automatic systems should "back off". Second, the stall-prevention system's actions (increasing thrust) contributed to the stall. This is a serious kind of failure, if a automatic system designed to prevent a problem makes it worse, it should do nothing at all!

-- Mark Stalzer (stalzer@macaw.hrl.hac.com)

---

## Re: Elevators, Car bumpers and Cryptography...

Peter Wayner <pcw@access.digex.net>  
Tue, 10 May 1994 15:37:05 -0400

I once talked to a major elevator company about doing just what the Schindler Elevator Corp. is accused of doing by the Toronto government. ([RISKS-16.04](#)). The company told me that they were in the habit of selling the elevators at a loss so they could make up the money in service contracts. Then they found themselves battling independent service companies who undercut their prices. They hoped to use cryptography to lock out any other service provider without the right key.

Of course, this loss-lead approach is common in many businesses. Car companies often sell their cars at a low price and hope to make it up selling spare parts later. That is why I discovered that a spare bumper for my car cost over

\$500.

The difference is that other companies are now making duplicate parts. The major automakers can try and discourage them, but they can't lock them out of the business.

Cryptographic locks, though, are a different story. They probably can't be broken in a reasonable amount of time. (See also 16-04) I'm not sure of the case law on this, but I would suspect that it might fall under questionable or illegal trade practices. At least in the US.

---

**Re: Bellcore cracks 129-digit RSA encryption code ([RISKS-16.04](#))**

*Fredrick B. Cohen <fc@Jupiter.SAIC.Com>*

*Tue, 10 May 94 19:33:36 PDT*

I think a lot of people are missing the real point about the RSA. On my pocket PC, I can create a code that requires 5,000 MIP years to break in a matter of seconds. If I am willing to use several more seconds, I can make a code that takes  $10^{25}$  MIPS years to break. Compare this to any other encryption scheme, and you will find that the workload amplification of the RSA is quite good.

And Shannon told us in 1949 that any non-perfect information transform can be broken with enough cyphertext - and developed the concept of workload for evaluating cryptosystems. If we want perfect cryptosystems we know how to get them, but it requires secure distribution. On the other hand, the RSA provides any degree of complexity we wish to generate (finite) and a fantastic complexity amplification factor, and the advantages of a dual public key system that can be used for both encryption and authentication.

The point is that the RSA has not been broken, rather it has shown just how much of a David is required to defeat a given Goliath. After all, in terms of that story, David would have been a MIP second and Goliath 5,000 MIP years in relative sizes for a break-even fight. I'll take that David any day. FC

---

**Re: Bellcore cracks 129-digit RSA encryption code ([RISKS-16.04](#))**

*Amos Shapir <amos@CS.HUJI.AC.IL>*

*11 May 1994 15:19:01 GMT*

> So where does the 40 quadrillion figure come from?

It comes from this very table.  $10^9$  is a billion, not a trillion, in the US system, and 40 quadrillion is  $4 \times 10^{16}$ , which is even less than what I get by interpolating to 425 bits (can anyone who has access to the original RSA article verify this?).

There seems to be an interesting risk here: most encryption methods rely on "hard" problems, i.e. problems whose "brute force" solutions require computation resources which are an exponential function of the key length.

But in a world in which computing power grows exponentially, such problems can be solved in polynomial (or even linear) time!

Amos Shapir, The Hebrew Univ. of Jerusalem, Dept. of Comp. Science.  
Givat-Ram, Jerusalem 91904, Israel +972 2 585706,586950 amos@cs.huji.ac.il

---

**Re: ACM Nightline (Kabay, [RISKS-16.03](#))**

*Robert Morris <ram@cs.umb.edu>*

*Wed, 11 May 1994 10:09:00 -0400*

>...they have \_no right\_ to use the product without that contractual agreement.

This confuses several issues--that of theft, that of use and that of licensing, and in an important case Kabay's implied position is wrong. Certainly---and this is his main point---theft of intellectual property is theft. However, property protected by U.S. intellectual property laws, notably copyright and patent protection (especially the latter)---can not simply be withheld from use at the whim of the owner. For example, patent holders **MUST** license equally to all who meet reasonable terms. Indeed, the \_purpose\_ of copyright and patent protection is to promote the widest possible access to the new ideas by insuring that their creators have economic motivation to do develop them. The owners of intellectual property who want to restrict its distribution are expected to look to the trade secret laws to protect them.

I'm not sure what requirements are imposed on copyright holders (and as an aside, I sure would like The National Computer Security Assn. to argue that copyright, not patent, is the only appropriate form of protestation for software! heh, heh, heh.), but I suspect they can not capriciously and arbitrarily withhold copy permission from some but not others, and it will even surprise me if they can put irrelevant terms in the copy permission. None of this speaks to licensing, but (I speculate) the only legal culprit in a licensing violation is the licensee who allowed the copy. And presumably that contract violation is a civil, not a criminal matter in American law.

Bob, not an attorney, Morris

---

**Don't always believe those E-Mail addresses**

*A. Padgett Peterson, Information Security <padgett@tccslr.dnet.mmc.com>*

*Wed, 11 May 94 08:17:46 -0400*

One of the more subtle RISKS of E-Mail is in believing what you see. Recently a good friend of mine was repeatedly accused of posting not-so-nice messages on various news-groups. Not so blatant as to be unbelievable but morally damaging. This irritates me.

A few months ago I was flamed in RISKS for talking about the use of Ethernet card firmware addresses as for tracking. Two weeks ago it enabled me to quickly and positively identify the source of repeated failed attempts to log into an Ethernet server as supervisor. When I asked the administrator for the

data in the log, he told me that he had never known that the six hex bytes had a meaning.

Similarly, forged E-Mail is possible only because many E-Mail packages throw away the Ethernet wrapper that made the communication possible in the first place, a wrapper that *\*must\** contain the return address or "the mail won't go through".

Here I have FTP Software's (plug) PCTCP which provides an MSDOS machine with more built-in features than many UNIX implementations (won't go into them all else it would be an adv't but will just say that it allows me to identify not only the source, but the path used to get here).

For example what most people see in an E-Mail posting is this (lines have been wrapped to 80 characters & true returns masked) - Judge and Goat are two PCs in my office.

```
-----  
From Crusader_Rabbit@Jay.Ward.Cartoons Wed 11 May 1994 07:34  
To: padgett@goat.ppp.qqq.rrr  
Return-Path: <Crusader_Rabbit@Jay.Ward.Cartoons>
```

Demonstration of message headers.

What was actually received from the SMTP server was this but most newsgroups & many mailers strip the "Received: from..." as above:

```
-----  
From Crusader_Rabbit@Jay.Ward.Cartoons Wed 11 May 1994 07:34  
X-Envelope-To: padgett@goat.ppp.qqq.rrr  
Return-Path: <Crusader_Rabbit@Jay.Ward.Cartoons>  
Received: from judge.ppp.qqq.rrr ([123.456.789.000])  
by Goat.ppp.qqq.rrr (SMTPSRV); Wed 11 May 1994 07:34
```

Demonstration of message headers.

Note that not only the originating name is sent but also the true IP address [123.456.789.000]. Again this *\*must\** be there.

Not to say that this is not a valuable capability since I prefer that all incoming E-Mail come to a common point, just don't rely on them since they can be *\*anything\** the sender wishes.

Don't just toss those wrappers, dispose of them properly.

Padgett

---

## EFF's Kapor announces new cyberspace tv show

Stanton McCandlish <mech@eff.org>

*Tue, 10 May 1994 20:47:23 -0400 (EDT)*

Stanton McCandlish \* mech@eff.org \* Electronic Frontier Found. OnlineActivist

Forwarded message:

Date: Tue, 10 May 1994 09:13:23 -0400

From: mkapor@kei.com (Mitchell Kapor)

Subject: My tv show

(I thought you might be interested in this.)

New Cyberspace TV Program

I am developing a new program on cyberspace in conjunction with WGBH-TV, PBS' Boston affiliate. The show is intended to be a window onto the world of computer networks for the television viewer, whose point of view is that the world of on-line communications is interesting because of what people do there, not because of the digital plumbing which enables it. We will be focusing on the human aspects of networking and the individual and social aspects of being on-line. Cyberspace will be portrayed as a not-so-really strange territory after all, where all of us will increasingly come to live and work. My role is to guide people through this new territory, introducing the audience to its native culture, its scenic attraction, and its sights and sounds.

We assume our audience is motivated by curiosity to learn more about what goes on in cyberspace, but we do not assume they are knowledgeable or, in general experienced with it. On the other hand, we will not trivialize the subject matter by reducing it to a least common denominator.

We will give the show a look and feel which is approachable and down-to-earth. Interview guests and roundtable participants will be drawn from the net community itself. There will be plenty of demos of cool net stuff from Mosaic, CU See Me, and other cutting-edge applications and services.

We are taping two test shows in mid-June which will be shown in Boston and other cities and hope to have some sort of national distribution (to be determined) in the fall for a regularly scheduled program. We are also going to create a WWW server for the show, the segments of which will be downloadable. The server will have on it additional material which won't fit into the show format.

An Invitation:

We would like to include some video clips of net citizens expressing their greatest hope and worst fear about the future of the net which we will edit into an on-air piece for our regular feedback session.

It's important to me to have the voices heard (and faces seen) of people already on the net. This is an opportunity for those of us who enjoy appreciate the decentralized and democratic character to express that sentiment to a mass audience. I hope you'll take advantage of the opportunity.

Guidelines:

Since an individual on-air clip will run at most 20-30 seconds, please keep your statement succinct.

In shooting the clip, please feel free to pick a location which says something about yourself, whether it's your computer, your pet, or the great outdoors.

We can accept Quicktime movies, VHS cassettes, or 8mm tapes. If you enclose a mailer, we will return your tape. We can also pick up digital submissions from any FTP site, etc.

Contact Information:

email: cybertv@kei.com

Postal: CyberTV  
c/o Kapor Enterprises, Inc.  
238 Main St., Suite 400  
Cambridge MA 02142

---

### **Automation: request for input**

*Ken Funk <funkk@ENGR.ORST.EDU>*

*Thu, 28 Apr 94 06:59:08 PDT*

Oregon State University, America West Airlines, and Honeywell are conducting a study of flightdeck automation for the Federal Aviation Administration which requires input from the scientific community.

The increasing use of automation on the flightdecks of commercial transport aircraft has raised concerns about the overall safety effects of this equipment. While several studies have attempted to address some of these automation issues, until now no one has tried to systematically identify all issues that exist about flightdeck automation. The objectives of this study are to collect and compile a comprehensive list of all flightdeck automation problems and concerns and to address them in order to identify or generate recommendations and guidelines for the FAA, manufacturers, and operators.

To achieve these objectives we are soliciting information on automation problems and concerns from individuals in a variety of disciplines. When we have compiled these problems and concerns we will prioritize them, study the highest priority items using analytic methods and simulator studies, and identify and develop recommendations based on our findings.

Although we are primarily targeting the aviation community for sources of automation problems and concerns, we recognize that individuals in other disciplines have knowledge of other kinds of system automation and know of automation problems or have concerns about automation that would be very

relevant to our study. Experts in computer science, human factors engineering, psychology, and other fields often deal with the automation of industrial systems, office equipment, and even consumer devices, so we welcome information from them.

If you have direct knowledge about system automation and you know of problems with or have concerns about the safety of such automation, you can help us by filling out a copy of our Automation Problems and Concerns Questionnaire. This is an opportunity for you to contribute to flight safety and, if you wish, we will put you on our distribution list to receive copies of reports on the results of our study.

If you would like to fill out a questionnaire, send a message to [flight@engr.orst.edu](mailto:flight@engr.orst.edu) (don't post your request to this newsgroup!). Request a copy of the Automation Questionnaire, and I will send you a copy via e-mail. When you have completed it (which should take between 15 and 30 minutes), just e-mail the completed version back to me. The problems and concerns you identify will be added to our database and used in our study.

Ken Funk, Assistant Professor of Ind. and Mfg. Engineering, Oregon State Univ.  
[flight@engr.orst.edu](mailto:flight@engr.orst.edu), [funkk@engr.orst.edu](mailto:funkk@engr.orst.edu) (503) 737-2357 FAX: (503) 737-5241



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 16: Issue 6**

**Thursday 12 May 1994**

## Contents

- [Plane accidentally ejects pilot into sea](#)  
[Frank E Carey](#)
- [Tax preparation programs; IRS privacy; IRS computerization](#)  
[PGN and COOVER](#)
- [Digital Defamation in the UK](#)  
[Brian Randell](#)
- [We spy harder!](#)  
[Mich Kabay](#)
- [Killers sue over phone taps](#)  
[Mich Kabay](#)
- [Journalists attack credit card account](#)  
[Mich Kabay](#)
- [Fragmenting of the News](#)  
[Mich Kabay](#)
- [Software piracy vexes industry](#)  
[Mich Kabay](#)
- [Ultra-high dependability and the Channel Tunnel](#)  
[R.J. Stroud](#)
- [Re: Future of US health care?](#)  
[Amy McNulty](#)
- [Re: China Air A300 Crash](#)  
[David Wittenberg](#)
- [Re: Copyright/patent owners: quick correction](#)  
[Mark Seecof](#)
- [Re: Amusing computer-related anecdote about cable](#)  
[Ry Jones](#)  
[Paul N Hrisko](#)
- [Re: 11-digit ZIP code](#)  
[Ed Ravin](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Plane accidentally ejects pilot into sea

*F E Carey* +1 908 949 8049 <[fec@arch4.ho.att.com](mailto:fec@arch4.ho.att.com)>

Thu, 12 May 94 13:15:56 EDT

TOKYO (Reuter) - The test pilot of a trainer jet built for the Japanese air force was accidentally ejected when the emergency bailout system mysteriously functioned, the plane's makers said Tuesday. Pilot Masahiko Kameishi was later plucked from the sea by a military helicopter. He was reported to have suffered minor injuries to his arms and knees. Kameishi was flying the T-4 two-seater over the Pacific Ocean southwest of Tokyo on Monday when he was suddenly ejected into the sea with a parachute, a spokesman for manufacturers Kawasaki Heavy Industries Ltd said. His co-pilot, seated in the rear, landed the plane safely at a nearby military base. The Kawasaki spokesman said the company was looking into whether the ejection was activated by mechanical malfunction or by something the pilot may have touched. More than 100 T-4s are already in service with the Air Self-Defense Force, Japan's air force. Kameishi's plane was to have been handed over to the air force June 1.

Frank Carey at Bell Labs    f.e.carey@att.com

---

### **Tax preparation programs; IRS privacy; IRS computerization**

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

Wed, 11 May 94 15:47:47 PDT

1. The following item is apparently from COOVER@MITRE.ORG . It was sent by SnailMail to Will Tracz, the new editor of Software Engineering Notes, presumably for the RISKS section. Will faxed it to me.

From Law Practice Management, April 1994, p. 16:

Well, it's April again and time for the annual buying frenzy for All The Latest tax-return software. Just so you're on notice -- last year at this time \*PC Magazine\* did a comparison of twenty different tax-return packages. When they ran a test scenario through the packages (see -- I don't actually have to say it out loud anymore -- you people know what's coming), that's right, \*every single package\* computed a different total tax due.

Sort of like calling the IRS Help Line.

2. Colin Smiley sent me a note observing that his social security number was visible through the window of the envelope that contained his refund check, and pointing out the evident risks.

3. The IRS is now beginning the integrated computerization of its entire tax process. This presents many interesting risks relevant to our newsgroup, such as those relating to security, integrity, authenticity, insider abuse, fraud, violations of privacy, bogus returns, and so on.

4. Your RISKS Moderator is now a member of the IRS's Commissioner's Advisory Group (CAG), and cochairman of its Subgroup on Technology, Security, and Privacy. If you have problems that you believe need to be addressed, please send them to me (neumann@csl.sri.com) if you do not want them to appear in

RISKS. The next meeting is coming up in midJune.

PGN

---

## Digital Defamation in the UK

*Brian Randell <Brian.Randell@newcastle.ac.uk>*

*Thu, 12 May 1994 17:48:26 +0100*

The following article is quoted in its entirety from the (UK) Computer Weekly, issue dated 12 May 1994.

[Brian Randell, Dept. of Computing Science, University of Newcastle, Newcastle upon Tyne, NE1 7RU, UK +44 91 222 7923 ]FAX = +44 91 222 8232]

### Why bulletin boards are a libel minefield

Nick Braithwaite warns of the dangers of digital defamation and how network and bulletin board operators must guard against being unwitting participants in user's libellous missive

Libel doesn't figure prominently in most network operators' list of priorities. Many assume that transient screen messages are private and unlikely to damage anyone's reputation. Electronic mail and bulletin boards foster informal communication, so users may be resistant to the idea that defamation risks are attached to electronic "conversations" .

But beware if you run network or database. You could be in the firing line for a libel claim.

In the first case of its kind in the UK, Canadian academic Dr Laurence Godfrey issued a libel writ in London against another academic based in Geneva claiming he was defamed by a bulletin board message posted on the Usenet system. If the claim succeeds, hosts and users could soon be contemplating sizeable pay-outs.

In fact, there's nothing novel about the Godfrey case. Libel suits have been an occupational hazard for information providers and electronic database operators for many years, but now network hosts too have begun to experience defamation problems. Only recently, Compuserve was sued for libel in the US, while individuals in both the US and Australia have faced claims over uncomplimentary bulletin board messages.

Are electronic messages "published" for libel purposes? The first requirement is a degree of permanence in the communication. Most experts now agree that, if defamatory, even transitory computer messages flashed on screen are sufficiently permanent, once stored in memory, to be libellous. Slurs posted on bulletin boards are even more likely to be held libellous.

The "publication" requirement is minimal, satisfied if just one person other than the plaintiff sees the material.

Despite the international aspects of the Godfrey case, one solitary viewing of

a bulletin board in England allows a case to be litigated in London, where libel actions are hard to defend.

The author of a defamatory statement is an obvious libel target, but corporations with deep pockets usually make more enticing defendants. Happily for US-based computer networks, the court in the CompuServe case ruled CompuServe could not, without editorial control, be liable for defamatory statements by users.

In England, it is likely that operators will have to prove they were not negligent or reckless in allowing the statement onto the system. So if you follow the US standard, you should not exercise any editorial control at all. If you follow the English standard you should exercise maximum control.

In fact there ought to be no real conflict, because it is difficult to imagine a court insisting that an operator should vet all messages on the system.

Whichever standard of care prevails, database and public access network operators will have every incentive to minimise editorial control over what they carry.

Plainly, for some databases and networks that will not be practical. But for libel purposes, the ideal is probably to emulate a telecoms carrier, disclaiming all responsibility for the content of messages. Some practical steps to keep the lawyers at bay are:

Check you have a warranty from the subscriber that they will not input defamatory material. Or, if you are worried about staff messages, put a warning in their contract of employment. Consider a statement in your user contract that the operator has no editorial control over traffic on the system. Display a warning on-screen that the host does not endorse any defamatory statements. These may not solve every problem, but will help reduce risk.

[Nick Braithwaite is a lawyer in the London-based media group of solicitors Clifford Chance]

---

## **We spy harder!**

*"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>  
11 May 94 21:51:19 EDT*

>From the Reuter newswire via Executive News Service (GO ENS) on CompuServe:

"FORT LAUDERDALE, Fla, May 9 (Reuter) - Three former owners of Value Rent A Car Inc pleaded guilty Monday to racketeering charges and face prison sentences of two to five years and fines totalling \$2 million."

They are also accused of having wiretapped the offices of Mitsubishi Motors executives. Mitsubishi Motors owned 80% of the firm at that time.

[MK: This is known as taking an interest in management.]

---

## Killers sue over phone taps

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>  
12 May 94 12:25:19 EDT

United Press newswire (94.05.11 @ 09:59 EDST) via Executive News Service on CompuServe:

CAMBRIDGE, Mass., May 11 (UPI) -- A Massachusetts judge continued a hearing on a suit by eight convicted murderers who seek to end the state's new practice of monitoring inmate phone calls to the outside.

The eight lifers, saying they are representing all 10,000 state prisoners, filed suit against Nynex and Massachusetts corrections officials for tapping their phone calls."

The article continues with the following key points:

- o William "Lefty" Gilday, convicted of murdering a policeman, claims that the phone monitoring system is unconstitutional.
- o Corrections officials argue that "the taps are necessary to curb fraud, harassment and drug dealing by inmates."
- o Gilday was convicted in 1984 of running a credit-card fraud operation from prison and defrauding American Express of \$4,000.

[MK:  
set flame = on

Interesting perspective on rights and responsibilities, eh? These folks remind me of the self-righteous anger of some criminal hackers when legal processes interfere with their self-proclaimed rights to attack other people's computer systems. "Rights for me, not for you; duties for you, not for me." Could we maybe apply the Key-Escrow Proposal to criminals? How about "Lock 'em Up and \_Throw Away\_ the Keys"?

set flame = off

Why is my neck turning red?]

Mich Kabay / not representing anyone else this time.

---

## Journalists attack credit card account

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>  
11 May 94 21:51:29 EDT

>From the Reuter newswire via CompuServe's Executive News Service (GO ENS):

"FRANKFURT, May 10 (Reuter) - A journalist from a well-known German satirical

magazine has cut off fugitive real-estate tycoon Juergen Schneider from one source of cash -- by ringing up Schneider's credit card company and cancelling his account.

The magazine Titanic said journalist Bernd Fritz had telephoned the Eurocard company and blocked the account by giving Schneider's name and date of birth."

The article explains that Schneider has been on the run for over a month and has filed for bankruptcy. He is under investigation for credit fraud.

Asked for identifying information, including Schneider's bank, the journalist picked a bank at random--and was right.

The magazine writers now claim that they will try to block credit cards for other fugitives.

[Comment by MK: I have been saying for a long time we need PINs for credit cards! I hold no brief for the accused man, but it does seem odd that someone else be able to cancel a person's account. How would you like it if some prankster cancelled \_your\_ credit/bank/phone/... account with a simple phone call?]

Michel E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

---

## Fragmenting of the News

*"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>  
12 May 94 12:25:13 EDT*

The Washington Post newswire (94.05.11) includes an interesting essay by Michael McKeon entitled, "Fragmenting of the News." The author discusses the declining importance of the mass media for distributing news and the rising importance of electronic communities where opinions are more uniform.

<<

---

## Software piracy vexes industry

*"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>  
12 May 94 12:25:02 EDT*

United Press International newswire (94.05.11 @ 01:46 EDST) reports on an interview with Business Software Alliance President Robert Holleyman during his visit to Microsoft offices in Redmond, WA.

<<

---

## Ultra-high dependability and the Channel Tunnel

*Robert Stroud <R.J.Stroud@newcastle.ac.uk>  
Thu, 12 May 1994 11:49:04 +0000*

[Sent to RISKS courtesy of John Rushby <RUSHBY@csl.sri.com>. PGN]

From an article by William Hartston, \*Independent on Sunday\*, 8th May 1994, p.21 (numbers column)

A major accident in the Channel Tunnel resulting in 70 or more deaths will happen once in 100,000 years, according to a report by Eurotunnel. Impressive, but how was it calculated?

Give or take a few millenia, 100,000 years is the time homo sapiens has been around; 10,000 years ago, you could walk from England to France without getting your feet wet. So how did Eurotunnel look 100,000 years into the future? It began with statistics from 1984-90, which showed a total of 313 people killed in railway accidents in Britain, including 99 at stations. With 268 billion passenger kilometres traveled, simple arithmetic yields figures of 0.08 fatalities per 100 million passenger kilometres plus 0.95 fatalities per 100 million passenger journeys (for those killed at stations). These figures, and their French equivalents, were then combined and applied to the tunnel, as though it were a randomly selected 50km stretch of track, with a station at each end.

The figure may then be modified by the decreased likelihood of anyone throwing himself in front of a moving train under the Channel. Fires and derailments, however, (estimated at 4.4 per cent and 18.5 per cent respectively of the "total system risk") are likely to have more serious consequences, which are, in turn, balanced by more stringent safety procedures.

Eurotunnel concludes: 'The Channel Tunnel represents a significant advance in railway safety' which may be true. But for all the precision, it is little more than informed guesswork: 100,000 years is a long time on a train line. The Titanic was unsinkable. Has Eurotunnel overlooked an iceberg too?"

[I believe Eurotunnel is planning for 10 trains/hour. I think that makes one accident every 100,000 years a  $10^{-10}$  claim..

I also heard something about an independent report that had been suppressed that argued that the 10 trains/hour figure was unsustainable taking into account factors such as gradients, length and weight of trains, time to accelerate from stations, etc. Robert Stroud]

---

## Re: Future of US health care?

<Amy\_McNulty@vos.stratus.com>

Wed, 11 May 94 14:18 EDT

In [RISKS-16.04](#), Mark Stalzer (stalzer@macaw.hrl.hac.com) wrote about his HMO doctor's deliberate "misdiagnosis" of his baby daughter's rash as lupus, in order to get past the HMO restrictions for referring her to a specialist. He was understandably quite upset at having received notification of this diagnosis in the mail, without any previous phone call or explanation from the doctor or other HMO personnel.

In addition to the ridiculousness of the HMO doctor having to play games like this just to refer a patient to a specialist that the doctor feels the patient needs to see, there's another big risk in this story. In this age of nation-wide computer databases like the Medical Information Bureau, this little girl (and other people like her who were similarly "misdiagnosed" by the HMO doctors) may now be listed somewhere in some database as having a serious, pre-existing disease -- which could cause her to be unjustly rejected sometime next century when she applies for life insurance, medical insurance, a physically demanding job, college, or who knows what else. I won't try to address whether this kind of database is fair or just even when the information it contains is \*accurate\*, but it should be obvious to RISKS readers that in this case (and many others) it could also contain inaccurate, very damaging information.

-- Amy McNulty (amy\_mcnulty@vos.stratus.com)

---

### Re: China Air A300 Crash

David Wittenberg <dkw@cs.brandeis.edu>  
Wed, 11 May 1994 16:46:53 -0500 (EDT)

> The root cause of this crash seems to be a confused co-pilot.

I think you're being much too harsh on the copilot. He was trying to fly the plane in a standard way, and the plane's auto-pilot did something inexplicable. While perhaps the copilot could have responded better (but note several other odd auto-pilot actions later), I would have to say the root cause was the "go-around mode for unknown reasons".

Since people don't always diagnose unexpected behaviour correctly, it is important to decrease the chances of their being confronted with some unexpected behaviour in a time or place with little margin for error. The question one has to ask about the rather sophisticated auto-pilots now in use is not "are they perfect?" We know that they aren't. But, "How often do they fail, and can pilots reasonably be expected to recover from the failures?" By comparing the dangers of the new technology with the dangers of the old technology, we can make an intelligent choice. Unfortunately, the vendors try to convince us that their technology is perfect, which is clearly false.

--David Wittenberg   dkw@cs.brandeis.edu

---

### Re: Copyright/patent owners: quick correction

Mark Seecof PSD x77605 <marks@latimes.com>  
Wed, 11 May 1994 13:37:23 -0700

I won't name names, but another RISKS contributor suggested that copyright owners or patent holders "MUST" license to all on reasonable terms. That is not true. In general patents or copyrights may be licensed on any terms the owner can get and the owner may pick and choose licensees at will. The exceptions are few, and are related to antitrust issues that do not apply to

99.99% of situations. Some (other than the U.S.) countries have mandatory licensing of various kinds of patents and copyrights (e.g., mandatory licensing of educational textbook copyrights in India), but again, with a few exceptions, the U.S. doesn't work that way. And for other pedants like me: I'm not gonna launch into a discussion of "fair use," music-performance situations, copyright collectives, weapon patents, and other stuff which would explain some of the "exceptions" to the general rule I've alluded to.

Think about it. What competitive advantage would a patent confer if you had to license it to anyone? Ditto copyrights. The whole point of such rights is to limit the people who can exploit a certain work.

Mark Seecof <marks@latimes.com> Publishing Systems Dept. Los Angeles Times

---

### **Amusing computer-related anecdote about local cable service**

*Ry Jones <rjones@poseidon.usin.com>*

*Wed, 11 May 94 14:22:21 PDT*

TCI Cablevision of Washington often has a similar display with a Guru Error (Amiga) for days on end on the Public Info channels. Also, Cablevision of Terre Haute, IN used to have a Apple ][+ that would bomb out and draw random lines on the PI channel. Terre Haute First National Bank built a new building complete with 6 huge automated computer displays (light-bulb type) and they often got out of sync, triggering an alarm that would display a very distinct Commodore Basic prompt on all six signs all night.

---

### **Amusing anecdote about local cable svc. (Long, [RISKS-16.05](#))**

*PAUL N HRISKO <WJCS75A@prodigy.com>*

*Thu, 12 May 1994 16:54:23 EDT*

long-morrow@cs.yale.edu (H Morrow Long)

writes about the error he noticed on his local cable channel recently.

Our local cable system and a couple of the surrounding ones use Commodore Amigas for such things as the on-line cable guide (The Preview Guide), local programming information screens, etc... My guess is that there is specialized software available to the cable operator from whatever company broadcasts The Preview Guide which is customizable by region, content or whatever (ad packages come to mind).

A few years ago you could usually look forward to seeing the dreaded Amiga 'Guru Meditation Error' plastered on your cable guide screen whenever there was a big storm or over a long holiday weekend. It was amusing at first, but it soon became tiresome. Since it hasn't happened in the past couple of years I'm assuming they've invested in a battery backup or better equipment. One risk for them: Since Commodore has gone belly-up, what's going to happen to their equipment when it dies. Will they be relegated to searching the orphaned-computer parts bin at their local used computer store?

Paul

---

## Re: 11-digit ZIP code

Ed Ravin <elr@wp.prodigy.com>

Wed, 11 May 1994 12:14:25 +22321159 (EDT)

The existing 9 digit ZIP code already provides a path to your door -- in most cases, it maps out to either an individual house, four or five houses, apartment building, or cluster of floors in an apartment building.

So there's no new RISK with the 11 digit code -- as a matter of fact, it's already in use on some barcoded mail (but the 11 digit ZIP is only used in the barcode, so you haven't noticed it yet). The RISK is that zipcode bloat makes addressing mail more and more complicated and error-prone for humans, or that adding extra digits to the ZIP code is being touted instead of making better use of the existing digits to make things easier for the bureaucrats in the Post Office.

Ed Ravin, Prodigy Services Company, 445 Hamilton Avenue  
White Plains, NY 10601 +1 914 448 4737 elr@wp.prodigy.com

[Similar comments were received from

PMDebenham@email.meto.govt.uk, who noted Britain's system is often unique to 10 or 20 households,

grayjw <grayjw@helios.aston.ac.uk>, who noted the use of the first few digits to determine insurance rates,

Chuck Weinstock <weinstoc@SEI.CMU.EDU>,

Frederick Wheeler <wheeler@ipl.rpi.edu>,

marty@beta.lanl.gov (Martin G. Halvorson),

msb@sq.sq.com (Mark Brader), who wondered about the (non)difference between giving out a unique address and a unique ZIP, and

brown@wi.extrel.com (Vidiot), who noted that the U.S. Postal Service is already using the 11 digits. 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 16: Issue 7**

**Tuesday 17 May 1994**

## Contents

- [Crossover of Diagnosis and Procedure Code creates risk](#)  
[Paul Stoufflet](#)
- [The Italian Crackdown?](#)  
[Fabrizio Sala via Stanton McCandlish](#)
- [Umass/Amherst Suffers From Week-long Service Degradation](#)  
[Randy Sailer via Jonathan Welch and Sullivan](#)
- [More on the A300 crash at Nagoya on 26 April 1994](#)  
[Peter Ladkin](#)
- [Palm-reading and immigration](#)  
[John Oram](#)
- [Computer-based Notice Boards and Emergency Information](#)  
[John R. Gersh](#)
- [Re: Killers sue over phone taps](#)  
[Adam Shostack](#)
- [Revision to the Secure Hash Standard](#)  
[NIST message via Paul Carl Kocher](#)
- [Automated address changes](#)  
[Linus Sherrill](#)
- [Re: Tandem and California DMV](#)  
[Scott Hazen Mueller](#)
- [Tracking](#)  
[Phil Agre](#)
- [Secret... not so secret \[NYNEX PINs\]](#)  
[Alan Wexelblat](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Crossover of Diagnosis and Procedure Code creates risk

*Paul Stoufflet <pstouffl@dsg.harvard.edu>*

*Mon, 16 May 1994 15:23:49 +0000*

I work at a local HMO, Harvard Community Health Plan, on evenings and weekends. When we see patients, we get a printout of the recent visits by those patients, along with diagnoses, major and minor problems, medications,

etc. HCHP uses a 4 character code for most of these, consisting of a letter followed by 3 numbers (for example, O991 is a headache). However, the same code can mean different things in different areas. I saw one chart that had a diagnosis of Chronic Lymphocytic Leukemia, which is odd as an isolated finding in a young adult. Curious as to how this devastating diagnosis got on this persons chart, I did some looking, and finally found that the same code was a procedure code for the administration of a particular vaccine, but it had been cast as a diagnosis instead. I alerted the patient (and medical records) to the problem, since otherwise I could see this person being denied life insurance in the future.

Obviously, identical codes should not mean different things in different fields.

Paul Stoufflet, Decision Systems Group, Brigham and Women's Hospital  
75 Francis Street, Boston, MA 02115 pstouffl@dsg.harvard.edu (617) 732-7746

---

### **The Italian Crackdown? (fwd)**

*Stanton McCandlish <mech@eff.org>  
Mon, 16 May 1994 13:03:15 -0400 (EDT)*

[notes in brackets are mine. - mech@eff.org]

Forwarded message:

Date: Mon, 16 May 1994 12:29:14 +0200 (MET DST)  
From: Fabrizio Sala <fsala@varano.ing.unico.it>  
Subject: The Italian Crackdown??  
To: BBS-L@SAUPM00.ing.unico.it  
Cc: eff@eff.org

Hello. I'm the Sysop of one of the BBSs in Italy.

I'm writing this message in this list to inform you, the BBS community, of what is going on in Italy.

Some days ago, starting from Pesaro (Italy), our Police started a large perquisition through [inquisition against] many Amatorial [amateur] BBSs, mostly connected to the main networks (One for all: Fidonet... but also PeaceNet and many others)

They're getting everything they can find: computers, monitors, drives, hard disks, floppy, cdrom, streamer tapes ... everything, without looking if they are or not in any way "illegal" ...

Generally, every network in Italy is now full of holes... and many of us lost everything "in the name of the anti-piracy"...

Nobody of us is doing anything in any way illegal, but they are still getting everything...

They got more than 50 BBS and Police's work is still going on...

I hope that everyone diffuses this message ... or in any way tells everybody what's going on ...

...and if you have any way to help us...please do it! We made our best to make the Italian telecommunication scene working... they are killing us!

See you later... if they don't get me!

\_\_\_\_\_ end fwd \_\_\_\_\_

Stanton McCandlish \* mech@eff.org \* Electronic Frontier Found. OnlineActivist

---

## Umass/Amherst Suffers From Week-long Service Degradation

<sullivan@geom.umn.edu>

Mon, 16 May 94 20:56:51 -0500

Date: Mon, 16 May 1994 09:09:11 -0500

From: Jonathan\_Welch <JHWELCH@ecs.umass.edu>

Subject: Umass/Amherst Suffers From Week-long Service Degradation

Newsgroups: comp.dcom.telecom

X-Telecom-Digest: Volume 14, Issue 229, Message 4 of 14

After slightly over a week of unreliable phone service things returned to normal and the following appeared in the May 13th edition of "The Campus Chronicle".

Jonathan Welch VAX Systems Manager Umass/Amherst JHWELCH@ecs.umass.edu

- - -

Telephone system returned to normal

As you know, the University had a major problem with the campus telephone system which began last Monday, May 2. The symptoms of the problem included calls being cut off, static, a "fast busy" tone when calling on campus and telephones without dial tone. The symptoms were sporadic and fairly random for both academic/administrative telephones and residential telephones.

As soon as the problem started, Ericsson, the manufacturer and maintainer of the telephone system, responded. Ericsson staff worked straight through from Monday morning to late Thursday evening to diagnose and remedy the problem. In addition to the normal three on-site technicians, Ericsson brought in staff from their regional headquarters in Northboro, and flew in a high level technician/ system programmer from the Technical Assistance Center in Cypress, Calif. They also had programmers in Cypress and Sweden working remotely to stabilize the system and to determine the cause of the problem.

The problem with the system resulted from a unique set of circumstances involving software parameters, system clocking and a normal maintenance procedure performed on the system. The problem was exacerbated by the

increases of load on the telephone system we have experienced this year.

The campus telephone system is a complex, distributed computer. Such systems are designed with a great deal of redundancy and can self-correct for many faults. Once the problem occurred, parts of the system were continually trying to reset themselves. In this instance, the complexity of the system and its attempts at self-correction made it difficult to trace the problem and stabilize the system. By Wednesday afternoon, Ericsson had made substantial progress in correcting the problem. They made a configuration adjustment in the system and implemented a slight but important programming change in the software. This adjustment, while straightforward, was difficult to install on the system because of the heavy call volume on campus and the size of the campus system (18,000 lines on 119 system modules). What Ericsson accomplished is analogous to fixing an electrical problem in a car traveling down the highway at 50 miles per hour. The parameter they adjusted did not initiate the problem, but the change allowed the system to return to normal operations.

By early Thursday morning in the residence halls and noon on Thursday in the academic/administrative area of campus, service had considerably improved. Except for a brief interruption of service while circuits were being tested, calls in progress were no longer interrupted by static or cut off. There may have been some problems completing a call or placing long distance calls while work was in progress. However, in general TelCom was quite successful at assisting individuals in making their long distance calls. Ericsson has made adjustments in the system configuration, system clocking and maintenance procedures to ensure that this problem will not recur. I realize the telephone service problems last week were very frustrating for everyone. Telephone service is an important part of our daily lives and any interruptions or degradations in service are a very serious problem. I truly appreciate the patience of the campus community while we struggled to deal with the problem.

We in TelCom, as well as the Ericsson staff, were even more frustrated (if that is possible) at not being able to get the problem resolved quickly. We apologize for the difficulties and will work closely with Ericsson to prevent this problem from occurring again.

Randy Sailer, director, Telecommunication Services

---

### **More on the A300 crash at Nagoya on 26 April 1994**

*Peter Ladkin <Peter.Ladkin@loria.fr>*

*Fri, 13 May 1994 21:24:17 +0200*

On 26 April, a China Airlines A300-600 crashed on landing at Nagoya airport, killing 264 people. The crew had announced they were 'going around' (aborting the approach and gaining altitude to come back for another landing attempt), but continued the approach. Near the ground, the aircraft pitched up (raised its nose in the air), stalled, and 'hit the ground at a high rate of descent, tail-first and completely stalled'. (Flight International, 11-17 May 94, p5). Part of what is known so far is that the Flight Director or FD (a form of autopilot) was in 'go-around mode', and the co-pilot was physically trying to

counteract the guidance of the FD, specifically against published procedures (FI, op. cit.). The FD, trying to fly up with the co-pilot commanding fly-down on the elevator, counteracts with nose-up trim (the horizontal stabilizer at the tail is repositioned by the pilot or by the FD so as to maintain a desired attitude of the aircraft, climbing, cruising, or descending, simply by aerodynamic equilibrium. This is called `trim').

At 700 ft, both autopilots are disconnected. The aircraft pitches up steeply because full nose-up trim has been applied (this cannot be overcome by control-column input alone -- pilots must readjust trim). At 540 ft, the anti-stall system triggers full power, which gives additional pitch-up moment, and the aircraft enters a very steep climb with a pitch of 36 degrees. The pilots fail to readjust trim. At 980 ft, a pilot selects flaps-up to go-around setting causing a pitch-up to 52 degrees, and a speed decay from 124kt (slow) to 78kt (disastrously slow) (FI, op.cit.)

To give an idea, light planes stall (their wing ceases to provide lift) when the angle of the wing to the `relative wind' (the airflow vector considered relative to the wing of the aircraft) becomes roughly 15 degrees. Transport aircraft are similar, but I don't know the stall angle of the A300-600 wing in landing configuration.

The Japanese Transport Ministry's Aircraft Accident Investigation Committee is also looking into an apparent loss of all electrical power moments before the crash. The chairman, Manabu Matsumoto, has `no recollection of a case like this, an apparent failure of all power'. (International Herald Tribune, 11 May 94 p2).

Features of this accident of potential interest to RISKS readers at this point are (a) the preliminary confusion of the crew about which control mode was selected on the autopilot; (b) the full nose-up trim consequence of the interaction between the co-pilot and the FD; (c) the autopilot triggering full-power and therefore a high nose-up moment when the nose was already high; (d) the apparent failure of all power.

One should be cautious if trying to `second guess' the accident investigation. Airplanes such as this are meant to be flown a certain way, in which pilots are thoroughly trained. Pilots are generally legally required to hold to those procedures except in case of emergency.

Peter Ladkin

---

## **Palm-reading and immigration**

*John Oram <oramy92@halcyon.com>  
Sat, 14 May 1994 17:53:38 -0800*

In the May 12 Financial Times of Canada, there is an article entitled "How palm-reading can speed your way into the U.S."

==-----==

Put your hand up if you've had it with the interminable lineups to pass through airport immigration checkpoints when travelling to the United States. That upraised hand could be your ticket to zipping right through.

The U.S. Immigration and Naturalization Service (INS) is testing a new system that turns your hand into the only piece of identification you need to bypass immigration officials and skip right through customs, cutting up to 45 minutes off the procedure for heading south.

Called the INS Passenger Accelerated Service System (INSPASS), it works like this: a three-dimensional image of your hand is electronically recorded on a white, plastic, wallet-sized card. You run the card through a scanner, place your palm onto an electronic reader and, as long as your hand and the card match, you're issued a computer-generated receipt that opens a gate arm, sending you past immigration officials to custom inspection.

[Summarizing the next few paragraphs, INPASS is being tested at three sites: Pearson (Toronto), JFK, and Newark. The article goes on to explain registration at INS offices, which takes about 10 minutes and is free during the indefinite test period. Open to citizens of Canada, Bermuda, Japan, New Zealand, most of Europe and the U.S., but have to make at least three business trips per year to qualify.]

Concerned about privacy? Sally Jackson, director of public affairs for the Offices of the Information and Privacy Canada, says you shouldn't be. The only people participating are those who consent to putting their hand impression on the card; besides, no other record of the hand image is kept.

So far, 26,502 people have signed up for INSPASS, including 2,764 Canadians. More people, no doubt, will follow when they realize how, uhhh, handy the system is.

==-----==

What happens if the systems does not recognize your hand? I'm curious as to the recognition rate. For example, if you get married after registering, will a ring throw the system for a loop?

Also, I find it interesting that the image is kept on the card only. Will the INS keep a record of your travels? (Or do they already?)

John Oram oramy92@halcyon.com Victoria, BC Canada

---

## Computer-based Notice Boards and Emergency Information

John R. Gersh <John\_Gersh@aplmail.jhuapl.edu>  
Mon, 16 May 1994 10:29:07 -0400

[RISKS-16.05](#) and -16.06 included discussion of problems with cable-TV notice-generation systems crashing and leaving cryptic or amusing error messages for all to see ("Amusing computer-related anecdote about local cable

service," Long, Jones, Hrisko). Failures and usability problems with such computer-driven notice boards can sometimes have more serious consequences:

My father lives in a retirement community in a high-rise building. While I was visiting there recently the building's fire alarm went off. My father immediately said, "Turn on the TV -- channel 8."

The building's cable system includes a local notice-board channel that typically shows screens rotating through the dining room menu, daily events, and so forth. It's also used for emergency notices.

Sure enough, within a few seconds, the notice channel stopped showing the lunch menu and switched to something like:

The fire is on the 75th floor.  
Please follow the directions of your floor warden.

(Evacuation procedures apparently differ according to location above or below the fire floor.) The problem with this notice is that the building has only 24 floors!

Evidently someone in the management office soon realized the error. Everyone in the building was then treated to several minutes of cursor-dancing around the screen, as that person tried, unsuccessfully, to change the notice. A cursor would move around the screen, closing in on but failing to select the floor number; the screen would switch to a Master Menu Page and back to the fire notice again; more vain attempts would be made to select the floor number; back to the Master Menu; and so on. Finally things remained static for several minutes. "Aha," said I, they've gone to get The Expert." Sure enough, when screen activity resumed the floor number was immediately changed to a reasonable one, just in time for the all-clear. (It was a false alarm, as are most of the alarms in that building, but that's a different RISK.)

Electronic notice boards in public or semi-public settings can be used for things other than routine bulletin-board postings. If they're going to be used for getting across emergency information, then the same requirements for usability under stress and that we'd expect for other safety-critical applications apply to them, too. We'd also expect that users of such systems ought to be thoroughly trained for emergencies, but system design ought to allow for situations where a not-so-thoroughly-trained user is all that's available.

John R. Gersh (John\_Gersh@aplmail.jhuapl.edu)  
The Johns Hopkins University Applied Physics Laboratory

---

**Re: Killers sue over phone taps (Kabay, [RISKS-16.06](#))**

*Adam Shostack <adam@bwh.harvard.edu>  
Mon, 16 May 1994 15:10:55 -0400*

Mich Kabay complains about criminals wanting their 4th amendment



and remains a highly secure way to ensure the integrity and authenticity of data used in electronic mail, electronic funds transfer, software distribution and data storage applications. NIST expects that products implementing the current standard can be used until the technical correction becomes effective.

Researchers at the National Security Agency, who developed the formula and discovered the flaw in a continuing evaluation process, now believe that although the formula in FIPS 180 is less secure than originally thought, it is still extremely reliable as a technical computer security mechanism. The discovery of this flaw indicates the value of continued research on existing and new standards.

The Secure Hash Standard specifies a secure hash algorithm for computing a condensed representation of a message or data file. This 160-bit condensed message "digest" represents the original message and can be used in computing a digital signature to authenticate the integrity of the message. It is highly probable that any change to the message after it has been signed will result in a different message digest, and the recipient will not be able to verify the signature. Signing the message digest rather than the whole message usually improves the efficiency of the digital signature process.

It is very highly improbable that today's computation equipment can figure out any message that corresponds to a given message digest.

The standard applies to agencies of the federal government for protecting unclassified information when a secure hash algorithm is required. Private and commercial organizations have been encouraged to use this standard on a voluntary basis. The SHS was designed to be used with the proposed Digital Signature Standard, which is based on the digital signature algorithm and has not yet been approved.

As a non-regulatory agency of the Commerce Department's Technology Administration, NIST promotes U.S. economic growth by working with industry to develop and apply technology, measurements and standards. NIST also is responsible, under the Computer Security Act of 1987, for developing standards and guidelines for the cost-effective protection of unclassified federal computer systems.

National Institute of Standards and Technology, Public Affairs Division  
Admin. A903, Gaithersburg, MD 20899-0001

--- End Included Message ---

---

## **Automated address changes**

*Linus Sherrill <julius!sherrill@sky.com>  
Tue, 10 May 94 15:19:40 EDT*

Recently I've had a problem with incoming mail to my home address. A few months ago, mail started arriving (late) with just the wrong zip code and sometimes with the wrong town name too. The incorrectly addressed mail was usually magazines and junk mail but when credit card bills started arriving

(or not arriving) with the wrong address it was time to investigate.

My wife checked at the local post office and they said that this was a problem for the whole zip code; the whole town had been affected. The post office officials had no explanation as to how this might happen. They explained that it our responsibility to correct those who have the wrong address.

The more important ones were corrected over the phone, although it was sometimes difficult to convince the operator that we hadn't moved, the address had spontaneously changed.

Whatever generated the wrong address is still at work. After getting the mail addressed correctly for a few months, the wrong address would reappear.

The post office's solution to this problem is to print bar-coded labels with the correct zip code and stick them to the mail. Mail is now arriving on schedule even with the wrong address.

I've all but given up on correcting the wrong addresses.

I'm guessing that some address verification service shipped a data base with the wrong zip code for our town. (I wonder how many other towns were affected?) Some mailers just updated the zip code and others trying to get a canonical address used the new (wrong) zip code to determine the town name.

---

## Re: Tandem and California DMV

*Scott Hazen Mueller <[scott@zorch.sf-bay.org](mailto:scott@zorch.sf-bay.org)>*

*Sat, 14 May 94 21:20 PDT*

Recently a bit ran in risks about the California DMV computer upgrade fiasco; the original story mentioned Tandem Computers in a poor light. I'd just like to point to a reference on the World-Wide Web to Tandem's official statement on the issue, at <<http://www.tandem.com/press-releases/dmv.html>>. Also, a copy of the California Legislative Analyst's report on the topic is online at <<http://www.tandem.com/press-releases/cla-dmv.html>>; there is a hyperlink to this latter item from within the first document.

Claimer: Tandem is my day job. DisClaimer: I am not an official spokesperson for Tandem; one such is however listed in the dmv.html document.

Scott Hazen Mueller [scott@zorch.SF-Bay.ORG](mailto:scott@zorch.SF-Bay.ORG) or (tandem|ub-gate)!zorch!scott

[Thanks. The original item was in [RISKS-15.80](#). Actually, the item noted the DMV position that neither the software vendor nor the hardware maker were responsible. Of course, the consulting firm was fired from the job.

PGN]

---

**tracking**

*Phil Agre <pagre@weber.ucsd.edu>*

*Tue, 5 Apr 1994 15:31:31 -0700*

"There is something a little eerie about picking up a car phone and having a voice describe your location to within a few feet on a pleasant if unremarkable street of colonial and tudor-style houses."

That's a quote from a second article in the New York Times promoting the Avis project to track the company's rental cars through GPS hardware and wireless communications. The full reference is:

Peter Marks, For a few lucky motorists, guidance by satellite, New York Times, 2 April 1994, pages 1, 16.

The reporter apparently went for a ride with the system, and was enthralled. No doubt it was a fascinating experience. This article does at least mention privacy concerns, in a parenthetical note, as follows:

"On the Nynex computer screens, the cars show up as small dots moving along the roads on the computer maps. Nynex officials say, however, that for the sake of privacy, a car's position will only show up on a screen for the duration of a driver's call to the Project Northstar number."

Note that "privacy" only extends to what's presented on the operator's screen. Nothing is said about the more fundamental issue, what records are stored in the computer.

Phil Agre, UCSD

---

## **Secret... not so secret**

*"Alan (Miburi-san) Wexelblat" <wex@media.mit.edu>*

*Fri, 8 Apr 94 12:16:59 -0400*

[EDUPAGE:]

> A sweepstakes promotion sponsored by Nynex-owned New York Telephone used  
> replicas of customers' calling cards, including their secret personal  
> identification numbers, or PINs. The mailing has caused an uproar among  
> some of the three million recipients, who worry about unauthorized use of  
> their calling cards. Nynex has offered to change the PINs of customers who  
> complain and cover any fraudulent charges. (New York Times 4/7/94 A1)

What's wrong with this picture? Well, changing the PINs only of customers who complain is a bad plan -- what if I didn't see the ads and don't know I should change my PIN?

Giving out real data (even card #s, let alone PINs) to a 3rd party (the ad agency) is another bad plan.

Not treating customer data as secure is a third bad plan; it's especially galling since NYNEX sends out these little reminder cards to customers telling

us not to divulge our PIN to anyone.

Speaking of galling, how "generous" of them to cover fraudulent charges. As if they didn't already do this. It's a fancy way of saying "we're not going to do anything about this."

The thing that particularly strikes me is that it appears NYNEX is, once again, treating this as a special case. This is a particularly annoying RISK we see over and over again, where incidents are treated as aberrations and the symptoms are treated with no thought given to the structural problems which caused them.

I have no idea how to counteract this particular RISK, except by target educating the relevant people, assuming we can find them.

--Alan Wexelblat, Reality Hacker, Author, and Cyberspace Bard  
Media Lab - Advanced Human Interface Group wex@media.mit.edu 617-258-9168

[Also noted by wb8foz@netcom.com (David Leshler). 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 16: Issue 8**

**Weds 18 May 1994**

## Contents

- [Phone system crash at San Jose airport](#)  
[Tarun Soni](#)
- [Logging on as root is easy!](#)  
[Eddy](#)
- [Computer Crime on Wall Street](#)  
[Sanford Sherizen](#)
- [Going by the Book \[air accidents\]](#)  
[Richard Johnson](#)
- [Editor functionality mutates code](#)  
[Kevin Lentin](#)
- [UK ATM Spoof](#)  
[Mich Kabay](#)
- [The RISKS of complex procedures](#)  
[Ry Jones](#)
- [Tactical research](#)  
[Phil Agre](#)
- [FIPS to be tied... \[hashing hashed, Capstone\]](#)  
[Peter Wayner](#)
- [Re: INS recordkeeping](#)  
[Jonathan Corbet](#)
- [Re: killers sue over phone taps](#)  
[Robert Morrell Jr.](#)
- [Re: Secret... not so secret](#)  
[Tony Harminc](#)
- [Novel risk of medical records](#)  
[David Honig](#)
- [Crossover of Diagnosis and Procedure Code ...](#)  
[Carl Ellison](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Phone system crash at San Jose airport

*Tarun Soni* <[tarun@windchime.arc.nasa.gov](mailto:tarun@windchime.arc.nasa.gov)>  
*Tue, 17 May 1994 15:01:08 -0700*

I was travelling from San Jose to San Diego two weeks ago (Fri. evening: 29 April) and showed up at the airport an hour early (Fri. evening rush hour expectations.. ) This is when the fun started: I found that the phone systems in the airport were not working. The supposed reason was a pacific gas and electric problem (that's the local utilities company).

The immediate effects included:

a> air traffic control computers were no longer able to talk to each other? (Southwest airlines assured people that they would go back to the technology of the 60's and there was no real danger)

b> flights were delayed.

c> reservation computers were down and out..

- the fact that I had a reservation and for certain flight was known only to me and the airline personnel took me on trust.
- the fare amount was not known to the airline personnel in general, and they had to confer with their manager for some of the fares .. (in my case they accepted the figure I told them )
- The computers could not talk to the central database and this led to my being given a one way ticket while I really wanted a round trip. (This led to my waiting in line for another hour in San Diego on my return trip.. )

d> credit card approvals were no longer possible.. they took me on trust.

e> oh, the most comic of them all, flights were delayed and a number of people (I have to admit, I fell for it too !) were seen trying to call up their receiving parties in other parts of the country (and slowly realizing that the phone were not working !)

I assume there were other effects which i was not able to witness.

and to use a phrase I see on the digest fairly often :

The risks are obvious.

Tarun Soni

---

### **Logging on as root is easy!**

*eddy <eddy@gen.cam.ac.uk>  
Wed, 18 May 94 15:29:19 BST*

This *\_really\_* alarmed me; but this is Un\*x, so I guess it could just be a well-known 'feature' ...

We mount a couple of disks from a neighbouring department's machine, mbfs.bio. They had some emergency maintenance to do (well I assume it was an emergency -- taking the machine down with < a minute's warning is pretty d\*mn unsound otherwise) so did a shutdown. When I got the notification for this, I set about unmounting the disks asap:

```
eddy@eddy> su
Password:
NFS server mbfs.bio not responding still trying
```

but never got as far as delivering a password because of the downtime. So my machine hung and there was nothing I could do about it. Perfectly normal hassle, irritating but no surprises. So I go shopping and come back to find mbfs.bio is back up and running ... however, my `su' has `_succeeded_` despite the fact that I never typed the password:

```
NFS server mbfs.bio ok
eddy.gen.cam.ac.uk# whoami
root
```

Nice secure operating system this.

Eddy

---

## Computer Crime on Wall Street

*Sanford Sherizen <0003965782@mcimail.com>  
Sat, 14 May 94 11:40 EST*

I'm surprised that no one has commented on the case of Joseph Jett, a managing director/chief government bond trader at Kidder Peabody, who allegedly created an estimated \$350 million in phantom profits, resulting in his 1993 performance-based bonus of \$9 million. Experts quoted in recent articles indicate that he must have made something like \$35 BILLION in false trades without anyone asking questions or the controls raising alarms. At this time, lots of blaming is going on within Kidder Peabody as well as GE, the corporate parent of Kidder.

Is this a computer crime? It seems to me that this manipulation could only have been accomplished through extensive computer manipulation by Jett and possibly by others. This may turn out to be one of the largest computer crime losses to date. It illustrates several points.

1. The growing problem of high level executives who are not being adequately or in many cases even partially supervised. They are in position to commit crime by instructing others to enter a transaction and then destroying evidence of their instructions or the transaction. This is a growth area for computer crime. Not a hacker in sight for this case.
2. Audit and accounting controls are often insufficient for large financial systems and inadequate review requirements result in many of crimes being overlooked, buried, or disregarded. Wait until companies sign onto the Information Superhighway!
3. Computer crimes and financial misdeeds get some (but inadequate) coverage in the business press but very little in the material read by other relevant people, such as computer professionals. If this is a \$9 million crime (his false profits), a \$350 million crime (the company's false profits) or maybe an

even larger loss (the company's negative reputation and possible financial penalties due to legal proceeding), then how large of a loss must be reached before a crisis is indicated? Even the Volkswagen case of several years ago, where an employee working in foreign currency transactions used his access to computers to cause the loss of the equivalent of \$US 256 million, didn't raise many eyebrows in the business or computing communities. If around a quarter of a billion dollar loss doesn't indicate that computer crime is serious, then what figure is enough to decide that the controls and the laws are inadequate to meet the technological challenges?

Finally, anyone want to comment on the following statement of GE Chairman John F. Welch, Jr.? "It's a pity that this ever happened. (Jett) could have made \$2 or \$3 million honestly."

Sanford Sherizen, Data Security Systems, Natick, MA

---

## Going by the Book

*Richard Johnson <rdj@plaza.ds.adp.com>*

*Fri, 13 May 1994 08:11:26 -0700 (PDT)*

The 9 May 1994 "Aviation Week" (pp. 46-51) has an article on Controlled Flight into Terrain (CFIT) -- when controllers or procedures fly you into the ground short of the runway, usually in mountainous and/or poor weather conditions. The article includes the following data (but given as a bar chart, and oriented the other way).

Worldwide Airline Fatalities  
Classified by Type of Accident 1988 - 1993  
Source: Boeing (for aircraft > 60,000-pound takeoff weight)  
(Excludes sabotage & military action)

Category	# accidents	# fatalities
Controlled Flight into Terrain	28	1883
Loss of Control (airplane caused)	10	460
Loss of Control (crew caused)	14	357
Airframe	4	278
Mid-air Collision	1	157
Ice/snow	4	134
Fuel exhaustion	5	107
Loss of Control	2	79
Runway Incursion	3	43
Other	5	15

76 total accidents, 3513 fatalities. (How do you have \*1\* mid-air? They must be counting accidents, not aircraft involved.)

I'm dismayed by the size of the category called "Loss of Control (airplane caused)", especially since they differentiated between that and airframe. This implies (to me at least) software errors. I can't help but remember all

the discussions we've had in RISKS about poorly-designed cockpit management and fly-by-wire systems.

Rather than pointing out the obvious, as they do in the article, I chose to rework the table a little, and make the bins wider.

Category	Totals
Procedural	CFIT-28/1883, Mid-air-1/157, runway-3/43 32/2083
Aircraft	LoC (plane)-10/460, airframe-4/278 14/738
Crew	LoC (crew)-14/357, fuel-5/107 19/464
Weather	Ice/Snow-4/134, LoC (WX)-2/79 6/213
Other	???-5/15 5/15

One the one hand, if the flight crews blindly follow procedures, they risk CFIT. On the other hand, if they don't follow procedures, or forget things, they run out of fuel or into adverse weather or onto an active runway. We should also remember that, unlike private pilots, these transport pilots are expected to fly into and through moderate to severe weather all the time.

The risks? We can all learn from this, no matter what we're working on. We need to examine all of our procedures with an eye to long-term consequences when put into actual practice. The human tends to learn, then memorize, and eventually internalize (habituate) routine behavior. Sometimes this routine can be fatal. I'm not sure how we make procedures good enough to be complete and quick, yet flexible enough to not grow boring.

It's not just procedures in use on the aircraft, either. Consider our own motivation in whatever job we have. How many of those airframe failures could have been prevented on the shop floor? How many of those software failures could have prevented before the first compile? We who manipulate symbols all day don't often get the opportunity to "feel" the true meaning or impact of our work. Finding a way to do so might produce both better products and more satisfied programmers.

Richard Johnson (rdj@plaza.ds.adp.com) (richard@agora.rdrop.com)

---

### Editor functionality mutates code

*Kevin Lentin <kevinl@bruce.cs.monash.edu.au>*

*Wed, 18 May 94 11:57:10 +1000*

The following story was related to me by a colleague of mine this morning.

She was editing some C source using a 'vi' compatible editor called 'vim'. vim is a vi clone that adds some very useful features to the editor. Many of us use it in place of vi. On this occasion she was logged in to a Sparcstation via a terminal annex and modem from home.

She observed that numbers in here code kept on changing. Specifically, decreasing by one for no apparent reason. A screen redraw might change:

```
x = 1;
```

into

```
x = 0;
```

and then

```
x = -1;
```

It turns out that vim has a nifty feature whereby CTRL-A and CTRL-S add 1 and subtract 1 from a number respectively when in command mode. At the same time, her modem was set up for XON/XOFF flow control and it seems that somehow the CTRL-S's were getting through not only the modem but also through her stty settings which might otherwise have interpreted the CTRL-S as a STOP character.

The upshot of all this was that in an attempt to regulate data flow through the modems, the XON/XOFF protocol was actually mutating her source if the cursor was on a number when a CTRL-S came through.

The RISKS of this are painfully obvious. Critical code can end up being mutated and having serious effects later on if the changes are undetected. I am reminded of stories about a missing '-' causing a certain NASA mission to fail in decades past.

Whether this situation can occur easily or whether it was an unfortunate combination of settings, especially 'stty stop' which I suspect was changed from the normal ^s, I do not know, but I will certainly be verifying all my modem and terminal settings when I get home tonight.

Kevin Lentin kevinl@bruce.cs.monash.edu.au

---

## UK ATM Spoof

*"Mich Kabay [NCSA Sysop]" <75300.3232@CompuServe.COM>  
17 May 94 16:00:20 EDT*

According to the Reuter newswire (via Executive News Service on CompuServe),

LONDON, May 16 (Reuter) - Crooks used a stolen cash dispensing machine set up in a fake finance shop to steal 250,000 pounds (\$374,400) in a high-tech swindle, a British newspaper said on Monday.

The cash dispenser, ripped out of its legitimate location using a mechanical shovel and a fork-lift truck, was installed in a shop in London's Bethnal Green district painted to look like an advice centre for home loans, the Sun tabloid reported."

Apparently the stolen ATM simply recorded the card info and PIN of everyone who tried to use it.

Total thefts from other cash dispensers amounted to over 240,000 pounds in 6 weeks. The Sun reports that "A man has been charged with conspiracy to defraud...."

[MK comment: now consider whether this scam would have been effective if users were issued smart cards for their bank and credit functions. The user

approaches the ATM and inserts the smart card. The ATM challenges the smart card (or prints a challenge string on a screen) and the smart card responds with a cryptographic function of its serial number and a seed such as time of day and date (or the user enters the challenge on a membrane keyboard and copies the one-time response from the card's LCD into the keypad). The ATM or banking network validates the response and continues the transactions. Results of setting up a spoof on a stolen ATM: zero.]

M. E. Kabay, Ph.D., Dir Educ, Natl Computer Security Assn, Carlisle PA USA

---

## The RISKS of complex procedures

Ry Jones <rjones@poseidon.usin.com>

Tue, 17 May 94 16:15:55 PDT

I bought a lot of money orders at my local branch bank (to pay bills, they're free and clear faster) and watched the teller make them. Here's what goes on:

- 1) I give her the check.
- 2) She verifies the funds.
- 3) She makes the money orders.
- 4) She hands them to me.
- 5) She hits the "Hold Funds" button and stamps the check "HELD" in red ink.
- 6) Transaction ends.

I asked why she waited until she gave me the money orders to hold the funds. She said they do so because the procedure to un-hold funds is very difficult and time consuming, requiring many signatures.

Fraud opportunity:

- 1) Steps 1 and 2 as above.
- 2) While she is in steps 3 & 4, I use my cell phone to signal my accomplice.
- 3) My accomplice withdraws the cash from an ATM.
- 4) She does step 4. I run out (or hand off the money orders). Whatever.
- 5) She cannot HOLD the funds, but I have the money orders. My accomplice has the cash.

RISKS to this fraud?

- 1) They know me by name at my local branch.
- 2) My account is real. It would need to be enough cash to escape the country, yet be under my maximum daily withdrawal limit (\$1000). The maximum value of the funds would be \$2000, unless multiple people coordinated multiple simultaneous withdrawals (like the bank personnel wouldn't notice)
- 3) many others... the cash reward for the risk is too small, but the window of opportunity exists.

Ry rjones@halcyon.com

---

tactical research

*Phil Agre <pagre@weber.ucsd.edu>*

*Tue, 17 May 1994 14:04:49 -0700*

The 17 May 1994 Wall Street Journal includes an article, excerpted from a new book (which I have not seen) entitled "Tainted Truth" by Cynthia Crosson, about the practice of "tactical research", the creation of customized policy research as part of public debates. She details the example of computerized life-cycle analysis for cloth versus disposable diapers. As with most computer models, you can get a wide variety of answers depending on the estimates you give for a large number of hard-to-measure quantitative variables. (How many times does a cloth diaper get changed in its lifetime? How often do people use two diapers rather than one?) I have heard many, many anecdotes of computer models being manipulated to give the desired answers; you probably have too. It's certainly not a new phenomenon, having risen to prominence in during the zenith of the systems modeling fad in the 1960's.

Crosson's article tries to explain how this manipulation comes about. Are the modelers consciously trying to fool people? Much as I resist that answer, out of an ideological preference for more more complex and systemic kinds of answers, that's basically what she says. Once you start making your living making models whose answers are convenient to certain sorts of people, she says, a sort of treadmill gets going and it's hard to get off. The phenomenon is particularly important in the context of the ongoing US health care debate, in which a blizzard of made-to-order numbers circulates through advertisements and talk show hosts, all of them resting on more assumptions than you could shake a stick at.

What's the answer? How about a public education campaign about the concept of sensitivity analysis? The more reputable polling agencies might frequently use loaded questions, but at least they feel obligated to explain that the numbers have a statistical margin of error of +/- 3% or whatever. Likewise, people presenting models should expect to be asked, "what are your input variables, and how sensitive is your answer to the range of plausible values for each?" That's a simple enough question that a fairly large percentage of the population can understand and ask it. It's not adequate, of course, since assumptions can be built into computer models in a wide variety of ways. But I expect that it's sufficient to get rid of the first 90% of the bogus uses of modeling.

Phil Agre, UCSD

PS Here are some relevant references:

Cynthia Crosson, How "tactical research" muddied diaper debate, The Wall Street Journal, 17 May 1994, page B1 (marketing section).

Cynthia Crosson, Tainted Truth: The Manipulation of Fact in America, New York: Simon and Schuster, 1994.

Kenneth L. Kraemer, Siegfried Dickhoven, Susan Fallows Tierney, and John Leslie King, Datawars: The Politics of Modeling in Federal Policymaking, New York: Columbia University Press, 1987.

Ida R. Hoos, Systems Analysis in Public Policy: A Critique, revised edition,

Berkeley: University of California Press, 1983.

---

## FIPS to be tied... [hashing, Capstone]

Peter Wayner <pcw@access.digex.net>

Wed, 18 May 1994 10:39:28 -0400

There are two interesting lessons hidden in the fact that the NSA discovered some flaw in the Secure Hash Algorithm ([RISKS-16.07](#)) and announced that they were working on a fix:

\*) They're become slightly more open-- if only to authentication technology.

\*) This proves the RISK of using a hardware based standard. Apparently there is a whole batch of now obsolete CAPSTONE chips sitting in a warehouse. Capstone was supposed to be Clipper + authentication, but now it will have to wait for a new version.

Imagine if Capstone was widely distributed when the error was found? Would you replace your phone/modem/PCMCIA card if you had bought a version that was made obsolete by progress? How long would it take the country to recover from such a problem? What if the standard was blown wide-open?

---

## Re: INS recordkeeping

Jonathan Corbet <corbet@stout.atd.ucar.edu>

Tue, 17 May 1994 11:01:16 -0600

John Oram finishes an interesting submission about the installation of "palm readers" at the border with:

> Also, I find it interesting that the image is kept on the card only. Will > the INS keep a record of your travels? (Or do they already?)

Anybody who wonders about that need only have gone to Nicaragua in 1985, as I did. My travels take me out of the country a few times a year, so it became immediately apparent that I had made some sort of list when, on scanning my passport, the immigration officer would invariably write the magic code on my entry form that means something like "give this one a hard time." For about 4-5 years (after which I evidently aged off the list for lack of further "infractions") I had to allow a solid three hours of connection time when entering the country so that they could search my bags, count my money, grill me about my life, and so on. I had never been searched before this period; I have never been searched since. But I was searched *every* time in between.

Many people who travelled in Central America during that period have much worse stories to tell.

As a result of all this, (1) I am not worried about palm readers, since they give the INS no capability that they do not already have, and (2) I

have no illusions about the benign nature of government power, even in a relatively free (so far) country such as this.

Jonathan Corbet, National Center for Atmospheric Research, Atmospheric Techn. Div. corbet@stout.atd.ucar.edu <http://www.atd.ucar.edu/rdp/jmc.html>

---

### Re: killers sue over phone taps

*"Robert Morrell Jr." <bmorrell@isnet.is.wfu.edu>*

*Tue, 17 May 1994 13:12:14 -0400 (EDT)*

Adam Shostack, in bemoaning the invasion of convicted killer's privacy said probably the most outrageous thing I have ever seen in the RISKS forum:

"I've also yet to hear of criminals who want to deny others rights they claim for themselves"

Really? I believe that the right to =life=, =liberty=, and the pursuit of happiness is somewhat well known, and a convicted killer, kidnapper or robber has certainly shown a willingness to deny others those rights....

In our ongoing and totally justifiable drive to insure the integrity of our informational system, I think we should, at least once a day, do a reality check.

The RISKS of not doing so is to have safety, security and privacy =only= in virtual realities, and not in physical ones.

Bob Morrell

---

### Re: Secret... not so secret (Wexelblat, [RISKS-16.07](#))

*<tony.harminc@amail.amdahl.com>*

*Tuesday, 17 May 1994 13:11 ET*

Alan Wexelblat <wex@media.mit.edu> writes about NYNEX/New York Telephone mailing out replicas of customers' calling cards, complete with PINs.

There is an underlying historical problem with telephone calling cards in North America that leads to a lot of this sort of trouble: those last four digits were not intended to be a PIN in the first place. The concept of PIN as a 'something you know' identifier to be combined with the 'something you have' card was kludged on to the original calling card scheme only after massive fraud in the 1970s. A simple (and widely publicized) check digit scheme was previously used by operators to manually verify card numbers.

Current calling cards are unlike any other card one might carry, in that they usually have the 'PIN' embossed on the card and encoded on the magstripe. Some newer cards (typically those that do not have a phone number as the first ten digits of the number) do not have this problem.

Tony Harminc Antares Alliance Group Toronto Software Development Centre

## novel risk of medical records (comment on "Future of US health care?")

David Honig <honig@ruffles.ICS.UCI.EDU>

Sun, 15 May 1994 15:44:09 -0700

In [RISKS-16.06](#), Amy\_McNulty@vos.stratus.com writes about how a little girl's doctor's trick of using a serious 'diagnosis' to let the HMO's bureaucracy authorize a specialist "could cause her to be unjustly rejected sometime next century when she applies for life insurance, medical insurance, a physically demanding job, college, or who knows what else."

Its *worse* than that. The job she may be denied need not be "physically demanding". There is some big military-industrial firm (whose name I forget) which publicly claims it will no longer hire *smokers* because they increase the cost of group insurance. (I suppose this has not caused major activism as smokers "choose" to smoke.) One wonders what the future holds...

"I'm sorry, Ms Jones, but during your probationary period you overvisited the candy machine and that places you in ... "

---

## Crossover of Diagnosis and Procedure Code ... (Stoufflet, [RISKS-16.07](#))

Carl Ellison <cme@sw.stratus.com>

Tue, 17 May 1994 13:57:45 -0400

It is inexcusable to use code numbers in the first place, much less to re-use them. This is left over from human procedures on paper forms. The computer is capable of freeing us from this kind of stupidity -- with arbitrary length on-line form fields, either intentionally readable by a human or intentionally encrypted for privacy. Even in the latter case, a decent code for a field will be both unique and redundant (checked) so that a 1 or 2 digit typo won't hit another defined code word.

P.S. I'm a customer of HCHP and I'm not sure I want to continue to be, given this!



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 16: Issue 9**

**Weds 25 May 1994**

## Contents

- [Call Your OPERATER!](#)  
[Martin Minow](#)
- [Bank goof creates millionaire](#)  
[Andy Fuller](#)
- [Two risk-related articles from Edupage 5/24/94](#)  
[Terry Alford](#)
- [Dell monitors too hot to handle](#)  
[Mich Kabay](#)
- [Canada, The Internet, and the Homolka trial \[anonymous\]](#)
- [Risks of setting up awful puns](#)  
[Aaron Barnhart](#)
- [Re: China Airlines A300 Crash](#)  
[John Yesberg](#)
- [Re: Computer Crime on Wall Street](#)  
[Mike Rosenberg](#)  
[Marc Horowitz](#)
- [Cable / Closed Circuit TV Info Display Risks and 911](#)  
[Bob Richardson](#)
- [Re: Logging on as root is easy!](#)  
[Dan Franklin](#)  
[Eddy](#)
- [Re: UK ATM Spoof](#)  
[Gary Preckshot](#)
- [Privacy Digests](#)  
[reminder](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Call Your OPERATER!

*Martin Minow <minow@apple.com>  
Tue, 24 May 94 13:08:26 -0700*

From rec.humor.funny, but it belongs in Risks, too...

(True)

In an effort to snag more long distance telephone calls (charged to a credit card or a third number), AT&T reserved the toll-free number 1-800-OPERATOR. Not to be outdone, and perhaps knowing the public better, MCI reserved the number 1-800-OPERATER and has been scooping up calls intended for its arch-rival.

Walter C. Daugherty Texas A&M University [daugher@cs.tamu.edu](mailto:daugher@cs.tamu.edu)

[So now we need legislation on Truth in Mispelings and Mistouchtonings? PGN]

---

## Bank goof creates millionaire

*Andy Fuller <[acfa@callisto.eci-esyst.com](mailto:acfa@callisto.eci-esyst.com)>*

*Wed, 25 May 94 08:57:43 EDT*

>From the Tampa Tribune, Wednesday May 25, 1994

Howard Jenkins was a multimillionaire for about a half a day. About a week ago he lost his checkbook and called his bank to have a hold put on his account. "When he went to make a deposit Friday morning, he was told to check the automated teller machine outside to make sure the account was working." He made a small withdrawal and the receipt told him his account balance was \$889437.93. He went home and called the bank's automated telephone account inquiry system, and was informed that his balance was now more than \$88 million. He went back to the bank and asked a teller for his balance, and was given an 8 digit number. She asked if he had received "an inheritance or something".

He withdrew \$4 million in cashier's checks and cash, requiring a bank manager's signature on each check, and they "didn't bat an eye". He returned later that day, accompanied by his lawyer, and returned the money.

The bank attributes the erroneous balance to a computer error, probably linked to the hold transaction.

Several things stand out to me:

- 1) He was told to check an ATM to see if his account was working. Whoever told him this should have been able to check directly using the bank's terminal. The bank (and reasonably so) puts a great deal of trust in the computer.
- 2) The balance shown on the ATM receipt was different than that given him by the automated telephone information system and the teller. Is this a user interface problem, or something more involved?
- 3) The computer error is likely to be the fault of inadequate testing or a user interface inadequacy (calling up a deposit transaction instead of an account hold transaction). Both topics have been discussed at length in this forum.

4) Nobody questioned this withdrawal or the large deposit. The teller who checked his balance was the only one mentioned in the story that even noticed his windfall. Proper software and human procedural checks would have caught this error. If a pre-computer bank teller had been handed a deposit of this size, the bank manager would have been notified. When the withdrawal was made, the manager would have known about the deposit and been confident that the request was legitimate. Are similar human checks and balances included in modern banking computers?

Andrew C. Fuller, E-Systems, ECI Division, St. Petersburg, FL  
acfa@callisto.eci-esyst.com (813) 381-2000 x3194 72417.612@CompuServe.com

---

## two risk-related articles from Edupage 5/24/94

*Terry Alford <talford@mitre.org>  
25 May 1994 15:51:31 GMT*

### ATTENTION LIBRARIANS -- FATAL BOOKSHELVES

A union claims that Library of Congress employees are exposed to potentially fatal crushing hazards caused by sliding mechanical bookshelves, and asserts in a lawsuit that the bookshelves have occasionally started up unexpectedly, undeterred by safety sensors. The government insists the bookshelves have experienced "only three or four failures," none of which resulted in employee injury. (BNA Occupational Safety & Health Reporter 5/18/94 p.1787)

### RISK-TAKING

Information technology visionary George Gilder calls Michael Milken a risk-taker, "who was willing to plunge \$2 billion into a company with \$100 million in assets and \$200 million in revenues. He had a great eye and really did it brilliantly. The people who prosecuted him did not understand what he was doing at all. It was mysterious to them and he was making too much money to be legal [laughs]." (Upside, June 94, p.55)

---

## Dell monitors too hot to handle

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@CompuServe.COM>  
25 May 94 07:45:30 EDT*

Dell has issued a recall of 63,000 monitors after receiving 32 reports of overheating or fires starting. The problem monitors bear the number DL-1460NI on the back.

Owners of the monitors with that number should call 1-800-913-3355 to set up free pickup and repair.

Arrangements also can be made through Dell forums on CompuServe and America Online or by dialing Dell Computer Corp.'s bulletin board at 512-728-3589. Dell will ship packing materials to owners of the monitors, who then will send them by Airborne Express to the company for repair within three to five working days.

Michel E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

[Watch out for The Foamer in the Dell. PGN]

---

## Canada, The Internet, and the Homolka trial

<[anonymous]>

Fri, 20 May 1994 22:00:16 -0400 (EDT)

As reported in Toronto's EYE Newspaper [eye@io.org] (similar to New York's Village Voice) dated 19 May 1994:

The London Ontario detachment of the Ontario Provincial Police have begun a campaign of harassment against local University Internet users who are attempting to use the net to gain information on the Karla Homolka trial. A University of Western Ontario (London) student had his Internet account frozen by the university computer staff when requested by the Police. The reason for this lay in the student's name being left on the text of a FAQ of the details of the trial. Another student in Toronto had Faxed this material (which had been Emailed to him) to the Toronto media, and the offices of the Premier of Ontario and the Attorney-General as an act of provocation against the Ban (his regular anonymous forwarding site was not working). The problem was that he had forgotten to remove the other persons name and account number from the original E-mail that was sent out.

The police action against the student's account was done without a warrant, and also involved the questioning of the student at the local police station. Likewise the students home computer was searched without a warrant by using the threat of criminal charges. The Student's computer account was reinstated, but he was required to turn over all incoming Email to the police under the threat of criminal charges if he did not cooperate. A list of about 50 people who had received Homolka FAQ's were passed on to the police. The important part of this entire situation is that no one, including the Ontario Attorney-General office is certain that the ban applies to the Internet. The ban states that details of the trial cannot be published in the print media but there is no ban on possession of information. There is no mention of the Internet, nor the use of computer systems in the ban. Further, there is no official investigation of the Internet on the part of the Ontario Provincial Police, except for this one detachment.

One of the questions raised is the ethics of the University of Western Ontario's computer department. Their cooperation with the police was based on a fear of having their computer equipment confiscated (similar to the case of the University of Cambridge in England). If the situation had taken place with in the library system of the university, it would not have been tolerated by the library staff due to the long held tradition in that profession of the defence of freedom of speech. If the Internet is to remain open this set of values will have to become part of the professional commitment of the MIS staff of universities as well.

---

## Risks of setting up awful puns

Aaron Barnhart <barnhart@mcs.com>

Wed, 18 May 94 13:12 CDT

If Schindler Elevator gets a black eye as a result of the Toronto controversy, at least they have an ace in the hole.

They can just change their name to Schindler's Lifts.

[Remarkably, this was also suggested in various contexts by Mark Bartelt <sysmark@chipmunk.cita.utoronto.ca>, roedder@netcom.com (Spencer Roedder), jcook@epoch.com (Jim Cook), davis@ilog.ilog.fr (Harley Davis).

I am absolutely delighted that I am not carrying the entire burden of elevating the level of discourse. PGN]

---

## Re: China Airlines A300 Crash (Stalzer, [RISKS-16.05](#))

John Yesberg <jdy@itd0.dstov.gov.au>

Fri, 20 May 1994 10:14:31 --9-30

> ... This is a serious kind of failure, if an automatic system designed to  
> prevent a problem makes it worse, it should do nothing at all!

This is probably true for conventional aircraft. For fly-by-wire aircraft, however, the computer systems can never "do nothing".

I understand that the main computer system (in, e.g. A320) has six (approx) flight modes, and that it responds slightly differently to manual inputs depending on which mode it is in. Pilots are required to understand the differences between the modes. I imagine that, in non-emergency situations, the pilot would not need to worry about these differences: the aircraft would respond "intuitively" to command inputs. In very unusual situations, the required inputs to the machine may be counterintuitive. This can probably be overcome in two ways:

- (i) Give the flight computer more modes to be in, so that it could behave "properly" or "intuitively" in the various situations.
- (ii) Give the pilots enough simulator training so that the intuition takes into account the mode that the aircraft is in.

In critical manoeuvres, like landing and go-around, pilot confusion is to be avoided at all costs.

John Yesberg (jdy@itd0.dstov.gov.au)

---

## Re: Computer Crime on Wall Street ([RISKS-16.08](#))

Mike Rosenberg <mkr@fid.morgan.com>

Wed, 18 May 1994 14:48:51 -0400

re: joe jett's alledged fraud:

> It seems to me that this manipulation could only have been accomplished  
> through extensive computer manipulation by Jett and possibly by others.

I believe this is incorrect.

It probably happened because the accounting system did not handle the trade properly. i would guess that no outright manipulation of data or code was necessary. also, his gross strips position was probably growing larger and larger as time went on. this should have raised some red flags.

mike rosenberg mkr@fid.morgan.com

---

## Re: Computer Crime on Wall Street

Marc Horowitz <marc@MIT.EDU>

Sat, 21 May 94 16:45:30 EDT

<> 76 total accidents, 3513 fatalities. (How do you have \*1\* mid-air?  
<> They must be counting accidents, not aircraft involved.)

Although you are probably right, this is not impossible. Several months ago, several people were killed in a small airplane over Massachusetts when it collided with a skydiver (who survived with a broken leg). One plane, midair collision.

Marc

---

## Cable / Closed Circuit TV Info Display Risks and 911

Bob Richardson <bob@CSOS.ORST.EDU>

Tue, 17 May 1994 14:41:55 -0700 (PDT)

John Gersh writes regarding an information channel display that showed an incorrect floor number during a fire alarm. Other contributors have written regarding cable-TV channels reporting "Software Failure" for hours or days on-end. As a manufacturer of such equipment for the Cable Television Industry, I hope I can provide some insight.

A very common computer used in systems for broadcast applications is the Amiga. This is because of it's relatively low cost for this application, as well as the fact that it generates clean video at standard NTSC/PAL rates. On older versions of the operating system, if a program crashed severely (the Amiga OS does not provide memory protection or resource tracking, yet is fully multitasking), a flashing red "guru" message would appear, requiring an acknowledgement from the user to reboot the machine. Unfortunately, due to the nature of cable transmission, these machines are usually located in very remote sites. Of course, many cable companies are too lax in even monitoring

for crashed displays. Under newer versions of the OS, this problem is solved in that after a timeout (usually 30 seconds), these requesters go away and the reboot proceeds normally. Since the Amiga isn't a very widely supported or understood platform, most of these cable operators do not upgrade to newer OS's, and some machines cannot legally be upgraded (physically they can, but since ROMs are not available from Amiga, you have to make a copy of the OS and install it on the hard drive of the machine, which is technically illegal.)

Our solution for our customers was to create a "watchdog" program that would reboot the machine in the event that our main task failed in any way. We then discovered something interesting: Most of the crashes occurring were not a result of our program (or our competitors), but of line spikes and brownouts trashing the machine. We now insist that our customers at least purchase a line conditioner or a UPS as a result.

One contributor to this list asked what cable companies will do now that Commodore is out of business, regarding replacement parts. For quite some time now, it has been quite difficult to obtain support from Commodore anyway, so my company as well as others have been acquiring spare parts from used machines. One should note, however, that Commodore's death is being exaggerated on the net, and that there is indeed a buyer, but specifics have not been made public at this time.

An interesting incident reported to me by a customer: During the March, 1993 earthquake in Klamath Falls, Oregon, cable service was not interrupted. The 911 emergency center was being swamped with calls, many of them for non-life-threatening situations. They called the cable company and requested that a message be posted on the air to tell people with minor emergencies to use an alternate number to reach the 911 center. Unfortunately, the number provided to the cable company was incorrect, and was for the main 911 center's outgoing lines (non-emergency). The administrative office was then swamped with calls, and could not obtain an outgoing line to call the cable company and tell them to change the number. As a result, the 911 center wants modem access to our software so that they can alter displays themselves. (I don't see how that could have prevented this particular situation.) We are currently evaluating how best to achieve this. There are several liability issues that open up when you allow third parties access to your airwaves. Not to mention the fact that while our software is password-protected at this time, anyone with a password also has access to the billing and setup functions. We now have to segment our security further so that outsiders can not mess with private or operation-critical information.

Bob Richardson, Product Development Supervisor, Sound Concepts / MagicBox  
(503) 752-5542 bob@csos.orst.edu

---

## Re: Logging on as root is easy!

*Dan Franklin <dan@copernicus.bbn.com>  
Wed, 18 May 94 14:40:16 -0400*

I am somewhat skeptical of the apparent failure in security described by <eddy@gen.cam.ac.uk> in [RISKS-16.08](#). I have been in the situation eddy describes many times, and the "NFS server ..." message always appeared AFTER I

typed the password, if the password prompt appeared at all (sometimes it did not). In fact since the code in question queries you for the password and then waits to collect it, it is difficult to imagine what it could be doing in between those two operations that would involve NFS access.

Also, if the included transcript is literally accurate

```
eddy@eddy> su
Password:
NFS server mbfs.bio not responding still trying
```

then, since the "Password:" prompt does not end in a newline, eddy must have at least typed a newline before getting the "NFS server ..." message, and the possibility that the entire password was typed before that newline cannot be ignored; after all, until that much-loathed message appeared, eddy was presumably expecting to "su" as usual so as to be able to unmount the soon-to-disappear filesystems.

Of course, this is computer software, so I'm not saying it's impossible! But I'd like to see it duplicated before I believe it. Unfortunately eddy's message did not give the UNIX version involved in this scenario, so I cannot do it here.

The `_real_` risk is that once you've entered the password, you've got a nascent superuser shell that anyone can type at once the server comes back up. Yet one hardly wants to stick around and guard it... In a university environment, this seems risky indeed.

Dan Franklin

---

### Re: Logging on as root is easy! (Franklin, [RISKS-16.09](#))

*eddy <eddy@gen.cam.ac.uk>  
Thu, 19 May 94 13:35:12 BST*

> The `_real_` risk ... superuser shell that anyone ... In a university

Interesting point. The risks of leaving the terminal unattended aren't the usual ones for a university; this is a lockable office which I share with folk that I trust not to abuse a root shell and who would have locked the office if they'd gone out in my absence -- ie, we don't get random undergraduates wondering in in our absence -- but I hadn't typed the password, so this wouldn't have been a problem (except that I'd feel shy of letting random UG's get at `_my_` account, of course; which is one of our reasons for locking the door).

> ... if ... literally accurate ... possibility ... cannot be ignored ...

The transcript is literally accurate; I copied the text from the command-tool to the mail window by raw cut-and-paste. I had not typed anything at the password prompt when the NFS server message came up; what I did type (a tenth of a second later -- thus before I'd noticed the message) was only the first



"smart" card which cannot be obtained without correct authorization. Only an ATM hooked up correctly to the bank could obtain the passwords to unlock the card, which then provides some internal code unrelated either to the PIN or to the card account number. However, this raises other issues, such as how could you use such a card for phone charges? Or how could charges be validated at the point of sale? Somehow the same challenge/response would have to occur at Macy's as it does at the ATM, or what good would the internal validation code do? Thus, the challenge would be available for analysis on the general telecommunications system, and a significant communications burden would be placed on the system due to wide spread usage. Somehow, I don't think it's quite so simple.

Gary

DRTOPE@delphi.com

---

## Privacy Digests

<RISKS-request@csl.sri.com>

18 May 94

Periodically I will remind you of TWO useful digests related to privacy, both of which are siphoning off some of the material that would otherwise appear in RISKS, but which should be read by those of you vitally interested in privacy problems. RISKS will continue to carry general discussions in which risks to privacy are a concern.

\* The PRIVACY Forum Digest (PFD) is run by Lauren Weinstein. He manages it as a rather selectively moderated digest, somewhat akin to RISKS; it spans the full range of both technological and non-technological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line:

information privacy

as the BODY of a message to "privacy-request@vortex.com"; you will receive a response from an automated listserv system. To submit contributions, send to "privacy@vortex.com".

\* The Computer PRIVACY Digest (CPD) (formerly the Telecom Privacy digest) is run by Leonard P. Levine. It is gatewayed to the USENET newsgroup comp.society.privacy. It is a relatively open (i.e., less tightly moderated) forum, and was established to provide a forum for discussion on the effect of technology on privacy. All too often technology is way ahead of the law and society as it presents us with new devices and applications. Technology can enhance and detract from privacy. Submissions should go to comp-privacy@uwm.edu and administrative requests to comp-privacy-request@uwm.edu.

There is clearly much potential for overlap between the two digests, although contributions tend not to appear in both places. If you are very short of time and can scan only one, you might want to try the former. If you are interested

in ongoing detailed discussions, try the latter. Otherwise, it may well be appropriate for you to read both, depending on the strength of your interests and time available.

PGN



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 16: Issue 10**

**Tuesday 31 May 1994**

## Contents

- [Closed Doors in Glasgow](#)
- [Human.risks-- Scapegoats and Puddlejumpers...](#)  
[Peter Wayner](#)
- [Man charged with E-mail stalking](#)  
[John C. Rivard](#)
- [Police BBS in Silver Spring, MD](#)  
[Mich Kabay](#)
- [Re: alt fan karla homolka](#)  
[Phil Overy](#)
- [Eavesdropping hits NSA](#)  
[Peter Wayner](#)
- [Risks of too-simple responses](#)  
[Jerry Leichter](#)
- ["Zap!" by Sellers](#)  
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Closed Doors in Glasgow

<kh@dcs.gla.ac.uk>

Wed, 25 May 94 21:12:10 BST

GUARD DIED AFTER DOORS FAILED IN COURT FIRE.

The Glasgow Herald, Glasgow, Scotland, 25 May 1994

A failsafe system on security doors at Edinburgh's new sheriff courthouse did not work on the night of a fire in which a security guard died, a fatal accident inquiry heard yesterday. Graham Scott, 39, managing director of computer firm System 4, told the inquiry at Edinburgh Sheriff Court that security doors which should have opened automatically in the event of fire had remained locked. Security guard George Campbell, 57, of Claremont Grove, Edinburgh died when he was trapped in a lift by the fire on November 19 last year. Mr Scott said that a programmable computer chip in the system had its information wiped accidentally and did not signal the doors to open. The

doors normally worked by having a security card "swiped" through a device which identified the card and allowed them to open. The inquiry heard that efforts by another security guard to reach Mr. Campbell failed when his card would not open a door on to the sixth level where Mr. Campbell was trapped. Mr. Scott said that because the fire had burned for some time before being discovered, it had probably burned through the cable connecting the door to the main control computer, but a push button on the inside should still have opened it. He said that under the new system any door which was cut off from the main control for more than 10 seconds would automatically unlock itself.

[This tragedy seems to have been the result of a combination of problems: no escape route from the lift (elevator); no way of opening doors from the outside without the door computer working (sounds familiar!); and a specified but untested exceptional case. The new failure mode is interesting too: they'd better keep that computer working if they don't want thieves to break into the courthouse! KH]

---

### **Human.risks-- Scapegoats and Puddlejumpers...**

*Peter Wayner <pcw@access.digex.net>*

*Thu, 26 May 1994 09:03:58 -0400*

The May 25th edition of the Wall Street Journal has a long story by Daniel Pearl about a crash of a small commuter airplane. The company seems to be blaming the pilot and the story goes to long lengths to document his bad attitude. His anger, the theory proposes, lead him to screw up in the bad weather and misjudge the position of the ground by 300 ft.

The story is well-written and essentially balanced, but I wonder if the author really thought about the spin he was putting on the story. For instance, the author "documents" the pilot's anger and abrasive behavior as such:

"Always a meticulous person, Mr. Falitz became even more of a stickler. He filed 14 anonymous (sic) air-safety reports, including one about a flight attendant who didn't have up-to-date paperwork." (I hope their anti-terrorist security is better than their protections for anonymity.)

(Before the Flight) "Mr. Falitz had an angry argument with a gate agent over his paperwork, and a ramp worker in Minneapolis told the safety board that he saw Mr. Falitz chew out Mr. Erickson (the co-pilot) for not checking the landing light from outside the plane. After the Hibbing-bound passengers were aboard, Mr. Falitz insisted on bumping one passenger to meet the weight limit; a woman travelling with her family volunteered to get off."

To be fair, the writer also documents a time when Falitz slapped the headset of a co-pilot after the co-pilot set it to the wrong channel. There are a few other quotes that make Falitz seem a bit too disgruntled. For instance, Falitz was annoyed because the airline was forcing him to make the doomed flight and he would have to fly home on his day off.

But, I still was rather disturbed by the fact that the writer seemed to be building an argument about Falitz's abrasiveness by citing Falitz's desire to abide by the rules. The second paragraph I quoted ran directly under the sub-heading "Quarrels with Colleagues." I wonder if the woman who was bumped by the flight believes that the doomed plane should have taken off with too much weight as well?

The best "fact" that proves Falitz was an abrasive pilot with an attitude was that "On one sweaty flight, he announced to passengers that 'the company is too cheap to fix the air conditioner.'"

Incidentally, the co-pilot on this flight that crashed made \$18,000 a year. At the time, small commuter planes were not required to have low altitude warning devices that would have alerted the pilots to the fact that they were too low. Big jets had them, but the companies didn't have to spend the money on the little planes. They became required last month. The article also mentions that the altimeters often stick.

The most dangerous subtext hidden in the article is the fact that the Federal Aviation Administration is funding a program to develop personality tests for pilots. I just hope that they can find a way to tame the anger without turning the pilots into lemmings that accept low pay and badly maintained planes that are overloaded with passengers and luggage.

---

## Man charged with E-mail stalking

*John C. Rivard <jcr@garnet.msen.com>  
Thu, 26 May 1994 12:27:36 -0400*

A front-page story (!) in the May 26, 1994 *\_Detroit Free Press\_* tells the tale of a 31-year-old suburban Dearborn Heights man who has been arrested and charged under Michigan's new anti-stalking law for alleged harassment of a 29-year-old Farmington Hills (another Detroit suburb) woman via E-mail. The article refers to this as "one of the first cases of stalking based primarily on E-mail.

Under a large color photo of Mr. Archambeau with his arm draped casually over his computer, the story tells of how he was jilted five days into an E-mail relationship carried out over America Online. After the woman (anonymous in the article per her request) sent the "Dear John" E-mail message, he has been sending her E-mail trying to win her back.

The two met via a video dating service. The woman states that received a total of "about 20 E-mail letters" from Archambeau since the day she met him, hardly mail-bombing by most RISKS readers' standards. She has saved and printed the messages for her lawyers.

Archambeau claims that E-mail, by its nature, is non-harassing, because she can refuse to read the message after seeing the sender: "I was courting her in a way that she could easily ignore."

The recipient of his unwanted advances points out that her system won't

delete unread mail for 37 days, so she has to look at it for that long, "which is more harassing than postal mail."

After being contacted by a Farmington Hills detective, Archambeau sent several more messages to the woman, as well as one to the detective explaining his side of the story. The detective said that the woman wasn't "terribly concerned" about the E-mail until she received a phone message from Archambeau in which he apologized for watching her leave her workplace, which is a block away from where he lives.

The woman seems to be claiming that E-mail itself is harassing by its very nature. She does not claim that the content of any of the messages were in any way threatening, although the Farmington Hills detective said after he had initially contacted Archambeau, later messages contained "other methods of harassment if she carried through with a police complaint."

The Michigan "stalker" law makes it a misdemeanor to maliciously and relentlessly harass and pursue someone, punishable by up to a year in jail and a \$1,000 fine. This is the charge against Archambeau.

The offense becomes a felony if threats are made or the person is under court order to stay away from the alleged victim. Then the perpetrator faces five years and \$10,000.

Women's rights groups who helped draft the law say they are certain that it covers E-mail harassment, but the ACLU, which has expressed concern over the law being able to withstand constitutional challenge, is not so sure.

There is a strange and extreme dichotomy in this story. On the one hand, we have the alleged perpetrator is claiming that E-mail by its nature *\*cannot\** be threatening, and on the other hand, the alleged victim is claiming the opposite, that unsolicited E-mail is *\*harassing\** by its nature. Both positions don't consider about the *\*content\** of the message at all! This case brings the all the RISKS of treating the medium of E-mail differently than other channels of communication to the forefront in what may be a precedent-setting court case.

A second RISK is in the news media's overemphasis on E-mail as a stalking tool. In fact, the text of the article indicates that the only blatantly threatening act (watching the victim leave work) was related over the phone. Nonetheless, the media spin on this issue is solely the ground-breaking act of stalking by E-mail.

Deniability/accountability of E-mail is a RISK that is not dealt with in this article, mostly because Archambeau openly admits sending the E-mail in question.

John C. Rivard    jcr@mail.msen.com    JCR Design and Consulting

---

## Police BBS in Silver Spring, MD

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@CompuServe.COM>*

26 May 94 06:11:46 EDT

>From the Washington Post newswire (94.05.23) via Executive News Service (GO ENS)  
on CompuServe:

"In Silver Spring, the Public Can Log On to the Police Log"

By Veronica T. Jennings

Washington Post Staff Writer

"In the corner of a second-floor office in the Silver Spring district police station sits a computer terminal that may launch Washington area police agencies onto the information superhighway.

"The computer contains information on crimes and suspects and, as of last week, it's available to the public on a pilot basis."

The author makes the following key points:

<<

---

### re alt fan karla homolka

phil overy <PJO@ib.rl.ac.uk>

Thu, 26 May 94 15:07:40 BST

The newsgroup and offending details of this list also made their way to our machine; I suppose the Ontario police object to details being published in a case which is "sub judice". I have read (this may be wrong information) that the details are being published by people who object to a plea bargain by the (equally guilty?) Karla Homolka. This is not the way in which sub judice is dealt with in Austria (I have recently moved back to the UK); often papers will carry details from major court cases, but not name the defendants and not quote any prosecution allegations. Many VERDICTS do not contain the convicted man's name, so a "family" murder might be reported:

"Dragan K. stabbed his father to death after an argument over the war in Yugoslavia" - the report will continue to expand on what took place, but the name is not given (anyone who thinks "Dragan" is a good clue has not met many (Yugoslav)s..).

The biggest advantage I can see to this approach is presented in minor crimes- in the UK many minor crimes are wiped from the record 3 years after the end of the sentence, but local newspapers indefatigably pillory the local fast drivers, petty thieves etc by name - the only way to genuinely lose that conviction 3 years after leaving prison is to move away, because someone may dig up the newspaper report (indeed they WILL do so in Hicksville/ Nempnett Thrubwell).

"sub judice" publication of details of a case does of course cast doubt on fair trials; I am sure that the individuals named as Lt. Starbuck etc in the Homolka case do not want either of the accused to go free for lack of a fair trial, but their actions could well cause a mistrial to be declared.

The Risk? The Internet is providing a sort of international newspaper; at the moment it doesn't display a great deal of commitment to that role. If The Internet is "the new press", it's a pretty flabby alternative to the old one.

Phil Overy, Rutherford-Appleton Laboratory

---

## Eavesdropping hits NSA

*Peter Wayner <pcw@access.digex.net>*

*Sat, 28 May 1994 10:43:18 -0400*

The Baltimore Sun ran an AP wire story (5/27/94, pg1) reporting that Dunkin Donuts owners routinely places audio mikes in their stores for "security." The story notes that the DD near Fort Meade, MD (the home of the NSA) contains the equipment.

The story notes that the main corporate headquarters says that these hidden microphones would be wrong. But it also cites Security systems dealer Jeff Meuse who "told the Concord Monitor he has installed systems in 500 Dunkin' Donuts in Massachusetts in the last five years; of those, 300 had audio monitoring."

[No telling what might be hidden in the donut holes! PGN]

---

## Risks of too-simple responses

*Jerry Leichter <leichter@lrw.com>*

*Fri, 20 May 94 21:13:58 EDT*

Several articles in a recent RISKS caught my eye in their common style of taking too simple-minded an approach to a risk, thus missing important issues.

### 1. Editor functionality mutates code

Kevin Lentin reports on an "extended vi" editor that has a CTRL/S command which, if the cursor happens to be sitting on a number, decrements the number by 1. In a particular communication setup, CTRL/S was being used as XOFF and also passed through to the editor, resulting in random mutations of code being edited. Mr. Lentin suggests that the fix is to be more careful about terminal settings.

While this fixes the immediate problem, it ignores the underlying issue of adaptation to the real world. CTRL/Q and CTRL/S have been used for in-band signalling as XON and XOFF for many years. Using them as editing commands is simply *\*very\** poor design. It's very poor because it's inherently dangerous: There are too many ways to accidentally misconfigure an asynchronous terminal connection so that XON and XOFF end up being passed to programs. Further, in the case of dial-up or network connections, the "proper" settings often have to be made at so many intermediate systems, often systems with wildly different interfaces, that errors are certain.

EMACS has always been the primary focus of this particular problem. Its designer has made it a point to bitch and moan about and generally refuse to come to terms with any system that has the audacity not to deliver CTRL/Q and

CTRL/S. Well, OK; that's fine for after-dinner conversation. Safe software, however, must adjust to the realities - and the realities for CTRL/Q and CTRL/S are long established.

## 2. UK ATM Spoof

Mich Kabay reports on an incident in London in which thieves stole an ATM machine, repainted it, set it up in a shop, used it to gather card info and PIN's, and eventually used those to steal some 240,000 pounds. Mr. Kabay comments that had the banks used smart cards and a challenge/response system, this crime could not have occurred.

He's right, but for a different reason: Had banks waited for smart cards to be practical before setting up ATM's, there would probably still be few if any ATM's. ATM's date back about 20 years by now, and it took a good ten of those years from ATM's to become really widespread. Smart cards are only just becoming practical for mass use now. They are still considerably more expensive and fragile than the well-proven magnetic stripe card technology.

Meanwhile, the cost of conversion has inevitably mounted. There's a huge installed base of magnetic card readers, and a huge number of magnetic cards in customer hands. Conversion would be a very non-trivial task.

Should we as a society have waited before putting our trust in a technology that has proved to be so easily abused? A difficult question in general - among technologists, there's always a push to just go ahead and build the thing and see what happens. In this particular case, I think you'd be hard put to argue that waiting was called for. What's ignored in just going ahead, however, is that it inevitably raises the future costs of fixing the problems.

In practice, my bet is that we will *\*never\** see the replacement of magnetic stripe cards by smart cards. Instead, we'll see improvements in stripe card technology. I saw a report not long ago about a technique that samples the random noise on the magnetic stripe. This noise is unique to a particular card, is not changed by recording information on the stripe, and cannot be set in a particular way by any known technique. If, indeed, this technique is practical - and the principle certainly appears sound - it would eliminate the class of crime described here equally well. (Curiously, a similar thing is happening in the cellular phone arena, where the same kind of crime - the theft of identification information for the purpose of faking a valid access token - is being combated by analysis of the details of a phone's transmission characteristics, which again appear to be unique to each unit, and not forgeable. There's a significant commonality here: These crimes are made possible because in the digital world, "bits is bits". Those of us who deal with higher-level abstractions, where circuits really are binary - much less those of us to whom the lowest level of abstraction is the software architecture - easily lose sight of the fact that underlying our abstractions is a physical world in which parts are not exactly interchangeable. My prediction: We'll see many more techniques based on looking "below" the digital level in the years to come.)

## 3. FIPS to be tied... [hashing, Capstone]

Peter Wayner notes that the recently discovered flaw in, and modification to,

the Secure Hash Algorithm "...proves the RISK of using a hardware based standard." It proves nothing of the sort.

a. Software isn't nearly as "soft" as people like to think. There are still many systems out there running MSDOS Version 3. Security bugs reported and patched years ago are still live in many Unix systems. It's widely acknowledged that no fundamental change can be made in the UUCP algorithms or protocols, since many sites either would not, or simply could not, upgrade.

The world of the individual programmer, ever ready to replace his copy of gcc with the latest and greatest release of yesterday morning, has little to do with the way most of the world works.

b. Hardware may be easier to change than software, if appropriately designed. ROM updates are a common thing.

c. A ROM update blurs the line between software and hardware, but in practice any low-end implementation will have more of the characteristics of hardware than of software, simply because the economics favor something that can be duplicated very quickly and cheaply - and that's either a specialized chip, or a general purpose CPU plus ROM.

d. In any case, the Secure Hash Algorithm isn't a hardware-based standard - whatever that means - to begin with!

If, as Mr. Wayner worries, SHA were found to have a significant problem after it was in wide use - it really would make little difference *how* it had been realized. Software, ROM, custom hardware - updating a million instances of *anything* is an immense problem.

-- Jerry

---

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">  
Tue, 31 May 1994 15:46:51 -0600 (MDT)

Subject: "Zap!" by Sellers

BKZAP.RVW 940311

Peachpit Press, Inc.  
2414 Sixth Street  
Berkeley, CA 94710  
800/283-9444 or 510/548-4393  
Fax: 510/548-5991  
tbooth@peachpit.mhs.compuserve.com  
"Zap!", Sellers, 1994, 1-56609-021-0, U\$12.95/C\$17.95  
dsellers@hebron.connected.com

The industrial first aid class that I was in had come to problems associated with bones and joints. The instructor was discussing bursitis, and was using

the example of carpet layers. The tool used to stretch carpet is designed to be "kicked" with the knee while the worker is kneeling and tacking the carpet in place. Because of the repeated blows to the knee joint, bursitis is a fairly common result. Once it sets in, the worker can only hope to get a new job before the pain gets too bad. Someone in the class wouldn't accept this, and kept asking what could be done. The instructor patiently kept explaining that nothing could be done. Finally, the student pulled out what she thought was her trump card: what if the worker's whole \*life\* was carpet laying? "Well," replied the long-suffering teacher, "I guess he'd die, then."

This was immediately recalled to me by the anecdote used to open this book. Some conditions are tragic and some are preventable. The prevention, however, may not always be within the control of the worker.

Still, this is an important book. When you consider the possibly painful and costly alternatives, "Zap" is probably well worth the price for any and every computer user. Home users may cavil, but they are the ones who probably have the worst work setups and the most control over their environment. Certainly every large office should have a copy, although I suspect it will be used more by staff than management, alas.

Given that the book's chapters cover not only body systems but also external and environmental factors, it tends to seem a bit disjointed. The jumps from subject to subject are sometimes difficult. It is, however, undoubtedly useful in bringing together all manner of factors and problems into one place. The suggestions tend to be along the lines of common sense; relax; if something is uncomfortable at first, it will get worse with repetition; keep moving, etc.; but it is not to be despised on that account. When the subject gets more technical, as in the chapter on radiation, Sellers tends to waffle more. (He recommends a commercial monitor retrofit which can be accomplished more effectively and for less money at home with a roll of tin foil.) The resources at the end of almost every chapter are helpful for further study in specific areas. There are, however, some odd gaps (such as the chapter on back pain). Hopefully, future editions of the book will add more contacts and information.

The book is written to the user. This might seem an obvious audience, but it is probably management who need more prodding here. It is a pity that more information is not directed towards the solid business advantages of an "ergonomic" workplace. In discussing chairs, for example, one could note that the cheapest steno chair might be available for sixty dollars, whereas the most expensive is ten times that much. This might appear to be a substantial price difference--until you consider that the cheapest receptionist costs twenty times as much, per year, as the most costly chair. If you get only five percent more work out of someone with a better chair, you pay for the chair in a year.

While there are gaps in this work, it is significant for bringing together a number of health issues in one place. For this reason, I highly recommend it and look forward to improved editions in the future. Give it to your computer novice friend and it might just save his or her neck. Or eyes. Or hands ...

copyright Robert M. Slade, 1994 BKZAP.RVW 940311

Vancouver Institute for Research into User Security, Canada V7K 2G6

ROBERTS@decus.ca Robert\_Slade@sfu.ca rslade@cue.bc.ca p1@CyberStore.ca

---



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 16: Issue 11**

**Friday 3 June 1994**

## Contents

- [Flaw in Clipper detected](#)  
[Jim Huggins](#)
- [Re: Solo midair collisions](#)  
[Martyn Thomas](#)
- [Donuts with Ears, Part II](#)  
[Peter Wayner](#)  
[David Wright](#)
- [Ollie North on the high seas...Big toys, big egos, E-trails](#)  
[David Honig](#)
- [Nonexistent Risks \(Re: Call Your OPERATER!\)](#)  
[Gregory B. Sorkin](#)
- [Risks of faxing](#)  
[Adam Shostack](#)
- [The Ghost in the Modem](#)  
[Loka Alert 1:6 via Phil Agre](#)
- [Zimmermann statement on PGP 2.6](#)  
[Philip Zimmermann](#)
- ["The Hacker Crackdown" by Bruce Sterling](#)  
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Flaw in Clipper detected

*Jim Huggins <[huggins@eecs.umich.edu](mailto:huggins@eecs.umich.edu)>*  
*Thu, 2 Jun 1994 13:55:23 -0400 (EDT)*

The following is summarized from an article in the *\_Detroit\_Free\_Press\_*, 2 June 1994, pages A5-6. The article was written by John Markoff of the New York Times [and appeared on the front page of the Times on that day].

AT&T Bell Labs researcher Matthew Blaze has been quietly circulating a report among computer researches and federal agencies which demonstrates a flaw in Clipper. Using Blaze's technique, two parties can use Clipper to have a conversation which could not be decrypted by government officials using the

proper escrowed keys. The flaw would not permit third parties without the escrowed keys to decrypt the conversation either; essentially, this technique would reduce Clipper to the status of other commercially-available cryptography which is computationally infeasible to break.

Stanford's Martin Hellman, who has reviewed Blaze's work, states "People who want to work around Clipper will be able to do it." In a written statement, NSA directory of policy Michael Smith stated that Clipper would still remain useful: "Anyone interested in circumventing law-enforcement access would most likely choose simpler alternatives." Smith claims that Blaze's technique would be too difficult and time-consuming for practical use.

Comments: of course, this will probably re-ignite most of the Clipper controversy again, since this seems to strike at the heart of NSA's purposes in creating Clipper (secure cryptography with a mandatory back-door for the government). I'm more interested in NSA's statement that says in essence that Clipper can be avoided more simply: perhaps this shows that Clipper won't be all that useful after all?

Jim Huggins, University of Michigan (huggins@umich.edu)

---

### Re: Solo midair collisions

*Martyn Thomas <mct@praxis.co.uk>  
Wed, 1 Jun 94 11:19:15 +0100*

The account of a collision with a sky-diver reminds me of an incident some years ago when a commercial jet hit a salmon at altitude, which smashed through the nose, demolished the co-pilot's rudder pedals and broke his leg, ending against the rear bulkhead of the cockpit [the salmon, presumably, not the rudder pedals or the leg].

The accident report assumed an eagle had dropped it.

[The eagle salmoned up all its carriage? PGN]

---

### Donuts with Ears, Part II

*Peter Wayner <pcw@access.digex.net>  
Thu, 2 Jun 1994 18:17:26 -0400*

A spokesman from Dunkin' Donuts tells me that the chain has ordered all DD to remove their listening equipment. Apparently, the front-page news about their listening devices finally brought the public sentiment to their attention. Maybe if they had stronger mikes they would have gotten the message sooner?

---

### Re: Eavesdropping hits NSA [[RISKS 16.10](#)]

*David Wright <wright@hi.com>*

*Fri, 03 Jun 94 10:15:41 EDT*

[...] The security cameras that are installed in in many stores will remain, however; the company said they are a proved deterrent to robbery.

-- David Wright, Hitachi Computer Products (America), Inc. Waltham, MA  
wright@hi.com

---

## **Ollie North on the high seas...Big toys, big egos, electronic trails**

*David Honig <honig@binky.ICS.UCI.EDU>*

*Fri, 03 Jun 1994 11:41:15 -0700*

In the 3 Jun 1994 Wall Street Journal there is an article about a Whitbread sailboat race. The story includes a description of how one team is accusing one of its members of telling another team about the weather, which is apparently against their rules. The evidence for this is \*computer logs of faxes\* sent between the individuals, who are also possibly romantically linked. (There may also be financial motives connected with boat sponsorship.)

Anyway, the risk to perpetrators in not covering their electronic trails (tails?) is present even on a sailboat in the South Pacific.

---

## **Nonexistent Risks (Re: Call Your OPERATER!)**

*Gregory B. Sorkin <sorkin@watson.ibm.com>*

*Tue, 31 May 94 18:13:03 -0500*

There is the RISK of not double-checking dubious information, including information in the Risks Digest.

I dialed 1-800-OPE-RATO[R] (I didn't dial that last R -- for "redundancy"), and sure enough, I got a "(pong) AT&T".

Then I dialed 1-800-OPE-RATE[R], and sure enough, I got . . . nothing. Is there a regional discrepancy, or is the rumor of MCI's devious cunning just an urban myth?

[I got RINGING with NO ANSWER after 20 rings. Maybe that is exactly the point? Ultimate denial of service, intended to make you want to go elsewhere when you think you are getting AT&T? PGN]

There were also several Risks Digest items about clever color copiers blocking the reproduction of US and some foreign currencies. This seems almost impossible algorithmically, and indeed appears to be fictional, based on what testing one can do legally.

[We have gone around on that one in the past. PGN]

What are the Risks here? Just that people will go about spreading urban

myths, I guess.

Greg Sorkin (sorkin@watson.ibm.com)

---

## Risks of faxing

*Adam Shostack <adam@bwh.harvard.edu>*

*Wed, 1 Jun 1994 09:16:16 -0400*

This appeared in rec.humor.funny. I'm submitting it to RISks because nothing on the risks of faxing has appeared in a while. The problems are that there is often little way to ensure your fax is going to the correct place, and that the faxed paper is out of your control once faxed, and might be copied, and redistributed with your name & private correspondence.

Public-key encryption programs, such as PGP, would have allowed the unfortunate applicant to encrypt this (as email). If it was mail, he would have to type the wrong address twice, once for the mail address, and also for the encryption recipient. He might have had a chance at getting the job. (Of course, using the phone would also have avoided the problem, but can be inconvenient & expensive when colleagues are overseas.)

- > You might enjoy this.
- > A candidate for the Director of our Research Center faxed a
- > colleague to request a letter of recommendation. It was
- > accidentally faxed here instead. It read in part:
  
- > "Iowa is too wet and droll. But it's a directorship
- > so I should apply..."
  
- > The fax is now part of his permanent application file.

---

## The Ghost in the Modem (Loka Alert 1:6--from the Washington Post)

*Phil Agre <pagre@weber.ucsd.edu>*

*Sun, 29 May 1994 21:01:06 -0700*

Date: Sun, 29 May 1994 22:40:43 -0500 (EST)

From: RESCLOVE@amherst.edu

To: loka-l@amherst.edu

Subject: The Ghost in the Modem (Loka Alert 1:6--from the Washington Post)

Loka Alert 1:6 (May 29, 1994)

>From the Sunday \_Washington Post\_:

IF INFORMATION HIGHWAYS ARE ANYTHING LIKE  
INTERSTATE HIGHWAYS--WATCH OUT!

Friends and Colleagues:

This is one in an occasional series of e-mail postings on democratic politics of science and technology, issued by The Loka Institute. You are welcome to post it anywhere you feel is appropriate. The following essay, written by Loka Institute members, is reprinted from the Outlook Section of The Washington Post, Sunday, May 29, 1994.

--Dick Sclove

Executive Director, The Loka Institute, P.O. Box 355,  
Amherst, MA 01004-0355, USA  
Tel. 413 253-2828; Fax 413 253-4942  
E-mail: resclove@amherst.edu

\*\*\*\*\*

### THE GHOST IN THE MODEM

For Architects of the Info-Highway, Some Lessons  
From the Concrete Interstate

By Richard Sclove and Jeffrey Scheuer

Vice President Gore envisions the information superhighway as the second coming of the interstate highway system championed by his father, former U.S. Senator Al Gore, a generation ago. Let us hope that the junior Gore is proven wrong. Rush-hour traffic jams, gridlock, garish plastic-and-neon strips, high fatality rates, air pollution, global warming, depletion of world oil reserves--have we forgotten all of the interstate highway system's most familiar consequences?

It's not that Gore's analogy is wrong, only that his enthusiasm is misplaced. Comparing the electronic and asphalt highways is useful--but mostly as a cautionary tale. Building the new information infrastructure will not entail the degree of immediate, physical disruption caused by the interstate highway system. But sweeping geographic relocations, and accompanying social transformations, seem probable. And the risk of inequity in contriving and distributing electronic services--or, conversely, imposing them where they are not wanted--is clear.

Indeed, disparities in access to new information systems have already begun to surface. A study released this past week by a group of public interest organizations, including the National Association for the Advancement of Colored People and the Center for Media Education, notes that low-income and minority communities are underrepresented in U.S. telephone company's initial plans for installing advanced communications networks.

Unequal access is only the most obvious among many social repercussions that may lie in store for us. The real history of the interstate highway system suggests how we can think about and control the vast implications of new technologies and a new national public infrastructure.

It is widely assumed that Americans' infatuation with cars led to the construction of America's superhighways. But actually when Congress passed the Interstate Highway Act in 1956, car sales were slack, and there was no popular clamor for building a new road system. At the time only about half of

American families owned an automobile; everyone else depended on public transportation. Congress was responding to aggressive lobbying by auto makers and road builders, plus realtors who saw profits in developing suburban subdivisions.

The act's key provisions included support for bringing freeways directly into city centers and earmarking gasoline tax revenues for highway construction. As the interstate highways were built, city and suburban development adapted to the quickening proliferation of autos. Soon more Americans found themselves forced to buy a car in order to be able to shop or hold a job. The Highway Trust Fund, by assuring the rapid atrophy of competing public transit systems, bolstered this trend.

Thus the asphalt highways--and the society around them--are a reflection of successful lobbying by powerful business interests and external compulsion, not simply the free choices of consumers. There is no guarantee that the process of wiring consumers and employees into the electronic highway system will be different.

The effects of the interstate highway system on American communities were profound, especially in the cities. As historian James Flink notes, "Ambitious programs for building urban freeways resulted in the massive destruction of once viable poor and minority neighborhoods." In other cases, new highways encircled poor neighborhoods, physically segregating minorities into marginalized ghettos.

Gradually, a black and Hispanic middle-class did emerge. Its members too fled along the interstate to the suburbs, further draining economic and cultural resources from the inner city. This contributed to the emergence of a new social phenomenon: today's desperately deprived, urban underclass.

Elsewhere the effects were subtler but still significant. The noise and danger from growing numbers of autos drove children's games out of the street, and neighbors and families off their front porches. Before long, suburbs without sidewalks came to signal an unprecedented paucity of local destinations worth walking to. Suburban housewives found themselves leading increasingly isolated daytime lives at home.

Highways made shopping malls possible, enabling franchise and chain store sales to boom. But this sapped downtown centers.

For some teenagers and senior citizens, today's anonymous, consumption-mad expanses provide a semblance of community space-- having swallowed up the general store, the soda fountain, the Main Street sidewalk, and the town square. There is ample danger of the new electronic technology extending these losses.

Remember too that it is easy to romanticize new technology. The popular arts glorified life on the highway. People read Jack Kerouac's "On the Road," watched "Route 66" on television, and recall the Merry Pranksters' psychedelic bus-capades during the '60s. In fusing alienation and rebellion with youthful exuberance, each of these foreshadows contemporary cyberpunk culture. Yet real-life experience on the interstate is mostly banal and uneventful.

McDonald's, Pizza Hut, and Wal-Mart look about the same wherever you exit.

There are also political ramifications of a vast new public infrastructure. Interstate highways contributed to national and even international economic integration. But while GNP soared, mom-and-pop production and retailing declined. That meant greater local dependence on national and global market forces and on distant corporate headquarters--powers that communities simply couldn't control. The locus of effective political intervention thus shifted toward more distant power centers. But because those are realms in which everyday citizens cannot be as effectual as in smaller political settings, democracy was impaired.

If the growth of the highways is revealing, so too is the opposition to freeway construction that emerged. As citizens became more politically mobilized during the 1960's and early '70s, opposition to relentless highway expansion arose from environmentalists and from local communities, both rich and poor.

Transportation engineers reeled at the specter of upright citizens rejecting their good works. Many current telecommunications engineers and true-believing entrepreneurs are no less convinced of the unalloyed beneficence of their art.

The importance of the analogy between the information and asphalt highways lies in the political procedures that create them. What if a wider range of people, including non-car owners, had been involved in transportation planning all along? Considering the alternatives envisioned by critics such as Lewis Mumford, it seems likely we would have a smaller and different road system today. As in Europe and Japan, there probably would have been greater investment in public transit. Modern America might exhibit less sprawl, less dependence on foreign oil, and more cohesive urban neighborhoods.

Three lessons for the construction of the information superhighway suggest themselves:

- o No Innovation Without Evaluation: To help reduce adverse social impact, the federal government should mandate evaluated social trials of alternative electronic services. Analogous to environmental impact statements, these trials should precede full-scale deployment of any major components of new information infrastructures.

- o No Innovation Without Regulation: We should conserve cultural space for face-to-face social engagement, traditional forms of community life, off-screen leisure activities and time spent in nature. How about a modest tax on electronic home shopping and consumer services, rebating the revenue to support compensatory, local community-building initiatives?

- o No Innovation Without Participation: A number of European nations are out-competing America in including lay people in technology decision-making. For instance, the Danish government appoints panels of everyday citizens to cross-examine a range of experts, deliberate among themselves and then publish their own social assessments of technological alternatives. Sweden, Norway and Germany have pioneered processes for involving workers directly in designing new production systems.

The coming revolution in information systems is going to change life for everyone--including the multitude who, by circumstance or choice, never use computers. It is imperative to develop mechanisms for involving all segments of our society in designing, evaluating and governing these new systems.

Data highway enthusiasts may see such measures as wasteful obstructions of market forces. But what entrepreneurs call red tape is really democracy in action.

---

Richard Sclove is executive director of the Loka Institute in Amherst, Mass., a public interest research organization concerned with science, technology and democracy. He also directs the Public Interest Technology Policy Project at the Institute for Policy Studies. Jeffrey Scheuer, a New York writer, is a fellow of the Loka Institute.

\*\*\*\*\*

[If you would like more info regarding the Loka Institute, please send an e-mail message to that effect to: resclove@amherst.edu ; however, the staff warns that they may be slow in responding, due to travels. PGN]

---

## Zimmermann statement on PGP 2.6

*Philip Zimmermann <prz@acm.org>  
Fri, 3 Jun 1994 01:39:59 -0600 (MDT)*

-----BEGIN PGP SIGNED MESSAGE-----

From: Philip Zimmermann, author of PGP  
To: People interested in PGP  
Date: 28 May 94

On 24 May 1994, the Massachusetts Institute of Technology released PGP (Pretty Good Privacy) version 2.6. PGP is a software package that encrypts electronic mail, using public key cryptography. Over the past three years, PGP has become the worldwide de facto standard for email encryption. PGP 2.6 is being published under the terms of the RSAREF license from RSA Data Security, Inc (RSADSI). This is a significant milestone in PGP's legal development.

Export of this software from the US or Canada may be restricted by the US Government. PGP version 2.6 is being released through a posting on a controlled FTP site maintained by MIT. This site has restrictions and limitations which have been used on other FTP sites to comply with export control requirements with respect to other encryption software such as Kerberos and software from RSA Data Security, Inc. These special mechanisms are intended to preclude export of cryptographic software from the US. The MIT FTP site that carries PGP is net-dist.mit.edu, in the pub/PGP directory.

This new freeware version of PGP is for noncommercial use. For commercial use, you may get ViaCrypt PGP, available on a variety of platforms. ViaCrypt may be contacted at 602-944-0773, or via email at [viacrypt@acm.org](mailto:viacrypt@acm.org).

PGP 2.6 is as strong as earlier versions. It contains no back doors. It can read messages, signatures, and keys from PGP versions 2.5, 2.4, 2.3a, and 2.3. Beginning in September, a built-in software timer will trigger PGP 2.6 to begin producing messages, signatures, and keys that cannot be read by earlier versions of PGP. It will still retain its ability to read things from earlier versions after that date, so that users who upgrade to 2.6 will not be inconvenienced, particularly if everyone else upgrades by that time. The reason for the change in format is to grant RSADSI's request to MIT to encourage all users to stop using older versions. ViaCrypt's new products will support the new formats used by PGP 2.6. Details of the compatibility issues and their reasons are outlined in the PGP User's Guide, included in the release package. See also the official statements released by MIT for further details.

Version 2.6 also has some bug fixes and improvements of the version 2.5 released by MIT on 9 May 1994. Both the 2.5 and 2.6 versions were produced in a joint project between myself and MIT. Both versions were released by MIT after extensive review by MIT's administration and their legal counsel. I am told by MIT that MIT's legal counsel believes that both versions 2.5 and 2.6 do not infringe the RSA patents in any way, and they both comply with the terms of the RSAREF licenses that each were released under. But regardless of the noninfringing nature of version 2.5, I urge all PGP users in the US to upgrade to version 2.6, to help move toward eradication of earlier, pre-RSAREF versions of PGP. This will improve the overall political and legal landscape surrounding PGP. MIT will publish details on the simple format change so that earlier European versions of PGP may be independently upgraded by the Europeans.

This note does not attempt to answer all the questions you may have about the implications of this new release of PGP. For further details, see the information released by MIT, or see the PGP User's Guide in the new release package.

-----BEGIN PGP SIGNATURE-----

Version: 2.6

iQCVAgUBLegMXmV5hLjHqWbdAQE0NAQAiTafSwM8eNfYYvksINR6bun/GlelvziA  
M/9h5fn3zUQt2Bc6rkuz1TBlnMZUoduuffinI9eSr+cdXbfhxNIQmRARhw3EJd1f+  
siZaPmTR3YXvUwuXMcrUmbUvEYpSBmtBVrxTzxNSlwx3/hJB2z9sT1/B+UZdFwi  
EZx10/mpiZw=

=ULD1

-----END PGP SIGNATURE-----

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">  
Wed, 01 Jun 1994 12:50:45 -0600 (MDT)

Subject: "The Hacker Crackdown" by Bruce Sterling

BKHKRCRK.RVW 940314

Bantam Books  
1540 Broadway  
New York, NY 10036  
"The Hacker Crackdown", Sterling, 1992, 0-553-56370-X, U\$5.99/C\$7.50

It is important to keep in mind that the crackdown of the title refers to a specific incident: the series of raids in 1990 by various United States law enforcement agencies which tend to be collectively, if incorrectly, subsumed under the code name, "Operation Sundevil". The book brings together a number of the stories surrounding this event, as well as giving some background, particularly in regard to AT&T and the US Secret Service. There are, however, significant gaps which prevent it from being an overall analysis of either the cracker/phone phreak culture or the data security/law enforcement community.

As an overview of the 1990 raids, the book is entertaining, often informative, and generally well written. Digressions often provide very interesting background, although at times they consume entire chapters without much bearing on the central issues. Those who were around for the electronic discussions of the 1990 raids will possibly be glad of the collection of all the stories into one place. (Those who have dealt with the crackers, phone phreaks and wannabes will readily recognize some of the descriptions, as well as the repeated emphasis on braggadocio as a primary character trait.)

Although Sterling is aware of the debate over the term "hacker"; indeed, he worries over contributing to the degradation of the term; he does not distinguish between the various communities of electronic outlaws. In fact, he states, at one point, that all are the same. Similarly, his contacts with law enforcement and data security people are limited. For these reasons, the book is not useful as a general introduction to the field.

The writing is highly opinionated. The US-centric view of technology borders on jingoism. In general, neither law enforcement nor the cracking communities are seen with any favour. Although we can sympathize with Sterling's motivation in wanting to bring to light the injustice done to his friend, the extreme sarcasm which cloaks most of the first half of the book makes it difficult to understand what point he is trying to make.

For those involved in data security, a very entertaining read. For newcomers, please take it with a very large grain of salt.

copyright Robert M. Slade, 1994 BKHKRCRK.RVW 940314  
Vancouver Institute for Research into User Security Canada V7K 2G6  
ROBERTS@decus.ca Robert\_Slade@sfu.ca rslade@cue.bc.ca p1@CyberStore.ca



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 16: Issue 12**

**Wednesday 8 June 1994**

## Contents

- [RISKS OF RISKS again](#)  
[PGN](#)
- [Hazards of the real-time switchover of a prison system](#)  
[Ray T. Stevens](#)
- [Campaigns and Elections](#)  
[Phil Agre](#)
- [Library fines unstoppable after earthquake](#)  
[Geoff Kuenning](#)
- [Flames and viruses in e-mail - article in the New Yorker](#)  
[Martin Minow](#)
- [Tetris addiction?](#)  
[Mich Kabay](#)
- [Re: Closed Doors in Glasgow - Trapped Guard Dies in Fire](#)  
[John Vilkaitis](#)
- [Re: Risks of too-simple responses \(UK ATM Spoof\)](#)  
[Henry J. Cobb](#)  
[Mathew Lodge](#)  
[Jerry Leichter](#)
- [Re: Clipper](#)  
[Gene Spafford](#)  
[Sidney Markowitz \[2\]](#)  
[A. Padgett Peterson](#)  
[Paul Carl Kocher](#)
- [Info on RISKS \(comp.risks\)](#)

---

## RISKS OF RISKS again

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Wed, 8 Jun 94 12:00:01 PDT

Sorry for the inconvenience on [RISKS-16.11](#) for those of you who got a truncated original, and apologies for the duplicate in case any of you actually got an untruncated original copy. Our gateway was timing out on even moderately sized outgoing mail and FTPed files (also preventing me from

updating the CRVAX archive copy).

---

## Hazards of the real-time switchover of a prison system

"Ray T. Stevens" <74074.1746@CompuServe.COM>

04 Jun 94 15:56:30 EDT

Our local newspaper, The Herald Times, had a several page spread on the problems relating to a switchover of the local prison to a new control system. Given the length of the spread, and considering that most of it was human interest and not technical, I summarize it here.

The prison is being switched from a mechanical to a fully automated system, and this is being done while it contains prisoners. The jailers are complaining about huge amounts of overtime, and spending the whole day "on a dead run".

One incident of a technology breakdown was especially insightful. The lights are going to be controlled by this new system, and the wiring for the new system must be run through some of the old wire traces. In order to safely install the new wiring, the existing wiring had to be disconnected, for both the lights and an intercom system so that inmates can contact the guards for requests. To maintain functionality, temporary wiring was used to replace the existing wiring for the lights. To save money, no on-off switches were included. The prisoners must sleep with the lights on.

One of the prisoners has sued, requesting release because of cruel and unusual punishment. This has been rejected.

A more serious incident occurred with another prisoner. A light had started to burn out, but since it couldn't be turned off, it couldn't be changed, and it started blinking rapidly. One of the prisoners had epilepsy, and the blinking light triggered a seizure. The inmates injuries were exacerbated by the other prisoners not being able to call for help. Pounding on the cells did no good, as this is a common sound in the prison. A lawsuit is in progress.

Another prisoner is now using this as grounds for his immediate release. He has a heart condition, and is claiming that this situation puts him too much at risk. No ruling yet.

I see one more lawsuit from this. The best defence in a criminal case is frequently delay. I can see what may be a very valid comment from the a defendent's lawyer. "I must request a continuance on the basis of temporary incompetence of my client. The county has been illegally depriving my client of sleep, and he is now too sleepy of competently participate in his own defence." Under the right circumstances, I would say this might be worth about a two-month delay.

---

## Campaigns and Elections

Phil Agre <pagre@weber.ucsd.edu>

Mon, 6 Jun 1994 18:09:55 -0700

I encourage everyone to have a look at an issue of the magazine "Campaigns and Elections". It's a monthly, sold at many newsstands (in the US anyway), for the people who run political campaigns. Every issue includes numerous references to the growing role of computers in campaigning. Now I'm sure that this trend has its good sides and its neutral sides and its complicated sides. But inside the back cover of the May 1994 issue is an advertisement from a political software company whose headline is "The age of individual targeting is upon us". In other words, everyone gets their own personalized direct-mail pitch, based on a detailed database of information relevant to your likely political leanings. One use of such databases is basic demographics for choosing issues to emphasize; another is deciding who should be approached personally and urged to vote.

But a scarier use of such databases, not mentioned in the ad, is the tailoring of messages to individual voters. For example, a group of land developers in San Diego is promoting an initiative for tomorrow's primary election that would open up the last parcel of wild land in San Diego to development. Their campaign has been incredibly sophisticated, including numerous tactics that aren't relevant here. The part that *is* relevant here is a letter I received over the weekend encouraging me to vote Yes on the initiative. Along with the letter were two inserts containing endorsements from the leader of the local AFL-CIO and a Hispanic city council member from another district. Did the guy around the corner with the "Rush is Right" bumper sticker get the same inserts? He didn't have to, if the developers had access to a suitably "enriched" database. In the future you won't even have to bother putting together a coherent coalition; just find out what everybody's hot issues are and make them all whatever promises you need to make, one by one, the Saturday before the election, so nobody has time to compare notes.

Campaigns and Elections, 1511 K St NW #1020, Washington DC 20005, USA.  
Subscriptions \$30/year in the US, write for prices elsewhere.

Phil Agre, UCSD

---

## Library fines unstoppable after earthquake

Geoff Kuenning <geoff@FICUS.CS.UCLA.EDU>

Tue, 31 May 94 13:31:29 -0700

>From an article by Rebecca Bryant in the Los Angeles Times Valley  
Section, Thursday May 19th:

The Los Angeles City library system is sending out overdue notices for books that had been checked out before the January 17th earthquake. The only problem is that readers have been told that they can hang on to their books until the damaged branches reopen.

"Now wait a minute," writes Bryant. "Who[m] do you believe? The library? Or, uh, the library?"

The problem arose because the computer system used to generate the notices does not allow notices to be selectively disabled based on the branch at which the book was originally checked out. The only way to stop the notices would be to stop sending notices for all branches. But many branches remain open, and of course there are always delinquent readers. According to Robert Reagan, a library spokesman, the system is due to be replaced soon. Although the article does not state this explicitly, there is an implication that the new system will support better per-branch control.

This is in many ways not just a computer risk. The original programmers, designing an integrated system, can be forgiven for failing to predict the day when their customers would want to shut down only half of it, based on unforeseen criteria. Furthermore, it is easy to imagine an integrated manual system with the same (if you will excuse the expression) fault.

Nevertheless, readers are confused and the library is embarrassed. I guess it's a pretty minor, though amusing, footnote to a major disaster.

Geoff Kuenning geoff@ficus.cs.ucla.edu geoff@ITcorp.com

---

### Flames and viruses in e-mail - article in the New Yorker

*Martin Minow <minow@apple.com>  
Sat, 4 Jun 94 13:42:43 -0700*

RISKS readers might find John Seabrook's article in the June 6, 1994 issue of the New Yorker interesting. He had previously written a profile of Bill Gates, chairman of Microsoft (January 10, 1994) and received an obscene and obnoxious message from "a technology writer who does a column about personal computers for a major newspaper."

In true New Yorker tradition, Seabrook used this message as a vehicle to comment on network etiquette and on the possibility that some strange aspects of the message might indicate that the message contained a "worm" or "virus." (My own reading of the evidence presented is that there is nothing to worry about.)

Of particular interest to Risks readers might be Seabrook's fear that any strangeness in the message might indicate an attack, and on the general way in which extending the net to "an estimate twenty-three million users ... ten million of which have come on-line in the last nine months" has affected the culture of network communications.

RISKS readers -- at least those of us who have been around since the net was a self-regulated anarchy -- will find his comments on the way this anarchy is, or soon will be, dying away very interesting.

Martin Minow minow@apple.com

---

## Tetris addiction?

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@CompuServe.COM>  
28 May 94 21:41:39 EDT

>From a Canadian newspaper, \_The Globe and Mail\_, 28 May 1994, p. D1:

<<Stay out of the laundry room, son, your mother is playing Tetris: Computer software houses want to know why grown women are transfixed by one particular video game. Psychologists have been hired.>>

by Jim Carlton of the Wall Street Journal

<<Nintendo Co., master peddler of cyberpuzzles to young boys, has a riddle of its own: Why are so many grown women hooked on Tetris, the geometric video game? Fourteen-year-old Bobby Meade would certainly like to know. "Almost 24 hours a day she plays Tetris," the Johnstown, Ohio boy writes of his mother in a letter to Nintendo. "I can't hardly play more than one game a day." Peggy Rudden's family would also like to know. "My husband thinks I'm hooked on it," says 46-year-old mother of six in Englewood, Colo., who plays in her laundry room, away from the kids.>>

The author continues with the following key points:

<<

---

## Re: Closed Doors in Glasgow - Trapped Guard Dies in Fire

John Vilkaitis <javilk@netcom.com>  
Sat, 4 Jun 1994 00:37:06 -0700

Failure to provide a reliable emergency exit is usually a violation of local fire and other ordinances. The RISK is civil and criminal prosecution, not MERELY lost sales.

This, and many other seemingly senseless problems have at their root, a failure of the analyst to IMAGINE HIMSELF using the system. Sometimes this is the fault of the analyst, often it is simply because management refused to give the analyst (or the programmer) time to calmly "daydream" himself using the system and encountering typical situations and problems. If you cannot imagine in your head what you are building, you RISK building trash, often dangerous trash.

"Imagination is more important than facts" - Albert Einstein

It takes both FACTS and IMAGINATION to build good systems, but no one seems to teach us to use the broader power of our imagination, insisting we use the far narrower term "THINKING".

-JVV- (J. Vilkaitis, javilk@netcom.com, 408-983-0518 voice/fax)

[John, I guess you have to be THIN-KING to slip through the emergency exit.  
See my article, Psychosocial Implications of Computer System Development

and Use: Zen and the Art of Computing, in Theory and Practice of Software Technology, D. Ferrari, M. Bolognani, and J. Goguen, eds., North-Holland, 1983, for a discussion of how both left-brain and right-brain activities must be used and properly integrated. PGN]

---

**Re: Risks of too-simple responses (UK ATM Spoof) ([RISKS-16.10](#))**

"Henry J. Cobb" <[hcobb@fly2.berkeley.edu](mailto:hcobb@fly2.berkeley.edu)>

Wed, 1 Jun 1994 19:52:49 -0700

Jerry Leichter suggests that ATMs be "hardened" to spoofery by reading the "noise" built into the card during manufacture rather than the digital signals encoded on them.

The risk to this is once the scanner that detects the noise is out in the field in large numbers, it becomes just another fixed system to spoof.

Before you counter with "We'll just push down to the quantum level!" consider if you'd want real people in the real world walking around with cards depending on this. (And please no "Are you displeased to see me, or is that just a quantum in your pocket?" jokes from the moderator.)

Digitally secure smartcards are not only the geek thing to do, they're the right thing to do. As for the installed base of "dumb" cards, this can be wiped clean by proper legislation or simple liability. All that is needed is to abolish the NSA and go back to being a free nation.

---

**Re: Risks of too-simple responses (UK ATM Spoof) ([RISKS-16.10](#))**

Mathew Lodge <[lodge@ferndown.ate.slb.com](mailto:lodge@ferndown.ate.slb.com)>

Fri, 3 Jun 94 17:22:47 BST

Perhaps Jerry has never been to France. All French credit cards are smart cards, and have been in mass use for several years now. The French don't seem to be having any problems with fragility or expense.

As to backward compatibility, this is solved by the extraordinarily simple measure of allowing the card readers to deal with both smart cards and ordinary magnetic stripe cards. Thus I can use my Visa card in France with no problem (the only difference is that there is no immediate validation using my PIN as there is for smart cards).

> In practice, my bet is that we will *\*never\** see the replacement of magnetic  
> stripe cards by smart cards.

I think this is a little too pessimistic.

Mathew Lodge, Software Engineer, Schlumberger Technologies, Ferndown, Dorset,  
UK, BH21 7PP [lodge@ferndown.ate.slb.com](mailto:lodge@ferndown.ate.slb.com) +44 (0)202 893535 x404

## Re: UK ATM Spoof (Cobb, Lodge, [RISKS-16.12](#))

*Jerry Leichter <leichter@lrw.com>*

*Fri, 3 Jun 94 22:07:00 EDT*

On Henry J. Cobb's fixed system to spoof:

We've been using pin-tumbler and mechanical combination locks for many, many years. In fact, that's exactly what protects the money actually stored inside of ATM's - along with fairly simple electrical alarms, which haven't changed much in many years either. All "just another fixed system to spoof".

Clearly the only hope is "digitally secure smartcards", a technology that has seen all of 20 years worth of development and testing in the real world, against real attackers. By all means, let's convert everything immediately. After all, these new systems are based on \*digital computers\*! Clearly they are better, more secure! Computers never make mistakes, after all!

On Mathew Lodge's response to my statement ("In practice, my bet is that we will \*never\* see the replacement of magnetic stripe cards by smart cards."), saying that he thinks this is "a little too pessimistic":

As Mark Twain said, it's a difference of opinion that gives us horse races. (Well, he said it better, but I don't recall the exact words.) We've both made our predictions. I'll sharpen mine: Five years from now, smart cards will represent no more than 5% of the US market for bank and charge/debit cards; some variation of magnetic stripe technology will make up essentially all the remaining 95%. Shall we revisit this in 1999?

---

## Clipper

*Gene Spafford <spaf@cs.purdue.edu>*

*Fri, 03 Jun 94 19:20:45 -0500*

In today's mail I got a glossy brochure extolling Clipper. It promises to "Expand your creative universe with real-world solutions."

Is it a new ploy by the government to subvert our privacy? No, it's an advertisement by a company named Dynamic Graphics for their CD-ROM clip art magazine. "Clipper" is their registered trademark.

I wonder if they registered the trademark recently? I would have pitched the flier immediately had I not noticed the word "Clipper" in large letters. I can't recall hearing about them before, either.... Has "Capstone" been registered yet, or "Tessera"? :-) On the other hand, it might be they had the name picked out over a year ago and their business will go south as a result of recent events.

The risk? Naming a product something catchy just before a government agency nicknames something unpopular the same name. (Alternatively, there's a risk in trying to avoid this -- naming a product "Facist Thought Control" is likely safe from collision, but won't help sales. :-)

---

## Details of flaw in Clipper

Sidney Markowitz <sidney@taurus.apple.com>

Fri, 3 Jun 1994 20:14:29 -0700

I have seen lots of discussion about the New York Times report on Matt Blaze's discovery of a flaw in Clipper's key escrow system, with more confusion than anything else. Here is the best article that I have seen on the net explaining exactly what Dr. Blaze has found. There's also confusion about the implications. My understanding is that this method might allow someone with a Clipper chip device to have a secure communication with another person with a Clipper device that could not be decrypted by law enforcement \*and\* it does not require the cooperation of the second person. That last part is what makes this significant, since two people can agree to just encrypt their messages with, say PGP, if they want to be secure from law enforcement decryption. But if Blaze's method is practical, the widespread use of Clipper would make it harder on law enforcement by making it easier than it is now for someone to have secure communication with people without having to plan with them to do so.

-- sidney markowitz <sidney@taurus.apple.com>

[begin quote of Message-ID: <PERRY.94Jun3182655@snark.imsi.com>  
crossposted to sci.crypt, talk.politics.crypto, alt.policy.clipper]

[Run in RISKS with permission of "Perry E. Metzger" <perry@imsi.com>. PGN]

Many people have misconceptions about what Matt did.

Based on his paper (no, you can't have a copy since he told me not to distribute it; I'm sure he'll release it when its ready for prime time) and discussions with him, the trick is this.

[The Escrowed Encryption Standard is abbreviated as EES.]

The LEAF acts much as an key to tell the EES unit that it should function. It contains three elements:

- 1) the 32 bit unit id of the EES unit generating the LEAF
- 2) the 80 bit session key, encrypted in the escrowed key for that unit.
- 3) a 16 bit checksum based on the unencrypted session key and the initialization vector (IV) for the session.

All three components are concatenated to form a 128 bit unit, which is encrypted in the family key in order to produce the LEAF, reportedly using a unique mode of Skipjack.

The remote unit takes in the LEAF, decrypts it with the family key, and checks the cleartext session key and IV to see if they produce the proper 16 bit checksum. If so, it accepts the LEAF and functions properly. Note that the encrypted key inside the LEAF is useless to the remote EES since it doesn't

have the other EES's escrowed key. It has to rely on the cleartext session key and IV alone to check that the checksum looks right.

Sadly for the NSA, the checksum is only 16 bits long. Given a session key and initialization vector, I can fairly quickly generate a large number of fake LEAFs (chosen at random) and find one that a captive EES unit will accept as being the right LEAF for a given session key/IV. The contents of the LEAF will be garbage, but the remote unit will not know that, and will happily go along with using it. I needn't know the family key, or even the checksum algorithm.

The point here is, of course, that I can freely interoperate with non-rogue EES units -- I can communicate with non-subverted units without revealing my privates hidden beneath the LEAF. (sorry for the pun.) [\*]

By the way, Matt had to figure out the components of the checksum on his own -- the mechanism for calculating it and where it came from were not documented.

BTW, for those who have asked, in case the preceding didn't make it clear, can't you just reuse an old LEAF or a stolen LEAF because the session key/IV won't correspond and the checksum won't be right -- you have to generate and test.

Perry Metzger    perry@imsi.com

[end quoted message]

[\*] [Turning over a new LEAF is better than if you LEAF well enough alone, he suggested FIGuratively. PGN]

---

### **Blaze's Clipper paper available via ftp**

*Sidney Markowitz <sidney@taurus.apple.com>  
Mon, 6 Jun 1994 19:29:45 -0700*

Matt Blaze is the AT&T researcher who has made the news recently for discovering a flaw in the Clipper protocol. I saw an announcement from him that a preliminary draft of his paper "Protocol Failure in the Escrowed Encryption Standard" is available via anonymous ftp from resarch.att.com in the file /dist/mab/eesproto.ps in PostScript format. He cautions that there will be a final version of the paper which will likely include additional material on the production version of the PCMCIA card, and that this draft is based on his examination of a prototype card.

-- sidney markowitz <sidney@apple.com>

---

### **Flaw ? in Clipper**

*A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>  
Sat, 4 Jun 94 22:35:29 -0400*

This has already gotten out of hand on the Usenet. In simplest terms, what Matt Blaze found is that it is possible to spoof a CLIPPER LEAF (law enforcement access field).

IMHO this is almost meaningless since \*both\* ends will need to do this (AFAIR each side sends a LEAF. If only one LEAF is spoofed, it will just be necessary for a legal tapper to use the other one).

Thus to be effective, both ends will need special spoofing equipment and in that case they might as well use something other than Clipper. Even better use something different but prefix a valid Clipper LEAF. Right. Remember Occam's Gillette.

Dr. Blaze also mentioned that it would take about 20 minutes to come up with a valid checksum. Much easier would simply be to record a valid LEAF from another chip and use that.

The most important element is that the SKIPJACK algorithm is in no way affected by this and is as strong as ever, only the government's ability to use the LEAF may be compromised.

I still expect the government to drop key escrow when the hardware is ready and that there will still be two means available to defeat Clipper available to the government - without using any backdoor/trapdoor and without any weakness in SKIPJACK (see my earlier postings - one is similar to the way GSM can be tapped now).

Personally, I feel that Clipper is a valuable mid-range low-announced- cost device that is "good enough for government work". PGP or triple DES used in combination with Clipper is a viable next step up.

Padgett

P.S. Anyone notice Enigma-Logic's announcement of a one-time-password-token emulation for the PC @ US\$10/user (maybe less) ? Certainly an answer to sniffers.

---

### **Re: Flaw in Clipper detected (Huggins, [RISKS-16.11](#))**

*Paul Carl Kocher <kocherp@leland.Stanford.EDU>*

*Tue, 7 Jun 1994 03:19:55 -0700*

Although I doubt people will modify devices with hard-wired Clipper chips, this seems to be a very serious blow to Tessera (the government's PCMCIA card with a Clipper chip).

Tessera has a standard programming interface that passes the programmer's calls to the encryption card. Any experienced assembly language programmer could easily add "support" for Blaze's technique for bypassing the LEAF (Law Enforcement Access Field) validation check. This could be done transparently and without significantly impacting performance. It could also fix up the side effects of the attack (e.g. the first block is bad in CBC mode, etc).

Under MSDOS this could be done with a TSR that would intercept calls to the card directly, so it would work with all Tessera applications. The same TSR could also substitute pre-computed and/or brute-forced LEAFs for interoperability with non-cheating users.

We were told that the reason for having escrowed keys and a secret algorithm was to keep terrorists from having strong crypto. Now the bad guys have full-strength SkipJack, the public has a flawed "standard," and because the algorithm is classified we can't look for other problems. I'm also wondering what's going on inside NSA -- DSS originally had alarmingly-small keys and has been widely criticized, SHA was defective, and now this...

-- Paul Kocher [kocherp@leland.stanford.edu](mailto:kocherp@leland.stanford.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 16: Issue 13**

**Thursday 9 June 1994**

## Contents

- [RISKS summer slowdown](#)  
[PGN](#)
- [False alarm in Channel Tunnel](#)  
[John Colville](#)
- [Apathy toward computer errors](#)  
[Chip Seymour](#)
- [Mailing-list software security problem](#)  
[Jim Patterson](#)
- [GIF contains more than just a picture](#)  
[Matthew David Aldous](#)
- [Re: "The Ghost in the Modem"](#)  
[Scott Dickson](#)
- [Re: China Airlines A300 Crash](#)  
[Mark Terribile](#)
- [Re: Flaw ? in Clipper](#)  
[A. Padgett Peterson](#)  
[Robert I. Eachus](#)
- [WWW Virtual Library page on safety-critical systems](#)  
[Jonathan Bowen](#)
- ["Network Security Secrets" by Stang](#)  
[Rob Slade](#)
- [Re: "The Hacker Crackdown" by Bruce Sterling, via WWW](#)  
[John Oram](#)
- [Info on RISKS \(comp.risks\)](#)

---

## RISKS summer slowdown

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Tue, 7 Jun 94 9:42:08 PDT

RISKS is about to enter its customary summer slowdown period, including the next month or so during which I will have only sporadic net access. Please do not expect to get rapid response to your requests or frequent issues. However, please keep the incisive contributions coming, and I will get to

them whenever possible.

I wish you all a peaceful and productive summer season.

PGN

---

## False alarm in Channel Tunnel

*John Colville <John.Colville@brunel.ac.uk>*

*Wed, 8 Jun 1994 11:06:17 +0100 (BST)*

As reported on BBC Radio, Wednesday 8 June 1994:

A train travelling through the Channel Tunnel from England to France, was evacuated after an emergency light came on in the driver's cabin. The drivers of the 10 lorries [Amer: trucks (JC)] who were being carried on the train were evacuated to the English end of the Tunnel, through the access tunnel. This was the first emergency on the Channel Tunnel which officially opened last month.

It turned out that the emergency was a false alarm.

John Colville, Visiting Brunel University John.Colville@brunel.ac.uk  
+44 895 274000 ext 2561 until June 1994, from University of Technology, Sydney

---

## Apathy toward computer errors

*Chip Seymour <CHIP@bdso.cv.com>*

*Tue, 31 May 1994 08:27:36 EST*

The Worcester (MA) Telegram of Saturday, May 28, carries a front-page article regarding "a mistake by the city Election Commission [which] nearly cost [name deleted] his wife."

A week before, a city resident "opened his mail to find a computer-generated census form from the city." Apparently, he didn't look at the form closely, and when he handed it to his wife for her signature, she noticed the name of the person living with him at the same address was not hers.

She had just returned from one of many extended visits with an out-of-town daughter.

"'Who is this Beverly that's living with you?' his wife, Barbara demanded. 'Come on, Barbara ... nobody is living with me,' he shot back. 'Well, they got it right here,' she countered, pointing to the name Beverly A. [different last name] on the form. 'If I find out, I'm going to get a divorce.'"

After a call to the city Election Commission, he discovered that the presence of the Other Woman is an error that may be attributed to the fact that he lives in an apartment building for senior citizens, and the Other Woman lives in another apartment in the same building.

A spokesman for the Election Commission said if the victim "crosses out the incorrect information and mails the form back to City Hall, it will be corrected in the computer."

The victim "says he has no intention of signing and sending in the erroneous form - and if his name is removed from the voter registration list, which is the penalty for failing to respond to the census, 'somebody else is going to have a lot more trouble.'"

"'I'm not going to send it in. They make too many mistakes, and I'm not going to rectify their mistakes,' he said. 'I can't see why people have to keep paying for their mistakes all the time.'" He says this is the "last straw."

The RISKS? If the City Election commission relies solely on returned census forms, accidental and intentional inaccuracies will remain. Given the current economic climate in the NorthEast, it's not likely local government will verify the information on every returned census form containing corrections.

Another risk is the perceived apathy on the part the public. If this fellow refuses to correct and return the form, how is the Election Commission going to correct the error? What if others follow his lead?

A third risk was mentioned by the Other Woman, who had not received a census form this year: "The census form is supposed to be confidential, but went to the wrong place."

---

## Mailing-list software security problem

*Jim Patterson <jhp@photon.com>  
Tue, 7 Jun 1994 21:24:49 -0700 (PDT)*

Several perfect examples of software risks here. First is running a security mailing list with software that has security problems. Then the ever popular quick change to complicated software that generates unexpected (and annoying) results. Finally, there were the users sending messages complaining about the duplicate messages to the list which were promptly forwarded to the list, in triplicate.

from the keyboard of bugtraq-owner@cscns.com ->  
> Sorry. I made some changes to the list code because of a serious  
> security hole found within the list software (a popular one).  
> This apparently caused things to go bonkers. Please stay patient.  
> The author of the mailing list software will release information  
> regarding the security vulnerability within the next few days.  
> --Scott

Hope you found this as amusing as I did.

Jim Patterson Photon Research Assoc. jhp@photon.com

---

## GIF contains more than just a picture

Matthew David ALDOUS <aldous@mundil.cs.mu.OZ.AU>

Thu, 9 Jun 94 17:34:40 EST

I'm currently involved in a software development project, writing software to assist medical diagnosis of brain scans. Although I've ploughed through about 50 pages of documentation now, without actually coding a single line, I decided it was time to whip up some "vapourware" snap shots of the screen I was intending to use.

These I created in a paint program, and whisked off to the supervisor for a critical review, etc.. Paper can only say so much..

The response I got was going as would be expected. Some suggestions for layout, color schemes, font sizes, etc.. Until I got to section 6..

----

5 yellow cross-hairs stand out better - is the red arrow for some reason? Not apparent what (or if)

6 not knowing what all the options were, I tried playing with a few. I certainly ended up with some images I did not expect. I figured I should be able to get back to where I started by a judicious choice of operations. Alas - not so judicious. I certainly did not expect to get the text in mirror-image form, even if the picture was. I also thought 'normal' would redraw the original image, but this was not so. Is there some easy option to get back to where you started?

----

I was quite taken back. I had only submitted a gif, but my supervisor was suddenly telling me about all the "options" etc. Gollies, a GIF with a built in OS independent GUI..

Turns out, the supervisor had been using "xv" to view the GIF, and had accidentally clicked the right mouse button on the picture at some stage, opening the "xv edit screen", and assumed that the new window was part of the submission ,etc. (Gosh, that \_IS\_ overwork.)

The RISK ? Having a totally foreign program pretending to be mine, without any intent. Was "xv" too user-friendly? Gollies, I was subsequently told that if I hadn't questioned the response that it would have been assumed I was working extra hard.. :)

We all had a good chuckle over it, and went back to work :)

[Hmm, I suppose that someone is going to come along and refer to "xv" as the FIFTEEN program, which is NINE more than "vi", which is sometimes mistakenly referred to as the SIX EDITOR (according to a sighting reported to me by Caveh Jalali)! PGN]

---

**Re: "The Ghost in the Modem" ([RISKS-16.11](#))**

Scott Dickson <scott@ontek.com>

Wed, 8 Jun 94 11:11:41 PDT

Regarding a recent RISKS posting of the article "THE GHOST IN THE MODEM" by Richard Sclove and Jeffrey Scheuer of The Loka Institute, I fail to see how the rather insightful analysis of the impacts of government meddling in favor of highway-based transportation supports the conclusions:

- > Three lessons for the construction of the information superhighway
- > suggest themselves:
- >
- > o No Innovation Without Evaluation: ... federal government should
- > mandate evaluated social trials ...
- >
- > o No Innovation Without Regulation: We should conserve cultural
- > space ...
- > ... modest tax on electronic home shopping and consumer services ...
- >
- > o No Innovation Without Participation: ... the Danish government
- > appoints panels of everyday citizens ...

These conclusions would lead us down the same road of the government using regulatory and taxing powers to distort the application and development of technology. A common mistake is for people to observe or foresee a danger and demand that government do something about it. They fail to take into account the risks involved in getting government involved, with its tax and regulation sledgehammers. This is appropriate when the dangers to be mitigated are great enough, but is not something to be suggested lightly. In many cases, people may be better off accepting the risk of the danger than putting up with the effects of government involvement.

The kind of preemptive government involvement advocated in this case is particularly questionable, since the dangers aren't really known and premature government meddling may actually make things worse (as the authors argue may have happened in the case of transportation).

Scott Dickson scott@ontek.com

---

### Re: China Airlines A300 Crash (Yesberg, [RISKS-16.09](#))

<mole-end!mat@uunet.uu.net>

Fri, 3 Jun 1994 18:48:11 -0400

The proper solution is not to increase the number of modes, but to decrease the number of modes--to ONE.

`Less advanced' aircraft, which I believe include Boeing aircraft, use their sophisticated flight control systems to make the plane behave like a simple plane with simple controls. `Fly by wire', to their designers, means `make the best, and best-behaved, simulation of a plane with direct linkage from controls to control surfaces.' `More advanced,' in Airbus case, means `having a greater chance for error.'

This has been debated in the aircraft industry, but the FAA has not seen fit to refuse certification to Airbus. My own belief, unsupported by professional qualification of any kind, is that this is a serious mistake, perhaps unavoidable due to the political nature of the Airbus Consortium.

If I understand correctly, Airbus was forced to use these multimode control systems because some of its aircraft use sidestick controllers. Sidestick controllers provide very little range of motion compared to the traditional yoke (wheel on a moving stick/post), and the pilot effectively flies using pressure rather than position of the sidestick. This is fine during normal flight, but during takeoff and landing the control surfaces must be moved through large excursions, and the additional control modes are needed to allow this.

There is another serious problem with the control mechanism described: the autopilot used one set of control surfaces (stabilizer trim) while the pilot continued to operate another (elevators). In effect, the aircraft and its inherent flight laws provide the summing of the control inputs. For such an arrangement to work at all, the summing process must remain linear, must not interfere with the flight of the aircraft in other ways, etc. Clearly, this did not happen. An unqualified person such as myself has to wonder what happens when the stabilizer is canted one way and the elevator is canted the other. The result, it seems to me, should be excess drag and a disrupted airflow, leading to reduction or loss of control response to both inputs.

There is a third problem: the pilot has no indication through his controls that the autopilot--in effect, the aircraft's control laws--are actively working against him. In an emergency, there are only two things he is likely to pay attention to--the primary instruments and the controls under his hands and feet. If he were to put the plane to the edge of a stall, either the natural buffet of the stall or an artificial stick-shaker designed to simulate the buffet would alert him. That is probably the proper place to inform the pilot that he is working the aircraft against the edge.

I don't fly much, but if I find myself booked on an Airbus plane I will look for an alternate booking.

Mark Terrible mat@mole-end.matawan.nj.us, Somewhere in Matawan, NJ

---

## Re: Flaw ? in Clipper

A. Padgett Peterson <padgett@tcslr.dnet.mmc.com>  
Thu, 9 Jun 94 13:43:58 -0400

Earlier I wrote re Clipper LEAF spoofing:

<> IMHO this is almost meaningless since *\*both\** ends will need to do this  
<> (AFAIR each side sends a LEAF. If only one LEAF is spoofed, it will  
<> just be necessary for a legal tapper to use the other one).

and received the following correction:

>According to a talk here at MIT given by two NSA mathematicians the  
>day the NYT broke the story (a happy coincidence :-), this is not  
>>true. Using Capstone/Tessera, only one LEAF is sent, by the  
>originating party.

I wrote:

<> Dr. Blase also mentioned that it would take about 20 minutes to come  
<> up with a valid checksum. Much easier would simply be to record a  
<> valid LEAF from another chip and use that.

and was again corrected:

>Can't do that, as Perry said. The LEAF is a function of the session  
>key, so it needs to be spoofed for each session.

What happens appears to be (after reading the draft of Dr. Blase's paper but with some inference - any mistakes are mine) that the receiving Baltimore Clipper decodes the LEAF sent by the originator using the family key, replaces the sender's unit-key-encrypted session key with its own clear session key, mixes in the originator's unit id (also in the LEAF), calculates a new checksum, and compares this with the one received.

The obvious implication is that what Dr. Blase was altering may not have necessarily been the checksum (IMHO it was the unit ID) but probably was the last sixteen bits of the LEAF. I leave the implications to those who have the good fortune to have received samples.

But then and again it is all moot since IMHO the gov (or at least the Clips, Billary may not have been completely filled in) do not intend to use the LEAF anyway.

Padgett

[Various similar comments are not included here.]

---

### **Flaw ? in Clipper [Some duplication w. the previous item]**

*"Robert I. Eachus" <eachus@spectre.mitre.org>*

*Thu, 9 Jun 1994 10:28:23 -0400*

A. Padgett Peterson (padgett@tccslr.dnet.mmc.com) wrote:

> IMHO this is almost meaningless since *\*both\** ends will need to do  
> this (AFAIR each side sends a LEAF. If only one LEAF is spoofed,  
> it will just be necessary for a legal tapper to use the other  
> one).

As far as I am concerned, this is why the flaw Dr. Blase discovered is so damning. If the effect of an authorized wiretap on an EES phone is that the correspondents [?] key is removed from escrow, this destroys the entire

purpose of the system.

For example, a call in a mobile system would involve a chip in the phone, and a chip in the base station. If the result of a legal wiretap on a LEAF-blower equipped mobile phone is that the keys of all the base stations in the vicinity are turned over to the tappers, the escrow system protects no one.

- > Dr. Blase also mentioned that it would take about 20 minutes to
- > come up with a valid checksum. Much easier would simply be to
- > record a valid LEAF from another chip and use that.

This is a double misapprehension. First, the twenty minutes (divided by the number of chips used) delay is only associated with some modes of use. Second, the problem is not in collecting LEAFs, but in finding one that will be accepted by your correspondent for THIS call. In some cases that will be doable in advance, in others it will be easy, and in a few cases it may have to be done "the hard way" after the call has been initiated.

- > The most important element is that the SKIPJACK algorithm is in no
- > way affected by this and is as strong as ever, only the
- > government's ability to use the LEAF may be compromised.

Not quite true. Being able to "peer through" the crypto protection is usually the first step in a complete crack. In this case it opens up (actually makes more effective) avenues of attack, which while they seem computationally infeasible today, may shorten the effective lifetime of the EES system.

Robert I. Eachus

---

## WWW Virtual Library page on safety-critical systems

<Jonathan.Bowen@comlab.oxford.ac.uk>

Thu, 9 Jun 94 14:57:32 BST

I have created a WWW Virtual Library page on safety-critical systems, including links to on-line RISKS information, under:

<http://www.comlab.ox.ac.uk/archive/safety.html>

Relevant information with URL links for possible inclusion, preferably in HTML format, is welcome.

Jonathan Bowen Oxford University Computing Laboratory

<http://www.comlab.ox.ac.uk/oucl/people/jonathan.bowen.html>

---

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">

Thu, 09 Jun 1994 10:24:59 -0600 (MDT)

Subject: "Network Security Secrets" by Stang

BKNTSCSE.RVW 940324

International Data Group  
155 Bovet Road, Suite 310  
San Mateo, CA 94402 USA  
tel 415-312-0650 fax: 415-286-2740  
"Network Security Secrets", Stang, 1993, 1-56884-021-7, U\$49.95/C\$64.95  
norman@digex.com

It's hard to have confidence in a book on data security that starts off with two examples of "back doors" -- neither of which have the slightest connection to back doors. Then, there is the example of radiation risks which cites a study probably more related to chemical exposure. Do not lose heart, however. These are apparently aberrations in what is otherwise a very practical and down-to-earth security manual.

That opening chapter on specific examples starts a section on risk analysis. Security mavens may find it lacking in rigour and overlong in verbiage, but most micro/LAN/office managers have little formal training in the formal aspects of data security and need the example after example approach. The questionnaires and quizzes probably drive the point home as well as, or better than, Stang's love of charts.

Part two is a bit weaker. It opens with a questionable chapter on the "players" in the game: data security versus the hackers. There is a chapter on the security aspects of network design. Given Stang and Moon's background in the NCSA the two virus chapters are no surprise, and generally good.

Part three gives more detail (\*lots\* of detail in the tabular reviews of chapter 12) on security solutions, policies and products. Not exhaustive: the password chapter, in looking at security \*breaking\* programs, makes no mention of the HACK program for obtaining any passwords used over Ethernet or the KNOCK program which exploits a bug in versions of NetWare which allows anyone to gain SUPERVISOR access without passwords. Still, there is much practical help for the LAN manager here.

Part four looks at specific network operating systems and the security features and functions thereof. As well as comparisons of the different systems, there are chapters collecting the security commands and concepts of each. These are handy, but not necessarily more so than the original documentation. NetWare "effective rights", for example, continue to bedevil LAN managers using Novell's software. All the parts are included here, but the calculation of effective rights is not dealt with. (There is also one "oops". The chapter on UNIX security contains a description of the VMS "WANK" worm.)

Part five looks at ways to implement security. An unusual, but very valuable, section in the chapter on training is an extensive list of training available in a variety of security related areas. (Most of the virus courses seem to be given by an outfit called Norman Data Defense Systems. Oh well.)

Part six briefly describes the shareware files on the included disks. A series of appendices primarily give contact information.

It'll be difficult to get a busy LAN manager to sit still long enough to read this. But it'll be worth it.

copyright Robert M. Slade, 1994 BKNTSCSE.RVW 940324

DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733  
BCVAXLUG ConVAXtion, Vancouver, BC, Oct. 13 & 14, 1994 contact vernc@decus.ca

---

## Re: "The Hacker Crackdown" by Bruce Sterling, via WWW

*John Oram <oramy92@halcyon.com>*

*Thu, 9 Jun 1994 00:39:34 -0800*

Bruce Sterling has released 'The Hacker Crackdown' electronically. It is available via WWW at

[http://www.eecs.nwu.edu/hacker\\_crackdown/index.html](http://www.eecs.nwu.edu/hacker_crackdown/index.html)

(This is a mirror of <http://www.scrge.cs.tcd.ie/scrge/u/bos/hacker/hacker.html>)

[But be sure to read the preface about the copyright and why and how Bruce is also making the book available on-line. I have excerpted the beginning of the preface here, because it is too long to include here. PGN]

The Hacker Crackdown

Preface to the Electronic Release of The Hacker Crackdown

Out in the traditional world of print, The Hacker Crackdown is ISBN 0-553-08058-X, and is formally catalogued by the Library of Congress as "1. Computer crimes -- United States. 2. Telephone -- United States -- Corrupt practices. 3. Programming (Electronic computers) -- United States -- Corrupt practices." 'Corrupt practices,' I always get a kick out of that description. Librarians are very ingenious people.

The paperback is ISBN 0-553-56370-X. If you go and buy a print version of The Hacker Crackdown, an action I encourage heartily, you may notice that in the front of the book, beneath the copyright notice -- "Copyright (C) 1992 by Bruce Sterling" -- it has this little block of printed legal boilerplate from the publisher. It says, and I quote:

"No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher. For information address: Bantam Books."

This is a pretty good disclaimer, as such disclaimers go. I collect intellectual-property disclaimers, and I've seen dozens of them, and this one is at least pretty straightforward. In this narrow and particular case, however, it isn't quite accurate. Bantam Books puts that disclaimer on every book they publish, but Bantam Books does not, in fact, own the electronic rights to this book. I do, because of certain extensive contract

maneuverings my agent and I went through before this book was written. I want to give those electronic publishing rights away through certain not-for-profit channels, and I've convinced Bantam that this is a good idea.

Since Bantam has seen fit to peaceably agree to this scheme of mine, Bantam Books is not going to fuss about this. Provided you don't try to sell the book, they are not going to bother you for what you do with the electronic copy of this book. If you want to check this out personally, you can ask them; they're at 1540 Broadway NY NY 10036. However, if you were so foolish as to print this book and start retailing it for money in violation of my copyright and the commercial interests of Bantam Books, then Bantam, a part of the gigantic Bertelsmann multinational publishing combine, would roust some of their heavy-duty attorneys out of hibernation and crush you like a bug. This is only to be expected. I didn't write this book so that you could make money out of it. If anybody is gonna make money out of this book, it's gonna be me and my publisher.

My publisher deserves to make money out of this book. Not only did the folks at Bantam Books commission me to write the book, and pay me a hefty sum to do so, but they bravely printed, in text, an electronic document the reproduction of which was once alleged to be a federal felony. Bantam Books and their numerous attorneys were very brave and forthright about this book. Furthermore, my former editor at Bantam Books, Betsy Mitchell, genuinely cared about this project, and worked hard on it, and had a lot of wise things to say about the manuscript. Betsy deserves genuine credit for this book, credit that editors too rarely get. [...]



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 16: Issue 14**

**Monday 13 June 1994**

## Contents

- [Unconventional Telephones](#)  
[Mike Hoffberg](#)
  - [Ex-deputy police chief charged over Computer Records](#)  
[Mich Kabay](#)
  - [RISKS in UK Election Voting Process](#)  
[Thomas Rushton](#)
  - [Big brother wants the shirt off your back](#)  
[Lynn R Grant](#)
  - [Re: GIF contains more than just a picture](#)  
[Castor Fu](#)
  - [Re: How to feel safer in an Airbus](#)  
[Peter Ladkin](#)
  - [Airbus A3\(0?\)0 deductions](#)  
[Phil Overy](#)
  - [Correction for address of Clipper paper](#)  
[Sidney Markowitz](#)
  - [Chunnel vision](#)  
[David Honig](#)
  - [RISKS of real-time image processing](#)  
[Andy Cunningham](#)
  - [Re: Women and Tetris addiction](#)  
[Hilarie Orman](#)
  - [Re: Campaigns and Elections](#)  
[Robert J. Burkhart](#)
  - [Re: Apathy toward computer errors](#)  
[Tom Yurkiw](#)
  - [Security? Maybe....](#)  
[Neill Clift](#)
  - [Re: Call Your OPERATER](#)  
[Hardwire](#)
  - [Re: Risks of too-simple responses](#)  
[Ross Anderson](#)
  - [Info on RISKS \(comp.risks\)](#)
-

## Unconventional Telephones

Mike Hoffberg <hoffberg@aps.anl.gov>

Sun, 12 Jun 94 21:45:24 CDT

I just got a new 900 MHz telephone made by Bel-tronis. Plastered all over it is the fact that it "Styled by BRONDI, Italy". I guess I should be impressed.

Well today I prepare to make a call on it to SouthWest Airlines (1-800-I-FLY-SWA). Guess what? The phone does not have a "W" on it.

On the #9 key it has XYZ. It is missing the "Q" though.

It kind of reminds me of the (sorry about the non-PC reference) Polish joke of the day 555-POLZ. Except it would not work on this phone.

Michael Hoffberg hoffberg@phebos.aps.anl.gov mike@anl.gov

---

## Ex-deputy police chief charged over Computer Records

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@CompuServe.COM>

12 Jun 94 09:26:26 EDT

>From the Reuter newswire (94.06.10 @ 16:59) via Executive News Service (GO ENS) on CompuServe:

LOS ANGELES, June 10 (Reuter) - A former deputy police chief who is now a private detective has been accused of obtaining highly sensitive criminal records from his old department, a spokeswoman for the District Attorney's Office said Friday.

Spokeswoman Sandi Gibbons said Daniel Sullivan, former deputy chief of the Los Angeles Police Department, was charged Thursday with 11 misdemeanor counts of being in possession of criminal records.

According to the article, Sullivan allegedly used an inside collaborator to get the data. The collaborator and another private detective who received confidential police files were also charged with misdemeanors. Some of the stolen information concerned people in official witness-protection programs, relocated to protect their lives.

---

## RISKS in UK Election Voting Process

Thomas Rushton <RUSHTON@RMCS.CRANFIELD.AC.UK>

Fri, 10 Jun 94 16:24 BST

A colleague (call him ZX) has just told me about how he voted in the recent European Elections, and I thought I would share it with you.

He realised that he didn't have his voting card with him, but went to vote anyway. The voting hall contains several tables, where you exchange your card for a voting slip, and the usual booths / boxes etc.

The procedure: Go to the table which is labelled with your street name, hand over your card, and receive a voting slip.

ZX (with no card), went to the appropriate table, and explained that he wanted to vote, but did not have his voting card with him. The clerk said "Oh, that's OK -- which street do you live in?". ZX replied [RISK area -- pick a street, any street, from the following...]  
The clerk then looked up in his copy of the electoral register for that street, and asked ZX for the number of the house he lived in. [RISK area -- the names in the register were marked in a way that indicates who has voted already] ZX replied with his house number, the clerk said "Oh, you must be Mr X", and handed ZX a ballot slip.

The obvious conclusion is that J. Random Voter can go to any polling station, say he's left his voting card at home, give a street name (supplied on the tables), pick the number of a house on that street from which no one has voted (by reading the electoral roll copy), and vote, without having had to produce any form of ID.

The RISks here are even higher when you consider that approx only 30% of the total electorate participated in this election....

Question: Should the UK update its voting system?

Thomas Rushton SwEng / SEES, RMCS, Shrivenham, Swindon, WILTS, SN6 8LA, UK  
rushton@rmcs.cranfield.ac.uk      tel: +44 (0)793 785684

---

## Big brother wants the shirt off your back

*Lynn R Grant <Grant@DOCKMASTER.NCSC.MIL>  
Mon, 13 Jun 94 16:16 EDT*

Here's another risk on the horizon. We may have to wait a few years, though. From the June 1994 issue of Bobbin, "The premier news and information source of the global sewn products industry":

Groups such as the American Textile Partnership (AMTEX), a research consortium that links the sewn products industry with the Department of Energy's national laboratories, also are looking at RF technology as a means to improve the production process. In a research project called the Embedded Electronic Fingerprint, long-term work is underway to develop a computer-type device the size of a grain of wheat that could be attached to a garment and used through the entire product life cycle.

"A manufacturer could program into the device information unique to a garment, such as the size, color, style, line, or plant of manufacture, care instructions, etc.," explains Jud Early, director of research and development for the Textile/Clothing Technology Corp, [TC]\*\*2. "There also would be a large amount of blank memory that could be used for anti-counterfeit tracking and more."

Since each tag would have a unique identity, in-process inventory could be tracked easily using RF units--without ever touching garments or having to open shipping boxes. For example, a carton could be passed through a reading system, which would verify the contents against the packing list.

So, all that is needed is for the clerk at the store to capture the identity of the shirt, perhaps through a barcode on the tag (so they wouldn't have to install the special shirt readers), and they already know your identity from your credit card number (unless someone else buys your shirts for you), so they can track your movements by setting up shirt readers in various places.

But that might take more collusion between government and the stores than we want to speculate. So try this: a crime is committed. A few days later, you walk past a hidden shirt reader, and are immediately approached by an officer of the law, who arrests you for the crime. "But I was nowhere near the scene of the crime," you protest. "On the contrary," the officer counters, "one of our hidden shirt readers detected you shirt in the vicinity of the crime. You must be guilty."

One would hope that the manufacturers of these devices don't accidentally program duplicate serial numbers in them. And you should think twice about lending your shirt to your girlfriend.

Lynn Grant Grant@DOCKMASTER.NCSC.MIL

---

### **GIF contains more than just a picture (Aldous, [RISKS-16.13](#))**

*Castor Fu <castor@drizzle.Stanford.EDU>  
Thu, 9 Jun 1994 23:10:30 -0700*

So does this mean that xv - vi = une ix ?

[To which PGN replied,  
However, if ix were masculine, we would have un ix.]

[To which Castor replied,  
One could argue that the gender of Unix is somewhat ill-defined.]

[So, we need a language such as Latin with a neuter gender,  
and in which "un" is an indefinite article. PGN]

[Kevin Kenny (kennykb@dssv01.crd.ge.com) noted that the other  
popular image viewer, `xli,' is the FORTY-ONE program!]

---

### **Re: How to feel safer in an Airbus [Terrible, [RISKS-16.13](#)]**

*Peter Ladkin <Peter.Ladkin@loria.fr>*

*Fri, 10 Jun 1994 11:04:40 +0200*

Mark Terrible offered some interesting comments on Airbus aircraft design. But some of his speculation is ill-founded, and should not pass without comment.

- > If I understand correctly, Airbus was forced to use these multimode control
- > systems because some of its aircraft use sidestick controllers.
- > [...]
- > There is another serious problem with the control mechanism described:

This is confused. His first comment refers to the Airbus A320 aircraft, which is the first 'fly-by-wire' commercial transport. His second comment refers to the crash of a China Airlines A300 in Nagoya, which is a different aircraft, with the usual mechanical and hydraulic primary control systems and relatively limited use of computers. It does not have sidestick control.

His speculation on the A320, that Airbus were forced to use modes because they chose a sidestick design, is incorrect. Fly-by-wire aircraft use modes because they have to. What toys you give the pilot to convey her instructions to the computer is almost an independent choice. If the plane is flown by computer, she doesn't need a large lever to move the control surfaces.

- > There is another serious problem with the control mechanism described: the
- > autopilot used one set of control surfaces (stabilizer trim) while the
- > pilot continued to operate another (elevators).

This arrangement is used on more or less every transport aircraft flying, as well as all tiny planes big enough to warrant a three-axis autopilot. If this is a 'serious problem', all aircraft have it. (Also, the trim system is not primary control as the elevators are. It serves a different function.)

- > There is a third problem: the pilot has no indication through his controls
- > that the autopilot--in effect, the aircraft's control laws--are actively
- > working against him.

This is false for the A300, as for most conventional transports. In fact, the copilot who was flying had to work quite hard to counteract the nose-up trim. This is one of the puzzles of the accident.

A further comment about the Nagoya accident is appropriate. Current knowledge is that the pilots failed to follow normal, explicit procedure for control of the aircraft, and secondly that they had both been drinking alcohol, which is illegal for good reason. Responsible senior management of China Airlines has resigned because of this accident. The FAA has virtually insisted that China Airlines work with it on improving safety procedures including crew training and oversight. Trying to draw conclusions about aircraft design from details of this particular accident is probably unwise.

Those wary of fly-by-wire transport aircraft design might also like to know that Boeing's next airplane, the 777, is full fly-by-wire - just like the A320, but, of course, different.

Peter Ladkin

---

## Airbus A3(0?)0 deductions

*Phil Overy RAL <PJO@ib.rl.ac.uk>*

*Fri, 10 Jun 94 09:06:53 BST*

re: Mark Terribile's posting:-

1) Boeing sell similar automation to the A320 - they also caused the second-worst Japanese crash and in this case much more directly (the fuselage broke).

2) whether you se sidestick or yoke, a modern airliner has no direct "cables" to the rudders - it relies on multiple links either electrical or hydraulic which would work equally well with sidesticks. A300s have been around for 20 years - this was an A320.

3) This is one of three crashes involving a simple confusion that I remember - the first Tri-Star crash (neither pilot had switched off the auto-pilot); the Kegworth crash (on a BOEING - the pilot shut down the wrong engine when it caught fire) and this one (the younger pilot didn't switch off the auto-pilot and didn't relinquish control. I automatically think of my poor (fortunately very quick-witted) gliding instructors when I read of this particular crash - thank you for not letting me land on the crosswind runway, Barry Hogarth!).

4) as for mode-switching and elevators etc - the senior pilot seems to have tried to recover without switching off the auto-pilot, the junior pilot seems to have flown as if the auto-pilot wasn't on. Reports will not say this as it's a conclusion, not a fact - it does however sound like the explanation.

5) Since several A320s have crashed when silly things have been happening, perhaps the automation, like the "watertight" hull of the Titanic, is creating a too-complacent pilot. As a far-too-complacent pilot myself in the past, I can understand this.

I do not pretend any insight into the cause of the crash, all I can say is that if Mark Terribile is basing his preferred flight on the logic presented here, he won't fly at all.

Regards

Phil Overy

Rutherford-Appleton Laboratory

(computer programmer with a chequered past, not a pilot or a designer, although I have used gliders to exploit the many rain clouds over England)

---

## Correction for address of Clipper paper

Sidney Markowitz <sidney@taurus.apple.com>

Fri, 10 Jun 1994 13:18:05 -0700

Perhaps the subject should be "RISKS of not using available spelling checker technology". In [RISKS-16.12](#), I had a typo in the address for the ftp site containing Matt Blaze's paper. The correct site name is research.att.com and the file is in /dist/mab/eesproto.ps and is in PostScript format. Thanks and my apologies to the people who took my creative spelling of the word "research" literally and sent me mail informing me of the error.

-- sidney markowitz <sidney@taurus.apple.com>

[My spell checker always balks on net addresses, so the "resarch" slipped by me. It also let a Blase go through in [RISKS-16.13](#). PGN]

---

### Chunnel vision (beaten to the pun)

David Honig <honig@binky.ICS.UCI.EDU>

Fri, 10 Jun 1994 15:54:36 -0700

Colville reported in [RISKS-16.13](#) on the first false alarm in the Chunnel. One might predict that these will be common at first. In the public's lexicon "False Alarm" might be replaced by "Channel Tunnel Syndrome" :-)

---

### RISKS of real-time image processing

Andy Cunningham <andyc@eurovi.uucp>

Fri, 10 Jun 94 08:50:36 BST

I had a first hand demonstration of a new road-side traffic monitoring system here in the UK earlier this week.

I was driving into some road works on the M1 motorway and was slowing down to take account of the 50m.p.h. speed limit which had been imposed. Immediately (10 yards) after the speed limit sign was a bridge, and mounted on this bridge was a camera. On the other side of the bridge was a large dot matrix display, which immediately flashed up the message:

```
SPEEDING  
L123 ABC  
58 MPH
```

(actual registration number changed to protect the guilty).

RISKS: first of all, I'm expecting to get a warning about the consequences of speeding in the mail. (In the UK, the police usually won't give you a ticket unless you're at least 10mph over the speed limit). More importantly some drivers might be surprised by this and cause an accident.

This technology starts to get real "big brother" overtones if it's used to actually send out tickets (camera/radar systems which produce photographic

evidence of speeding are already in place, but human intervention is required to actually send out the tickets). And just how accurate is the character recognition anyway?

Andy Cunningham, VI Corporation (Europe), Ilex House, Mulberry Business Park, Fishponds Road, Wokingham, RG11 2GY +44 734 892111 Fax: +44 734 892090

---

## Re: Women and Tetris addiction

*Hilarie Orman <ho@cs.arizona.edu>*

*Fri, 10 Jun 1994 19:05:16 -0700*

There are indeed deep psychological forces that draw women to the game of Tetris. I've been a Tetris junky, and I can give my testament to the risks of this particular addiction. First, I admit that I am, by nature, susceptible. I've been through several 12 step programs to rid myself of addictions in the past: adventure, pacman, rogue, hack. Yes, I've been there, and in several other autotelic hells as well: elisp, C++, interrupt handler bugs, and more recently I've been developing a WWW browsing problem. It started in childhood with a Revell model of a "car of the future" (lime-green with huge tailfins and clear bubbles over the occupants in their bucket seats) and continued with more plastic cars, battleships, airplanes, then those chests of little steel girders, then calligraphy, ..., OK, OK, I'm autotelic, I'm a woman, and I'm going to tell my Tetris tale.

First, let me establish my credentials as a Tetris hard-core. I found it while on vacation in Maui. I dragged my family in our Aloha clothing to a video games den every evening after we cleaned up from a day on the beach. The clientele was young, local, kind of tough. Ordinarily I'd feel uncomfortable spending 5 minutes in such a place. But with a stack of quarters and a Tetris machine, I was transported. The locals would sit behind me sneering and asking if they could "PLEASE" use the machines. At first, I'd let them.

But things changed when we got back home to Los Angeles. I found a video parlor in Marina Del Rey with Tetris. The clientele was even more disturbing, but again, the game presented a world of its own. One afternoon, a woman with two small children attempted to take the machine away from me. While I was concentrating on the play, she informed me that her kids wanted to use the machine. Without looking up, I told her that I'd only yield if it was management policy to impose a time limit. After a moment of shock she began screaming insults at me and dragged the children away. Though I didn't ever look up to see what kind of person she was, it did pretty much ruin my timing for that level. I got busy with various home and work projects shortly after that, and I haven't played much since.

For a while I tried using xtetris on my workstation, but it wasn't the same. And I've never actually used a GameBoy, because it's hard to get the little kids to share them, and even if they do they won't let you play for more than a few minutes before they start whining. So I'm going to talk only about my experiences with the big machines in the video arcades.

So what is it exactly that draws women to Tetris? I think it's refrigerators. At first I thought it was cabinets, but I've been over this in my mind a lot, and I'm convinced that refrigerators are the key. The sociologist who mentioned women's "craving for order" seemed way off base, she'd obviously never been within a mile of a teenage girl's room, but still, that's the key to it. Women spend a lot of time trying to get things into refrigerators. The point is, they don't have a natural sense of order, but they've got to get the damn stuff into the fridge so it doesn't fall out, and that requires ingenuity. Cabinets are similar, but they use different reasoning skills than refrigerators. For example, it's OK to push something to the back of a cabinet and lose it for a year. And things that go into cabinets nest --- you've got to be careful with those graduated bowls if they're from different sets, because if you put one inside the other you'll need a screwdriver and pliers to get it out.

Now refrigerators and Tetris are much the same thing. The Tetris shapes are like Tupperware boxes and milk cartons and packages of cheese. But unlike real household items, they remain sparkling and attractive no matter how long you leave them there. And if you pack them very carefully along the bottom, instead of rotting and giving off foul odors, they are conveniently whisked away, while more continue falling. This is sort of like having your husband help unload the groceries --- there you are trying to get the vegetables packed carefully into the bottom bins, and there he is stuffing soft drink cans into the dairy products section.

As you move through the various difficulty levels of Tetris, it's even more like a refrigerator --- you don't get to start with a clean space, but instead have what looks like piles of debris from unknown previous users. Women know that these unseen entities are teenagers and you've got to be very resourceful and controlled to work around them.

But what's the payoff in this contest? Well, mainly it's being able to exercise a skill that women already have, but with lots more positive feedback than real life. And for me, the video arcade games have two really important features. One is a cute little Slavic dance tune that plays in the background and helps with the timing. But the real clincher is that as you get proceed through the difficulty levels, there's entertainment. Little Russian men come out onto the screen and dance in that style where they fold their arms and bend their knees and kick straight out. Yes, that's the real thing about Tetris for some of us older ladies, it's the dancing men. In all my years of cleaning out the refrigerator, I've never had a man dance a jig for me. Well, that's why I play Tetris; I'm not sure about anyone else.

---

## Re: Campaigns and Elections (Agre, [RISKS-16.12](#))

*"Robert J. Burkhart" <0006344755@mcimail.com>*

*Sun, 12 Jun 94 23:04 EST*

... just find out what everybody's hot issues are and make them all whatever promises you need to make, ...

And so (once again) fact follows fiction ...

Eugene Burdick (Co-Author of THE UGLY AMERICAN) wrote this script in his futurist novel THE 480. I thought this was also the same computer-assisted campaign process used for the last presidential campaign!

Bob Burkhart at Twin Cities ACM Senior Consultant - The Security Board

---

### Re: Apathy toward computer errors (Seymour, [RISKS-16.13](#))

"Tom Yurkiw (Tommy the Yurk)" <tnyurkiw@undergrad.math.uwaterloo.ca>  
Sat, 11 Jun 1994 17:57:23 -0400

>"I'm not going to send it in. They make too many mistakes, and I'm not going  
>to rectify their mistakes,' he said. 'I can't see why people have to keep  
>paying for their mistakes all the time.'" He says this is the "last straw."

The RISKS? If people place unreasonable trust and expectations on the accuracy of computer information, they are bound to be disappointed.

Also, people quickly forget the advantages of using a particular system, and zero in on the drawbacks. Does this guy really want to stand in line for 8 hours or so, like they do in non-computerized elections?

Finally, this illustrates the RISK of working for government institutions - people are far more aggressive in dealing with government agencies -- they speak in terms of `rights', they make demands rather than requests. The relationship is different from the company-customer framework - even the most obnoxious individuals must be humoured.

---

### Security? Maybe....

Neill Clift <neill@macro.demon.co.uk>  
Sun, 12 Jun 1994 08:47:13 BST

I posted this to comp.os.vms and somebody suggested it would be of interest to risks readers. I am a risks reader but it didn't cross my mind until I was told.

X-NEWS: macro.demon.co.uk comp.os.vms: 22614  
Path: macro.demon.co.uk!neill  
From: neill@macro.demon.co.uk (Neill Clift)  
Newsgroups: comp.os.vms  
Subject: Security? Maybe...  
Message-ID: <1994Jun11.221520.201@macro.demon.co.uk>  
Date: 11 Jun 94 22:15:20 BST  
Organization: None  
Lines: 38

One of our customers employees asked me to have a quick look at two security packages for VMS that he was evaluating. The purpose of my quick look was to

determine if there were any obvious holes that these packages introduced or if their auditing features were easily evaded. I spent less than a couple of hours on each one (I wasn't getting paid just having a laugh :-)).

#### Package 1

This s/w had a facility for performing checksums on various files to enable detection of tampering. I asked their representative what algorithm they used for their checksum. All he would say was that it was proprietary. You would expect 'proprietary' to mean that there was at least some thought behind it. I found the algorithm to consist of summing the file as a contiguous set of longwords and a recording of the modification date. Files could easily be fixed up after modification! Why didn't they implement one of the many checksums something like tripwire supports?

This s/w trapped AUDIT\_SERVER messages via a mailbox. The protection on the mailbox allowed read and write access to the world so that data could be read out before the auditing s/w could get at it with a simple copy command. Fake audits could also be introduced. This s/w had mechanisms for DCL command procedures to take actions based on the audits passing parameters extracted from the alarm data (evil grin).

#### Package 2

On looking what this s/w installed I spotted a privileged image that looked a good target. Within 20 mins I had decided that I could probably use it to obtain all privileges as an unprivileged user. After an hour or two of programming I had done just that. In the end I exploited what I thought was the quickest bug to use but this bit of code appeared to be teeming with problems.

Both of these packages looked very flash and professional from the outside.

Sad but true.

Neill.

Neill Clift neill@macro.demon.co.uk

---

### Re: Call Your OPERATER ([RISKS-16.09](#))

*Hardwire <0003436453@mcimail.com>*

*Mon, 30 May 94 18:57 EST*

I remember reading about this in NETWORK WORLD. It's kind of funny: MCI already owned 1800 OPERATER long before AT&T released 1800 OPERATOR (Which was 5 months after MCI released 1800 COLLECT). MCI was using the OPERATER number internally for something, but not collect calls. They noticed after AT&T released their collect call product: 800 OPERATOR they were getting a lot of calls from people who misdialed. MCI was directing them to the correct number or 800 COLLECT. Due to the large number of calls MCI finally decided to send 800 OPERATER to the 800 COLLECT system. According the NETWORK WORLD article, MCI was making about \$200K a month thanks to people with the 'Quayle' syndrome.

---

## Re: Risks of too-simple responses (Lodge, [RISKS-16.12](#))

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

Thu, 9 Jun 1994 17:51:46 +0100

> ... All French credit cards are smart cards, and have been in mass use  
> for several years now. The French don't seem to be having any problems  
> with fragility or expense.

This is not quite so. One of the standard ways of defrauding the French smartcard system is to destroy the chip, whether by stamping on it or by an overvoltage. This causes the terminal to revert to standin mode, which is quite vulnerable. Fraud was reduced slightly by the introduction of smartcards - in France it is about 0.08%, against 0.2% for MasterCard and 0.1% for VISA - bit it has by no means been eliminated (source: 'Cards International' 22 July 1993).

Quite apart from fraud, the French card failure rate of 3% was the reason why smartcards were not introduced in Belgium (source: 'Cards International' 27th October 1993).

Also, there was a furore recently when French banks announced that all merchants would have to move over to electronic terminals. This would have cost over half a million small family businesses perhaps Ffr20,000 each, and the main beneficiary would have been Bull - a struggling state-owned company which was losing billions and being supported by the French government (which seems to have been behind the move on terminals).

The risk? There are several - in not understanding the trade-off between security and reliability, and in letting governments set security standards before the technology is properly mature.

Ross Anderson <rja14@cl.cam.ac.uk> Cambridge University Computer Lab



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 16: Issue 15**

**Weds 15 June 1994**

## Contents

- [Privacy: Your Secrets For Sale](#)  
[Les Earnest](#)
- [Life imitates Bart Simpson](#)  
[Jeffrey S. Sorensen](#)
- ["Computer Ethics" by Deborah Johnson](#)  
[Rob Slade](#)
- [Re: More Chunnel vision](#)  
[Philip H. Smith III](#)
- [Re: Airbus](#)  
[Mary Shafer](#)  
[Robert Dorsett](#)  
[Phil Overy](#)  
[Wesley Kaplow](#)
- [Re: Risks of speed enforcement](#)  
[Jonathan Clark](#)  
[Clive D.W. Feather](#)
- [Re: RISKS in UK Election Voting Process](#)  
[Doug Tooley](#)  
[Kent J Quirk](#)  
[John C Sager](#)  
[Sean Matthews](#)  
[Peter Robinson](#)  
[John Gray](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Privacy: Your Secrets For Sale

*Les Earnest* <[les@sail.stanford.edu](mailto:les@sail.stanford.edu)>  
Sun, 12 Jun 94 17:39:31 -0700

ABC's Nightline programs on June 9 & 10 focussed on invasions of privacy that are facilitated by computers and other electronic media. The program mainly covered things that we are familiar with but performed a valuable service, I believe, by bringing some important privacy issues to the attention of the

general public in a fairly clear and direct way.

The program began with Ted Koppel presenting results of a public opinion poll on two questions:

Is the sale of records to mail order companies an invasion of privacy?

YES - 73% NO - 27%

Are you concerned about threats to your privacy?

YES - 85% NO - 15%

Koppel went on to assert that the amount of personal information that is available online is currently quadrupling each year. An interview followed with an information broker named Al Schweitzer, who they mentioned is currently on probation for bribery in connection with information gathering. They gave him names and social security numbers of a couple of people and he showed that in less than 24 hours he could get a great deal of information about them from legal sources, including their residential addresses going back a number of years, the amounts of all outstanding loans and credit card debts and terms of a divorce settlement.

Schweitzer could not resist mentioning that he could get additional information, including detailed phone bills and lists of credit card purchases through illicit but readily accessible channels and could get the person's income through another such channel at a cost of \$50. He showed a list of kinds of information, both legal and illegal, that are available and the schedule of fees for these services.

There was a discussion of the fact that state and local governments sell a great deal of information to direct marketers, including voter registration, property owners lists, court records, and (in many states) motor vehicle and drivers license registrations. These agencies derive a great deal of income from selling this information, which has assisted direct marketers to keep track of 80 million Americans. Thus they have a mutually beneficial relationship, arguably at the expense of the public.

It was mentioned that Barbara Boxer's bill, which has passed the U.S. Senate, would restrict dissemination of information by all state departments of motor vehicles.

They interviewed a "reformed hacker" named Ian Murphy who is now a security consultant. Murphy pointed out that all calls to 800 or 900 numbers make the caller's phone number available and that with a computer and an available database this can be mapped into the subscriber's name and address. He also discussed how it was possible to intercept a telephone conversation from a specific cellular phone. He noted that this is illegal but that it is almost impossible to catch anyone who does it. He concluded that "Laws can't keep up with technology."

In a discussion of the Clipper Chip there was a short interview with John Perry Barlow in which he remarked that with it "The government can sit in your living room and hear everything you say."

A woman from Houston, Texas, named Carol Gibbs told her horror story about

having her credit usurped by another person and the fact that it has taken her two years to get her life back together.

It was pointed out that even though it is now illegal to sell video rental records, it is perfectly legal to sell personal medical records!

The second program concluded with a discussion between Koppel, Schweitzer, Sally Katzen of the "Clinton Privacy Group" and Representative Ed Markey, who discussed his proposed "Privacy Bill of Rights." Markey said that this bill would impose two requirements:

- (1) That individuals must be given knowledge that information is being gathered about them electronically;
- (2) Individuals must be given notice when information that has been gathered is proposed to for a use other than the one for which it was gathered.

Katzen mentioned that it has been over 20 years since the Code of Fair Information Practices was developed and that technology has changed substantially: in 1973-74 most records were paper-based but computer-based records now dominate. She asserted that the law has to catch up.

In parting it was mentioned that a representative of one of the "big three" credit information houses had originally agreed to participate in the discussion but decided not to come after learning who else would be there.

-Les Earnest

---

## Life imitates Bart Simpson

*"Jeffrey S. Sorensen" <sorenj@rpi.edu>*

*Mon, 13 Jun 1994 23:14:34 -0400*

This is a Risk only fans of The Simpsons will appreciate:  
(Paraphrased from New Haven Register Sunday, June 12, 1994 [With my comments!])

Northeast Utilities reported that it had failed to follow proper safety procedures on 2 occasions in April at its Millstone 2 plant in Waterford.

On April 23, an indicator showed that some of the control rods were stuck. The crew concluded that the problem must have been with the indicator and left for the day. When the new crew arrived, they discovered the rods were indeed stuck but failed to shutdown the reactor as quickly as they should have and underclassified the seriousness of the event.

[See stdrisks.h sections on incredulous operators ignoring unexpected warnings. Also see section on It's Not MY Problem/It's Miller Time (After a HOT day at work, everyone's \_dying\_ to get home)]

After the incident, some of the plant's operators failed a Northeast Utilities test on reactor theory and were removed from duty for training.

The utility's report blamed the problem in part on the operators' failure to understand reactor theory and a failure of plant management to "fully appreciate the implications" of the safety-related event and to provide sufficient oversight.

[sound clip of Homer: Dough!]

[sound clip of Mr. Burns: Excellent...]

The other incident involved a coolant leak from the plant's reactor. In this case, the operators again underclassified the seriousness of the event. Notification of federal authorities was delayed by 16 hours.

[Guess they were just letting off a little steam after failing their tests...]

[sound clip of Bart: Aye Carumba!]

Jeffrey Sorensen [sorenjs@pb.com](mailto:sorenjs@pb.com)

---

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">  
Tue, 14 Jun 1994 11:55:07 -0600 (MDT)

Subject: "Computer Ethics" by Deborah Johnson

BKCOMPETH.RVW 940322

Prentice Hall  
113 Sylvan Avenue  
Englewood Cliffs, NJ 07632  
(515) 284-6751  
FAX (515) 284-2607  
[phyllis@prenhall.com](mailto:phyllis@prenhall.com)  
70621.2737@CompuServe.COM Alan Apt  
Beth Mullen-Hespe [beth\\_hespe@prenhall.com](mailto:beth_hespe@prenhall.com)  
"Computer Ethics", Johnson, 1994, 0-13-290339-3

Unlike the famous quote about life in the state of nature being nasty, dull, brutish and short, Johnson's examination of the state of ethics in computing is readable, interesting, discerning--and short.

Unlike the usual treatment of ethics as proof by exhaustion, Johnson does a complete and reasonable job. Without recourse to mounds of collected work (of dubious merit), the major points of professionalism, property rights, privacy, crime, and responsibility are addressed. Even in this brief space, ethics are studied more rigorously than in more weighty tomes. Not content with the usual reliance on relativism and utilitarianism, Johnson points out the flaws in each.

"Complete" is, I suppose, an overstatement. Although it is difficult to imagine a scenario that the book does not touch upon at some point, ultimately this book is a good primer and discussion starter. Although possibly the definitive work in the field to date, it does not, in the final analysis, get

us much closer to a computer ethic.

Recommended. Should be required reading for all computer science students.  
Exposure wouldn't hurt any number of professionals and executives, either.

copyright Robert M. Slade, 1994 BKCMPETH.RVW 940322

=====

DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733  
BCVAXLUG ConVAXtion, Vancouver, BC, Oct. 13 & 14, 1994 contact vernc@decus.ca

---

## More Chunnel vision

703) 506-0500 <PHILS@RELAY.RELAY.COM (Philip H. Smith III),>  
Tue, 14 Jun 94 06:46:18 EDT

I had always hoped the Chunnel would allow auto traffic, with HOV restrictions, thus enabling the dreaded "Carpool Tunnel Syndrome".

...phsiii

---

## Airbus A3(0?)0 deductions (Overy, [RISKS-16.14](#))

Mary Shafer <shafer@ferhino.dfrf.nasa.gov>  
Tue, 14 Jun 94 07:51:24 PDT

Phil> 1) Boeing sell similar automation to the A320 - they also caused  
Phil> the second- worst Japanese crash and in this case much more  
Phil> directly (the fuselage broke).

Not true--Boeing does not have any fly-by-wire aircraft in operational status.  
They have flown precisely ONE fly-by-wire aircraft, the prototype 777. And it made its first flight last week.

Phil> 2) whether you se sidestick or yoke, a modern airliner has no  
Phil> direct "cables" to the rudders - it relies on multiple links  
Phil> either electrical or hydraulic which would work equally well  
Phil> with sidesticks. A300s have been around for 20 years - this was an A320.

Not entirely true, as the Douglas DC-11 and DC-12 have cables that run from the pilot controls (yoke and rudder) all the way back to the wing and tail, for ailerons or elevators and rudders respectively. The control surfaces are hydraulically actuated, it's true, but most of the control run is cables. I think that the 747 also has similar cables.

Phil> 5) Since several A320s have crashed when silly things have been  
Phil> happening, perhaps the automation, like the "watertight" hull of  
Phil> the Titanic, is creating a too-complacent pilot. As a  
Phil> far-too-complacent pilot myself in the past, I can understand this.

Well, no doubt, but wasn't this accident a 300, not a 320? The 300 has a conventional FCS, not fly-by-wire. Just because they both start with 3's doesn't make them the same aircraft. That's like saying that an A-10 and a KC-10 are identical because they both have 10 in the designator.

Mary Shafer SR-71 Chief Engineer      NASA Dryden Flight Research Center,  
Edwards, CA   shafer@ferhino.drf.nasa.gov

---

**Re: How to feel safer in an Airbus Ladkin, [RISKS-16.14](#)**

*Robert Dorsett <rd@netcom.com>*

*Mon, 13 Jun 1994 19:41:40 -0700*

>His speculation on the A320, that Airbus were forced to use modes  
>because they chose a sidestick design, is incorrect. Fly-by-wire  
>aircraft use modes because they have to.

This is not true. Early FBW aircraft were essentially open-loop analog systems. They were reactive, very simple, providing very simple feedback and control loops. They were not anywhere near as modal as modern systems. Keep in mind that Airbus' position is that fly-by-wire systems have to provide a supermarket of user features. In reality, the primary operational benefit is to be simplicity and weight savings. What a manufacturer does from that point onwards is totally arbitrary and subject to market forces.

The Airbus design has long struck me as a being in support of an interface which, in turn, was probably the result of a marketing decision. Certainly, the decision to use sidesticks--which provide no active feedback, and which are not interlinked--ran contrary to the preferences of many pilots. The lack of said characteristics has resulted in more modes (and the necessity of protections) and a variety of rather impressive kludges (such as the "take-over" arrows which point to the other pilot when he pushes his "take-over" button).

>From what I've read of the Boeing 777 design, it's much less modal than the Airbus design, providing unified and conventional flight characteristics from takeoff roll through landing roll.

>A further comment about the Nagoya accident is appropriate. Current  
>knowledge is that the pilots failed to follow normal, explicit  
>procedure for control of the aircraft,

Really? I've not seen that anywhere. "Explicit" suggests that the systems' characteristics were clear and well-understood. Such is not the case here. In fact, given that Airbus control philosophies tend to be rather subtle in their feedback and invocation procedures, I'd certainly not suggest that "pilot error" was a likely or trivial error in this case, at least not at this point.

>and secondly that they had both  
>been drinking alcohol, which is illegal for good reason.

This has also not been substantiated. The investigators will not comment, and it is not clear whether the presence of alcohol in the corpses was a result of ingestion or decomposition of tissues. In any event, the \*presence\* of alcohol is not illegal. The illegality is determined by the \*amount\* of alcohol present.

>senior management of China Airlines has resigned because of this accident.

Because of the fifth major accident in as many years, was the way I understood it.

And Phil Overy RAL <PJO@ib.rl.ac.uk> writes:

> re: Mark Terribile's posting:-

> 1) Boeing sell similar automation to the A320 - they also caused the second-  
> worst Japanese crash and in this case much more directly (the fuselage broke).  
I do not understand this paragraph. To the naive reader, it could appear that you're claiming a Boeing automation issue was responsible for the structural failure of an airplane. This is clearly false.

Nor was the JAL crash the simple result of structural failure: it was primarily the result of a faulty repair, which destroyed the tail, taking the airplane's hydraulic systems along with it.

Moreover, Boeing automation is significantly different from AI automation, from the ground up. The 777 flight control system (assuming you're referring to flight control systems) uses a different machine architecture and has a fundamentally different mission requirement, governed by the use of a different interface.

If you're referring to more conventional functions, such as cockpit automation and the navigation systems, again, Boeing philosophy is demonstrably different from Airbus philosophy. It's debatable whether either is "better," but to even a casual observer, they are sufficiently different to cause at least a few customers to scratch their heads when it comes to running fleets with airplanes from multiple vendors. In many cases, the differences are not trivial.

> 2) whether you use sidestick or yoke, a modern airliner has no direct  
> "cables" to the rudders - it relies on multiple links either electrical or  
> hydraulic which would work equally well with sidesticks.

In point of fact, the hydraulic actuators are controlled via cables. And in a few airplanes (727, DC-9 derivatives) the pilots still retain aircraft control via control tabs in the event of complete hydraulic failure.

> 4) as for mode-switching and elevators etc - the senior pilot seems to have  
> tried to recover without switching off the auto-pilot, the junior pilot seems  
> to have flown as if the auto-pilot wasn't on. Reports will not say this as  
> it's a conclusion, not a fact - it does however sound like the explanation.

And reports also claim a 15-year-old boy crashed an A310-600 when he nudged against the control column. Hmm. I wonder why two airline pilots couldn't figure THAT one out.

Robert Dorsett rdd@netcom.com

---

## **Correction of my post on "A-THREE-HUNDRED" crash at Nagoya**

*Phil Overy <PJO@ib.rl.ac.uk>*

*Wed, 15 Jun 94 08:38:51 BST*

After a mail from Peter Ladkin I am now sure of my ground and wish to write what I wanted to write in the first place - despite your correspondent (and a newspaper report I unfortunately used to check my memory, not my Independent or Peter Ladkin's Herald Tribune which got it right), the worst crash in Japan was AN A300 (ie an "old", un-computerised type NOT with sidesticks).

The Taiwanese plane did not crash after any kind of automation or airframe failure, but when the auto-pilot was left on until too late. Peter Ladkin tells me that the president of the airline resigned after the crash, so it doesn't sound as if they are trying to transfer responsibility to the manufacturers.

The crash at Nagoya was not like Japan's second-worst disaster when a Super 747 (high-altitude model) crashed when the pressure bulkhead at the rear collapsed; on that occasion the makers were Boeing, however I leave accusations to lawyers -- there are plenty of these around and I may have flown on one (and lived :-). [lawyers?]

I could have phrased it better, but I would point out that Boeing also now use fly-by-wire (on the brand new 777), so the earlier correspondent was misguided in thinking that Boeing were staying away from fly-by-wire. The 777 is also a much bigger plane than the A320...

Phil Overy

---

## **Does it matter why A3??'s have a poor record?**

*Wesley Kaplow <kaploww@cs.rpi.edu>*

*Tue, 14 Jun 1994 09:51:48 -0400*

The average persons response to all of the A3?? technical discussion would probably be that it frankly it does not matter why these planes crash!. To me, if we play only on the statistics, I want a airplane with a good safety record. Already, Airbus Industry has lost more planes per delivered plane than other major aircraft manufacturer in the past 3 decades (Lockheed, Boeing, MD). To the average person, who for example reads in Consumer Reports that XYZ product can burst into flames after extended use, does not care why!. The same is true for airline equipment.

It is also reassuring to note that some committee decided (or individual) decided that an A320 does not think it has landed until the wheels spin up to something like 90 kts. How reassuring to think that all of the possible consequences of this decision have been carefully thought

out and that a full fault-effect analysis has been performed.

Wesley K. Kaplow, AT&T Bell Laboratories, Rensselaer Polytechnic Institute  
kaplow@att.com kaploww@cs.rpi.edu

---

**Re: risks of speed enforcement (Cunningham, [RISKS-16.14](#))**

*Jonathan Clark <jhc@hostel.lincroftnj.ncr.com>*

*Tue, 14 Jun 94 12:13 EDT*

Andy Cunningham mentions some possible risks of over-zealous speed enforcement, with (presumably) a radar gun linked to a video camera and some automatic licence-plate recognition software.

Such a system was until last year under test in New Jersey. A law was then passed banning it after it was found that there was no way to let people off after they had been ticketed, so that politicians, off-duty police officers and other members of the nomenklatura would then have to conform to the same rules of the road as the rest of the populace. I guess the risk here is that of trying to apply rules to people they obviously weren't meant for! Designers take note - you always have to leave *\*some\** way to circumvent the system :-)

I should note that in the U.S. speeding tickets are frequently (many would say primarily) used to generate revenue, rather than for any considerations of safety or traffic management.

On the other hand, I understand that photo-radar systems work in the infra-red. This is preferable to an experience I had some years ago while driving late at night at high speed on an autoroute in Belgium - I drove under a bridge and was dazzled by a *\*powerful\** flash going off behind me. Now there's an unexpected risk of driving too fast...

Jonathan

---

**RISKS of real-time image processing (Cunningham, [RISKS-16.14](#))**

*"Clive D.W. Feather" <clive@sco.com>*

*Tue, 14 Jun 1994 11:10:07 +0100 (BST)*

> ...actually send out tickets (camera/radar systems which produce photographic

I don't think this is a likely problem. The current camera/radar systems don't work like that. The radar is used to detect likely speeders, and then the camera takes two pictures a known time apart; the position of the car in each is used to determine whether the car was speeding.

Clive D.W. Feather, Santa Cruz Operation, Croxley Centre, Hatters Lane, Watford  
WD1 8YN, United Kingdom clive@sco.com Phone: +44 923 816 344

---

## Re: RISKS in UK Election Voting Process

Doug Tooley <djtooley@undergrad.math.uwaterloo.ca>

Tue, 14 Jun 1994 12:44:41 -0400

The UK is not alone in their lack of voting security.

In Canada, as "proof of identification" all we had to do to identify ourselves at the registration station was to bring an envelope mailed to our address (with our name on it) with a second piece of identification.

Sounds straightforward... The people are nice and accommodating too: A roommate of mine couldn't make it to the registration, so we were able to register for him *\*very\** easily.

Given the (lack of) care being put into actually checking the identification (to test this, I deliberately didn't show them the address on my envelope, I merely waved it at him, and that was sufficient) literally anyone could have registered to vote.

The registration process was optimized for speed (we had to wait 30-40 mins) and for friendliness, (they were very willing to accept my word at face value) but no REAL effort was made to authenticate the participants.

Doug Tooley 4C Co-Op CS/C&O student at U of Waterloo, Ontario, Canada  
djtooley@undergrad.math.uwaterloo.ca

---

## Re: Voting Systems - UK, US

Kent J Quirk <kentq@world.std.com>

Tue, 14 Jun 1994 03:22:40 GMT

In the two towns I've lived in here in Massachusetts, they have a similar voting system to that mentioned in England, except that no voter card is required. They ask for a street address and a house number, but anyone who can read upside down could simply pick a name out of a hat.

The risks to the would-be fraudulent voter is that even in our relatively large town of 25,000 people there is a decent chance that the person behind the counter knows the person you are naming, or that the person will later attempt to vote and uncover the fraud (not that there's much that could be done about it at that point).

The news media, in covering questionable elections around the world, often speak of "massive election fraud". It seems to me that since massive fraud is really the only kind that has any predictable benefit, spoofing the blue-haired volunteers behind the desk is not really all that much of a worry.

[Similar comment regarding Mass. from Andrew\_Marc\_Greene@frankston.com .]

---

**Re: RISKS in UK Election Voting Process (Rushton, [RISKS-16.14](#))**

John C Sager <jcs@zoo.bt.co.uk>

Tue, 14 Jun 94 09:17:49 BST

This is not uncommon - I did exactly the same thing. Admittedly there is a RISK, but you also have to consider cultural factors. Accusations of ballot-rigging in UK elections are rare. If someone picked an address at random and voted as a resident there, as suggested, then there would be major investigations & lots of publicity when the real voter turned up with a valid poll card. Yet this does not happen. There is no culture of ballot-rigging in the UK (except long ago in Northern Ireland, but that was done a different way).

John C Sager B67 G18, BT Labs, Martlesham Heath, IPSWICH IP5 7RE England  
jcs@zoo.bt.co.uk +44 473 642623

---

**Re: RISKS in UK Election Voting Process**

Sean Matthews <sean@mpi-sb.mpg.de>

Tue, 14 Jun 94 10:32:18 +0200

> Question: Should the UK update its voting system?

Answer: No.

Actually, at least, in Northern Ireland, the election procedure has been tightened: because there is a real, as opposed to theoretical, problem with impersonation (vote early, vote often) they insist that you now have to have some form of ID with you (or at least did, I haven't voted there for some years, but I don't imagine that it has changed). Traditionally, polling stations in Britain have someone local who is familiar with the people of the area, a doctor or vicar or something, around as an informal check for impersonation (this would probably work better in rural, than urban areas though).

I don't think there is much of a problem really, with the UK procedure. If they need to be careful (like in NI) they can make things much better, just by always asking for ID, or to see the registration card. But since they don't actually need to at the moment, why bother. After all, a problem with voter impersonation would be obvious if it happened on any sort of scale and if it does happen there are separate procedures for dealing with it.

There is the risk here of fixing something that is not obviously broken, by assuming a purely theoretical worst case.

Sean Matthews <sean@mpi-sb.mpg.de> Max-Planck-Institut fuer Informatik  
Im Stadtwald, D-66123 Saarbruecken, Germany +49 681 302 5363

[Further similar comments from Peter Robinson <Peter.Robinson@cl.cam.ac.uk>]

Date: Tue, 14 Jun 94 11:33:31 BST

From: grayjw <grayjw@helios.aston.ac.uk>

Subject: Re: Risks in UK Election Voting Process (Rushton, [RISKS 16-14](#))

Thomas Rushton is correct to identify this problem (of getting names from the electoral roll. There are two points to make.

1) You don't need ID to vote in the UK. Instead you must satisfactorily answer two "statutory questions" having given the name and address:

- a) Are you XY, resident at (address) (yes)
- b) Have you already voted in this election (no)

2) The problem is worst in the case where the "real" turnout is low, because it would be possible, in disguise, to vote several times under different names. However, in a high turnout election, it's more likely that the person whose ID you have used will turn up to vote. They are *\*not\** denied a vote.

If you turn up at the polling station, and give your name, and it's already marked on the register, then you will be asked the questions, and given a different colour of ballot paper, which you complete in the same way. If the final result is close enough for these papers to matter, then the election may have to be resolved in court.

I agree that for low-turnout elections there is a problem with the system. This strikes me as a common risk in any democratic system: if you don't use your influence, someone else will.

John Gray



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 16: Issue 16**

**Weds 15 June 1994**

## Contents

- [Congressman Jack Brooks' Statement on Crypto](#)  
[David Banisar](#)
- [WSJ article: RFI hoses medical equipment](#)  
[Robert Allen](#)
- [Summary of safety-critical computers in transport aircraft](#)  
[Peter Ladkin](#)
- [More on Airbuses](#)  
[Robert Dorsett](#)  
[Peter Ladkin](#)  
[Wesley Kaplow](#)  
[Pete Mellor](#)  
[Kaplow again](#)  
[Bob Niland](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Congressman Jack Brooks' Statement on Crypto

David Banisar <[Banisar@epic.org](mailto:Banisar@epic.org)>

Tue, 14 Jun 1994 14:20:25 -0400

The following statement by Rep. Jack Brooks (D-TX) was today entered in the Congressional Record and transmitted to the House Intelligence Committee. Rep. Brooks is Chairman of the House Judiciary Committee and played a key role in the passage of the Computer Security Act of 1987 when he served as Chairman of the House Government Operations Committee.

David Sobel <[sobel@epic.org](mailto:sobel@epic.org)>

Legal Counsel

Electronic Privacy Information Center

=====

ENCRYPTION POLICY ENDANGERS U.S.

## COMPETITIVENESS IN GLOBAL MARKETPLACE

For some time now, a debate has been raging in the media and in the halls of Congress over the Administration's intention to require U.S. corporations to use and market the Clipper Chip, an encryption device developed in secret by the National Security Agency.

The Clipper Chip will provide industry and others with the ability to encode telephone and computer communications. The use of the Clipper Chip as the U.S. encryption standard is a concept promoted by both the intelligence and law enforcement communities because it is designed with a back door to make it relatively easy for these agencies to listen in on these communications.

The law enforcement and intelligence communities have a legitimate concern that advances in technology will make their jobs more difficult. But the issue here is whether attempts to restrict the development, use and export of encryption amounts to closing the barn door after the horse has already escaped.

The notion that we can limit encryption is just plain fanciful. Encryption technology is available worldwide -- and will become more available as time goes on.

First, generally available software with encryption capabilities is sold within the U.S. at thousands of retail outlets, by mail, even, over the phone. These programs may be transferred abroad in minutes by anyone using a public telephone line and a computer modem.

Second, it is estimated that over 200 products from some 22 countries -- including Great Britain, France, Germany, Russia, Japan, India, and South Africa -- use some form of the encryption that the Government currently prohibits U.S. companies from exporting. According to the May 16, 1994 issue of *Fortune*, not only are U.S. companies willing to purchase foreign encryption devices, American producers of encrypted software are also moving production overseas to escape the current export controls.

Third, encryption techniques and technology are well understood throughout the world. Encryption is routinely taught in computer science programs. Text books explain the underlying encryption technology. International organizations have published protocols for implementing high level encryption. Actual implementations of encryption -- programs ready to use by even computer novices -- are on the Internet.

The only result of continued U.S. export controls is

to threaten the continued preeminence of America's computer software and hardware companies in world markets. These restrictive policies jeopardize the health of American companies, and the jobs and revenues they generate.

I support, therefore, the immediate revision of current export controls over encryption devices to comport with the reality of worldwide encryption availability.

I believe law enforcement and the intelligence community would be better served by finding real, and targeted ways to deal with international terrorists and criminals rather than promoting scattershot policies, which restrict American industries' ability to design, produce and market technology.

Now -- more than ever -- we cannot afford to harm our economic competitiveness and justify it in the name of national security.

---

### **WSJ article: RFI hoses medical equipment**

*Robert Allen <Robert.Allen@eng.sun.com>*

*Wed, 15 Jun 1994 11:37:44 -0700*

The 15 Jun 1994 Wall St. Journal has an interesting front-page article about how RFI generated by radios & cellphones is screwing up operation of sensitive medical equipment such as heart defibrillators, diagnostic equipment, and even electric wheelchairs.

Some of the horror stories sound apocryphal, like the electric wheelchair "zapped by radio waves" that sent its passenger over a cliff. Others sound entirely possible: a 72 year old man died in an ambulance when the heart defib. device he was on failed due to RFI from the ambulance two-way radio. The ambulance mfr. had replaced the steel roof with a fiberglass dome, and put the antenna on top (duhhhhh). The best story however was about some poor sap who had a pacemaker installed after diagnostic equipment indicated he needed one. It was later discovered the diagnosis was in error, and was caused by RFI from a television in the same room. Runners up for best story were from the mother who's use of a cellphone in the car affected the ventilator her child was using in the back seat. In a hospital ward a whole bunch of ventilators alarmed when the handyman keyed his transceiver.

As is demonstrated by the TV case, even having technicians install and test new equipment can't account for the fact that just moving the stuff around during a spring cleaning might put two pieces in juxtaposition to cause problems.

Having recently seen more than my share of medical equipment, I'm solely unimpressed with the ruggedness of it (it sort of reminds me of ICOM radios). Still, with more and more people using cellphones I figure we'll have more and more problems. I wonder if cellphones will be the health hazard in the '90's that radium watch dials were in the '40's?

Robert

---

## Summary of safety-critical computers in transport aircraft

*Peter Ladkin <Peter.Ladkin@loria.fr>*

*Wed, 15 Jun 1994 22:13:19 +0200*

Given the interest in RISKS on computers in aviation, and some confusion concerning characteristics of Airbus aircraft, I thought it might be useful to summarise for RISKS readers some of the current state of things.

I believe there have been three major accidents involving Airbus aircraft in the last year: an A320 ran off the end of the runway in Warsaw in September 1993, killing two people and injuring many; the crew of an Aeroflot Airbus A310 lost control during cruise flight, which led to the death of everyone on board; and a China Airlines A300 crashed recently tail-first (!) on landing at Nagoya, killing all or almost all on board.

The A300 and A310 aircraft have 'conventional' control, that is, physical control of the aircraft is transmitted by mechanical or hydraulic means to most of the flight control surfaces. The normal flight control of the Airbus A320, A321, A330 and A340 aircraft, in contrast, is achieved by computer, to which the pilots' sidestick movements are one set of inputs. This is colloquially known as 'fly-by-wire'. 'Fly-by-wire' aircraft have been in regular use by the military for over 20 years, but the A320 is the first commercial 'fly-by-wire' transport, introduced in the early 90's. Pilots have extremely limited direct physical control of A320/21/30/40 aircraft should the flight control computers be unavailable, a situation which is anticipated not to occur during the lifetime of the fleet.

The first flight of the Boeing 777 took place on Sunday 12 June, 1994. The B777 is Boeing's first 'fly-by-wire' commercial transport, which it is hoped will be 'certificated' in April 95 with delivery to its first customer, United Airlines, in May 95.

The B777 is a significantly different design from the A320, and I would be very surprised if there were to be any accidents attributable to features common to A320/21/30/40 and B777 aircraft which are not also common features of conventional aircraft such as the B737.

Airbus claims its design philosophy is 'evolutionary', that is, the systems are not designed from scratch, but introduced gradually into the company's designs after success in previous designs. Nevertheless, there are steps, such as that to 'fly-by-wire' in the A320, which RISKS readers may consider more significant than others. See the article by J.P. Potocki de Montalk, Head of Airbus Cockpit/Avionic Engineering at Airbus, in *Microprocessors and Microsystems* 17(1).

A useful and readable reference for those interested in A320 accidents is RISKS contributor Peter Mellor's long paper 'CAD: Computer-Aided Disaster!' which contains a description of the design of the A320 Electrical Flight

Control System, and detailed commentary on all A320 accidents to date, and is to my knowledge the only single source to do so. A version of this paper is to appear in High Integrity Systems journal.

Apart from the flight control on A320/321/330/440s and B777s, there are potentially RISKy computer-based systems on almost all modern transport aircraft, of which maybe the most important are the autopilot/Flight-Director and the FADEC (Full-Authority Digital Engine Control). All commercial aircraft have autopilots of various degrees of sophistication (and most have Flight Directors, which provide passive guidance rather than active control), and these may be suspect in certain incidents (e.g. the Collins autopilots on B757 and B767 aircraft: see PGN in [RISKS-15.08](#), and my posting in [RISKS-15.13](#)). Many modern aircraft also have FADEC, which has occasionally come under investigation, but I can't think of occasions so far on which they have been considered primary cause of accidents or incidents.

Human factors are very important. A taskforce has recently been convened to study incidents of 'controlled flight into terrain', in which the continued safe flight of the aircraft is impeded by a cloud with a crunchy center (see The Economist, June 4-10 1994, p92). In these accidents the physical performance of the airplane is generally not a factor, but they may nevertheless be computer-related, since guidance and air traffic control relies on computers to various degrees.

Aircraft accidents are amongst the most well-studied of failures in any engineering discipline. I have never held any position in the aviation industry, but some of my research interests and hobbies bring me there. My continuing experience is that it pays to try to take as much care in forming opinions about them as it does to report them accurately in the first place. I wish I could be better at both.

Peter Ladkin

---

**Re: Overy, [RISKS-16.15](#)**

*Robert Dorsett <rd@netcom.com>  
Wed, 15 Jun 1994 13:56:56 -0700*

From: Phil Overy <PJO@ib.rl.ac.uk> wrote:

Subject: Correction of my post on "A-THREE-HUNDRED" crash at Nagoya  
>

> The Taiwanese plane did not crash after any kind of automation or airframe  
> failure, but when the auto-pilot was left on until too late.

This is not clear. There are normally three or four ways to disengage any autopilot:

- a switch on the glareshield.
- a deactivate switch on the yoke
- pushing or pulling forcefully on the yoke
- a circuit breaker as a last resort

In this case, it appears the crew were aware of the problem for over TWO

MINUTES--an eternity--and fought the airplane to the ground. I refuse to see this trivially dismissed as "operator error" or "they didn't turn off the autopilot until it was too late."

This is a horrifying situation, and if there is a mechanical or interface or modal failure lurking beneath the scenes, it needs to be rectified. AND UNDERSTOOD: if it's even as simple as a service or maintenance issue, then the problem could recur on other airplanes.

> Peter Ladkin tells me that the president of the airline resigned after the  
> crash, so it doesn't sound as if they are trying to transfer responsibility  
> to the manufacturers.

Again, after a long string of crashes. I believe the president or VP of JAL was ultimately compelled to resign after the 747 SR crash in Japan. This has nothing to do with culpability: it's accountability. A form of personal responsibility which seems to be quite absent in Western corporate culture. There is nothing more one can draw from it than that.

>I could have phrased it better, but I would point out that Boeing also now use  
>fly-by-wire (on the brand new 777), so the earlier correspondent was misguided  
>in thinking that Boeing were staying away from fly-by-wire. The 777 is also a  
>much bigger plane than the A320...

Airbus has continued evolving its aircraft line. There are now the A330 and A340, heavy long-range transports. Same interface.

And

> From: Wesley Kaplow <kaploww@cs.rpi.edu> writes:

> Subject: Does it matter why A3??'s have a poor record?  
> The average persons response to all of the A3?? technical discussion would  
> probably be that it frankly it does not matter why these planes crash!.

There are many people reading this newsgroup whose job descriptions include understanding and solving these problems so that future generations of aircraft do not cost lives or resources.

The reason that RISKS keeps harping on airplane automation is that it has broad ramifications to the computer industry in general, and safety-critical systems in particular. What gets established as "safe" in aviation will undoubtedly define standards of "safety" for other disciplines: this includes specification and development paradigms. So these crashes should be of interest to ALL computer professionals and computer scientists.

And there are certainly people out there whose job descriptions do include making managerial-level equipment decisions, who may not be aware or sensitized to some of these issues.

## Quarrelling over spilt airplanes [Dorsett, [RISKS-16.15](#)]

Peter Ladkin <Peter.Ladkin@loria.fr>

Wed, 15 Jun 1994 21:18:54 +0200

In [RISKS-16.15](#), Robert Dorsett disagrees with two quotes from my posting in [RISKS-16.14](#). I disagree with his disagreements:

> > Fly-by-wire aircraft use modes because they have to.

>

> This is not true. Early FBW aircraft were essentially open-loop analog

> systems.

I wasn't thinking about history when I made my assertion. There are many fly-by-wire aircraft types around \*nowadays\*, all but two of which are military, as of last Sunday. Do any of these aircraft \*not\* use modes? I can't think of one (but I would like to know of the exception that proves my rule). Robert's strong rejection may be as misleading as he thought my assertion was.

Robert holds the view that sidestick control may have been the result of non-engineering decisions. That may be true (or not), but I don't consider it relevant to whether sidestick control is well-engineered or not in a given aircraft.

> >A further comment about the Nagoya accident is appropriate. Current

> >knowledge is that the pilots failed to follow normal, explicit

> >procedure for control of the aircraft,

>

> Really? I've not seen that anywhere.

Flight International, 11-17 May 1994 p5, "a pilot pushes forward on the control column to counteract the autopilot nose-up input. \*This is against the published procedures ...\*" (my emphasis). FI and David Learmount are regarded as accurate on such matters.

> >and secondly that they had both

> >been drinking alcohol, which is illegal for good reason.

>

> This has also not been substantiated. The investigators will not comment,

Robert's assertions do not necessarily contradict mine. It may help to understand more of the context. The investigators will not comment officially, but then they're required not to - the official report on the Warsaw A320 accident is not out yet either, but that doesn't stop us knowing most of the factors involved there. Concerning the Nagoya A300 accident, there are normally-reliable aviation journal reports (sorry, the ref's buried) on the precise blood-alcohol level of the pilots which lead to my conclusion.

> >senior management of China Airlines has resigned because of this

> > accident.

>

> Because of the fifth major accident in as many years,

> was the way I understood it.

..which are two ways of reporting the facts associated with the same event.

Peter Ladkin

---

### **Not quite (re: Pete Mellor)**

*Wesley Kaplow <kaploww@cs.rpi.edu>*

*Wed, 15 Jun 1994 13:50:41 -0400*

Thanks to Peter Mellor it has come to my attention that my statement about loss of craft per craft delivered is not true. Unfortunately, I added that comment based on previous information about per-mile crash rates. The focus that I intended was that the average person does not really care why, only that they perceive that there is a potential safety problem. A good parallel might be the Audi 5000 series of reported "sudden-acceleration" problems. Although the Audi 5000 may not have had a larger incident rate of sudden acceleration than other cars, ultimately perception was the driving factor. People did not say: "oh that sudden acceleration problem, well that Audi 5000 was owned by someone from the '3rd' world, it must be his fault". Ultimately, the car had at least its name changed, and it probably cost Audi car sales. At least in the case of the Audi, I could choose not to buy the car. In the case of airline travel, and cannot make the choice between airframes because the information is not available. I may be making the choice based on poor information, but it is my poor decision to make.

Also, the airframe loss statistics can be somewhat misleading as well, as crashes in the information Peter sent to me does not say, for example, if the 747 statistics includes losses such as the Canary Island collision, or the Lockerbee terrorist loss.

Once again, I apologize of the incorrect statement.

Wesley Kaplow, AT&T Bell Laboratories & Rensselaer Polytechnic Institute

---

### **Re: Does it matter why A3??'s have a poor record?**

*Pete Mellor <pm@csr.city.ac.uk>*

*Wed, 15 Jun 94 17:52:23 BST*

Wesley Kaplow <kaploww@cs.rpi.edu> writes in [RISKS DIGEST 16.15](#):

> Already, Airbus Industry has lost more planes per delivered plane  
> than other major aircraft manufacturer in the past 3 decades (Lockheed,  
> Boeing, MD).

I would be interested to learn the source of this information.

The following table shows the number of crashes per hull in service for different aircraft types. The source is Lufthardtindustrie, and the table

is quoted from "Der Traum von Total Sicherheit", Focus, 38, 1993, pp18-21.

Aircraft Type	No. in Service	Hulls Lost	% Losses
DC-9/MD-80	2065	68	3.29
Boeing 727	1831	62	3.39
Boeing 737	2515	57	2.27
Boeing 747	988	22	2.23
DC-10	446	21	4.71
Airbus A300/310	636	7	1.10
Airbus A320	411	4	0.97

Peter Mellor, Centre for Software Reliability,  
City University, Northampton Square, London EC1V 0HB  
Tel: +44 (71) 477-8422, Fax.: +44 (71) 477-8585,  
E-mail (JANET): p.mellor@csr.city.ac.uk

---

### Re: Does it matter why A3??'s have a poor record? (Re: Mellor)

Wesley Kaplow <kaploww@cs.rpi.edu>  
Wed, 15 Jun 1994 13:29:15 -0400

Dear Pete,

Unfortunately I did a back of the envelope calculation that is probably more suited to comparing the number of takeoffs/landings against accident rates. I remember seeing statistics on the number of 757 lost per total mile (or sorties) vs. A3??. The numbers were quite heavily in favor of the Boeing.

However, you are absolutely correct. I should not have made sure that I have accurate data before such a broad statement. Please delete that section the message. I should know better.

The real point that I wanted to make is that the general public does not care about root-cause analysis, fly-by-wire, or different flight modes. Perceptions of safety, like those that plagued the DC-10 for several years, and like the Audi 5000, are what people care about. Our rationalization that these crashes occurred due to pilot error in 3rd world countries does not make me feel any safer.

It would be interesting to know the breakdown of the essential reasons for the airframe losses in the table you provided. There are three categories I would like to see:

- 1) Loss on the ground (at least 2 of the 747's were lost this way)
- 2) Loss due to mechanical defect
- 3) Crew error.

Also, which accidents cause a total loss or just loss of the frame. For example, a 747 was lost part of its skin, but landed safely (with MOST of its passengers). A 737 got a moon roof, but landed safely (with all of its

passengers and MOST of the crew). A DC-10 (with the blown cargo door) landed with most of its passengers and crew. I assume that these airframes are gone, but are they really "losses" in the sense that the average person would think they are crashes. Moreover, some of these craft were blown out of the sky by terrorists, or set fire on the ground. I believe that this changes the numbers in the table. For example, if one does the following

22 hulls lost for the 747 (are there really only 988 in service?)

- 2 Canary Island
- 1 Lockerbee

-----

19 "Crashed Hulls"

19/988 = 1.92% losses

this is compared to the 2.23% losses in the table.

Another possibly category, since the blame seemingly points to problems of third world operators, is how many of these crashes are airlines that have questionable maintenance.

The last category is time. Although I am chancing fate, when was the last DC-10/MD-11 crash? What is the current rate, as compared to previous years. Do these planes just need to get over "infant" problems, or is the rate essentially constant?

Moreover, if we look at unexplainable crashes, at least for the Boeing and DC/MD planes we can usually identify a real design flaw to pin the crash on (cargo doors, engine mount pins) I can proudly say (well not really) OUR DARN AMERICAN PLANS CRASH BECAUSE OF DESIGN FLAWS WE CAN FIGURE OUT AFTER A COUPLE OF REALLY BIG CRASHES! (a smiley face goes here). However, there is a point here and that is why are the A3?? losses seemingly predominately cause by some pilot to ship interface problem.

Once again, I'm sorry to have submitted unsubstantiated information, and I promise not to do it again.

Wesley Kaplow, AT&T Bell Laboratories & Rensselaer Polytechnic Institute

---

**Re: Airbus (Kaplow, [RISKS-16.15](#))**

*Bob Niland <rjn@hpfcla.fc.hp.com>*

*15 Jun 1994 16:42:03 GMT*

> ... if we play only on the statistics, I want a airplane with a good  
> safety record. ...

If the statistics bear this out, it raises a point I haven't seen mentioned in the periodic discussions about the AirBus Industrie family of flying machines.

If AI is indeed experiencing more hull losses than comparable airframes from other makers, then as a passenger, I don't really care that AI is having

greater success in obtaining "pilot error" determinations in many of the crashes. If their aircraft are more susceptible to pilot error, then AI's aircraft in fact have a problem, and I won't ride them.

Whether computer or airliner, successfully blaming system inadequacies on the user is no substitute for designing usable systems in the first place. A comparison of incident/accident rates by airframe, showing the percentage resolved as "pilot error", would be interesting.

Bob Niland 1001-A East Harmony Road, Suite 503, Fort Collins  
Colorado 80525 USA rjn@csn.org CompuServe: 71044,2124



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 16: Issue 17**

**Friday 17 June 1994**

## Contents

- [Poulsen guilty of L.A. charges](#)  
[Mich Kabay](#)
- [Counterfeit graduation tickets](#)  
[Mich Kabay](#)
- ["Virtual Billboard" on TV](#)  
[R. Peter Jackson](#)
- [Misdirected Mail](#)  
[Jeffrey Austen](#)
- [Revenue Canada database allows birthday change](#)  
[John Howard](#)
- [NIST Response to Blaze Attack on Clipper](#)  
[Ed Roback](#)
- [ROLM phones and "Do Not Disturb": how to lose calls](#)  
[Rob Levandowski](#)
- [A320 hull losses: Lies, damned lies and statistics](#)  
[Pete Mellor](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Poulsen guilty of L.A. charges

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@CompuServe.COM>  
16 Jun 94 18:01:35 EDT

>From the United Press International newswire (94.06.14 @ 18:45 EDST) via  
Executive News Service (GO ENS) on CompuServe:

"Hacker Pleads Guilty to Fraud", By ELKA WORNER

LOS ANGELES, June 14 (UPI) -- A computer hacker accused of breaking into computer systems to rig promotional contests at radio stations, eavesdrop on private citizens and thwart police investigations, pleaded guilty Tuesday to fraud. Kevin Poulsen, 28, of Menlo Park, faces 40 years in prison and a \$1,750,000 fine when he is sentenced Oct. 17.

He pleaded guilty in federal court to computer fraud, interception of wire

communications, mail fraud, money laundering and obstruction of justice.

The author summarizes the case against Poulsen [I added details she didn't include]:

- o [manipulated the phone systems to cheat in radio-station call-in contests that awarded prizes to a specific caller in sequence]; he stole "two Porsches from radio station KIIS-FM, \$20,000 in cash from KPWR-FM and at least two trips to Hawaii and \$2,000 in cash from the same station."
- o used lies and counterfeit IDs to claim and then sell his prizes.
- o uncovered FBI-run businesses, spotted FBI wiretaps and listened in on conversations of ordinary citizens.
- o called a confederate "minutes after his arrest to ... hide the computers used in his illicit activities."
- o lived on the run for 18 months after being indicted in San Francisco by a grand jury until his arrest in April 1991 .
- o in July 1994, he will be tried "on 18 counts of telecommunications and computer related fraud, including charges that he stole Pacific Bell access codes to invade an Army computer network and to obtain information used in FBI investigation of former Philippine President Ferdinand Marcos."
- o worked for the Soviet consul in S.F. by obtaining unpublished telephone numbers."

Michel E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

---

## Counterfeit graduation tickets

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@CompuServe.COM>  
16 Jun 94 18:01:29 EDT*

>From the Reuter newswire (94.06.14 @ 14:25 EDST) via Executive News Service (GO ENS) on CompuServe:

### DARTMOUTH ALUMNUS CAUGHT SELLING PHONY GRADUATION TICKETS

HANOVER, N.H., June 14 (Reuter) - A former Dartmouth College student was arrested for selling counterfeit graduation tickets for the event at his Ivy League alma mater, police said Tuesday. Corby Edward Page, 23, a computer programmer from Houston, Texas and a 1992 Dartmouth graduate, admitted to making the fake tickets on his computer and selling them before the June 12 graduation for \$15 each, said Hanover Police Sergeant Christopher O'Connor."

According to the story, a student who bought a bogus ticket "called police after noticing the fake tickets were different from the real ones." The idiot grad was caught "in the lobby of the posh Hanover Inn, opposite the Dartmouth campus, as he sold tickets, police said."

He was charged with fraud.

---

## "Virtual Billboard" on TV

"R. Peter Jackson" <pjackson@rain.org>

Thu, 16 Jun 1994 23:07:10 -0700 (PDT)

On Wednesday, June 15, 1994, the Los Angeles Times reported on page D7 in their relatively new weekly section called "The Cutting Edge Computing/Technology/Innovation" the following:

"Virtual Billboard" Is Sign of the Times

Baseball teams would love the revenue from behind-the-batter billboards, and advertisers like the idea of being on screen without fear of remote-control zapping. But purists denounce the idea as antithetical to the tradition of the game, and some players say the signs make it harder to see the ball.

Now inventors have devised a system that will create electronic billboards visible only to people watching on TV. Princeton Electronic Billboards Inc. in Princeton, N.J., has been testing "virtual billboards" with the Baltimore Orioles and its telecasters. Working with the David Sarnoff Research Center, the firm developed a computerized system that inserts images electronically into TV shows.

Before a game, the TV cameras scan the arena and "memorize" features of the park, such as creases in the padded wall behind home plate and other boundaries that define a virtual billboard. When the camera passes those features during the telecast, the system inserts the sign, or the part of it visible in the camera's frame of reference.

Ballplayers on the field appear to walk in front of the sign. Ideally, the TV audience will be unable to tell whether the billboard hangs in the ballpark or only in cyberspace. Local sponsors could buy a billboard in a national telecast, and a national advertiser could deliver different messages in each market.

Princeton Electronic hopes to make the system available commercially before the baseball season ends this fall."

It seems obvious that the RISKS increase as the truth of the picture in the TV medium can be selectively and partially modified. It is difficult enough now for many people to tell whether what is seen on TV is real or fake [note the many similarities between national network TV news, major metropolitan network news and the recreated news in Hard Copy and its several competitors.]

R. Peter Jackson, Mariposa Computer Services, 982 Jimeno Road, P. O. Box 149, Santa Barbara, California 93102-0149 USA 1-805.963.4305 <pjackson@rain.org>

---

## Misdirected Mail

Jeffrey Austen <jra1854@tntech.edu>

Thu, 16 Jun 1994 11:24:16 -0600

I received the following in the mail the other day. Quite amusing. I wonder if the CIA would send out a similar message if one of their secrets got out?

>One of IBM's electronic mail distribution nodes experienced a  
>problem routing mail from Wednesday June 8, 1994, through  
>approximately 7:00pm Thursday June 9, 1994. This may have  
>resulted in your having received proprietary information that  
>was not intended for you. If you have received such  
>information, please return it to the Internet address:

> xxx@xxx.ibm.com

>without retaining any copies of it. If you have already  
>destroyed or discarded the information, please confirm this by  
>sending a note to this address stating that the information  
>you received has been destroyed.

>

>If you are not sure whether you should have received certain  
>information or if you have any other questions, please call  
>xxx xxx at (xxx) xxx-xxxx.

Jeffrey Austen, Tennessee Technological University, Box 5004  
Cookeville Tennessee 38505 U.S.A. jra1854@tntech.edu (615) 372-3485

---

## Revenue Canada database allows birthday change

John Howard <jhoward@sol.uvic.ca>

Thu, 16 Jun 94 23:03:48 PDT

Something has just come to light that might be of interest to Risks readers concerning my end of the year taxes here in Canada. For whatever reason, my new accountant (who resides in a different city) filed my tax with a typo on it: my birthday was off by one day. Well, as expected, the system the Feds have sent me a note saying my birthday had changed from the last time I had filed. The form asked me to come down to my local office to correct the error, or if this wasn't an error don't worry about it.

How can they say "don't worry about it"? As far as I know people aren't allowed to change their birthday! I chatted with the teller that helped me correct the error. He said that his most memorable error was a situation where a senior had transposed the middle digits of his year of birth to make him younger by decades. The error was caught when the computer found a young person claiming pension benefits.

The teller enlightened me by saying that personal data is taken from only the most recent filing. I suppose this would be ok for a change of address or even of name, but of birthday! Imagine your favorite ten risks....

John Howard

---

## NIST Response to Blaze Attack on Clipper

<ROBACK@ENH.NIST.GOV>

Thu, 16 Jun 1994 17:29:40 -0400 (EDT)

Note: The following material was released by NIST in response to recent articles regarding AT&T/Matt Blaze and the key escrow chip. A second more technical response follows.

-----  
June 2, 1994

Contact: Anne Enright Shepherd  
(301) 975-4858

The draft paper by Matt Blaze\* describes several techniques aimed at circumventing law enforcement access to key escrowed encryption products based on government-developed technologies.

As Blaze himself points out, these techniques deal only with the law-enforcement feature, and in no way reduce the key escrow chips' inherent security and data privacy.

- "None of the methods given here permit an attacker to discover the contents of encrypted traffic or compromise the integrity of signed messages. Nothing here affects the strength of the system from the point of view of the communicating parties..." p. 7.

Furthermore, Blaze notes that the techniques he is suggesting are of limited use in real-world voice applications.

- "28 minutes obviously adds too much latency to the setup time for real-time applications such as secure telephone calls." p. 7.
- "The techniques used to implement them do carry enough of a performance penalty, however, to limit their usefulness in real-time voice telephony, which is perhaps the government's richest source of wiretap-based intelligence." p. 8.

Anyone interested in circumventing law enforcement access would most likely choose simpler alternatives (e.g., use other nonescrowed devices, or super encryption by a second device). More difficult and time-consuming efforts, like those discussed in the Blaze paper, merit continued government review -- but they are very unlikely to be employed in actual communications.

All sound cryptographic designs and products consider trade-offs among design complexity, costs, time and risks. Voluntary key escrow technology is no exception. Government researchers recognized and accepted that the law enforcement access feature could be nullified, but only if the user was willing to invest substantial time and trouble, as the Blaze report points out. Clearly, the government's basic design objective for key escrow technology was met: to provide users with very secure communications that will

still enable law enforcement agencies to benefit from lawfully authorized wiretaps. It is still the only such technology available today.

Today, most Americans using telephones, fax machines, and cellular phones have minimal privacy protection. The key escrow technology -- which is available on a strictly voluntary basis to the private sector -- will provide the security and privacy that Americans want and need.

\* Statements from "Protocol Failure in the Escrowed Encryption Standard," May 20 draft report by Matt Blaze, AT&T Bell Laboratories

-----

Note: The following provides additional technical material in response to questions regarding a recent paper by Matt Blaze on key escrow encryption.

-----

#### Technical Fact Sheet on Blaze Report and Key Escrow Encryption

Several recent newspaper articles have brought attention to a report prepared by Dr. Matthew Blaze, a researcher at AT&T's Bell Labs. These articles characterize a particular finding in Blaze's report as a ~flaw~ in the U.S. government's key escrow encryption technology. None of the findings in Dr. Blaze's paper in any way undermines the security and privacy provided by the escrow encryption devices.

The finding which has received the most publicity could allow a non-compliant or ~rogue~ application to send messages to compliant or ~non-rogue~ users which will not be accessible by law enforcement officials through the escrowed encryption standard field called the Law Enforcement Access Field (LEAF).

Dr. Blaze's approach uses the openly disclosed fact that the LEAF contains 16-bit checkword to prevent rogue users from modifying the law enforcement access mechanism. This 16-bit checkword is part of the 128-bit LEAF, which also includes the enciphered traffic key and the unique chip identifier.

Dr. Blaze's method is to randomly generate different 128-bit LEAFs until he gets one that passes the checkword. It will take on average 216, or 65,536 tries. This is not a formidable task; it could be done in less than an hour. Dr. Blaze questions the adequacy of a 16-bit checkword and suggests using a larger one, to ensure that the exhaustion attack would be so time consuming as to be impractical.

The chip designers recognized the strengths and limitations of a 16-bit checkword. Following are the reasons why they chose to use a checkword of only 16 bits:

\* There were four fundamental considerations that the designers considered in choosing the LEAF parameters.

These were:

- (1) ease of access by authorized law enforcement agencies,
- (2) impact on communications,
- (3) a sufficiently large identifier field which would not constrain manufacturers, and
- (4) the difficulty required to invalidate the LEAF mechanism by techniques such as those described by Dr. Blaze.

\* The purpose of the LEAF is to preserve law enforcement's ability to access communications in real-time. The encrypted traffic key, which enables them to do this, is 80 bits long. In addition to this 80-bit field, the LEAF must contain the unique identification number of the key escrow encryption chip doing the encryption.

\* The size of the identifier field was the subject of considerable deliberation. In the earliest considerations it was only 25 bits long. The chip designers recognized that 25 bits did not offer enough flexibility to provide for multiple manufacturers of key escrow devices. Different chip manufacturers would need manufacturer identifiers as well as their own chip identifiers to ensure that identifiers are unique. Eventually, the designers agreed that 32 bits would adequately meet this requirement.

\* In many environments, error-free delivery of data is not guaranteed, and there is considerable concern by communication engineers that requiring error-free transmission of a fixed field (the LEAF) could make the encryption device difficult to use. In early discussions with industry, they were opposed to any checksum. In the end, they agreed it would be acceptable if the size of the LEAF was restricted to 128 bits. This left 16 bits for a checksum to inhibit bypassing the LEAF. While recognizing the possibility of exhausting these 16 bits, the designers concluded that 16 bits are adequate for the first intended application. Security enhancements are being made for other applications, such as the TESSERA card.

Note that computations are required to search for a matching checksum, which then has to be properly substituted into the communications protocol. The performance and cost penalties of the search operation are significant for telephone, radio, and other such applications, thus providing adequate protection against this technique for bypassing the LEAF.

In summary:

\* Although this technique would allow one to bypass the LEAF, the security provided by the escrow encryption devices would not be altered. Users' information would still be protected by the full strength of the encryption algorithm.

\* Dr. Blaze was accurate in noting that these attacks are of limited effectiveness in real-time telephony.

\* When designing the key escrow chip, NSA emphasized sound security and

privacy, along with user friendliness. The attacks described by Dr. Blaze were fully understood at the time of initial chip design. The use of 16 bits for the checkword was an appropriate choice in view of the constraints of a 128-bit LEAF. It provides excellent security for real-time telephone applications with high assurance that law enforcement's interests are protected.

\* Dr. Blaze's research was done using prototype TESSERA cards. As part of the family of planned releases/upgrades, NSA already has incorporated additional security safeguards into the production TESSERA cards to protect against the kinds of attacks described by Dr. Blaze.

---

## **ROLM phones and "Do Not Disturb": how to lose calls**

*Rob Levandowski <rlvd\_cif@uhura.cc.rochester.edu>*

*Thu, 16 Jun 94 12:26:55 GMT*

Here at the University of Rochester, students are given ROLMphone 120DCMs in their rooms. These phones (or, more precisely, the digital switch that they are connected to) have a function called "do not disturb". When the appropriate code is entered into the keypad, the line is put into DND mode, and it -will not ring- for any reason. However, if someone tries to call, they hear ringing.

There are two problems with the implementation of this feature. First, the code to activate and de-activate the feature is anything but intuitive. Having lived off-campus for a while, I forget the exact code, but it is along the lines of #6x. The code for speed-dialing numbers is #3x. On more than one occasion I meant to hit a speed-dial and instead activated do-not-disturb.

This wouldn't be a big problem... except that there is no indication whatsoever that you are in DND mode. No lights, no tones, no message to callers. I missed calls for days the first time I did this... and a lot of people got concerned because I "was never home".

This system should at the least have some sort of different dialtone or indicator light to show that you won't be getting any calls. (God knows the ROLM 120 has enough blinky-lights...) Likewise, since the switch is equipped with PhoneMail, it would be nice if it could give an announcement... "The party you have dialed is not accepting calls at this time."

The privacy may be nice when you're using your dorm room for, shall we say, after-hours social research ;) -- but if you're forgetful like me, the implementation is pretty troublesome.

Rob Levandowski, Computer Interest Floor associate / University of Rochester  
macwhiz@cif.rochester.edu

---

## **A320 hull losses: Lies, damned lies and statistics**

Pete Mellor <pm@csr.city.ac.uk>

Thu, 16 Jun 94 19:45:06 BST

This thread of the discussion was originally started by Wesley Kaplow <kaploww@cs.rpi.edu> in [RISKS DIGEST 16.15](#) under the title: "Does it matter why A3??'s have a poor record?"

To recap, Wesley said (without citing a source):

> Already, Airbus Industry has lost more planes per delivered plane  
> than other major aircraft manufacturer in the past 3 decades (Lockheed,  
> Boeing, MD).

I contradicted this in [RISKS 16.16](#), citing a table of statistics from an article entitled ``Der Traum von Total Sicherheit" ["The Dream of Total Safety"], in the German magazine Focus, 38, 1993, pp18-21, and Wesley has since agreed that his statement requires support (see his follow-up mailings). The table was as follows:-

>Aircraft >Type	No. in Service	Hulls Lost	% Losses
>			
>DC-9/MD-80	2065	68	3.29
>Boeing 727	1831	62	3.39
>Boeing 737	2515	57	2.27
>Boeing 747	988	22	2.23
>DC-10	446	21	4.71
>Airbus A300/310	636	7	1.10
>Airbus A320	411	4	0.97

Focus magazine cited "Luftfahrtindustrie" (NOTE: not "Lundfahrtindustrie", as I originally transcribed it) as the source.

Since then, I have been jumped on from a great height by several RISKS contributors who have accused me of abusing statistics. Since this is not something I do deliberately, I would like to make the following points (taking into account the various objections raised by those who have written to me):-

1. I am well aware that the statistics above are incomplete. They do not allow for the total operating time of each type. They do not distinguish between losses due to on-board system failure and losses due to other causes which could not possibly be blamed on the manufacturer (e.g., the Lockerbie bombing, the Vincennes shoot-down). They do not take account of wear-out and natural retirement, so that the number shown may be the "number sold" and not the "number in service". I quoted them because they were all I had at the time (while being acutely aware of their imperfections).
2. Wesley's original statement *\*is\**, however, refuted by these statistics *\*provided they are correct\** (see point 3). A secondary question arises: "Is this a meaningful measure of the safety of a type of aircraft?" I will return to this in point 4.

3. Peter Ladkin pointed out to me that the source name that I had originally misread as "Lundfahrtindustrie" and assumed to be some official body which records air accident statistics, is in fact "Luftfahrtindustrie" (well, it was in small print! :-)) and means simply "Air Travel Industry". In other words, the source cited by Focus magazine is totally vague, and (as Peter said) about as authoritative as "I read it on the net"! :-)) The statistics I naively quoted therefore need substantiation.

4. What would convince Joe Public that a given aircraft type was safe to fly? There are several possible measures of the safety of an aircraft design (note: I do *\*not\** pretend that this list is exhaustive):-

a) Deaths per passenger mile on the given type. This is used by the aircraft manufacturing industry. Conclusion: air travel is the safest way of going anywhere.

b) Deaths per passenger *\*hour\** on the given type. This makes flying about as safe as driving, but the risk would seem to be tolerable, since a probability of  $10^{-4}$  per year of dying in a road accident doesn't seem to worry most people (figures based on official UK statistics).

c) Crashes (i.e., hull write-off) per revenue flight hour. This is used by the certification agencies (FAA, JAA, etc.) when awarding an airworthiness type certificate. The target is a maximum probability of loss of aircraft of  $10^{-6}$  per flight hour due to *\*all\** causes. Historically, statistics show that *\*system-related\** causes account for 1 in 10. The conservative assumption that there are 100 critical systems on board then leads to the famous  $10^{-9}$  requirement for probability of failure of an individual flight-critical system.

d) Crashes per cycle (take-off plus landing).

e) Crashes per example delivered (which is where we came in! :-))

f) Passenger deaths per cycle.

g) Serious incidents per flight hour or per cycle. (Q: "How many accidents has the A320 had?" A: "Five - You forgot about Lille, where an A320 landed on top of a Mooney, taking off both its wings and the empennage, and collapsing the A320's front gear. Since nobody was hurt, it doesn't count, or does it?")

The whole picture is confused by the fact that the public perception of risk is biased *\*against\** rare events that kill lots of people, and less against common events that kill a few. (In assessing any event that loses the aircraft, you must assume the worst case: that you kill everyone on board. If you crash a car, it's just you and the guy you hit!)

I don't pretend to give an answer here, simply raise a few pertinent questions, whose answers (IMHO) are far from obvious.

5. A fairer comparison would be between the A320 and competing aircraft *\*of the same generation\**. I would like to thank Robert Dorsett for

the following:-

757 = 0 in eleven years.

767 = 1 in twelve years. (Lauda)

A320 = 4 in five years. (Air France, Indian Airlines, Air Inter, Lufthansa)

6. Given that all the statistics above are deficient (basically, they lack an exposure time base), they do still tell us \*something\*. (In considering a fleet above a certain size, we could assume roughly the same operating hours per day for each example, and things like maintenance time, etc., would average out.) We could \*tentatively\* conclude that the A320 is a long way from being a flying coffin, but also a long way from being the safest aircraft ever, or even as safe as it should be, given its modernity. The public perception of the A320 seems to be that it is the most dangerous thing that ever left the ground. IMHO this is wrong, and we should be careful not to spread false alarm.

There are, of course, better statistics (e.g., from Flight International) and I shall attempt to locate a few. The best come from the air insurance industry, but I am not sure that I can get my grubby paws on those for reasons of confidentiality.

In the meantime, if anyone knows of a good source ... :-)

Also, how can I phrase an argument to convince my mother that I stand a greater chance of being run over crossing St. Johns Road while walking from Farringdon tube station to the University than I do of dying in an air crash? Then I won't have to make long distance 'phone calls from the airport in B\*m\*\*\*k Egypt to tell her we landed safely every time I go to a conference! :-)  
Peter Mellor, Centre for Software Reliability, City University, Northampton Sq  
London EC1V 0HB +44 (71) 477-8422 p.mellor@csr.city.ac.uk



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 16: Issue 18**

**Tuesday 21 June 1994**

## Contents

- [Physical Location via Cell Phone](#)  
[Derek Atkins](#)
- [RF Interference](#)  
[unattributed alt.shenanigans item via Elana](#)
- [EDI mail storm](#)  
[Cheryl Berthelsen via Brian D. Renaud](#)
- [Re: Campaigns and Elections](#)  
[Peter J. Denning](#)
- [Re: Airframe Safety](#)  
[Bill Murray](#)  
[Mark Staler](#)  
[Andy Dingley](#)  
[Tom Lane](#)
- [Shopping Risks...](#)  
[Philip R. Banks](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Physical Location via Cell Phone

*Derek Atkins <warlord@MIT.EDU>  
Sun, 19 Jun 94 01:32:47 EDT*

I'm sure many people have heard this already, even though it only happened yesterday (Friday, 17 June). I'm sure most people have heard about O.J. Simpson [he was charged with a double murder], and Friday evening he took a long drive around the LA Highway system. Police said that they discovered his location (and even his very car) through the use of the Cellular Phone system.

The RISKS are obvious: Being able to locate someone just by their cell phone, and by extension, just keeping a cell-phone turned on transmits enough information to be located. For example, if anyone carries a Digital Personal Communicator (DPC), or other such flip-top cell phones, or any cell phone, for that matter, they can be physically tracked, basically, anywhere in the country through the cellular phone system.

And as the cells get smaller, the location detail gets better. What will happen when we have micro-cellular phones, a cell for every building, or even a cell for every office! Think about the level of personal tracking that can be done with this level of detail!

-derek

---

### **a risk from alt.shenanigans of all places (!!!)**

*Elana Who? <elana@netcom.com>  
Sun, 19 Jun 1994 02:18:02 GMT*

[No, I did NOT make this post up!!! Elana]

>From alt.shenanigans...

scott.baldwin@castles.com (Scott Baldwin) writes:

>M>because we tend to get blamed for any interference unless we can find  
>M>the actual source!  
>M>Radio direction finding is fun...

> We used to do this all the time as well! HF radios of course. What I  
>found to be pleasing, is this old VW Bug (about a '63 I think) would  
>always be going down the freeway during the afternoon at the same time I  
>would be going to work. I heard that if you had high enough RF power  
>you could disturb the electric fuel pump, so I tried this one day using  
>a 600 Watt PEP amp and keyed an AM carrier, and what did I see???

> A VW bug slowing down and starting to pull over >:) I did this for an  
>entire week... hehe!

---

### **EDI mail storm**

*Brian D. Renaud <brena@hcia.com>  
Fri, 17 Jun 94 11:14 EDT*

[Seen on the Health Information Management Listserv -- Brian]

Date: Thu, 16 Jun 94 23:04:54 -0500  
From: Cheryl Berthelsen <cherylb@fiona.umsmed.edu>  
Subject: IS THE WHAT EDI IS ALL ABOUT?

The following article was published today in the Jackson Clarion-Ledger.  
Is this what Electronic billing does for us? Are the Medicare fiscal  
intermediary software programs for claims processing really that stupid?

WOMAN GETS THE MESSAGE, OK?

Dorothy Joyce's mailman brought her 131 letters in one visit, and

none of it was junk mail. All were from one correspondent: MEDICARE. "The postman said, 'Lady, I've never delivered so much mail to one person before,'" Joyce, 77, said. Each envelope contained four notices concerning Joyce's claim for a \$29.97 doctor's visit. Each cost 46 cents to mail; the government spent \$60.26 to tell Joyce her claim was invalid.

After her May 17 visit to Dr. Samuel P. Robinson's Gulfport office, Robinson's computer notified Medicare's computer that Joyce had been there. And kept on notifying, said Margaret Brundidge, a clerk with Travelers Insurance Co. Medicare office in Jackson.

Cheryl Berthelsen, PhD, Assistant Professor, Univ. of Mississippi Medical Center, School of Health Related Professions (SHRP), Jackson, MS 39216

---

## Re: Campaigns and Elections (Agre, [RISKS-16.12](#))

*Peter J. Denning <pjd@cne.gmu.edu>*

*Fri, 17 Jun 94 12:51:23 EDT*

Phil Agre recently said he found it "scary" that some political campaigners are apparently tailoring political ads to probable interests of individuals, based on extracts from available databases. He is, however, describing an activity that is already happening with advertising in general. I don't understand the grounding for his assessment that tailored political ads are "scary". Few of us like the telemarketers who call at dinner and seem to know things about us, but most people would call this "annoying" not "scary".

Peter Denning

---

## Airframe Safety

*William Hugh Murray <0003158580@mcimail.com>*

*Thu, 16 Jun 94 17:27 EST*

If I recall correctly, this thread began when someone asserted that AI aircraft were just too unsafe for him. I remember thinking at the time that that was a "nationalist" position not supported by facts. One set of facts looks something like this:

>DC-9/MD-80	2065	68	3.29
>Boeing 727	1831	62	3.39
>Boeing 737	2515	57	2.27
>Boeing 747	988	22	2.23
>DC-10	446	21	4.71
>Airbus A300/310	636	7	1.10
>Airbus A320	411	4	0.97

According to this data a rational person might actually prefer AI airframes.

Based upon the data a rational person would certainly prefer the A320 to, let us say the B727. However, based upon public perception, one would

certainly prefer the B727. The 727 enjoys a well-deserved public reputation for safety. On the other hand, those of us who have been adults since the 727 was introduced remember that early in their use they fell out of the sky like hail stones. In response to a number of crash landings the operations manual was changed. The landing configuration was changed from nose-down low-revs to nose-high high-revs. That change contributed greatly to the enviable safety record of the 727.

Based upon the data above, one might prefer the A320 to the DC10. On the other hand, the data could be very misleading. The DC10s, having been around a great deal longer, may have lost far fewer airframes per operation.

(Besides, I like to fly on DC10s. In many configurations, they are the most comfortable planes in the air. I do not pretend to be completely rational. If I were, I would certainly prefer any of these planes to my car.)

My point is that, given the sizes of the (Ns) numbers above and given what they measure, it is simply not possible to make a rational choice between the planes. It probably is not possible even to rationally prefer them to automobiles.

I make my living trying to help my clients make rational and safe choices in areas where there is all too much data about the consequences of an event and all too little about the rates of occurrence. Given the statistical significance of this data, I doubt that I could change the client's life expectancy by more than a few seconds, one way or the other, by making a systematic choice between those planes, on that or any other available data, even if she took a flight every day.

Taken across the entire population likely to fly on those planes, I could do a tiny bit better. However, I could not do sufficiently better to justify public policy. I sympathize with those charged with doing so.

There seems to be a political demand, or at least an expectation, in our current culture for zero risk. The real world does not work that way.

William Hugh Murray New Canaan, Connecticut 06840

---

## Flighty statistics

<stalzer@macaw.hrl.hac.com>

Thu, 16 Jun 1994 13:01:03 +0800

In [RISKS-16.16](#) p.mellor@csr.city.ac.uk presented the following data:

>Aircraft	No. in	Hulls	% Losses
>Type	Service	Lost	
>			
>DC-9/MD-80	2065	68	3.29
>Boeing 727	1831	62	3.39
>Boeing 737	2515	57	2.27
>Boeing 747	988	22	2.23
>DC-10	446	21	4.71

>Airbus A300/310 636 7 1.10  
>Airbus A320 411 4 0.97

Unfortunately, there is no way to interpret this data. Maybe the DC-10s were flown several times a day and the A320s were parked. You must supply miles flown vs. hulls lost, or, even better yet, hops vs. hulls lost (since most accidents happen in takeoff/landing).

Mark Stalzer stalzer@macaw.hrl.hac.com

---

## Airbus Risks

Andy Dingley <dingbat@codesmth.demon.co.uk>

Thu, 16 Jun 94 21:27:58 GMT

On a lighter note, this discussion of Airbus RISKS reminds me of an article in Flight International a few years ago, on the Airbus and its software problems.

The Airbus has many new software-related systems, and had many teething troubles with them. Navigation systems were mentioned as problematic, as were the concerns about fly-by-wire. The crucial problems, as far as operations were concerned, weren't about any of these high profile systems; they were about something as mundane as the computer controlled lavatory valves. If you have a navigational failure, the co-pilot needs to get their manual plotter and charts out again, but you can still fly on. OTOH, a plane full of a few hundred incontinent pensioners on their way to Tenerife isn't going \*anywhere\* unless the toilets are working !

Andy Dingley Codesmiths of Newcastle dingbat@codesmth.demon.co.uk

---

## How to lie with statistics (Re: Does it matter why A3??'s have a poor record?)

Tom Lane <tgl@netcom.com>

Sat, 18 Jun 94 20:50:15 -0700

Pete Mellor <pm@csr.city.ac.uk> writes:

> The following table shows the number of crashes per hull in service for  
> different aircraft types.

I can't believe that anyone would propose such numbers as a useful measure of safety. The Airbus models are much newer than the ones they are being compared to. 727s, for instance, are quite old (most of 'em are approaching retirement, are they not?) and would have seen many more flights than A3xx craft. The low rates reported for A3xx probably just reflect the youth of the fleet.

I would find loss rates per mile flown, or perhaps per departure, far more credible. Anyone have that data?

tom lane

---

## Shopping Risks...

<banksie@khantazi.actrix.gen.nz>

Sat, 18 Jun 1994 13:40:01 +1200

I am sure most people reading the RISKS DIGEST have been bitten by the automated supermarket checkout machines. However, having been bitten recently, I believe it bears repeating.

It has been a weekly routine with my family to help my mother on thursday nights do the shopping. Normally we take along a list, a calculator and generally have a fairly good chat while we take care of the groceries. Now the supermarket we shop at has a checkout system based on a barcode scanner that they pass the goods over to tot the price up. We double check the price using the calculator by adding up the shelf listed prices as we procure the items from the shelf.

But in over two years of doing this we have *\*never\** had a calculator result that tallied exactly with the given price. Often this can be explained as human error but the supermarket has an array of interesting tricks that often account for this difference.

- 1) Not listing the price. Anywhere. This is often the case in the bread section.
- 2) Listing the *\*wrong\** price. Several times we have bought a product that has been listed at one price and has rung up on the checkout counter at another price. Usually we only spot the difference once we have returned home and tried to identify why the calculator result was out. Invariably the price change is in the supermarket's favour.
- 3) Double scanning products. That way it gets rung up twice and you get charged twice for the one product.
- 4) The bar code information is for the wrong product. Presumably data entry errors occur and the bar code on the product you are buying is linked to the wrong price data.

Now I am not suggesting that any of these practices are deliberate but it is easy to see why supermarkets are not terribly keen to stamp out such problems. All it requires is a hundred or so errors, a week, like this to occur and the supermarket accrues, on average, another \$300 of profit. (Our average difference is usually around the \$3 mark.)

What makes it worse is that alot of the supermarket staff believe the computer to be infallible and incapable of error. When I assure them that, due to my profession of programming the things, I know very well that they can go wrong it a large number of ways they almost invariably remain dubious of my assertion.

The risks are fairly clear. It is worthwhile double checking the price you get charged for your groceries. While the system itself is fairly reliable it

naturally cannot cope with the human error side of things due to faulty use or data entry into the system.

Philip R. Banks Syntax: mail < banks\_p@kosmos.wcc.govt.nz >



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 16: Issue 19**

**Tuesday 5 July 1994**

## Contents

- [A330 crash: Press Release](#)  
[Pete Mellor](#)
- [States crack down on "cyberfraud"](#)  
[Mark Seecof](#)
- [AI to screen bad from good cops in Chicago](#)  
[Christopher Maag](#)
- [Going to a Computer Conference? Don't use your real name!](#)  
[Steve L. Rhoades](#)
- [Fraud on the Internet](#)  
[Mich Kabay](#)
- [ACM Releases Crypto Study](#)  
[US ACM](#)  
[DC Office](#)
- [USACM Calls for Clipper Withdrawal](#)  
[US ACM](#)  
[DC Office](#)
- [Re: Physical Location via Cell Phone](#)  
[Lauren Weinstein](#)  
[Willis H. Ware](#)  
[Robert Morrell Jr.](#)
- [Cellular Confusion](#)  
[Bob Frankston](#)
- [Info on RISKS \(comp.risks\)](#)

---

### A330 crash: Press Release

*Pete Mellor* <[pm@csr.city.ac.uk](mailto:pm@csr.city.ac.uk)>

*Fri, 1 Jul 94 16:44:40 BST*

The following are the contents of a fax message sent to me today by Dan Hawkes of the CAA (to whom my thanks).

Pete Mellor, Centre for Software Reliability, City Univ. Northampton Square, London EC1V 0HB +44 (71) 477-8422, [p.mellor@csr.city.ac.uk](mailto:p.mellor@csr.city.ac.uk)

AI/GC-I 22/94R

30th June 1994

Issue 1

A330 FLIGHT TEST ACCIDENT, 30TH JUNE 1994

Airbus Industrie regrets to confirm that a flight test A330, powered by Pratt & Whitney PW4168 engines, crashed at 17.50 today at Blagnac Airport, Toulouse, within the airport boundary. Seven people were on board the aircraft: four members of Airbus Industrie personnel, including the Chief Test Pilot, and three airline pilots. There were no survivors.

The aircraft involved in the accident was serial number 042, which made its first flight on 14th October 1993 and had accumulated 362 flight hours as part of Airbus Industrie A330 flight test programme.

The flight being undertaken aimed to test a new autopilot standard intended for certification with Pratt & Whitney engines for all-weather Category III operations.

The test was planned to take place with maximum aft centre of gravity, at minimum speed and with maximum angle of climb.

Immediately after take-off, once the maximum flight attitude was reached (between 25 and 30 degrees), the test sequence involved switching on the aircraft's autopilot, simulating an engine failure and cutting off the engine's associated hydraulic circuit.

For reasons which are yet to be determined, the aircraft suffered a sudden loss of lateral control. Although it would appear that the pilot regained control, the altitude of the aircraft was too low to avoid impact with the ground, especially bearing in mind the extreme conditions of this particular test flight.

For further information, please contact:  
AIRBUS INDUSTRIE - PRESS DEPARTMENT  
Tel.: (33) 61.93.33.87 or 61.93.34.31

[A list of the deceased was appended to the original. PGN]

---

## States crack down on "cyberfraud"

*Mark Seecof PSD x77605 <marks@bierce.latimes.com>  
Fri, 1 Jul 1994 13:25:43 -0700*

Commentary, quote choice, and paraphrasing by Mark Seecof <marks@latimes.com>.

In a story on page D-2 of the 1 July 1994 Los Angeles Times by Scot J. Paltrow, we learn of "investigations and enforcement actions directed at individuals who solicit money for dubious or fraudulent investments through the financial bulletin boards of on-line services such as Prodigy, America Online, and CompuServe."

Missouri, New Jersey, and Texas regulators are leading the charge with the

members of the "North American Securities Administrators Assn., the organization of state regulators" behind them.

"The action also represents an effort by state regulators to assert jurisdiction over financial solicitations on the bulletin boards, even if the messages are posted from other states or countries. The Securities and Exchange Commission enforcement staff confirmed Thursday that the federal agency is also looking into the issue."

Among other things, "regulators say penny-stock scammers have moved onto the bulletin boards, hyping thinly traded low-priced stocks by posting notes with wildly inflated claims about the companies' prospects."

"The on-line services say they are cooperating with regulators but are not equipped to police the thousands of messages posted daily. They also say it is not a proper role for service operators to limit the free flow of communication, although on-line services often censor sexually explicit or politically offensive messages."

---

## AI to screen bad from good cops in Chicago

*Christopher Maag <exe00461@char2.vnet.net>*

*Mon, 4 Jul 1994 15:55:12 -0400 (EDT)*

[PGN excerpting]

Good cop, bad cop at fingertips: Computer could see possibilities  
Peter Kendall, The Chicago Tribune, 1 July, 1994

The Chicago Police Department has a new computer program that they say will produce a list of officers likely to "go bad" by committing crimes using excessive force or participating in other offenses that can get them fired. The program, built on an \$850 off-the-shelf software package, looks at demographic data and work histories of officers who have been fired for disciplinary reasons, then scours police personnel databases for current officers with similar profiles. Officers who appear on the list would be contacted by supervisors and counseled on how to avoid committing acts that could get them fired, sued or even arrested.

The profile of "bad" cops was developed on the basis race, sex, age, education, number of traffic accidents, reports of lost weapons or badges, marital status and other factors, relating to 191 officers discharged between 1988 and 1993. A comparison of that profile with 2,000 current officers turned up 141 of those officers who were considered "at risk" for committing an offense that could get them fired.

Not surprisingly, the officers' union, the Fraternal Order of Police, is wary. "It's another form of Big Brother watching you," said Bill Nolan, president of the FOP.

---

## Going to a Computer Conference? Don't use your real name!

Steve L. Rhoades <srhoades@netcom.com>

Wed, 4 May 1994 01:54:33 GMT

[Excerpted from MicroTimes April 18, 1994 Issue #122]

At the fourth Computers, Freedom, & Privacy conference in Chicago last month, the spotlight was on the growing conflict between the rights of individuals and the role of government in the digital age. A luckless Whitehouse House representative and a lawyer for the NSA tried to convince a varied and skeptical crowd that government control of cryptography was somehow a Good Thing;

Meanwhile, in their search for fugitive criminals Kevin Mitnick and wooden-legged "Agent Steal", the FBI erroneously arrested one unfortunate attendee whose name happened to resemble one of Mitnick's aliases and interrogated two others, including an ex-Marine and CIA veteran Robert David Steele of Open Sources. ...

Steve L. Rhoades, :30 Second Street, Mt. Wilson, Calif 91023  
(818) 794-6004 srhoades@netcom.com

[An article by John Markoff on Mitnick appeared on the front page of The New York Times, July 4, 1994. PGN]

---

## Fraud on the Internet

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>

30 Jun 94 12:13:32 EDT

>From the Associated Press newswire via Executive News Service (GO ENS) on CompuServe:

"I-Way Robbery", By DAVID GRAM, AP Writer

MONTPELIER, Vt. (AP) -- Say you're cruising the information superhighway from the comfort of your home computer and come across what appears to be private, inside information on a hot new company.

"You spend \$10,000 on stock -- and lose your money.

"You've just become a victim of what securities regulators say is the latest trend in investment scams: frauds perpetrated over computer networks or bulletin board services by hard-to-track hucksters.

"Call it I-way robbery."

The author explains that there is a growing number of scams on the Internet and local BBSs.

Some of the frauds perpetrated through Cyberspace are no different from the usual techniques: false claims of expertise, theft of investments. The only specific technique involves deliberately posting what is intended to look like private communications in a public venue, then taking advantage of

unscrupulous people's attempt to make a killing in the stock market. The specific case mentioned by the author involved two "Canadian companies ... heavily hyped on computer bulletin board services. Their stock prices tripled or more in a short period of time, then collapsed. One of the companies was said to have won a major housing contract in the former Soviet Union; the other was said to own a diamond mine in Zaire where a major strike had been made."

The author identifies the nominal non-commerciality of the Internet as a reason for its popularity among thieves.

[Comment from MK: perhaps these frauds will eventually lead to requirements for effective identification and authentication of users. Ultimately, it would be helpful to see non-repudiation as a feature of all electronic communications. For the time being, caveat lector.]

Michel E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

---

### **ACM Releases Crypto Study**

*"US ACM, DC Office" <usacm\_dc@acm.org>  
Thu, 30 Jun 1994 16:34:47 +0000*

Association for Computing Machinery  
PRESS RELEASE

Thursday, June 30, 1994

Contact:

Joseph DeBlasi, ACM Executive Director (212) 869-7440

Dr. Stephen Kent, Panel Chair (617) 873-3988

Dr. Susan Landau, Panel Staff (413) 545-0263

COMPUTING SOCIETY RELEASES REPORT ON ENCRYPTION POLICY;  
"CLIPPER CHIP" CONTROVERSY EXPLORED BY EXPERT PANEL

WASHINGTON, DC - A panel of experts convened by the nation's foremost computing society today released a comprehensive report on U.S. cryptography policy. The report, "Codes, Keys and Conflicts: Issues in U.S. Crypto Policy," is the culmination of a ten-month review conducted by the panel of representatives of the computer industry and academia, government officials, and attorneys. The 50-page document explores the complex technical and social issues underlying the current debate over the Clipper Chip and the export control of information security technology.

"With the development of the information superhighway, cryptography has become a hotly debated policy issue," according to Joseph DeBlasi, Executive Director of the Association for Computing Machinery (ACM), which convened the expert panel. "The ACM believes that this report is a significant contribution to the ongoing debate on the Clipper Chip and encryption policy. It cuts through the rhetoric and lays out the facts."

Dr. Stephen Kent, Chief Scientist for Security Technology with the firm of Bolt Beranek and Newman, said that he was pleased with the final report. "It provides a very balanced discussion of many of the issues that surround the debate on crypto policy, and we hope that it will serve as a foundation for further public debate on this topic."

The ACM report addresses the competing interests of the various stakeholders in the encryption debate -- law enforcement agencies, the intelligence community, industry and users of communications services. It reviews the recent history of U.S. cryptography policy and identifies key questions that policymakers must resolve as they grapple with this controversial issue.

The ACM cryptography panel was chaired by Dr. Stephen Kent. Dr. Susan Landau, Research Associate Professor in Computer Science at the University of Massachusetts, co-ordinated the work of the panel and did most of the writing. Other panel members were Dr. Clinton Brooks, Advisor to the Director, National Security Agency; Scott Charney, Chief of the Computer Crime Unit, Criminal Division, U.S. Department of Justice; Dr. Dorothy Denning, Computer Science Chair, Georgetown University; Dr. Whitfield Diffie, Distinguished Engineer, Sun Microsystems; Dr. Anthony Lauck, Corporate Consulting Engineer, Digital Equipment Corporation; Douglas Miller, Government Affairs Manager, Software Publishers Association; Dr. Peter Neumann, Principal Scientist, SRI International; and David Sobel, Legal Counsel, Electronic Privacy Information Center. Funding for the cryptography study was provided in part by the National Science Foundation.

The ACM, founded in 1947, is a 85,000 member non-profit educational and scientific society dedicated to the development and use of information technology, and to addressing the impact of that technology on the world's major social challenges. For general information, contact ACM, 1515 Broadway, New York, NY 10036. (212) 869-7440 (tel), (212) 869-0481 (fax).

Information on accessing the report electronically will be posted soon in this newsgroup.

---

## **USACM Calls for Clipper Withdrawal**

*"US ACM, DC Office" <usacm\_dc@acm.org>  
Thu, 30 Jun 1994 16:35:37 +0000*

U S A C M

Association for Computing Machinery, U.S. Public Policy Committee

\* PRESS RELEASE \*

Thursday, June 30, 1994

Contact:

Barbara Simons (408) 463-5661, [simons@acm.org](mailto:simons@acm.org) (e-mail)

Jim Horning (415) 853-2216, [horning@src.dec.com](mailto:horning@src.dec.com) (e-mail)

Rob Kling (714) 856-5955, [kling@ics.uci.edu](mailto:kling@ics.uci.edu) (e-mail)

COMPUTER POLICY COMMITTEE CALLS FOR WITHDRAWAL OF CLIPPER  
COMMUNICATIONS PRIVACY "TOO IMPORTANT" FOR  
SECRET DECISION-MAKING

WASHINGTON, DC - The public policy arm of the oldest and largest international computing society today urged the White House to withdraw the controversial "Clipper Chip" encryption proposal. Noting that the "security and privacy of electronic communications are vital to the development of national and international information infrastructures," the Association for Computing Machinery's U.S. Public Policy Committee (USACM) added its voice to the growing debate over encryption and privacy policy.

In a position statement released at a press conference on Capitol Hill, the USACM said that "communications security is too important to be left to secret processes and classified algorithms." The Clipper technology was developed by the National Security Agency, which classified the cryptographic algorithm that underlies the encryption device. The USACM believes that Clipper "will put U.S. manufacturers at a disadvantage in the global market and will adversely affect technological development within the United States." The technology has been championed by the Federal Bureau of Investigation and the NSA, which claim that "non-escrowed" encryption technology threatens law enforcement and national security.

"As a body concerned with the development of government technology policy, USACM is troubled by the process that gave rise to the Clipper initiative," said Dr. Barbara Simons, a computer scientist with IBM who chairs the USACM. "It is vitally important that privacy protections for our communications networks be developed openly and with full public participation."

The USACM position statement was issued after completion of a comprehensive study of cryptography policy sponsored by the ACM (see companion release). The study, "Codes, Keys and Conflicts: Issues in U.S. Crypto Policy," was prepared by a panel of experts representing various constituencies involved in the debate over encryption.

The ACM, founded in 1947, is a 85,000 member non-profit educational and scientific society dedicated to the development and use of information technology, and to addressing the impact of that technology on the world's major social challenges. USACM was created by ACM to provide a means for presenting and discussing technological issues to and with U.S. policymakers and the general public. For further information on USACM, please call (202) 298- 0842.

=====

USACM Position on the Escrowed Encryption Standard

The ACM study "Codes, Keys and Conflicts: Issues in U.S. Crypto Policy" sets forth the complex technical and social issues underlying the current debate over widespread use of encryption. The importance of encryption, and the need for appropriate policies, will increase as networked communication grows.

Security and privacy of electronic communications are vital to the development of national and international information infrastructures.

The Clipper Chip, or "Escrowed Encryption Standard" (EES) Initiative, raises fundamental policy issues that must be fully addressed and publicly debated. After reviewing the ACM study, which provides a balanced discussion of the issues, the U.S. Public Policy Committee of ACM (USACM) makes the following recommendations.

1. The USACM supports the development of public policies and technical standards for communications security in open forums in which all stakeholders -- government, industry, and the public -- participate. Because we are moving rapidly to open networks, a prerequisite for the success of those networks must be standards for which there is widespread consensus, including international acceptance. The USACM believes that communications security is too important to be left to secret processes and classified algorithms. We support the principles underlying the Computer Security Act of 1987, in which Congress expressed its preference for the development of open and unclassified security standards.

2. The USACM recommends that any encryption standard adopted by the U.S. government not place U.S. manufacturers at a disadvantage in the global market or adversely affect technological development within the United States. Few other nations are likely to adopt a standard that includes a classified algorithm and keys escrowed with the U.S. government.

3. The USACM supports changes in the process of developing Federal Information Processing Standards (FIPS) employed by the National Institute of Standards and Technology. This process is currently predicated on the use of such standards solely to support Federal procurement. Increasingly, the standards set through the FIPS process directly affect non-federal organizations and the public at large. In the case of the EES, the vast majority of comments solicited by NIST opposed the standard, but were openly ignored. The USACM recommends that the standards process be placed under the Administrative Procedures Act so that citizens may have the same opportunity to challenge government actions in the area of information processing standards as they do in other important aspects of Federal agency policy making.

4. The USACM urges the Administration at this point to withdraw the Clipper Chip proposal and to begin an open and public review of encryption policy. The escrowed encryption initiative raises vital issues of privacy, law enforcement, competitiveness and scientific innovation that must be openly discussed.

5. The USACM reaffirms its support for privacy protection and urges the administration to encourage the development of technologies and institutional practices that will provide real privacy for future users of the National Information Infrastructure.

---

**Re: Physical Location via Cell Phone**

*Lauren Weinstein <lauren@vortex.com>*

*Tue, 21 Jun 94 10:39 PDT*

A particularly disturbing aspect of the cell phone story as it relates to the Simpson case is that one of the local L.A. television stations had obtained, by the night of the chase, the printout of all calls made from Simpson's phone, and was showing the printout, in detail with all numbers exposed, on the air. They were also busily calling the numbers and questioning whoever answered. By Monday evening, the station was demonstrating how Simpson's original voicemail announce message had been changed (I would presume by a hacker) to something I'll categorize as being in very bad taste.

--Lauren--

---

**Re: Physical Location via Cell Phone (Atkins, [RISKS-16.17](#))**

*"Willis H. Ware" <Willis\_Ware@rand.org>*

*Tue, 21 Jun 94 11:43:54 PDT*

There is some apparent confusion in what was reported by Atkins re locating the Cawlings-Simpson Bronco. The following is from local media reporting.

The local TV news interviewed a young couple who were on the way to the beach, pulled alongside the Bronco, recognized Cawlings, fell back and got the license number, stopped at the first roadside emergency fone [which are spaced every mile along Southern California freeways], and reported the event/location. Parts of the phone conversation with the emergency dispatcher were played over TV, and the young couple were both present on TV to tell their story.

Shortly thereafter, a police [Santa Ana ??] patrol car spotted the Bronco and the Great Freeway Chase was underway. The same car was said to be the lead vehicle throughout the chase right up into the driveway at the home.

The Sunday LATimes did have an article concerning the role of the cell phone in the event. It is correct that the car received and originated many calls during the chase. Some of the calls were from people trying to persuade Simpson to surrender [e.g., McCabe his former coach], others were from the police in a negotiating mode, others were with the chase cars alerting them intended turnoffs onto other freeways and reporting the status of the occupants. Parts of some of these calls have been played on TV, and the content of others described verbally.

The Sunday article reported that "local law enforcement" subpoenaed the cellular carrier [AirTouch] to cooperate, and the company reported that it did monitor calls to/from the cellular number. The article also reports that law enforcement had obtained a court warrant authorizing tapping of the cell phone, but it is not completely clear whether this was a separate action or related to the subpoena action.

The legal facts are that actual tapping does require a court-authorized warrant [the Wiretap Act of 1968] but access to "transaction records"

requires only a subpoena. It is possible that law enforcement did both things just to be safely legal.

The Times interviewed a security consultant from Houston who seemingly speculated that triangulation had been used to locate the Bronco. I put it that way because there has been no statement by law enforcement that it did more than have AirTouch monitor the calls. Moreover triangulation equipment for a fast moving nearby target is not likely something that the local law enforcement authorities would have. There has been no mention of the FBI but it is conceivable that it played a support shadow role; it probably does have triangulation equipment.

The local reporting has been quite explicit that visible sighting of the car was the basis of locating it, and that the cellphone became involved only in attempting to resolve the situation. There have been no official statements that the cellphone was involved in location; there were the comments by the consultant that triangulation was - or could have been - used.

General comment. A cellular system must know which cell an active call is in because the system control must monitor adjacent cells and be prepared to pass the call to one of them when the signal level falls below some threshold. So the Bronco's location within some cell could have been known but it would not be very precise. If cells get smaller in the future, then the precision of location will increase - as Derek Atkins properly points out. In the case of the Cawlings-Simpson chase, however, the evidence is that visible sightings were the basis for initiating and conducting the chase. Seemingly the facts got garbled as they wandered around the country and were rewritten for various media occasions.

A cellphone in standby mode also is in contact with cell stations so that its location will be known for incoming calls. Again, the location will be known by the system but only to within the extent of a cell-size. A cellphone that is turned off does not transmit and is invisible to the system. Whether system designs are such that "sustaining background monitoring data" is available to the operators is beyond my knowledge -- the same LATimes article did make reference to AirTouch conducting monitoring for the purpose of detecting fraud.

Willis H. Ware

[Some of this was also noted by Mark Stalzer, stalzer@macaw.hrl.hac.com .]

---

### **Re: Physical Location via Cell Phone (Atkins, [RISKS-16.17](#))**

*"Robert Morrell Jr." <bmorrell@isnet.is.wfu.edu>  
Tue, 21 Jun 1994 14:26:50 -0400 (EDT)*

Derek Atkins wrote of the risk of cellular phones as exemplified by the OJ Simpson case. I say, what risk? The risk that an accused double murderer will be arrested? That is a RISK? Often I have heard of politicians, criminals (my redundancy checker is broken) caught unawares by the lack of privacy of

cellular phones. There is no insidious plot to this, only the fortunate stupidity of the cell phone user, who has forgotten how the technology works. Just because a previous form of communication afforded a degree of privacy, one cannot assume, or logically legislate that all succeeding forms have the same. If you use a form of communication it is incumbent upon you to match your expectations of privacy with the technology, not the other way around.  
Bob Morrell

---

## Cellular confusion

<Bob\_Frankston@frankston.com>  
Sun, 3 Jul 1994 17:27 -0400

Just ran across confusion about cellular service in two disparate sources.  
Ann Landers and CNN.

The AL column mentioned Cellular in the headline. The centerpiece was a claim by Ameritech about how hard it is to listen in and that it was possible to get secure phones (from whom?). This is, of course, disinformation. The risks of listening in are not that someone will carefully follow both sides of a conversation, but that listeners will glean key information from portions of random conversations. One can argue about how big the threat is, but we know it is real. The key to the confusion is that the risk is viewed in terms of tapping a land phone line rather than recognizing that the nature of the risk has changed because cellular phones are not simply phones with long wires but a very different base technology.

This same confusion is the basis for the CNN story. As with Ann Landers, CNN itself is confused. First it reported the story as if this is a new problem that occurs only far away in the Philippines. The issue is a simple one -- assigning duplicate ESN numbers to phone. The "legitimate" excuse is that multiple ESN's are simply a way to allow a relative to use your number without an additional monthly charge and the theft of service is viewed as the real threat. The loss was quoted as \$1,000,000 a year -- obviously a serious underestimate. I would guess that the provider is attempting to minimize the fears. What was interesting was the terminology used mimicked landlines. In fact, they talked about using some one else's "line". The use of duplicate ESN's is also based on the model of adding an extension not recognizing the complexities of call routing.

Whatever the risks are of new technologies, viewing them in terms of the old technology adds a new level of risk and confusion.

As an aside, I'll give the local Cellular One provider (SW Bell) credit for having a companion phone charge of just \$10/month. But, in general, I'm frustrated by getting a separate bill for each number as opposed to having an account. This is a different aspect of the inability of the Telcos to move beyond a model of single line phone service to the home. (OK, Sprint and some others supposedly do have smarter ways of handling this).

Of course, there are those that would view this difficulty in changing models as what keeps technology from changing too fast and is thus a way to reduce

risk.



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 16: Issue 20**

**Weds 6 July 1994**

## Contents

- [EM RF RISK turns into life-saver](#)  
[Ralph Moonen](#)
- [Mosaic risks](#)  
[Faisal Nameer Jawdat](#)
- [Airbus](#)  
[Robert Morrell Jr.](#)
- [ACM crypto policy panel chairman's statement](#)  
[Steve Kent](#)
- [Re: Physical Location via Cell Phone](#)  
[A. Harry Williams](#)
- [Phone records](#)  
[Lauren Weinstein](#)
- [Video cameras in City Centres](#)  
[Scott A. McIntyre](#)
- [Re: AI to screen bad from good cops in Chicago](#)  
[Piers Thompson](#)
- [Re: Scary](#)  
[Jim Horning](#)
- [Environmentally Aware Computing](#)  
[JAN Lee](#)
- ["Repetitive Strain Injury" by Pascarelli](#)  
[Reviewed by Rob Slade](#)
- ["Computer Ethics" by Forester/Morrison](#)  
[Reviewed by Rob Slade](#)
- ["A Short Course on Computer Viruses" by Fred Cohen](#)  
[Reviewed by Rob Slade](#)
- [Re: Rob Slade's review of "The Hacker Crackdown"](#)  
[Richard Schroepel](#)
- [Info on RISKS \(comp.risks\)](#)

---

### EM RF RISK turns into life-saver

*Ralph Moonen* <[ralph@inter.nl.net](mailto:ralph@inter.nl.net)>

*Wed, 6 Jul 1994 09:52:04 +0200*

The oft discussed risk of EM RF radiation to devices like pacemakers can now sport a case of anti-risk. A 42-year old man of The Hague (Netherlands) collapsed in front of a swimming pool when his pacemaker failed. A police officer in the vicinity radioed for help, and as soon as he did, the pacemaker started working again. The officer was able to keep the man alive until an ambulance arrived by using his transceiver.....

--Ralph

[The remote jumpstart has all sorts of interesting possibilities.  
Next we will find a way to remotely beam an electrical charge into a car ignition when the battery is low, without jumper cables. PGN]

---

## Mosaic risks

*Faisal Nameer Jawdat <faisal+@CMU.EDU>  
Wed, 6 Jul 1994 09:29:14 -0400 (EDT)*

Clarinet reports that Spyglass, Inc. has signed a licensing agreement with the NCSA for the right to work with, enhance, and redistribute versions of Mosaic as a commercial product.

The obvious risk comes in the confusion that could ensue with some people thinking that their commercial version is also freeware, and distributing it, or some people getting in trouble for distributing the free version because someone else thinks it's the commercial version. Also, there are risks due to the differing feature sets provided by each.

The more menacing risks (to my thinking, at least) come from the fact that Spyglass will be working on some security and authentication systems to allow credit card transactions over the net. I am highly dubious of the www's ability to safely protect credit card transactions (although I could think of ways this could be handled, I do not trust a browser system that was not originally designed with highly secure transmission in mind).

Also, sources to various NCSA projects are not particularly difficult to find (I found Telnet on wuarchive, and I've seen Mosaic at CMU) - with access to Mosaic sources people could build fakes of the commercialized Mosaic to trap credit card numbers.

--faisal

---

## Airbus

*"Robert Morrell Jr." <bmorrell@isnet.is.wfu.edu>  
Tue, 5 Jul 1994 23:13:19 -0400 (EDT)*

I recently had the opportunity to discuss at length the various RISKS Digest pieces on air safety and computer controls with a relative who is an experienced military and civilian industry pilot.

He agreed with the thrust of the threads here, but added a specific and general comment about the A-320.

Specifically he noted that the greatest problem with the aircraft is that it is unique in lacking a unified "off switch" for the autopilots. All other aircraft have one control that can be flipped or pressed that will turn off the computer pilot(s) and return control to the aircraft. Apparently doing this in the A-320 is no small matter.

Generally, though he and other pilots like the A-320, it is known for having a "mind of its own" literally. Most pilots, according to my relative, have stories of the plane suddenly "up and deciding to begin an approach, go around or enter a traffic pattern" It seems amusing usually, but then my relative had never had it happen low to the ground....

---

### **ACM crypto policy panel chairman's statement [See [RISKS-16.19](#)]**

*Steve Kent <kent@BBN.COM>*

*Wed, 29 Jun 94 10:15:09 -0400*

[The following statement could have been included along with the crypto policy panel message and the USACM message in [RISKS-16.19](#), providing an explanation of the distinction between the two messages and their origins. Steve's statement was read as part of the press conference noted in [RISKS-16.19](#), which Steve could not attend. I have chosen to reproduce it here. PGN]

Barbara Simons, chair of the USACM committee recruited me to organize this panel a little over a year ago, after the announcement of the escrowed encryption initiative. Barbara provided suggestions for candidate panel members, but allowed me complete freedom in inviting panel members. Barbara also pointed me towards Susan Landau as a candidate staff member to support the panel, and I am especially grateful for that recommendation as Susan has done a tremendous job in writing this report, from inputs provided by the panel members, from her own research, and through extensive editing sessions including all of the panel members.

The panel I assembled is intentionally a mix of individuals with represent differing perspectives on the complex issues surrounding crypto policy. These individuals work for a variety of organizations, including government agencies, academia, commercial and non-profit organizations. These organizations graciously donated the participants' time so that they could participate in this activity. The panel members did not represent these organizations in the production of this report, but rather contributed as individuals.

The panel members worked together in a cooperative effort to produce a consensus report. Not all panel members agree with all of the statements contained in this report and the report contains no policy recommendations, because of the diverse panel membership. The report distinguishes between facts, opinions and speculation. It provides a very balanced discussion of

many of the issues that surround the debate on crypto policy, and we hope that it will serve as a foundation for further public debate on this topic. I personally became better informed about some of these issues as a result of working on this report and I suspect many of the panel members also gained personally from their participation.

The statement of the USACM committee, which Barbara will read, and which is available in hardcopy form, should be viewed as independent of this report. The USACM committee reviewed this report, and suggested a variety of changes, some of which were acted upon while others were not. Both the panel and the USACM committee agree on the need for continued public debate on this topic. However, the specific recommendations of the USACM committee do not reflect the consensus views of the panel nor are they necessarily supported by the contents of this report. The press, policy makers, and the public should read the report and use it as a starting point in reaching their own conclusions about these issues.

---

### Re: Physical Location via Cell Phone (Atkins, [RISKS-16.18](#))

*"A. Harry Williams" <HARRY@VM.MARIST.EDU>*

*Sun, 03 Jul 94 20:46:10 EDT*

>And as the cells get smaller, the location detail gets better. ...

While recently cruising the WWW, one of the people here discovered a location in England using active pagers to track their staff in the building. While some of it was best guess on our part, There was definitely some kind of meeting going on, since many of the staff were identified as being in a conference room(even which phone was closest to their location.) From our observations, it looks like there is no "cell" for either the hallways, or the rest rooms. There was however, identification of those last spotted at the car park exit, and how long they had been out of the building.

/ahw

---

### Phone records

*Lauren Weinstein <lauren@vortex.com>*

*Wed, 6 Jul 94 00:24 PDT*

The question of phone records is an interesting one. On one hand, there's the release of records to law enforcement under court action. There are many cases where this is important to the solving of a crime and the merits need to be determined in each individual case.

What I found disturbing in the recent Simpson situation was the \*television station\* getting the records and airing them (complete with numbers exposed) so rapidly. I've been unable to determine if the release of these records to the station was somehow legal, or was completely under the table. The station had what appeared to be complete, detailed computer printouts in hand.

If you read your phone bill inserts carefully, you may have already received a notice allowing you to choose whether or not you want your called number information released to VENDORS of telecommunication services! Apparently a new FCC ruling requires this choice be made by subscribers--I believe it defaults to "no call info" if the subscriber doesn't respond and has no prior instructions on file. Of course, this begs the issue of how widespread the practice was of telcos and long distance companies handing out this info for commercial purposes in the past.

This is an appropriate area for discussion over in the PRIVACY Forum Digest. Send the line:

information privacy

as the only text in the body of a message to:

privacy-request@vortex.com

for details.

--Lauren--

---

## Video cameras in City Centres

*"Scott A. McIntyre" <scott@shrug.org>  
Wed, 6 Jul 1994 11:50:25 +0100 (BST)*

In a report on the BBC last night (Tue July 5, 1994) the merits and RISKS of the recent installation of a city centre wide television monitoring system in Liverpool was discussed.

After the abduction and murder of James Bulger a year or so ago, most of the residents of Liverpool were all in favour of having their movements monitored by the bank of high resolution cameras, covering all streets in the main centre of town.

A private company is in charge of the system, but the police (both local, and as the report suggested, national) have instant access to any of the camera views. There was some discussion as to the dangers of companies, organisations, and even the government obtaining access to these tapes to discover who shops where, buys what, etc; yet by and large people seemed willing to allow Big Brother to move in to combat crime and make the streets safer.

The RISKS are obvious. With enough crime, poverty, social decay, people may be willing to assign away all personal freedom in the perhaps futile attempt to recover the lost days of leaving your front door open and unlocked, and your car window rolled down whilst you shop.

Scott

---

## Re: AI to screen bad from good cops in Chicago

Piers Thompson <pjt1@scigen.co.uk>

Wed, 6 Jul 94 11:21:49 BST

What is the legal position on this? The article lists the factors used by the program to make decisions: it does not consider the weighting given to these factors. The software could quite possibly be ignoring one or more of the factors. In the worst case, the software might just be considering the race or sex of a police officer. This would be blatant racism/sexism. When race and sex are combined with other factors to produce a criminality estimate does not their inclusion still amount to sexism/racism?

If the program's output were to have any influence on the promotion prospects of an individual and that individual could demonstrate that changing only their race or sex (as inputs to the program rather than genetically!) moved them into the non-potential-criminal group then would that not provide grounds for them to claim discrimination and take whatever legal action was appropriate?

Piers Thompson pjt1@scigen.co.uk

[Also a good topic for PRIVACY... PGN]

---

## Re: Scary (Denning on Agre, [RISKS-16.18](#))

<horning@src.dec.com>

Tue, 21 Jun 94 10:12:59 -0700

I suspect that what Phil finds scary is that an unknown candidate (a la Perot) can appear to each voter to be promising exactly what that voter wants, and diametrically opposed voters could wind up voting for a candidate who actually didn't intend to satisfy either of them. With broadcast media, there is some chance that everybody will see what the candidate is promising other people.

It's not quite so scary when applied to a brand of perfume or motor oil, maybe because they don't have fixed terms of office.

Jim H.

---

## Environmentally Aware Computing

J. A. N. Lee <janlee@vtopus.cs.vt.edu>

Wed, 6 Jul 1994 14:06:53 -0400 (EDT)

[This would be a useful item for RISKS, so I am including JAN's request here. Please respond to him and CC: RISKS. PGN]

I am interested in having our students in our Computer Professionalism course do a homework writing assignment related to the development of environmentally

favorable machines, systems, etc. While there has been some newspaper articles about the "clean-up" of Silicon Valley and the hazards of working in computer manufacturing environments, there seems to be little in the "technical" press. I am looking therefore to collecting a bibliography of articles which address these topics -- including not only hazards and clean up, but also references to "Green Machines". Along the same line there has been some references to VDT radiation and RSI but I do not know of a bibliography in this area.

Your assistance is sought.

John A. N.(JAN) Lee, Dept. of Computer Science, Virginia Tech, Blacksburg VA  
24061-0106, Ph: (703) 231-5780 FAX: (703) 231-6075 E-mail: janlee@cs.vt.edu

---

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">  
Sat, 02 Jul 1994 12:43:58 -0600 (MDT)

Subject: "Repetitive Strain Injury" by Pascarelli

BKRSI.RVW 940401

Wiley  
5353 Dundas Street West, 4th Floor  
Etobicoke, ON  
M9B 6H8  
416-236-4433  
fax: 416-236-4448  
or  
22 Worchester Road  
Rexdale, Ontario  
M9W 9Z9  
800-263-1590  
800-567-4797  
fax: 800-565-6802  
or  
605 Third Avenue  
New York, NY 10158-0012  
USA  
800-263-1590  
800-CALL-WILEY  
212-850-6630  
Fax: 212-850-6799  
jdemarra@wiley.com  
aponnamm@jwiley.com  
"Repetitive Strain Injury", Pascarelli, 1994, 0-471-59533-0, U\$18.50

My first actual case of repetitive strain injury (or RSI), as a first aid attendant, was not in the logging camps, railway gangs or spacing crews, but with a young student athlete at an outdoor school. He had, literally, outdone himself the day before on a steep downhill hike. He was one of the best jocks in the school and had no problems with stairs and hill climbs--none of which

had prepared him for the repeated extension of his foot which downhill walking required.

Work-related repetitive strain injury has been known for a long time now. Writer's cramp shows up in an Italian treatise almost three hundred years old. Research and treatment, however, has lagged. For one thing, RSI generally involves soft tissue damage which does not show up on x-rays (or, indeed, on anything much besides microscopic examination of the tissue). For another, few jobs up until this century have required the kind of environment where actions had to be repeated so often without variation. Until very recently, the most common repetitive strain situations involved gross motor activities, where strains showed up early and responded well to exercise. With the advent of the computer keyboard and data entry as major factors in job situations, RSI has become a serious issue in the workforce.

This is a comprehensive, factual and practical guide to RSI. It is directed primarily to the computer user or repetitive strain injury sufferer, covering facts about RSI, symptoms and warning signs, diagnosis, choosing a physician, recovery, legal aspects, maintenance and prevention. A major emphasis is to put users/sufferers in charge of, and responsible for, their own health.

The book continually counsels patience. My student athlete, when asked if he could walk out with the rest of the group, visibly tried to calculate how much better he could be in the three days before they had to leave. I had to ask him if he could do it right then, since I knew it wasn't going to heal very fast, and he had to admit he couldn't. His case was actually extremely mild, after only a few hours, and would have faded within a week or so of reduced activity. Most RSI cases, however, traumatize the area for months or even years, and the healing process is correspondingly lengthy.

Although the book is written for users, I would strongly recommend that every manager get a copy. Averaged over all employees, RSI accounts for about \$200 expense per year and per person. If you have four people working for you, using computers, it is almost certain that at least one will develop RSI at some point. RSI is almost entirely preventable, and is almost entirely caused by ignorance. Most of you reading this are probably nodding your heads and muttering something about carpal tunnel syndrome--unaware that this over-diagnosed syndrome actually accounts for only one percent of RSI, according to one study cited in the book.

Highly recommended. A very minor investment in keeping free of an ailment which could severely affect your job--not to mention everything else you do with your hands and body.

copyright Robert M. Slade, 1994 BKRSI.RVW 940401  
Vancouver Institute for Research into User Security Canada V7K 2G6  
Robert\_Slade@sfu.ca rslade@cue.bc.ca p1@CyberStore.ca p1@arkham.wimsey.bc.ca

---

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">  
Wed, 22 Jun 1994 13:15:55 -0600 (MDT)

Subject: "Computer Ethics" by Forester/Morrison

BKCPTETH.RVW 940406

The MIT Press  
55 Hayward Street  
Cambridge, MA 02142  
USA

Robert V. Prior, Editor - Computer Science prior@mitvma.mit.edu  
Maureen Curtin, Int'l Promo. - curtin@mit.edu  
"Computer Ethics", Forester/Morrison, 1994, 0-262-56073-9, U\$14.95

As a collection of stories on computer crime and problems, this is fascinating and wide ranging. As a text on the social, ethical and professional issues facing the information technology community, it is interesting and possibly provoking. As a textbook for a course on computer ethics it lacks analysis, ethical background and structure. The sub-title, "Cautionary Tales and Ethical Dilemmas in Computing," is much more descriptive of the book. It is full of "tales"; a cross between "Spectacular Computer Crimes" and "Digital Woes". The ethical dilemmas are an add-on, but generally well written. As an adjunct in a course on computer ethics, or the social implications of technology, it would certainly hold students' attention. The authors seem to be slightly too aware of this. The preface states that the authors found computing students to lack "awareness of social trends, global problems, or organizational issues," and that the book had been correspondingly directed to the closer details of what students would face on a daily basis. One can sympathize with the frustrations the authors must have felt, but this very example would seem to indicate that students must be given a broader view of society rather than a narrower one.

Chapter one gives a good introduction and overview, as well as a brief explanation of the major current ethical philosophies. It is, unfortunately, the last statement on ethics that is made. Until chapter nine, a set of scenarios for classroom discussion, the remainder of the book is the various tales, padded with a thin structure of observations from other writings. Chapter two covers computer crime. It has a slight tendency to edge towards the border of the hacking/cracking/phone phreak topic, but the discriminating reader will note what law enforcement agencies generally find: most computer crime is an inside job. Chapter three deals with software theft and notes, perhaps a bit smugly, the litigious mess of the American software industry. (The authors hail from Australia and Singapore, respectively.) Chapter four explores "Hacking and Viruses" and, given the confusion of hacking with computer abuse, is more than slightly confused. Chapter five looks at issues of computer reliability or the lack thereof. Chapter six purports to deal with invasion of privacy, but spends much of its time with computer errors and, then, a significant space talking about workplace surveillance (which anticipates chapter eight). The examination of artificial intelligence, in chapter seven, seems mostly to have been a recap of the reliability issues from chapter five.

Instructors, even when simply using the book as a discussion starter, should be on top of the subject. The MacMag/Brandow virus appears, not in chapter four, but in chapter three as an illustration of software piracy. This indicates that the authors have no understanding of viral spread. Indeed, the authors define a virus as a self-replicating program that causes damage--even though

three out of the five specific examples do no "damage". A "trojan horse" is also defined as a program that allows access to an already penetrated system-- with no mention of pretense, deceit or damage at all. (The authors also report the "Twelve Nasty (sic) Tricks" trojan as a virus, the "AIDS" extortion attempt as a virus and the "Desert Storm" virus as fact.)

This book is definitely a good adjunct text for a social, ethical or professional computing course. It will definitely provide interesting material. It does not, however, provide the necessary background for such a course without other materials.

copyright Robert M. Slade, 1994 BKCPTETH.RVW 940406  
DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733

---

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">  
Tue, 05 Jul 1994 13:22:51 -0600 (MDT)

Subject: "A Short Course on Computer Viruses" by Cohen

BKSHRTVR.RVW 940329

Wiley

5353 Dundas Street West, 4th Floor

Etobicoke, ON

M9B 6H8

416-236-4433

fax: 416-236-4448

or

22 Worchester Road

Rexdale, Ontario

M9W 9Z9

800-263-1590

800-567-4797

fax: 800-565-6802

or

605 Third Avenue

New York, NY 10158-0012

USA

800-263-1590

800-CALL-WILEY

212-850-6630

Fax: 212-850-6799

jdemarra@wiley.com

aponnamm@jwiley.com

"A Short Course on Computer Viruses", Cohen, 1994, 0-471-00768-4, \$34.95

fc@jupiter.saic.com

This book is fun. I mean, it starts out with the statement, "I would like to start with a formal definition," followed by about a paragraph's worth of symbolic logic, followed by, "So, much for that!" I assume that the surface

joke is accessible to all: for those who know of the troubles Dr. Cohen has had over the years with those who insist on an informal translation of his work, it is doubly funny. From that beginning right through to Appendix A (a joke) the light tone is maintained throughout, and it makes for a thoroughly enjoyable read.

Besides being fun, though, the book is solid material. Possibly one could raise quibbles over certain terms or minor details, but almost nothing of substance. The only halfway controversial point in the book is Dr. Cohen's continued crusade on behalf of "benevolent" viral programs. While I agree that the concept is worth further study, Dr. Cohen has not yet applied the rigour of his earlier work to proofs that such programming can be guaranteed safe or that benevolent viral programs are the best way to accomplish the examples used.

The material in the book will be accessible to any intelligent reader, regardless of the level of computer knowledge. The most benefit, however, will be to those planning data security or antiviral policies and procedures. They will find here a thoughtful, provoking and insightful analysis.

copyright Robert M. Slade, 1994 BKSHTVR.RVW 940329  
Vancouver Institute for Research into User Security Canada V7K 2G6  
Robert\_Slade@sfu.ca rslade@cue.bc.ca p1@CyberStore.ca p1@arkham.wimsey.bc.ca

---

### Rob Slade's review of "The Hacker Crackdown"

"Richard Schroepfel" <rsc@cs.arizona.edu>  
Wed, 29 Jun 1994 15:03:11 MST

THC is available for downloading from Project Gutenberg for free. Courtesy of Bruce Sterling, who deliberately retained the electronic distribution rights.

Rich Schroepfel rsc@cs.arizona.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 16: Issue 21**

**Thursday 7 July 1994**

## Contents

- [Risks of REDIAL](#)  
via [Lance Hoffman and others](#)
- [Online services taking big hits](#)  
[Alan Wexelblat](#)
- [Tax Software to Avoid: CA Simply Tax](#)  
[Smith Craig](#)
- [IRS SSN risks may abate](#)  
[Michael Gerlek](#)
- [Re: Fraud on the Internet](#)  
[Jeff Barber](#)
- [Signatures in electronic commerce](#)  
[Benjamin Wright](#) via [Mich Kabay](#)
- [Re: Scary](#)  
[Peter J. Denning](#)
- [Just the Facts, Ma'am \(AI to screen bad from good cops\)](#)  
[David Honig](#)
- [Re: Video cameras in City Centres](#)  
[Robert Allen](#)
- [Digitized CC Signatures](#)  
[Eric Richards](#)
- [Re: Shopping Risks...](#)  
[Jane Anna LANGLEY](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Risks of REDIAL

"Lance J. Hoffman" <[hoffman@seas.gwu.edu](mailto:hoffman@seas.gwu.edu)>  
Thu, 7 Jul 1994 09:53:59 -0400 (EDT)

[via various intermediaries... PGN]

WIRES CROSS AS LOVERS DIAL M FOR MOTHER

LONDON, July 2 (Reuter) - A terrified British mother put police on red alert

after mistaking the sound of lovemaking for a cry for help from her daughter. \*The Independent\* newspaper said on [July 2] that two accidental phone calls woke the woman in Devizes, southern England, in the small hours of the morning. Hearing moaning, groaning and shouting, she dismissed the first as an obscene call, but in the second she recognised her daughter crying: "Oh my God," and heard a man's voice.

Convinced her daughter was being attacked in her bedroom 100 miles (160 km) away, she dialed the emergency number 999 and a police squad sped to the daughter's home to investigate. "Officers rushed round and found she wasn't being attacked -- in fact she was quite willing," a police spokesman said. "They explained that during the moments of passion one of the couple accidentally pushed the last-number redial button on the bedside telephone with a toe. Unfortunately on both occasions it was the girl's mother's phone number," he said. "This is a warning for other people -- if you're going to indulge in this sort of thing, move the phone."

The mother and daughter have apologized to police for the confusion.

[Reach out and toe someone? This gives new meaning to "having your buttons pushed". And the mother was left to her own Devizes. PGN]

---

## Online services taking big hits

"Alan (Miburi-san) Wexelblat" <[wex@media.mit.edu](mailto:wex@media.mit.edu)>  
Wed, 29 Jun 94 12:15:22 -0400

On Saturday night, during Game 6 of the Stanley Cup Finals on ESPN, a commercial for the Prodigy on-line computer service came on. They were talking about how great the hockey game was, but it didn't compare to the excitement available on Prodigy. They cut to the computer screen showing Prodigy, and all of the sudden a big window came up on the screen, saying "COMMUNICATION ERROR". Users of Prodigy say that when that happened, the system locked up for almost a minute, then their screen went completely blank. ESPN quickly cut away to another commercial.

The curse of the live demo!

On another ranch, AOL managed to get its main server building flooded, knocking out the whole network for hours and denying email service for hours more after that. No word yet on lost data... [You'd think after the mess in Chicago a few years back they'd've learned something.]

--Alan Wexelblat, Reality Hacker, Author, and Cyberspace Bard, Media Lab  
Advanced Human Interface Group [wex@media.mit.edu](mailto:wex@media.mit.edu) 617-258-9168

---

## Tax Software to Avoid: CA Simply Tax

"Smith Craig" <[smith\\_craig@mn14.ssec.honeywell.com](mailto:smith_craig@mn14.ssec.honeywell.com)>

1 Jul 1994 16:42:38 U

This time of year, taxes are far from mind. That is until I received a letter from the IRS stating that I had incorrectly figured the credit for child care expenses on my 1993 return. This is the first year my tax preparer, an enrolled agent (EA), used the 1040PC format: only the necessary lines are printed without descriptive text. My EA checked and reports that the software, Simply Tax by Computer Associates (CA) of MD, carried the incorrect figure to line 4 of form 2441. To my surprise, he said there were a number of such bugs resulting in incorrect line transfers on other forms, but he corrected them manually. What's the point of software that's automatically wrong? Interestingly, the software can print either the 1040PC version or a graphic facsimile of the IRS forms. When the graphic facsimile was printed, Simply Tax calculated a second \_different\_ set of incorrect numbers. I would have assumed the program implemented a single algorithm, with different output options. It now appears that the software implements independent (and different) calculations, depending on which output format is selected! This complicates the debugging task.

The RISK? Aside from reliance on software that is revised every year (never debugged?), the 1040PC version threatens to further obfuscate our tax system and create a new elite of tax preparers. Since I have my taxes prepared professionally, the IRS no longer sends the forms and instructions. How comfortable will I be signing next years 1040PC, which I can not decipher, in the face of suspected bugs? The IRS is moving away from graphic facsimiles, so that may no longer be an option. In future, expect to file taxes by hand, 1040PC, or electronically. Graphic facsimiles will be allowed only if identical to the IRS form including the color of the ink (you'll need a full color printer).

My EA believes that the programmer was not a tax expert. Unlike straight line programming, tax forms have backwards references (to wit, my incorrect transfer from line 25 to line 4 on the same form). He suggests tax software be tested by former IRS agents with experience preparing taxes for the public (there are many such qualified individuals).

The IRS, with uncharacteristic understanding, is requiring only the tax and interest, waiving the penalty for an "honest" error. Have they recognized a software bug? My EA insisted on paying the interest (a paltry 0.5% per month).

Apparently there is a preparer's code covering this. CA, on the other hand, is under no such obligation. In most industries, a defective product is exchanged, refunded or repaired by the seller. With the short use life of tax software, CA assumes no such liability. According to one theory, profits are maximized when the cost of quality assurance equals the cost of defective returns. When there is no cost to the seller for defects, quality will be minimized :-{

Craig A. Smith, Solid State Electronics Center, Honeywell Inc., 12001 State Hwy 55 Plymouth, MN 55441-4799 (612)954-2895 smithc@ccsvax.ssec.honeywell.com

[By the way, the IRS endorses none of the tax preparation programs, and is not responsible for any errors they may cause. PGN]

## IRS SSN risks may abate

Michael Gerlek <gerlek@cse.ogi.edu>

Wed, 6 Jul 94 13:13 PDT

>From the Wall Street Journal, 6 Jul 94 (pg A1, col 5):

IRS officials are considering removing Social Security numbers from the mailing labels taxpayers stick on their returns. The reason: "Some concerns about privacy," an IRS spokesman says.

-[mpg] gerlek@cse.ogi.edu

[Good news! I raised that topic along with some related problems raised by RISKS readers (such as the amount of the check peeking through the envelope window) at my IRS Commissioner's Advisory Group meeting in DC three weeks ago. I'm delighted to see a speedy reaction! PGN]

---

## Re: Fraud on the Internet (Kabay, [RISKS-16.19](#))

Jeff Barber <jeffb@sware.com>

Wed, 6 Jul 1994 09:03:50 -0400 (EDT)

>[Comment from Michel E. Kabay:]

>[...] perhaps these frauds will eventually lead to requirements for  
>effective identification and authentication of users. Ultimately, it would be  
>helpful to see non-repudiation as a feature of all electronic communications.  
>For the time being, caveat lector.]

I find it distressing though not necessarily surprising that Dr. Kabay would "solve" this "problem" by requiring more stringent I&A. My own reaction was that the "unscrupulous" investors got exactly what they deserved. Do we really need to require users to show their identification papers before they can participate on the Internet?

Jeff Barber        jeffb@sware.com

---

## Signatures in electronic commerce

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>

05 Jul 94 23:26:34 EDT

[Ben Wright, an attorney teaching the online seminar on The Law of Electronic Commerce in the NCSAFORUM of CompuServe, has granted permission to post the following article on signatures. I recommend that it be posted in RISKS because it addresses assumptions about the need for non-repudiation of contracts--an area which has been fuzzy for many of us. I hope it will be as useful for others as it has been for me. --MK]

<<

---

**Re: Scary (Horning, [RISKS-16.19](#))**

*Peter J. Denning <pjd@cne.gmu.edu>*

*Wed, 6 Jul 94 15:34:19 EDT*

Political prevarication is part of the scene, unfortunately, and part of the reason that politicians are finding themselves faced with term-limit referenda around the country. (I support those movements.) At the same time, I am not "scared" by the prospect that Perot (or any other) might tell me "promises" that are tailored for me and antithetical to the "promises" that he makes to you. Why? The same technology that enables him to do that enables him to be revealed. Many of the people who get such tailored notes are going to compare notes on public bulletin boards. Prevarications, if they exist, will be instantly revealed and the candidate discredited. This will help prevent them from getting elected. Let them reveal their stripes early, I say. Let the prevaricators be detected before election, not after.

Peter

---

**Just the Facts, Ma'am (was Re: AI to screen bad from good cops)**

*David Honig <honig@buckaroo.ICS.UCI.EDU>*

*Wed, 06 Jul 1994 13:08:00 -0700*

In Volume 16 : Issue 20 : pjt1@scigen.co.uk (Piers Thompson) worries about the legal implications of screening cops for attributes shared with bad cops, when attributes include race and gender.

In machine learning work I once came across, techniques that automatically build decision processes were applied to known data to estimate students' expected performance in college. These techniques find the most information-theoretically useful attributes and use these to sort new instances. It turned out that race was found to be a very useful attribute in making predictions in this domain, but for political reasons the decision process had to be doctored to exclude this.

I think similar things have been found in financial areas, eg., predicting loan defaults.

(NB: Since present politics allows age and geographical discrimination, auto insurance companies can and do use these properties in their assessments.)

---

**Re: Video cameras in City Centres ([RISKS-16.20](#))**

*Robert Allen <Robert.Allen@eng.sun.com>*

*6 Jul 1994 20:24:40 GMT*

An interesting report. Even more interesting to me because I first read about the efforts to instrument society w/ video cameras in a comic book about 5 years ago, and the comic had been written at least 10 years ago. For those

interested in seeking it out, the comic was a limited series (perhaps 10 issues) called V for Vendetta. It was written by an English author (I believe it was Alan Moore) who had a 1 page editorial in one of the issues wherein he decried the slide of English society into what he saw as facism. In his preface he wrote that he hoped to get himself and his family out of England as soon as possible because of what he saw happening to society. I believe he specifically mentioned TV cameras on street corners, and these were definitely central to the story. They also had audio pickup capability, and vandalizing them was a capital crime. The story dealt with how the English gov't became facist after a 3rd world war. "V" is a lone hero (?) who bucks the system, assassinating various gov't figures, with an ending I won't spoil for you.

Life imitates art. The complete series is available at any decent comic book store (check your yellow pages) or even a large book store, in bound, graphic novel format.

Robert Allen, rja@sun.com

---

## Digitized CC Signatures

*Eric Richards <ericr@SSD.intel.com>*

*Wed, 6 Jul 94 13:29:03 PDT*

While buying a bag of cat food at a local PetCo, I was asked to sign my credit card receipt upon the machine that printed the receipt out. After the receipt was torn from the machine, I noticed that I had written my signature on a rubber pad of some sort. I asked the young lady what exactly this was.

She then went into a cheerful explanation of this machine, showing me how it keeps a low resolution digitized "picture" of the customer's signature. She put it into test mode and had it print her signature back out.

Her final comment raised my eyebrows: the full system will simply digitize the customer's signature and keep it as proof of purchase. No second copy at all -- the customer keeps what the customer signs.

There are, however, a few bugs to fix first, she admitted.

I haven't seen discussion of this machine before and casual examination of the machine didn't reveal the name of the company that makes it. I'm not especially thrilled of the notion that someone can have a digitized version of my signature. Does anyone else have information about the machine and/or comments on risks of this CC machine's use?

---

## Re: Shopping Risks... (Banks, [RISks-16.18](#))

*Jane Anna LANGLEY <squirrel@mundil.cs.mu.OZ.AU>*

*Fri, 1 Jul 1994 11:47:13 +1000*

In Australia there is a code of practice for supermarkets that use scanners.

Here if the item scans at a price higher than the price shown on the shelf you are entitled to receive that item free. If you are purchasing several of the same item and this happens, you get one free and the rest at the lower price.

Of course supermarkets do not go out of their way to draw your attention to this, although some state it on a tiny sticker at each checkout. A few months ago an elderly couple who had some difficulty with English were ahead of me in the checkout queue when one of their items scanned at a higher price they complained, and the checkout operator's did not know about the code of practice. I pointed out the store's stated policy to both the customers and the operator, who then referred it to the supervisor.

If you want to avoid being ripped off at the checkout, find out if there is such a code of practice in your area, and make sure your supermarket sticks to it. If they don't, make a complaint or go someplace else.

Jane



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 16: Issue 22**

**Saturday 9 July 1994**

## Contents

- [Roller coaster accident -- computer blamed](#)  
[Jonathan Moffett](#)  
[Marcus Marr](#)
- [Re: Tax Software to Avoid: CA Simply Tax](#)  
[Rick Smith](#)  
[Barry Margolin](#)
- [Re: Risks of vote fraud](#)  
[Lawrence Kestenbaum](#)
- [Literary treatment of street-corner cameras](#)  
[Mark Seecof](#)
- [Re: Just the Facts, Ma'am](#)  
[Bob Frankston](#)
- [Re: Mosaic risks](#)  
[John R Levine](#)
- [Any data of Bill Gates's Info-highway book?](#)  
[Richard Botting](#)
- [Re: A330 crash](#)  
[Curtis Jackson](#)  
[Peter Ladkin](#)
- [Re: ACM Crypto Policy Statement](#)  
[Nap & Erik van Zuuren](#)
- [Re: Fraud on the Internet](#)  
[D. Owen Rowley](#)
- [EMI of 'VW? NOT!](#)  
[Chris Norloff](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Re: Roller coaster accident -- computer blamed

*Jonathan Moffett <jdm@minster.york.ac.uk>*  
*Fri, 08 Jul 1994 11:32:16 +0100*

27 Hurt in Roller-Coaster Train Crash  
By Victoria Combe, London Daily Telegraph, 8 July 1994

More than 20 people were hurt last night in an accident on the world's highest and fastest roller-coaster at Blackpool's Pleasure Beach. Two trains on the new 12 million pounds ride, The Big One, collided 30 feet above ground. Eight passengers, trapped by jammed safety bars, had to be cut free. 27 people were taken to hospital with minor injuries, while others were treated for shock. The ride's computer-driven trains reach 85 mph but had slowed to 40 mph when the crash happened.

The Pleasure Beach said "One train collided with the rear of another which had stopped in the braking system. "At the moment we have no idea how this could have happened. The fullest enquiries are being undertaken." Mr Geoffrey Thompson, the Managing Director said: "I have asked the American designer to return as quickly as possible. Until then the ride will be shut."

On the roller-coaster's first day, May 28, 30 people were trapped 235 feet up after a fault in the computer system.

[Mr Thompson said on BBC Radio 4's Today programme this morning that the collision had taken place at 5 or 6 mph, not 40 mph. (quote from memory)]

Jonathan Moffett Dept of Computer Science University of York, UK

[5 or 6, not 40? Big difference! But probably not 50 or 60...  
American designer, eh? Perhaps the same one that did the Timber Wolf at KC's Worlds of Fun ([RISKS-9.96](#)) and Hercules at Dorney Park ([RISKS-14.83](#)), both of which had crashes? PGN]

---

## Re: Roller coaster accident

Marcus Marr <marr@dcs.ed.ac.uk>

Fri, 8 Jul 94 15:39:31 BST

[More on same from television news (ITN, 10pm, 7th July)...]

[...] Because the passengers needed to be cut out, I would assume that the safety bars worked as designed (they failed locked rather than failed open, especially important for the inverted loops), though an unlocking mechanisms may have been a useful addition.

Marcus

---

## Re: Tax Software to Avoid: CA Simply Tax (Craig, [RISKS-16.21](#))

Rick Smith <smith@SCTC.COM>

Thu, 7 Jul 94 18:16:42 CDT

The essence of this 1040PC RISK is that a signature on the 1040PC does not indicate that the filer understands and agrees with what it says. A readable version is absolutely required to make an informed decision. I prepared my 1040 with personal tax software this year and submitted 1040PC. I keep printed

copies of the full return as well as the PC version for my records. They matched up well enough to sign.

I find it incredible that a preparer only provided the PC version for review and signature. At the very least the preparer should submit both versions for review. In Craig Smith's case, this would have flagged the fact that buggy tax prep software was being used. If the two didn't match, he shouldn't have signed either, and perhaps should have looked for a different preparer.

Today, the IRS accepts their own printed forms, facsimiles produced by particular software packages, 1040PC, and electronic filing. For years, the IRS has accepted facsimile forms generated on "letter quality" dot matrix as well as plain laser printers. They have never required reproduction the colors appearing on their original forms. While I believe the IRS will widen their use of machine readable input, I don't believe the IRS could eliminate readable forms even if they wanted to. There are too, too many people in this country that just don't get it when it comes to encoded line numbers and other such intangible stuff. They'd suffer a really sharp rise in compliance problems if they eliminated "real" forms (a similar argument applies to the likelihood of a completely cashless society).

I have been a consumer of tax software for several years and have some perspective on the problem with "bugs." The bottom line is that the tax software vendor had better not sell buggy software two years in a row, or nobody will come back for Year 3. There is a competitive market for tax software and unreliable products suffer a deserved disadvantage.

Regarding "endorsement" of tax programs, there does seem to be a process by which the IRS will "approve" the appearance of signable forms generated by various tax programs. There's no implication that they approve of the programs' tax computations, just the appearance of critical forms like 1040.

Rick Smith smith@sctc.com roseville, minnesota

---

### **Re: Tax Software to Avoid: CA Simply Tax (Craig, [RISKS-16.21](#))**

*Barry Margolin <barmar@Think.COM>*

*Fri, 8 Jul 94 16:25:45 EDT*

>Apparently there is a preparer's code covering this. CA, on the other hand,  
>is under no such obligation. In most industries, a defective product is  
>exchanged, refunded or repaired by the seller.

While there's no legal obligation, and CA may not have such a policy, note that some other tax software vendors do. I believe ChipSoft promises to pay any penalties you incur due to a miscalculation by Macintax or TurboTax.

Barry Margolin System Manager, Thinking Machines Corp.  
barmar@think.com {uunet,harvard}!think!barmar

## Re: Risks of vote fraud (Rushton, [RISKS-16.14](#))

Lawrence Kestenbaum <22914LCK@msu.edu>

Thu, 07 Jul 94 20:10:02 EDT

It often seems to take people by surprise when they realize how lightly secured voter authentication is in most elections. Thomas Rushton's note, and some of the replies in 16.15, are typical examples. This concern, coupled with deep cynicism about politics, leads people to generalize this "lack" of security into a vision of a risky process open to easy fraud and stolen elections. But this conclusion is wrong.

I'm not specifically familiar with voter authentication and balloting practices in the UK, Canada or Massachusetts. What is described, though, sounds substantially similar to practices here in Michigan, where I have been a voter, an election worker, and a county commissioner.

Michigan voters receive a voter registration card, but it plays no role in the actual voting process. Indeed, no identification card of any kind is required; if presented, it is waved away.

The voter fills out a slip of paper with name, address and signature. Supposedly, the signature on the slip is verified against the signature in the voter files. In truth, almost any signature will do. The training for election workers doesn't discuss this step; especially in busy precincts, the signature may not even be glanced at. In any case, the card with the voter's official signature is a public record, which anyone could have inspected prior to election day.

Another way to "spoof" the process would be to register to vote multiple times -- no proof of identity is required.

Thus, it would be easy for a miscreant to vote twice, three times, a dozen times. So why aren't we worried about this?

The fact is that Michigan's election laws have evolved over a century and a half of responding to different kinds of fraud and vote buying schemes. (For example, if a voter reveals or displays his ballot in the polling place, it is invalid.) Most other jurisdictions have had similar experiences. Considering both the laws and the practicalities, effective vote fraud is very difficult to do.

First, the law: vote fraud is a felony. The penalties are in the same range with things like arson and armed robbery. Certainly there are people who are willing to commit felonies, but most people are not. The public thinks of vote fraud as being a crime of serious moral turpitude, something more like stealing cars than exceeding the speed limit. Moreover, a perpetrator of vote fraud is at serious risk of being caught; and the more people who are involved, the greater the risk. On the other hand, the fewer people who are in on it, the more difficult it is to "spoof" a sizable number of false votes.

The nature of the political scene magnifies this problem. Practically by definition, someone who wants to commit vote fraud has to be a person

with some investment in the political process. Scoffing about politicians aside, practically all of them are strongly motivated to avoid any taint of criminal activity. Though there have been cases where a sitting officeholder has been re-elected despite indictment or conviction, on the whole it usually spells the end to one's political career. Further, a felony conviction in many states (though not Michigan) terminates one's voting rights as well.

But there's still another problem: until the vote totals start to appear, it is never clear how many stolen votes would be needed, and for whom. Polling can't tell you this -- not with the requisite degree of precision. The costs and risks of vote fraud are pointless if your candidate is winning anyway, or losing by too wide a margin.

Effective election stealing (with a minimum of co-conspirators) requires knowing exactly how many votes you need. Thus, it has to be an "inside job" and happen AFTER the polls close.

The most famous American vote fraud of all time, Lyndon Johnson's stolen victory in the 1948 Democratic primary runoff for U.S. Senator from Texas, took place AFTER it was known that Johnson was 115 votes behind his opponent, Coke Stevenson. Word was passed to George Parr, the infamous "Duke of Duval," with a plea to come up with at least that number of votes; and Ballot Box #13, Alice TX (with 202 votes for Johnson and none for Stevenson) showed up THREE DAYS after the election. LBJ was declared the winner by 87 votes.

I'd guess that Texas in 1948 was far more corrupt than any state is today. In any case, the political process \*does\* sometimes learn from experience; the most exacting safeguards in election law have been built around the (vulnerable) tabulation and reporting phase.

Lawrence Kestenbaum, School of Criminal Justice, Michigan State University  
22914LCK@msu.edu

---

## Literary treatment of street-corner cameras

*Mark Seecof PSD x77605 <marks@bierce.latimes.com>*

*Thu, 7 Jul 1994 14:12:39 -0700*

The social implications of street-corner (etc.) cameras have been the subject of literary exploration for much longer than 10 years. For a particularly deep (though not exceptionally old) fiction treatment I refer you to David Drake's stories about a character named Jed Lacey, last collected in full I believe in a paperback titled "Lacey and his Friends." Drake explores the implications of cameras everywhere. Just to name one, people might be forced to share their living and work space with many others to minimize the number of cameras required (separate offices would require many cameras, bullpens could be covered by a few). Mark Seecof <marks@latimes.com>

---

**Re: Just the Facts, Ma'am (was Re: AI to screen bad from good cops)**

<Bob\_Frankston@frankston.com>

Thu, 7 Jul 1994 17:32 -0400

The issue of screening is an old one. I've already pointed, in RISKS, that arrest records are probably a very good predictor of whether one is guilty. But arrest records are not conviction records! Some of the problems arise because such statistical analysis denies the individual's ability to depart from the stereotypes. If I was once mistaken for someone who robbed a liquor store because I happened to have a beard at some point in my life, am I now less entitled to protect from unreasonable searches? Or does my profile mean that I am now subject to extra scrutiny.

I might accept the idea of a profile in airport security (fallible though the approach is). I'm much more reluctant to accept it if it denies an individual opportunity.

Of course, this assumes that the statistics and analysis are meaningful -- a very big assumption.

---

**Re: Mosaic risks (Jawdat, [RISKS-16.20](#))**

John R Levine <johnl@iecc.com>

Thu, 7 Jul 94 12:17 EDT

[re the Spyglass version of Mosaic, and using it for credit card transactions]

There are several licensees of Mosaic who are building their own enhanced versions of the program. As far as I can tell, the primary security feature that is likely to be added is some sort of public key digital signature, so a client can send a message to a server in a presumably unforgeable way.

> Also, sources to various NCSA projects are not particularly difficult to  
>find (I found Telnet on wuarchive, and I've seen Mosaic at CMU) - with access  
>to Mosaic sources people could build fakes of the commercialized Mosaic to  
>trap credit card numbers.

This Trojan Horse threat is indeed a possible one, although it seems to me that the same "safe software" techniques that one uses to avoid getting a virus with one's PC software would be appropriate to avoid getting Trojan MosaiCs.

Regards,

John Levine, johnl@iecc.com, jlevine@delphi.com, 1037498@mcimail.com

PS re Trojan MosaiCs: Actually, most of the mosaiCs in that part of the world are Byzantine, but from what I've heard about the internals of the Mosaic source code, we have a Byzantine Mosaic now.

---

## Any data of Bill Gates's Info-highway book?

*"Dr. Richard Botting" <rbotting@wiley.csusb.edu>*

*Sat, 9 Jul 1994 11:07:40 -0700*

In the July 6th 1994 issue of our local paper - The San Bernardino Sun-Telegram there is an odd letter from one Daniel Jeffs of Apple Valley, date June 29th.

I'm not sure if I'm seeing evidence of the RISK of luddite paranoia or a useful early warning of a real risk to the public. It states that Bill Gates "is authoring a book about the information highway" which "will provide you with a left-handed warning about what's in the works for us" [...] "your PC will be miraculously be replaced and transformed into your PE(Personal enslaver) and PD (personal demon)"[...].

So far I'd suspect a clever publicity stunt... but the letter ends with an appeal for "unselfish foresight and vision"[...] "traffic controls of public policy in the hands of all people"[...]

So

- (1) Does Bill Gates vision actually imply a RISK worse than any other vision?
- (2) Have similar letters been appearing in other local papers - a mail merged version of internet spamming?

Dr. Richard J. Botting, California State University, San Bernardino, CA 92407  
Copyright(1994)Copy and use as long as you include this copyright and signature.

---

## A330 crash

*Curtis Jackson <cjackson@adobe.com>*

*Fri, 8 Jul 1994 23:33:43 GMT*

The confirmation of the A330 crash stated that "the altitude of the aircraft was too low to avoid impact with the ground."

Perhaps there is additional information that was withheld in the name of brevity, but why would Airbus conduct such an amazingly dangerous test so bloody close to the ground? If they were just after maximum aft centre of gravity, high angle of attack, and maximum climb, why couldn't they do the same at 2000 metres? At least until they got it right at altitude, and only \*then\* bring it down to ground level and simulate it shortly after a real takeoff.

Perhaps we in the software industry should take a cue from Airbus. For instance, network software developers should start testing their pre-alpha catastrophic failure recovery code on live heavily-trafficked networks...

Curtis Jackson cjackson@mv.us.adobe.com (preferred) or dod721@aol.com

## The Scoop on the A330 Accident [3rd Version - see 1st note]

<Peter.Ladkin@loria.fr>

Sat, 9 Jul 1994 19:09:39 +0200

Air et Cosmos, 11-24 Juillet 1994, p15, contains an extensive report on the A330 accident of 30 June 1994 by Jean-Pierre Casamayou. The general story has been reported by Peter Mellor ([RISKS-16.19](#)). The new info is highly relevant, and implies that control of the aircraft was lost while the aircraft was under automatic control. This is the first case, to my knowledge, in which this has been proved to have happened to Airbus aircraft, without any concomitant pilot error. Sadly, the test pilots allowed the departure from control to continue for up to 12 seconds in order to analyse the incident. This delay was gallant but fatal. That's the English for you (RIP Capt. Nick Warner).

The autopilot was using experimental software. This A330 was undergoing a flight test required for certification of the autopilot for Category III operations with Pratt and Whitney 4168 engines (the other A330's already in operation use CF6-80E1's, and such equipment has already been through this particular flight test sequence). Category III operations mean use of the autopilot for landing, up to and including main gear on the runway, and requires special certification of both aircraft and crew. It follows that a Category III operation can potentially be aborted, i.e. the pilots can select go-around while under autopilot control, with the main gear on the runway, and in the worst case an engine can fail at this point. One can see why it's required to conduct this test from an actual takeoff, rather than at altitude.

The flight was supposed to test the mode SRS (speed reference system) of the autopilot, which should control the speed and angle of attack (AoA) of the aircraft in case of an engine-out. AoA is defined to be the angle that the wing makes with the undisturbed airflow in front of the wing. The test was performed at rearmost center-of-gravity.

Following is a translation of a continuous fragment of the article. I have included the originals of phrases I am unsure of. My thanks to Pete Mellor for confirmation of some of the meanings. I don't have a dictionary of French aeronautical terms (although such exist, and they're quite large). It refers to the following 'V-speeds', defined in FAR Subchapter A Part 1 Para 1.2 for those in the US. V<sub>1</sub> is takeoff decision speed (the speed at which the decision is made to abort or to continue takeoff in the case of engine failure); V<sub>R</sub> is rotation speed (the speed at which the pilot commands nose-up); V<sub>2</sub> is takeoff safety speed (the speed at which the airplane may takeoff safely, even with one motor out); V<sub>{mca}</sub> is the minimum single-engine control speed (the speed at which control of the aircraft may be maintained with one engine out).

[begin translation]

The takeoff (V<sub>1</sub> = V<sub>R</sub> = 126kts and V<sub>2</sub> = 135kts) took place at 136kts, 25 seconds after full power was arrived at ('la mise en plein puissance des moteurs'), then the aircraft took its speed of climb of 150 kts. After the takeoff, an altitude of 600m QNH (roughly 460m QFE) was selected on the flight

director FCU [the Flight Director on the A330 is called the FCU. pbl] This means that the aircraft should restore level flight [‘retablir en palier’] at 450m from the ground.

Conforming to the test order, the pilot attained a speed of 150 kts, and 28 degrees AoA in order to maintain this speed. Six seconds after takeoff, the autopilot was engaged, then the left engine retarded and the corresponding hydraulic pump cut to simulate a complete failure of the left engine. As predicted, the AoA began to diminish and passed from 29 degrees to 25 degrees, the limit authorised by the FMGES (Flight Management Guidance and Envelope System) which protects the flight envelope. But quickly, because of the low altitude selected on the FCU, the autopilot departed from mode SRS and entered mode ALT-STAR, the mode for acquisition and retention of altitude, in which mode the autopilot tries to attain altitude as quickly as possible, without taking into account the limiting conditions that the airplane was in: rear most CoG, one engine retarded and the other at full power, high ‘incidence’ [another word for AoA. pbl] [this is not a good explanation of ALT-STAR mode. pbl]. Result: the AoA started to increase again, and the speed decreased extremely quickly [‘brutalement’].

The flight team noted immediately the anomaly, but purposely let the situation degrade for about 12 seconds, in order to analyse it better, as is their role. The AoA attained 33 degrees with speed decaying to 100kts, which is 18kts less than  $V_{\{mca\}}$ , the minimum single engine control speed . At this moment, the pilot disconnected the autopilot and took over control. But the speed continued to decrease. At about 90 kts, 28kts less than  $V_{\{mca\}}$ , the aircraft departed in a stall [‘part en décrochage’] to the left with an angle of bank [‘angle de roulis’] which attained 110 degrees.

The pilot reacted quickly and well in retarding the right engine then bringing the wings horizontal. Unfortunately, because of the low altitude and fast rater of descent, he couldn't avoid impact with the ground, 35 seconds after takeoff.

[end translation]

Peter Ladkin

---

## Re: ACM Crypto Policy Statement (ACM, [RISKS-16.20](#))

*Nap & Erik van Zuuren <100042.3164@compuserve.com>  
07 Jul 94 11:18:15 EDT*

On the ACM Crypto Policy Statement -- to which I strongly agree - and all the discussions on Clipper and associated phenomena, I would like to state my opinion with my European mind and my European trust in some of our authorities; in this case our Police authorities. All the meddling of the National Security Agencies ( not only the U.S.A.'s NSA ) with reference to Sealing, Signing -- and last but certainly not least -- Encryption is very hard to understand, as for their own and MIL data/voice traffic these authorities up to now use their own means. They want to go COTS ( Commercial Of The Shelf ), but have a problem in stating the categories of "time of

protection" wanted for strategic, tactical and 'national interest' information, thereby making it difficult for COTS-suppliers to help them out the "COTS" way.

RE: The "listening in" part:

- 1) For some purposes, one could even make a statement through "clear" telephone, which has a different meaning to the intended recipient; thus "listening in" is of 'no' use, even for a "clear" communication
- 2) It is a "bloody shame", and the CEC-INFOSEC ( European Commission-INFOSEC ) people know my opinion on that for a long time now, that not all data-communications is enciphered in some "standardised" way, just to have a 'general' barrier against 'criminal energy'.  
The adversary then has to spend processing power = money to decipher and will lose out by using money on -- for him -- unuseable information.
- 3) The only way, to solve the legal part, is NOT to forbid encryption, but provide legislation on the obligation of 'handing' over the required info on mechanism(s), algorithm(s), and key(s) used, if required -- case by case -- in proven law cases [ to be edited by a lawyer, specialised on the subject ]
- 4) Just as a reaction on what is going on, the use of PGP ( even 2.6 ) is exploding over here; and a European EFF will be there within short.
- 5) Furthermore many European RSA-based, FEAL-based and "other"-based products are on the market, and in use !

RE: Relation to "Police Forces", including e.g. Criminal Investigation Teams:

Apparently the some European Police Forces, and related Forces, are still considered -- in general -- to be the "friends" of the population, by the population. The requirements for reaching such a relation with the 'public' are:

- to be "of assistance to the public"
- trustworthy staff
- to be a trustworthy organisation, accompanied by a free press and political will
- to be supported by the judicial apparatus, for the Forces to stay motivated
- a "quality of life" worth defending it

We will need a lot of "trustworthy" energy to protect us -- and our children -- against "criminal" energy.

Our Police organisations use several means to protect access to their various Databases, and this protection has to be the strongest available, because of the 'real risks' involved.

I fully agree with the following statements in the article by Ted Bunker in LAN Magazine of August 94:

- "We must give our full support to the development of OPEN international security standards, that protect the interests of all parties fairly
- There is a "constant" tension between the need for privacy and the need for protection

- We do have serious privacy concerns
    - NOTE: e.g. when a Police official is performing an SQL request on a number plate, the official in the van should only get information on:
      - whether the car is looked for
      - whether the probable driver is looked for
      - whether the probable driver might be armed
- and nothing more, surely not the address of the pretty lady-driver !

Do NOT get me wrong:

- I also fell victim to injustice ( to my opinion ) in a case versus an 'official'.
  - I even have been insulted in writing by a member of the Council of Ministers.
- But, we have to trust ( and at the same time: control ) the forces which should protect the "law-abiding" ( or = sullen ? ) citizen, and are paid by that same citizen to do so ! Might be the price of "democracy".

Nap van Zuuren, CompuServe 100042,3164

---

### Re: Fraud on the Internet (Barber, [RISKS-16.21](#))

*"D. Owen Rowley" <owen@autodesk.com>*

*Thu, 7 Jul 1994 11:53:58 -0700*

> ... Do we really need to require users to show their identification  
>papers before they can participate on the Internet?

Your reaction is naive. The short answer is yes.

However, there is no \*the internet\*, what you refer to is an internetwork of internetworks. The current popular conception is to have one huge internetwork that serves all needs and desires of all participants all the time in all of its parts. In short - I don't think so.

Just as we zone our physical space, we must zone our data-space. Our internetworked services and data-spaces, must provide proper security in the form of authentication and authorization for those transactions that absolutely require such. Our internetworked services and data-spaces, need not provide over-zealous security with absolute authentication and authorization for those transactions that don't require it. ( or where such is undesirable).

This whole ball of wax falls into what I call The Un-real estate business.

LUX ./ . owen Inner Zone Unrealty Co.

---

### EMI of 'VW? NOT! (Elana, [RISKS-16.17](#))

*<cnorloff@tecnnet1.jcte.jcs.mil>*

*Fri Jul 8 07:59:16 1994*

[No, I did NOT make this post up!!! Elana]

> ... I heard that if you had high enough RF power  
>you could disturb the electric fuel pump, so I tried this one day using  
>a 600 Watt PEP amp and keyed an AM carrier, and what did I see???

SOMEBODY is making this up! 1963 VW Bugs had a MECHANICAL fuel pump (a fact I am totally certain of). I believe VW Bugs at least until the 1970's had a mechanical fuel pump.

Good story, but only a story.

Chris Norloff cnorloff@tecnnet1.jcte.jcs.mil



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 16: Issue 23**

**Weds 13 July 1994**

## Contents

- [Inmates con jail computer](#)  
[Peter Ilieve](#)
- [White House Buys Off EES Patent Holder](#)  
[Brock N. Meeks via Stanton McCandlish](#)
- [New National ID Card Proposal](#)  
[David Banisar](#)
- [SimCity](#)  
[Phil Agre](#)
- [Teletext run amok](#)  
[Michael J. Stern](#)
- ["Glyphs" may track your demographics](#)  
[Walter C. Daugherity](#)
- [EMI of 'VW'? YES](#)  
[Rick Cook](#)
- [Correction to A330 report](#)  
[Peter Ladkin](#)
- [Re: Promises and "Scary"](#)  
[Phil Agre](#)
- [Laptop Danger for Airplanes](#)  
[Dan Arias via Martin Howard](#)
- ["If Ajax had a good computer system, Peter would still be alive."](#)  
[Daniel P. B. Smith](#)
- [Re: Roller coaster accident -- computer blamed](#)  
[Clive D.W. Feather](#)
- [Re: ACM Crypto Policy Statement](#)  
[Dave Golber](#)
- [Re: Phone records](#)  
[S. E. Grove](#)
- [Re: Signatures in electronic commerce](#)  
[Robin Kenny](#)
- [Re: Digitized CC Signatures](#)  
[Mark Brader](#)
- [Re: Shopping Risks...](#)  
[Philip H. Smith III](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Inmates con jail computer

Peter Ilieve <peter@memex.co.uk>

Tue, 12 Jul 94 13:14:57 BST

There was a piece under the above headline in the Times (a UK quality paper) on 5 July. The byline is Adam Fresco.

`Prisoners at a top security jail beat an expensive security system using a mirror and a piece of wire to join each other in late-night card games. Inmates at Albany prison on the Isle of Wight had been roaming around at night for weeks, unknown to staff.

`The sophisticated computerised security system was designed to end slopping out by allowing one prisoner at a time from each landing to go to the toilet during the night. [Sanitation is not the UK prison system's strong point, prisoners usually have to make do with a bucket in the corner of the cell, even if there are 2 or 3 people in the cell. Buckets are `slopped out' into a drain in the morning. PJI] By pressing a button in his cell, a prisoner was allowed out for a certain amount of time. When he returned he was supposed to punch in a number which would appear on a console inside his cell and the door would lock. The computer would then let the next inmate out.

`However, the prisoners were staying outside their cells, shutting the door and threading a wire though the hinge to tap in the required number, which they could see through the mirror, set up before they closed the door. The computer, thinking the prisoner was back in his cell, would let the next person out.

`The prisoners were found out when they made too much noise one night. An astonished guard discovered three of them in one cell playing cards.

`Max Morrison, the governor, has started an enquiry into the incidents and has turned off the system, which has been installed in other prisons around the country. A Home Office [the government department responsible PJI] spokesman declined to comment on the cost of the equipment, which was installed a few months ago, but confirmed that the computer system had been suspended and alternative sanitation arrangements introduced.'

Peter Ilieve peter@memex.co.uk

---

## Administration Buys Off EES Patent Holder (fwd)

Stanton McCandlish <mech@eff.org>

Tue, 12 Jul 1994 17:52:21 -0400 (EDT)

Date: Mon, 11 Jul 1994 14:53:56 -0700

From: "Brock N. Meeks"

---

## New National ID Card Proposal

David Banisar <Banisar@epic.org>

Tue, 12 Jul 1994 20:11:46 -0500

CBS Evening News just reported that Clinton has "tentatively signed off" on a National ID card recommended to him by a commission on immigration reform. The ostensible reason for the card is for employment and immigration. Each card will contain a name, photo, mag stripe with info and a "verified SSN." It was supported by Senator Alan Simpson of Wyoming, a long-time supporter of ID cards. Gov. Pete Wilson of California has apparently offered to make California a test-bed for the proposal. The proposal was opposed by Xavier Beccera, a Congressman from California. A previous effort to impose a national ID card was rejected by Congress in 1986.

EPIC is working with Privacy International to investigate this report. PI has led successful campaigns against national ID cards in Australia, New Zealand, and the Philippines.

In Australia, the PI-led campaign led to the dissolution of both houses of the federal Parliament in 1987 after hundreds of thousands marched in protest. The Australian campaign brought together groups from all parts of the political spectrum from the Communist Party to the Libertarian Alliance, farmers and conservation groups, rock stars, academics, large businesses such as banks and mining corporations, but the overwhelming support came from the public who created the biggest civil protest in Australian history.

David Banisar (banisar@epic.org) Electronic Privacy Information Center  
666 Penn. Ave, SE #301, Washington, DC 20003 202-544-9240 (v) 202-547-5482 (f)

---

## SimCity

Phil Agre <pagre@weber.ucsd.edu>

Tue, 12 Jul 1994 16:25:35 -0700

The spring issue of the liberal journal "The American Prospect" includes a detailed critique of policy simulation programs such as SimCity. The full reference is:

Paul Starr, Seductions of Sim: Policy as a simulation game, The American Prospect 17, Spring 1994, pages 19-29.

The gist is that the real politics of policy and its implementation are much more complicated than the basic framework of such simulations can possibly accommodate.

Phil Agre, UCSD

---

## Teletext run amok

"Michael J. Stern" <stern@panix.com>

Sat, 9 Jul 1994 16:35:21 -0400

The following comes from *\_New Scientist\_*, 21 May 1994.

#### FEEDBACK

JOHANNA Darlington often watches the news on television with her mother, who is deaf and relies on teletext to follow what is broadcast. Darlington has discovered that the words spoken by the news-caster and the words on the teletext frequently disagree with each other in surprising ways. Over the past 18 months she has culled a list of teletext "translations", some of which we give below. The first words in the list are what the newscaster said, the second are the teletext version:

initially: in Italy  
romantics: Roman tricks  
Europe: querp  
Liverpool: limp pool  
nutrition: new electrician  
psychologist: sigh ecologist  
semblance: semi ambulance  
succeed: suck see  
rescue: regulars cue  
it really: trillion  
his street: history  
ozone: owe zone  
lesbians: lez beans  
solves: as far as  
categoric: cat gurk

Darlington also reports a long news item about someone called the Princess of Whales. She adds, unsurprisingly, that watching the news is sometimes a rather baffling experience for her mother. Feedback finds these errors fascinating and wonders how they arise. Is a voice-recognising computer involved? Or is our old friend the spellchecker running amok again?

/stern stern@deshaw.com stern@panix.com

---

### "Glyphs" may track your demographics

*Walter C. Daugherty <daugher@chisholm.cs.tamu.edu>  
Mon, 11 Jul 94 18:38:10 -0500*

EDUPAGE (gopher to educom.edu) cites the 7/10/94 New York Times (Sec.3, p.9):

#### ARE YOUR DOCUMENTS FULL OF GLYPHS?

A Xerox technology known as glyphs will allow documents to carry thousands of characters of information placed unobtrusively in gray background patterns. One possible use: "If you see a spreadsheet in an annual report, it sits there, lifeless on the paper. But if there was a glyph border that had the mathematical model of the spreadsheet, you could scan that into a computer and make it come to life." Another possible use would be to encode info about the recipient of a direct mail piece or a survey, for ease of processing when the document is returned. (End quote from EDUPAGE)

In that case, I'll be sure to xerox [sic] the anonymous survey form at a "light" setting to keep from telling them who I am.

Walter C. Daugherty, Dept. of Computer Science, Texas A & M University  
College Station, TX 77843-3112 daugher@cs.tamu.edu uunet!cs.tamu.edu!daugher

---

## EMI of 'VW'? YES

<rcook@BIX.com>

Sun, 10 Jul 1994 05:03:31 -0400 (EDT)

VWs of a certain vintage are indeed subject to EMI. This is a known 'bug' (so to speak) and is mentioned, I believe, in the later editions of "How To Keep Your Volkswagen Alive For The Complete Idiot" -- the standard reference for VW shade tree mechanics.

The confusion arises from two things. First, it was not the 1963 models which were affected. The '63s had a thoroughly conventional ignition and fuel system. (I have owned two of them). Second, I don't think it was the fuel pump per se that was the problem.

The problem comes in the later models fitted with the Bosch fuel injection system, one of the most misbegotten pieces of crap ever hung on an automobile. This used electronically operated injectors controlled by an on-board computer. Unfortunately the Bosch implementation as found on the 1969 or so VWs was not well designed, to put it mildly. Not only was it subject to EMI, but I am told it also had no way to adjust for the changing resistance of the wires as they aged. Meaning the thing would get flaky as it aged and there was nothing you could do about it.

The standard advice on getting a bug or squareback with Bosch fuel injection was to discard the system and replace it with carburetors. As a result I've never had much dealings with the system personally -- except for pulling it.

--Rick Cook

---

## Correction to my [RISKS-16.22](#) account of the A330 report

Peter Ladkin <Peter.Ladkin@loria.fr>

Mon, 11 Jul 1994 19:42:23 +0200

In my partial translation of the article from Air et Cosmos 11-24 Juillet concerning the A330 crash on 30 June, I translated 'assiette' as 'angle of attack', or 'AoA'. Mea culpa. 'Assiette' means 'pitch', the angle that the airplane makes to the horizontal ('incidence' is 'angle of attack'). The difference is important. Goodness knows what caused me to write that. The mistake may be rectified by replacing all occurrences of 'AoA' (except only in the parentheses in which I comment on 'incidence') by 'pitch'.

An autopilot can effectively command pitch, but not effectively angle of

attack. Whether an aircraft stalls or not depends on the angle of attack. The two concepts are related via angle of climb. Roughly,  
 $\text{angle of climb} = \text{pitch} - \text{angle of attack}$ .

Other vocabulary omitted from my article for US residents and non-pilots: QNH is indicated altitude above sea level with the altimeter set to mean pressure at sea level for that day/time (as given by Flight Control). QFE is indicated altitude above highest elevation of the field with the altimeter set to airport measured pressure. So 460mQFE = approximately 460m above the airport surface's highest point.

Peter Ladkin

---

## Re: Promises and "Scary"

*Phil Agre <pagre@weber.ucsd.edu>*

*Fri, 8 Jul 1994 15:51:25 -0700*

In [RISKS-16.21](#), Peter Denning <pjd@cne.gmu.edu> asks why I find it scary that politicians might use individually targeted communications to make personalized promises based on information from demographic databases. He considers that contradictory promises would be exposed through public bulletin boards. This is conceivable, but it's not something I'd want to bet the future of democracy on. Nobody would be stupid enough to make clearly contradictory promises to different people. Rather, extrapolating some current practices, they would find out the "hot button" themes for particular segments of the electorate and tailor strongly worded but vague statements for each group, based on its particular themes.

(Right now the most common way to find out the "hot button" themes is to call people on the phone and ask them under the guise of poll-taking. If someone doesn't have any buttons you can press, you simply say "thank you" and leave them out of your get-out-the-vote plans. The expense of this method limits its application, but once the data collected this way is pooled, stored, and merged with other available databases, the costs should come way down.)

When analyzing the pathologies of electoral systems, I think it's a big mistake to focus on "politicians". It's a system with a logic, and changing the faces won't change the logic. Quite the contrary, term limits (which PD says he supports) will intensify the role of money and campaign experts, since candidates will be even more unknown to voters on average than before. (For those outside the US, the US is currently experiencing a wave of plebiscites, promoted by a far right-wing organization, limiting political candidates to one or two terms of office.)

The computer-related Risk here pertains to the construction of the sphere of public debate. When public debate is conducted through a common medium, such as the newspaper, there exists at least a \*chance\* that public decisions that affect everyone equally will be made by the citizenry reasoning together as a group. But when every campaign has a separate channel to every voter, the whole notion of a public goes out the window, replaced by fragmentary micropublics who know they're being manipulated but cannot do anything about

it without investing enormous effort in organizing. If computer networks facilitate that organizing then that's terrific, but first we need to achieve something much more like universal access to them.

Phil Agre, UCSD

---

## Laptop Danger for Airplanes

MARTIN <MARTIN@411.uptown.com>

11 Jul 1994 17:49:31 +0800

From: Martin Howard, Hong Kong

Reposted from comp.protocols.ibmcp.tcp-ip

From: darias@netmanage.com

Subject: Laptops and Airplanes Not Recommended

Date: Thu, 7 Jul 1994 23:01:59 GMT

Here's something to think about for anyone who's considering using their laptop computer, cellular phone, or radio on an airplane.

Non-pilots should be aware that a course deviation of plus or minus 10 degrees is the maximum tolerance for an approach to landing using instruments, e.g., in clouds or bad weather. In general flying more than 10 degrees off course is considered "flying all over the sky."

This excerpt is reproduced from "Callback" which is a safety bulletin for pilots derived from the reports of pilots, controllers, and other aviation personnel to NASA's Aviation Safety Reporting System. ASRS is a research organization and not a regulatory organization such as the Federal Aviation Administration nor an oversight organization such as the National Transportation Safety Board.

--Dan Arias, Cupertino, CA

=====

Callback, Number 180, May 1994

A Monthly Safety Bulletin from The Office of the NASA Aviation Safety Reporting System, P.O. Box 189, Moffet Field, CA 94035-0189

### Flight Interference

More than 40 reports submitted to ASRS over the last few years indicate that in-flight operation of personal electronic devices by passengers may be a factor in aircraft track deviations, communications problems, and other incidents. While some crews are quick to pick up on the possibility of electronic interference, others find these events initially difficult to detect. More from this ASRS report:

\* After takeoff, we were given a turn direct to the fix. The ONS (Omega Navigation System) checked good on the ground and was used to turn towards

fix. The heading seemed good, cross-checking with the VOR. There was a strong crosswind from the northwest which made determining a quick fix-to-fix on the VOR only a rough estimate... Center gave us about a 20 to 30 degree correction to the right or north of course to intercept... We then noticed an intermittent "DR" [Ded Reckoning] light on the Omega... Jet route was intercepted and VOR track was annunciated on our FMA [Flight Management Annunciator]. We appeared to be tracking Jet route outbound when Center gave us about a 20 to 30 degree turn to the north, saying it was "a vector for climb." We were now around 25,000-27,000 feet. The VOR fluctuated 30 to 40 degrees again, settled down, and we appeared to be south of course. Upon intercepting Jet route, Center gave us a left turn of 10-20 degrees and said we were established on Jet route and to continue our flight planned course... [This] was a surprise to us since we had not been apprised we were off course initially...

After level-off, the Captain went back through the cabin and found a portable radio with headset in use. A cellular phone was also found on, although its owner claimed it had not been used. We believe the VOR fluctuations and navigation problems could have been caused by these items... Several passenger announcements were made explaining the importance of leaving these items off as well as the required announcements concerning electrical items.

#### Loss of EFIS and Autonav

\* During climb EFIS [Electronic Flight Instrumentation System] screens blanked suddenly, then indicated missed approach fail along with loss of all auto nav functions. We immediately reverted to manual lateral nav and kept the aircraft climbing on autopilot while requesting the flight attendants to see if any personal electronic devices were in use. As this aircraft is equipped with inertial reference units that were properly aligned at the gate, it was very suspicious that a failure occurred. The flight attendants found 3 passengers using laptop computers and one listening to a portable radio. We asked that they be turned off and, after reprogramming the FMS [Flight Management System], resumed auto nav. At cruise altitude the laptops were allowed to be used... [but] the listener was asked not to use his [radio].

A serious study needs to be made of the electronic interference problem on today's modern fleets in order to resolve the issue of what the newspapers are telling the public that they may bring aboard and use in-flight. The printed material on the aircraft does not seem to be effective. While in this event no serious harms was done, the effect could have been different if the aircraft was in heavy weather flying a complicated departure or arrival...

#### Compass Deflection

\* In cruise flight at FL310 [31,000 feet] 24 NM [nautical miles] west of the VOR, the #1 compass suddenly precessed 10 degrees to the right. I asked the First Flight Attendant if any passenger-operated electronic devices were in operation in the cabin. She said that a passenger had just turned on his laptop computer. I asked that the passenger turn off his laptop computer for a period of 10 minutes, which he did. I slaved the #1 compass, and it returned to normal operation for the 10-minute period. I then asked that the

passenger turn on his computer once again. The #1 compass immediately precessed 8 degrees to the right. The computer was then turned off for a 30-minute period during which the #1 compass operation was verified as normal. It was very evident to all on the flight deck that the laptop computer operation was adversely affecting the operation of the #1 compass. I believe that the operation of all passenger-operated electronic devices should be prohibited on airlines until the safe operation of all of these devices can be verified.

#### Short Hops

Turning to a different type of flight interference, here's a report that gives new meaning to the expression, "short hop":

\* On a night flight... we had a passenger with a massive bladder attack and poor timing. Traffic was stacked up and we had a 20-minute delay in taking off. We were cleared into position on the runway behind landing traffic and prepared for an immediate takeoff ahead of traffic on a two-mile final approach. We had signaled the flight attendants (F/As) that we were taking the active runway when a passenger bolted out of his seat and headed into the lavatory. The flight attendant asked him to return to his seat. He ignored her request. She then demanded he be seated. He still ignored her command. She promptly called the lead F/A who called us in the cockpit. We cancelled our takeoff clearance and headed for the nearest exit. It was blocked by departing traffic. We then headed 2,000 feet down the runway to the next turnoff. Traffic on final approach was closing in on our tail as we departed the runway, an aircraft whizzing past our tail with precious few feet to spare. It was the quick thinking and timing of our flight attendant that allowed me the time to clear the runway...

=====

Uptown 411 Online Information Exchange

---

### **"If Ajax had a good computer system, Peter would still be alive."**

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

*Mon, 11 Jul 1994 19:41:53 -0400 (EDT)*

OK, it's fictional. I don't know if it's interesting to the RISKS readership or not, but it caught my eye. (Someone else can figure out whether it actually indicates some kind of actual RISK).

from Sara Paretsky's mystery novel, "Indemnity Only," copyright 1982, chapter 15, p. 206 in the Dell 1990 reprint:

"... one of the things they asked him to do was check records of claim drafts against claim files--see if they matched, you know. Did Joe Blow get fifteen thousand dollars when his file shows he should only have gotten twenty thousand dollars. That kind of thing. They had a computer program that did it, but they thought there was something wrong with the program, so they wanted Peter to do a manual check.... You know, if Ajax had a good computer

system, Peter would still be alive. I think of that sometimes, too, and it makes me want to shoot all their programmers."

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

---

**Re: Roller coaster accident -- computer blamed ([RISKS-16.22](#))**

*"Clive D.W. Feather" <clive@sco.com>  
Mon, 11 Jul 1994 14:58:38 +0100 (BST)*

I heard an item about this on the radio last week. According to this item, the roller coaster is of a standard design: trains are hauled up to the high point, and then run free under gravity without brakes until they approach the station. On the approaches to the station are several more braking units - movable clamps which grip the train wheels to slow it down. The system should stop each train just behind the previous one. The various stopping points are called "berths" in railway terminology.

The problem appears to be that there was one train in the station, and a second waiting to enter. The third train was braked so as to stop in the berth nearest the station (occupied by the second train), rather than the previous (empty) berth.

Clive D.W. Feather, Santa Cruz Operation, Croxley Centre, Hatters Lane, Watford WD1 8YN, UK clive@sco.com Phone: +44 923 816 344 Fax: +44 923 210 352

---

**Re: ACM Crypto Policy Statement (van Zuurens, [RISKS-16.22](#))**

*Dave Golber <dgolber@uniblab.aero.org>  
Mon, 11 Jul 1994 09:09:19 -0700*

You claim that there is no reason for the police stopping a vehicle to know the registered address of the vehicle or the driver?

"Officer, I was just going out to buy some groceries."

"But why do you shop for groceries 150 miles from your home?"

Sounds pretty believable to me.

I think this is more than just me being picky. Rather than me trying to explain why, just ask yourself, Dear Reader: Why did you first read Mr van Zuuren's statement as being reasonable? What does that tell you about your own prejudices?

Dave Golber

---

**Re: Phone records (Weinstein, [RISKS-16.20](#))**





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 16: Issue 24**

**Thursday 14 July 1994**

## Contents

- [Quoth the Maven, Livermore! \(porno repository\)](#)  
[PGN](#)
- ["DUMB FROGS AHEAD"](#)  
[Tom Zmudzinski](#)
- [Digital display boards on highways](#)  
[Jason Hanson](#)
- [Mailers that add "Company Confidential"](#)  
[Paul Szabo](#)
- [Scams](#)  
[Phil Agre](#)
- [Re: Secure use of Internet](#)  
[Tom Patterson](#)
- [Re: Shopping Risks...](#)  
[Philip H. Smith III](#)
- [Re: Brock Meeks article on Clipper](#)  
[Jerry Leichter](#)
- [Cellular phone risks/privacy](#)  
[Phillip Brown](#)
- [Literary treatment of street-corner cameras](#)  
[Scott Dorsey](#)
- [Teletext](#)  
[Bob Richardson](#)  
[Clive D.W. Feather](#)  
[Bob Frankston](#)
- [Re: Laptop Danger](#)  
[Bob Frankston](#)  
[Joe Chew](#)  
[Lars-Henrik Eriksson](#)  
[Tony Abo](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Quoth the Maven, Livermore!

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Wed, 13 Jul 94 13:31:25 PDT

Lawrence Livermore National Laboratory (one of the U.S.'s three nuclear weapons labs) has had one of its unclassified Internet computers hacked to provide a repository for 2 Gigabytes of pornographic images, storing over 1000 pictures. (You thought a picture is worth 1000 words? In this case it is worth 2000 kilobytes, i.e., 2 megabytes each.) This was reported in a Los Angeles Times article by Adam S. Bauman (appearing in the San Jose Mercury, 12 July 1994, front page); the Times article also noted that the Software Publishers Association and the FBI are tracking something like 1600 B-boards that contain pirated software. [Thanks to Nachum Shacham for bringing in the clipping.]

---

## "DUMB FROGS AHEAD"

"Tom Zmudzinski" <zmudzint@cc.ims.disa.mil>

Thu, 14 Jul 94 15:27:41 EST

This is one for the Highway, not the I-way (Information Dirt Road):

On 2 July 1994, on Route 29 in Virginia, one of those roadside variable message electronic signs was reported as flashing:

"DUMB FROGS AHEAD"

This wasn't a case of someone fat-fingering "dense fog ahead". Some prankster(s) had gotten access to the controls and had a little fun confusing the public. Stacy Pruitt, spokesbeing for Virginia Department of Transportation (VDOT), was quoted in the Washington Post as saying, "We think someone got in there during the night. What is mysterious is that it takes a password to sign onto the system. We're calling it 'highway hacking'." VDOT officials reported that the security box (on the back of the unit) was left unlocked, allowing physical access to the keyboard.

Obviously, the so-called highway hacker(s) could have concocted a far more dangerous prank (the mind boggles!) but that merely begs the REAL question:

How do you tell the smart frogs from the dumb ones?

Tom Zmudzinski [Unreformed Paronomasiac] Zmudzint@CC.IMS.DISA.MIL  
CAUTION! INCORRIGIBLE PUNSTER! PLEASE DON'T INCORRIGE!

[A chunk of the 13 July 1994 Washington Post article (which appeared in the "Dr. Gridlock" column about local auto and traffic issues) was sent to RISKS by marc@sti.com (Marc Pawliger), with the Subject line "FROGGY BOTTOM". As I try not to use copyrighted material in its entirety (although I sometimes FROGETTE, as in the case of the amusing "TOUCH-TOE" [sic!] item "Risks of REDIAL" in [RISKS-16.21](#)), I have in this case chosen Tom's adaptation. I TOAD the line on this one. TOUCH-TOAD or TOUCH-TOED? "This carflee tastes like ZMUD to me!" "It should. It was GROANED this morning." PGN]

---

## Digital display boards on highways

Jason Hanson <jhanson@cs.wisc.edu>  
Thu, 14 Jul 1994 16:40:04 -0500 (CDT)

Often when driving, one is confronted with those big digital display boards that warn of impending traffic conditions. On top, there always appears to be a cellular antenna. Am I correct in thinking that there is a modem on the cellular "line"?

The risks are somewhat obvious - one could call and change the message! While "COP AHEAD - SLOW DOWN" would be a bit amusing, a change from "BRIDGE OUT AHEAD" to "WEST HIGH RULEZ" would be disastrous.

Jason J. Hanson, Univ. of Wisc., 22 Langdon Street #220 Madison, WI 53703-1344  
(608) 256-1004 Ham: N9LEA (Extra) jhanson@yar.cs.wisc.edu

---

## Mailers that add "Company Confidential"

Paul Szabo <szabop@tualatin.pen.tek.com>  
Thu, 14 Jul 94 17:42:01 PDT

I received an e-mail that was distributed over a large mail-group today. It had a line, just below the "Subject" line, that read:

> Sensitivity: Company-Confidential

There are several RISKS here:

- 1) Misuse of this label can cause your company problems when it comes time to sue someone for stealing confidential information. This label should mean what it says in order to be valid in court. My company has told the employees several times to use this label ONLY for actual confidential material, for this reason.
- 2) It did not say which company the material was confidential for. It would not be a valid in court on actual confidential material because the company's name is not mentioned.
- 3) The person who sent this message is not paying attention to lines that their mailer adds. Lesson: Learn how your mailer works!

Paul Szabo, Test Engineer, Tektronix Test and Measurement, Beaverton, OR  
503-627-5811

---

## Scams

*Phil Agre <pagre@weber.ucsd.edu>*

*Wed, 13 Jul 1994 18:13:59 -0700*

The 24 June 1994 issue of The Wall Street Journal contains a long article about a wave of "fax scams" that has been emanating from Nigeria. People receive quasi-official-looking faxes with elaborate stories about money that needs to be parked in their bank accounts for short periods, with large profits promised. The recipients of these faxes, of course, start dreaming of big bucks. Just before the deal is closed a temporary "hitch" arises, requiring the person to send over some money or goods to bribe a government official. Needless to say, the money and goods are never seen again. Part of what makes these scams so effective is that the scammers manage to come up with enough personal information about the victim to play on his or her weak points and make the faxed "documents" more compelling. The scam requires faxes rather than just airmail because the parties need to exchange increasing numbers of faxes as things get more complicated, and speed presumably helps keep doubt from setting in. The article says:

Nigerian scam artists have claimed so many victims in Texas that the Nigerian soccer team and its fans have received a less-than-enthusiastic welcome at the World Cup games there. In Addison, the Dallas suburb where the Nigerian team is practicing, a local newspaper quoted the police chief warning restaurateurs to beware of Nigerians bearing credit cards. After outraged Nigerians called for his resignation, the chief said his remarks had been misinterpreted.

The full reference is:

Geraldine Brooks, How a recurring scam cost an accountant and his wife \$54,000, The Wall Street Journal, 24 June 1994, pages A1, A6.

The Risk, of course, is not specific to faxes. When communications are cheap and personal information is readily available, scams like these can readily cross borders, so that criminal communications can originate in "off-shore" locations where they are not likely to be punished. Just think what will be possible when global broadband communications become widely available.

Phil Agre, UCSD

---

### **Re: Secure use of Internet ([RISKS-16.22](#))**

*Tom Patterson <patterson@mcc.com>*

*Mon, 11 Jul 1994 09:39:17 -0600*

Re: Mosaic risks (Levine, [RISKS-16.22](#))

At the RISK of sounding like a commercial, "Mosaic" (a brand-name for the generic World Wide Web (Web) technology) is and has been available in privacy and integrity enhanced versions from the MicroElectronics and Computer Technology Corporation (MCC - my employer). MCC EINet has secured Web client versions on Mac and Windows, as well as Unix servers. Web is the latest in a series of internet products that MCC has secured, including WAIS and FTP. We

also maintain commercial grade access control and key servers on the network, available to any registered user.

The two most obvious RISKS in an internet Web environment are the authentication of the user and the server. Just as a user must authenticate to a server, responsible users will want non-reputable evidence that the server is what it says it is. This two-way authentication process is fully deployed today. And before everyone responds, we agree that there are many more RISKS, and secured clients and servers are only part of our system, which includes an internet security plan, risk analysis, fully integrated firewalls, and transparent encryption.

Re: Fraud on the Internet (Rowley, [RISKS-16.22](#))

... Your reaction is naive. The short answer is yes.

The internet is a wonderful collection of networks of all shapes and sizes, for many purposes. There is no reason to try to impose additional rules and regulations on it. What is happening, however, is that as commercial entities are looking to make use of it, they want additional security features in place. If a company puts in links to the internet with a firewall and authenticating server, that does not 'require' the rest of the users to change anything. It just means that one organization is making use of an advanced technology in a safe and secure manor.

Tom Patterson, Director, INFOSEC, MCC [patterson@mcc.com](mailto:patterson@mcc.com)

---

### Re: Shopping Risks... ([RISKS-16.21](#))

703) 506-0500 <[PHILS@RELAY.RELAY.COM](mailto:PHILS@RELAY.RELAY.COM) (Philip H. Smith III),>  
Wed, 13 Jul 94 08:14:49 EDT

A minor but (mildly?) interesting bar-code risk lies in coupons which are part of the packaging of products. The manufacturers have figured out that they shouldn't put barcodes on those which appear on the outside of packaging, lest the store pay you for taking the product (although this means that the scanner cannot verify that you bought the necessary product when redeeming the coupon), but continue to put barcodes on those which appear \*inside\* the product.

In the case of Healthy Choice frozen fake eggs, the coupon happens to be on the inside, but \*opposite the normal product bar-code\*. I found myself paying for 2 products instead of paying for one and cashing a coupon, when the checker scanned the wrong side of the coupon!

Hardly earth-shattering, but a nice gotcha.

...phsiii

---

## Re: Brock Meeks article on Clipper

Jerry Leichter <leichter@lrw.com>

Wed, 13 Jul 94 16:00:56 EDT

It's Silvio M\*i\*cali. Meeks got it consistently wrong throughout his article, and unfortunately now even extracts are repeating the mistake. :-)

-- Jerry

[Your moderator knew that also, and somehow neglected to fix it. PGN]

---

## Cellular phone risks/privacy

"Brown, Phillip" <Phil@gtemc.sprint.com>

Thu, 14 Jul 1994 18:01:30 -0400

One more contribution on the use and abuse of cellular phone technology, if the forum can tolerate it. As a technology planning engineer in the trade, I find the amount of ignorance-fueled fear of telephony and the vast amount of misinformation on cellular telephony in particular to be a source of constant amusement (but hey, I'm easily amused :). I'll address some specific remarks from earlier contributions first, then raise the noise floor another few dB with my own views.

Willis H. Ware writes:

>If cells get smaller in the future, then the precision of location will  
>increase ...

In a subsequent issue of Risks, Lauren Weinstein writes:

>If you read your phone bill inserts carefully, you may have already  
> received a notice allowing you to choose whether or not you want your  
> called number information released to VENDORS of telecommunication services!

The concern about monitoring is justified only up to a point -- remember, the only reason for this information to be saved is because it has value to someone. Wireline telcos long ago abandoned detailed billing, and today don't even retain that information unless required by a government agency; the cost of collecting and storing this tidal wave of data is still too prohibitive to make it useful on an everyday basis (this is a situation I don't see changing in the foreseeable future, either). The cellular phone industry, on the other hand, has employed detailed billing from its infancy, for reasons driven both by customer needs (why did this call cost so much?) and economies of scale (the processing needs have been orders of magnitude smaller than what is required by our wireline brethren, and at the same time the silicon revolution has made low to midrange computing power cheap -- many smaller cellular phone companies still do billing on a single PC!). So, for instance, seeing LA reporters with copies of OJ's cellular phone bill are no surprise at all, given that the information is readily at hand and the weakest security link in a system is usually the human operator. For all the high tech, gee whiz methods of obtaining cellular phone IDs, the most common way is still for unscrupulous sorts to bribe or blackmail company insiders into sharing lists

of valid subscribers. In the case of a large company like AirTouch (or my own), a corruptible someone with access to subscriber data can probably also get billing data.

Robert Morrell, Jr. and Bob Frankston pointed out different aspects of the risks of eavesdropping on cellular phone conversations (Mr. Morrell made the point that it is incumbent upon the user to ascertain and protect his level of privacy, and Mr. Frankston pointed out the fallacy of comparing wired and wireless technologies from a privacy perspective). The so-called security of the wired telephone is conceptually similar to "security through obscurity" in that it is the medium itself that makes listening to an otherwise unencoded communication difficult. It is something that virtually no phone user has thought about but takes for granted anyhow. I could agree with Mr. Morrell's extreme-sounding position if there was some assurance that once the user body was educated about the risk and began demanding truly secure communication (which I believe will happen eventually) the option was still available. Right now the US government is trying to usurp the issue while the body politic is still ignorant, and I see that as a violation of the public trust. BTW, several companies make scramblers for analog cellular phones (which work in conjunction with a companion device on the target phone, either wired or compatible cellular). The big drawback to these is that they must do most of their cryptographic work in the frequency domain, and 3300 Hz is not a lot of bandwidth to play in.

On the general issue of location tracking, I think the greater concern should be with real-time monitoring. I can sit at my desk today and find out which cell sites in our network any given phone number has placed calls on for the last 24 hours (after which time the data is rolled off into oblivion but continues to be available offline in printed detailed billing reports). But, as has already been correctly pointed out, this information is highly imprecise. Triangulation can be employed with a greater degree of precision (within a few hundred feet at best), but not consistently enough to be reliable. Data from technologies such as GPS must be transmitted in-band, so it is useless to the phone company unless the receivers are integrated into the network. However, I can't -- and probably won't ever be able to -- get any of the same information from a competitor, because that type of data is highly competitive in nature. No competing carriers will share that information with one another, nor will they be enthusiastic about providing the data to a clearinghouse where it might be generally accessible. So in this case competition is our friend. In any event, every large cellular carrier is already performing real-time network monitoring, and using called number information to get to the weak human link is probably more effective for law enforcement anyhow.

Phil Brown GTE Mobilnet pdb540@gtehq7.mail4.gtemc.sprint.com

---

### **Literary treatment of street-corner cameras**

*Scott Dorsey <kludge@grissom.larc.nasa.gov>*

*Thu, 14 Jul 1994 13:26:55 -0400*

I believe the first instance I can think of is Orwell's novel 1984, although

I would not be surprised that the idea predated that as well. I do recall having seen 1930s Gene Autry serials in which the evil mole-men placed television transmitters throughout an unsuspecting town.

--scott

---

### Teletext (Closed Caption) Methods (Stern, [RISKS-16.23](#))

*Bob Richardson <bob@CSOS.ORST.EDU>*

*Wed, 13 Jul 1994 17:04:07 -0700 (PDT)*

Michael Stern writes in [RISKS-16.23](#) about an alarming number of errors in a closed-captioned news program, and wonders if these are induced by faulty voice-recognition systems or spell-checker bugs. The truth is far simpler. Many live programs (such as news) are live-captioned by a service provider. In other words, a live human stenographer listens in (and usually views) the program while it is being broadcast, and types along as best as they can keep up. This is a somewhat outdated method when it comes to news, but many stations still use it, and it is quite error-prone. This is probably what happened in the reported case.

More modern newsrooms with integrated teleprompting/news composition software, have the newsroom computer automatically generate live close-captioning data from the teleprompter display. So the home viewer actually gets to see the news slightly before the anchor reads it off the display. The problem here is that commentary from persons on screen, such as people live in the field, must still be provided manually or not at all.

Some stations elect to caption the news program after it has aired, then re-broadcast it during the late-night hours. The problem here, of course, is that hearing-impaired viewers aren't able to get the news until hours after everyone else.

Bob Richardson, OmiCo Industries                      bob@csos.orst.edu  
PO Box 1404              Corvallis, OR 97339              503-758-5018

---

### Teletext run amok (Stern, [RISKS-16.23](#))

*"Clive D.W. Feather" <clive@sco.com>*

*Thu, 14 Jul 1994 09:00:31 +0100 (BST)*

Unlike most programmes, teletext conversion of the news is done live. As I understand it, a typist transcribes what the newsreader is saying using a special phonetic keyboard (like those devices you sometimes see being used in Parliamentary Committees or Congress). This is linked to a computer, which makes a "best guess" at the corresponding words and outputs the teletext directly. Obviously there is no time to correct errors.

Clive D.W. Feather, Santa Cruz Operation, Croxley Centre, Hatters Lane, Watford  
WD1 8YN, UK    clive@sco.com    +44 923 816 344    Fax: +44 923 210 352 |

---

**Re: Teletext run amok**

<Bob\_Frankston@frankston.com>  
Thu, 14 Jul 1994 21:39 -0400

It's interesting that one looks for a high tech explanation for these errors. Many Risks readers seem to forget that we already have a fairly reliable speech to text system. I presume that the TV stations use the same kind of system that one encounters when using the text to speech mechanism that is employed in the page networks. This is an efficient system that runs on 2000 to 3000 calories a day and can handle a wide variety of speech.

A human.

Unlike the paging systems which allow the typist to confirm the message (though I do get messages like my wife's request that I buy some "weak germ"), the TV systems require someone to type at a furious pace without any chance to correct or think. It's surprising how few errors occur. Wait for the story on Unix.

---

**Re: Laptop Danger for Airplanes**

<Bob\_Frankston@frankston.com>  
Thu, 14 Jul 1994 21:39 -0400

Is it too much to expect that when airlines find problems with laptop computers they report which ones? It is possible that particular manufacturer's machines are out of compliance. As part of assuring safety, it would be worthwhile to report the brands to the FCC rather than just condemning all devices.

As to lavatories, is it indeed worth risking an aircraft because one passenger is in the lavatory without a seatbelt on?

---

**Re: Laptop danger for airplanes (Martin, [RISKS-16.23](#))**

*Ad absurdum per aspera* <JTCHW@lbi.gov>  
14 Jul 1994 21:51:45 GMT

I hate to second-guess somebody who probably used the available information and did what he thought was best, but... jumpin' jehoosephat! Rather than violate procedures by taking off with somebody in the potty, he came within a "few feet" of re-enacting Tenerife on at least one occasion, maybe more? Not all RISKS involve computers...

--Joe

---

**Re: Laptop Danger for Airplanes (Martin, [RISKS-15.23](#))**

<lhe@sics.se>

Thu, 14 Jul 94 08:46:36 +0200

I recently saw the Flight Safety Department of the Swedish CAA comment on interference by the use of cellular phones.

In one instance, operating a cellular phone caused the aircraft transponder to stop replying to interrogations from ground secondary radar stations. When the phone was turned off the transponder replied normally again.

The FSD speculates that transmissions from the cellular phone on frequencies close to the interrogation frequency of the transponder had caused the sensitivity of the transponder receiver (which is automatically adjusted) to be reduced to the point where it could no longer receive interrogations.

Neither the cellular phone type (NMT or GSM) nor the aircraft type was given.

(PS. A "transponder" is a device that provides ground radar stations with coded replies that identifies the aircraft and gives information about its altitude.)

Lars-Henrik Eriksson, Swedish Institute of Computer Science, Box 1263  
S-164 28 KISTA, SWEDEN lhe@sics.se (intn!): +46 8 752 15 09

---

**re: Laptop Danger for Airplanes ([RISKS-16.23](#))**

Tony Abo <tabo@hitech.com>

Wed, 13 Jul 94 19:28:36 -0700

I may not be as up on this issue as I should be. I do however fly fairly often, and have become aware of the subject of interference to in-flight instruments by electronic devices being used by passengers, and the rules regarding the use of electronic devices.

It is clear that there is plenty of circumstantial evidence reported by flight crews of this phenomenon. When this first became an issue my understanding was that no one was sure that there was any link between the electronic devices and the occurrences, however for safety's sake, the restrictions were being instituted.

What I don't understand is why after all this time there isn't more substantial data available. How hard would it be to reproduce the problem? Certainly if one such device can cause a problem, then a cabin full of devices, which can be switched on and off in a controlled experiment should yield some measurable effect. Has something like this been done already? Has this been done without being able to reproduce the problem?

It isn't that I don't believe there is a problem. It just seems to me that the kind of evidence I've seen reported does not help pinpoint the problem. Therefore, the restrictions on the electronic devices may inconvenience travelers without diminishing any risk. Or perhaps once the effect can be reproduced and isolated, alterations could be made to shield the

instrumentation from the effect. This would be a far more effective approach than expecting a few flight attendants to police an entire cabin full of potential abusers.

Also, if the phenomena are caused by other unidentified sources, then there is certainly a risk that too much attention to this theory could be diverting attention from the real cause of the potentially disastrous occurrences.



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 16: Issue 25

Tuesday 19 July 1994

## Contents

- [NASDAQ computers crash](#)  
[PGN abstracting](#)
- [An Irish Sting Operation](#)  
[Brian Randell](#)
- [TCAS story on NBC Dateline 7/14/94](#)  
[Andres Zellweger](#)
- [Vindication](#)  
[Winn Schwartau](#)
- [Re: Risks of electronics on aircraft](#)  
[Phil Overy](#)  
[F. Barry Mulligan](#)  
[Chris Norloff](#)
- [Re: Digital Display Boards on Highways](#)  
[Don Root](#)
- [EDCC-1, Final Program \[European Dependable Computing Conf.\]](#)  
[Erik Maehle](#)
- [Info on RISKS \(comp.risks\)](#)

---

## NASDAQ Computers Crash

*Peter G. Neumann <Neumann@csl.sri.com>*

*18 Jul 1994 08:43:17 -0800*

NASDAQ Computers Crash, Halting Trading for More Than Two Hours  
By Diana B. Henriques, The N.Y. Times, 16 July 1994 [PGN ABSTRACTING]

The U.S. automated over-the-counter NASDAQ marketplace went down for 2.5 hours on the morning of Friday, 15 July 1994 when the computer system died. (It was finally restored just before N.Y. lunchtime.) The problem was traced to an upgrading to new communications software. One new feature was added each morning, beginning on Monday. Thursday's fourth new feature resulted in some glitches, but the systems folks decided to go ahead with the fifth feature on Friday morning anyway. It overloaded the mainframes (in Connecticut). Unfortunately, the backup system (in Rockville, MD) was also being upgraded,

in order to ensure real-time compatibility. The backup of course died as well. "[The backup system is] really for natural disasters, power failures, hardware problems that sort of thing," said Joseph R. Hardiman, Pres and CEO of NASDAQ. "When you're dealing with operating software or communication software, it really doesn't help you."

Volume on the day was cut by about one third, down from a typical 300 million shares. The effects were noted elsewhere as well, including several stock indexes, spreading to the Chicago options pits, trading desks, and the media. That in turn affected the large stock-index mutual funds.

---

## An Irish Sting Operation

*Brian Randell <Brian.Randell@newcastle.ac.uk>*

*Fri, 15 Jul 1994 14:47:37 +0100*

Cable TV fiddlers ensnared by Garda's World Cup trap  
Alan Murdoch in Dublin, The Independent, 15 Jul 1994

HUNDREDS of fraudsters in Cork have been nabbed in an ingenious "sting" targeting three human weaknesses: greed, cable television, and the World Cup. For two years Cork Communications, a cable television supplier to 30,000 homes, has been plagued by revenue-sapping fiddlers. Former subscribers were getting their "black box" cable decoders tampered with to let them watch pay-only channels such as Sky Sport and the Movie Channel for free. An illicit black-box black market appeared, supplied by a wave of house burglaries. "Hot" decoders were sold at an average Ir#60 a time. The result was 4,500 miscreants watching on the cheap, defrauding the firm of an annual Ir#750,000. The solution had echoes of an FBI sting in the mid Eighties when dozens of US crooks were lured with congratulations on winning a non-existent competition, only to be arrested on arriving to collect their "winnings". The solution devised by Cork Communications blended hi-tech ingenuity with an unerring sense of the one passion guaranteed to unite criminal classes this summer. A continuous message was broadcast on a cable channel which could be received only by decoders on which the scrambler system had been illegally by-passed. "To mark Ireland's first ever May Day bank holiday, YFBT Promotions is offering an Irish World Cup T-shirt absolutely free," if promised, giving a freephone number. Some 2,000 replies were taped. Weeding out those who heard about the offer in the pub, local gardai focused on former subscribers among the earliest callers. Last Monday Cork District Court granted 416 search warrants. The next 48 hours saw a blitz of raids such as J Edgar Hoover would have relished. An initial 150 people face charges and possible fines or imprisonment. A Garda spokesman said. "I hope this will prove a deterrent. We've scared a lot of people." Incidentally, three letters of the name YFBT Promotions stand for "Your Box is Tampered".

Dept. of Computing Science, Univ. of Newcastle, Newcastle upon Tyne NE1 7RU, UK  
Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923 FAX = +44 91 222 8232

---

**TCAS story on NBC Dateline 7/14/94**

*"Zellweger, Andres" <azellweger@mail.hq.faa.gov>*

*Fri, 15 Jul 94 10:26:27 EST*

Some of you may have seen the rather unbalanced piece NBC Dateline piece on the aircraft collision avoidance system, TCAS (July 14). The Dateline piece implied that TCAS was unsafe and, in fact, increased the risk of flying. Before the piece was aired, The Air Transport Association (ATA), Air Line Pilots Association (ALPA), and the Allied Pilots Association (APA), along with TCAS manufacturers, sent a joint letter to the President of NBC News expressing concern about the Dateline: NBC segment on TCAS. The letter states that indications from those already interviewed, "as well as promotional pieces already aired, clearly suggest that the segment will not present a factual, balanced viewpoint of TCAS."

The fact is that TCAS substantially reduces the risk of midair collisions. Airlines and pilots overwhelmingly support it, and in a number of incidents pilots credit TCAS with saving lives. The most recent testimony involved a situation over the Pacific between Northwest and Cathay Pacific jumbo jets in which TCAS helped avert a potential disaster. The Northwest pilot later said something to the effect that "700 people owe their lives to TCAS." (No mention of this by NBC.)

FAA's R&D Service has concluded after extensive analysis that when both aircraft are equipped with TCAS 2, the risk of collision is reduced by a factor of 26. And, despite what was reported on Dateline, TCAS has not induced a single collision or near collision. These assertions are not made lightly. They come after four years of experience with the operational evaluation of TCAS II that FAA began in 1990 in cooperation with the aviation community, including pilots and controllers. This represents some 25 million hours of TCAS operation. During that time, almost 14,000 reports from pilots and controllers have been received.

A quote from one of FAA's Public Affairs staffers puts this in context: "Clearly, the trend in television news is towards the news magazine shows, versus the straight news news programs. Even CNN, whose straight news broadcasts are among the best, is losing audience share, according to recent statistics. Bucking this trend, I plan to focus a lot more of my attention on televised sports, although I haven't broached that subject with my wife yet. Sports is one thing that TV does exceptionally well. Which reminds, if you still think soccer is boring after watching Romario of Brazil and Baggio of Italy, then you need help. Might as well just jump in your jammies, put on your slippers, watch the news magazine shows, and wait for the final bell."

---

## **Vindication**

*"Winn Schwartau" <p00506@psilink.com>*

*Fri, 15 Jul 94 12:09:18 -0500*

Now it seems that since an aviation authoritative source is talking about the RISKS that I have been identifying for over 4 years, it's OK to be wary. But how easy people forget.

It is not in the best interest of the government, the FAA, the airlines or the aircraft manufacturers to openly discuss, much less admit what \*could\* go wrooonnngggg. RISKS readers should be referred to my original works on the subject which appear in:

RISKS: (You know the issue better than I do.)

Security Insider Report, August, 1993. "The FAA Discovers  
HERF: Is John Q. Flyer in Danger?"

"Information Warfare: Chaos on the Electronic Superhighway,"  
Thunder's Mouth Press. ISBN 1-56025-080-1.

In ongoing research in related areas, we are presently identifying at least 19 (nineteen) actual HERF attacks against high tech organizations. We will be publishing the results of this work when we are permitted to release the names and events.

I stand by the original work despite the nay-sayers. If anything, recent events and current discussions fully support what I have been saying since 1990: Magnetic weapons are the nuclear arms of the Information Age, and governments from hither and yon are trying to figure out what to do about it. Kind of puts Michelangelo in perspective, doesn't it.

Thanks to RISKS for staying on the leading edge of technology and for not being distracted by those who would prefer the subject be kept in the closet.

---

## risks of electronics on aircraft

*Phil Overy <PJO@ib.rl.ac.uk>*

*Fri, 15 Jul 94 09:55:49 BST*

Since Lockerbie was caused by a device hidden by consumer electronics, and since it appears to be at least suspected that navigational devices are vulnerable to interference from outside consumer devices carried by passengers, has anyone thought that a terrorist attack might be carried out on the avionics instead?. It is not easy to screen for electronic devices in baggage etc. After all the mail about the A320, I have come to realise that avionics are already past the point of no return in modern jets - on an architecture programme last night, Norman Foster was extolling the virtues of the 747; on the flight deck was a very simple layout using four CRTs; is anyone claiming that the plane is not avionics-dependent when the instruments are condensed in this manner?. I am sure there are means of switching it all off, however what is the plane like to fly after the switch-off? When my car's power steering failed, I was VERY glad to be travelling slowly even though the steering would have been quite normal to a van driver: I can imagine that this effect is at its worst in helicopters.

In the more mundane computer world, are any desktops vulnerable to reverse TEMPEST attacks aimed at denying service? We have some 286s I would quite gladly test..

Phil Overy

---

## Re: Laptop Danger for Airplanes

"F. Barry Mulligan" <MULLIGAN@ACM.ORG>

Fri, 15 Jul 1994 05:49:07 -0500 (CDT)

In [RISKS DIGEST 16.23](#) it was reported:

> A cellular phone was also found on, although its owner claimed it had not  
> been used.                   ^

It should be noted that a cell phone periodically transmits to the control site so that the system knows its location, even if it's not 'in use'. A powered-up phone could easily generate the intermittent problems reported.

---

## Laptops in Aircraft

<cnorloff@tecnnet1.jcte.jcs.mil>

Fri Jul 15 07:30:47 1994

I agree we need more information on using electronic devices in aircraft. The following article has the most particular information I've seen yet. However, I don't know if the suspect laptop computer was examined for FCC interference compliance. If all these "electronic devices" are so dangerous, why are our aircraft so sensitive, and why aren't computer manufacturers shielding their products better?

### Compass Deflection

[begin quote] In cruise flight at FL310 25 NM west of the VOR, the #1 compass suddenly precessed 10 degrees to the right. I asked the First Flight Attendant if any passenger-operated electronic devices were in operation in the cabin. She said that a passenger had just turned on his laptop computer. I asked that the passenger turn off his laptop computer for a period of 10 minutes, which he did. I slaved the #1 compass, and it returned to normal operation for the 10-minute period. I then asked that the passenger turn on his computer once again. The # 1 compass immediately precessed 8 degrees to the right. The computer was then turned off for a 30-minute period during which the #1 compass operation was verified as normal. It was very evident to all on the flight deck that the laptop computer operation was adversely affecting the operation of the #1 compass. I believe that the operation of all passenger-operated electronic devices should be prohibited on airlines until the safe operation of all these devices can be verified. [end quote]

\_Callback\_, number 180, May 1994. A monthly safety bulletin from The Office of the NASA Aviation Safety Reporting System, P.O.Box 189, Moffett Field, CA 94035- 0189 (no copyright notice displayed).

Chris Norloff cnorloff@tecnnet1.jcte.jcs.mil

---

## Re: Digital Display Boards on Highways ([RISKS 16.24](#))

Don Root <der@oes.ca.gov>

Fri, 15 Jul 94 08:44:35 PDT

I note that the California Department of Transportation (CalTrans) is in the process of greatly expanding it's network of Changeable Message Signs (CMS) and freeway surveillance cameras. In many cases, cameras are being installed in locations where they can observe the text on the nearby CMS. (in many remote locations, CalTrans is using VSAT technology to feed a CMS and monitor a camera).

Don Root, Assistant Chief,  
Telecommunications, Calif. Office of Emergency Services

---

### EDCC-1, Final Program

"Erik Maehle" <maehle@131.234.158.1>

Fri, 15 Jul 1994 17:07:12 +0200

#### F I N A L P R O G R A M

##### EDCC-1

1st European Dependable Computing Conference

Berlin, Germany

October 4-6, 1994

[The original message from Erik was huge. I have excerpted the program. Send E-mail to Erik to receive the full package on-line. There is a 1 August 1994 deadline on getting the conference rate for the hotels, so act quickly. PGN]

#### ORGANIZED BY:

- \* Joint Technical Interest Group "Fault-Tolerant Computing Systems" of the GI, ITG and GMA, Germany
- \* AFCET Working Group "Dependable Computing" France
- \* AICA Working Group "Dependability in Computer Systems", Italy

In association with the Council of European Professional Informatics Societies (CEPIS)

#### IN COOPERATION WITH:

- \* GI Technical Interest Group "Dependable IT Systems"
- \* GI Technical Interest Group "Test and Reliability of Circuits and Systems"
- \* IFIP Working Group 10.4 "Dependable Computing and Fault-Tolerance"
- \* IEEE TC on Fault-Tolerant Computing
- \* IEEE TC on Real-Time Computing
- \* EC-ESPRIT CaberNet Network of Excellence on Distributed Computing System Architecture

\* EWICS Technical Committee on Safety, Reliability and Security (TC7)

#### INTRODUCTION and BACKGROUND:

Organizations and individuals are becoming increasingly dependent on sophisticated computing systems. In differing circumstances, the dependency might for example center on the continuity of the service delivered by the computing system, the overall performance level achieved, the real-time response rate provided, the extent to which catastrophic failures are avoided, or confidentiality violations prevented. These various concerns can be subsumed into the single conceptual framework of dependability, for which reliability, availability, safety and security, for example, can be considered as particular attributes.

This, the first European Dependable Computing Conference, aims to provide a European venue for researchers and practitioners from all over the world to present and discuss their latest research results and developments. The conference scope addresses all aspects of dependable computing, including: fault-tolerant systems and components, safety critical systems, software dependability, secure systems, validation, verification, testing and evaluation. The conference program has been purposely organized in a single track to encourage cross-fertilization between different viewpoints of dependable computing.

EDCC-1 is the successor of two European conference series on fault tolerance and dependability as well as on aspects of testing and diagnosis. The first series, known as the "International Conference on Fault-Tolerant Computing Systems" was organized (from 1982 up to 1991) by the German Technical Interest Group "Fault-Tolerant Computing Systems". The other series, known as the "International Conference on Fault-Tolerant Systems and Diagnostics", was annually organized (from 1975 up to 1990) by Universities and academic research institutions in the former Czechoslovakia, Poland, Bulgaria and the former GDR. EDCC will be organized every two or three years in different European countries.

#### ORGANIZATION COMMITTEE:

##### General Co-Chairs

Klaus Echte	Dieter Hammer
University of Dortmund	Humboldt-University of Berlin
Germany	Germany

##### Program Chair

David Powell  
LAAS-CNRS, Toulouse  
France

##### Publicity Chair

Erik Maehle	Finance Chair
University of Paderborn	Volker Schanz
Germany	VDE-ITG, Frankfurt/Main
	Germany

International Liaison Chairs

North America: Jacob Abraham      Asia: Yoshi Tohma  
University of Texas, Austin,      Tokyo Institute of Technology  
USA                                      Japan

TECHNICAL PROGRAM

Tuesday, October 4, 1994

09:30 Opening Ceremony

10:00 Session 1: Fault-Tolerance Techniques

Chair: Winfried Goerke, University of Karlsruhe, Germany

A model for adaptive fault-tolerant systems

Matti A. Hiltunen, Richard D. Schlichting (University of Arizona,  
Tucson, USA)

Designing secure and reliable applications using FRS: an  
object-oriented approach

Jean-Charles Fabre, Yves Deswarte (LAAS-CNRS, Toulouse, France),  
Brian Randell (University of Newcastle-upon-Tyne, United Kingdom)

A fault-tolerant mechanism for simple controllers

Joao Gabriel Silva, Luis Moura Silva, Henrique Madeira, Jorge  
Bernardino (University of Coimbra, Portugal)

11:30 Session 2: Formal Methods

Chair: John McDermid, University of York, United Kingdom

Formal semantics for Ward & Mellor's transformation schema

Carsta Petersohn, Cornelis Huizing, Jan Peleska, Willem-Paul de  
Roever (Christian-Albrechts-University of Kiel, Germany)

Formal reasoning on fault coverage of fault tolerant techniques: a  
case study

C. Bernardeschi, A. Fantechi, Luca Simoncini (University of Pisa,  
Italy)

12:30 Lunch

14:00 Session 3: Evaluation

Chair: Bjarne Helvik, DELAB, Trondheim, Norway

On performability modeling and evaluation of software fault  
tolerance structures

Silvano Chiaradonna, Andrea Bondavalli, Lorenzo Strigini  
(CNUCE/CNR, Pisa, Italy)

Optimal design of fault-tolerant soft-real-time systems with

imprecise computations

Cesare Antonelli (University of Perugia, Italy), Vincenzo Grassi  
(Tor Vergata University of Rome, Italy)

Computational restrictions for SPN with generally distributed  
transition times

Andrea Bobbio (University of Brescia, Italy), M. Telek (University  
of Budapest, Hungary)

15:30 Break

16:00 Session 4: Hardware Testing

Chair: Bernd Straube, Fraunhofer - EAS, Dresden, Germany

Test generation for digital systems based on alternative graph  
theory

Raimund Ubar (Tallinn Technical University, Estonia)

The configuration ratio: a model for simulating CMOS intra-gate  
bridge with variable logic thresholds

M. Renovell, P. Huc, Y. Bertrand (University of Montpellier II,  
France)

Coverage of delay faults: when 13% and 99% mean the same  
Andrzej Krasniewski, Leszek B. Wronski (Warsaw University of  
Technology, Poland)

17:30 Session 5: Fault Injection

Chair: Jean Arlat, LAAS-CNRS, Toulouse, France

RIFLE: a general purpose pin-level fault injector

Henrique Madeira, Mario Relas, Francisco Moreira, Joao Gabriel Silva  
(University of Coimbra, Portugal)

On single event upset error manifestation

Rolf Johansson (Chalmers University of Technology, Goteborg,  
Sweden)

18.30 End

Wednesday, October 5, 1994

08:30 Session 6: Software Testing

Chair: Pierre-Jacques Courtois, AIB-Vincotte Nuclear, Brussels,  
Belgium

Injecting faults into environment simulators for testing safety  
critical software

Hong Zhu, P.A.V. Hall, J.H.R. May (The Open University, Milton  
Keynes, United Kingdom), T. Cockram (Rolls-Royce plc, United  
Kingdom)

On statistical testing of synchronous data flow programs  
Pascale Thevenod-Fosse, Christine Mazuet, Yves Cruzet (LAAS-CNRS,  
Toulouse, France)

09:30 Session 7: Built-in Self Test

Chair: Andrzej Hlawiczka, Technical University of Gliwice, Poland

Hierarchical test analysis of VLSI circuits for random BIST  
G. Masseboeuf, J. Pulou (Laboratoire d'Automatique de Grenoble),  
J.L. Rainard (CNET, Meylan, France)

Zero aliasing compression based on groups of weakly independent  
outputs in circuits with high complexity for two fault models  
Peter Boehlau (University of Potsdam, Germany)

10:30 Break

11:00 Session 8: Software Diversity

Chair: Hubert Kirrmann, ASEA Brown Boveri AG, Baden-Daetwil,  
Switzerland

Systematic and design diversity - software techniques for hardware  
fault detection  
Tomislav Lovric (University of Dortmund, Germany)

Detection of permanent hardware faults of a floating point adder by  
pseudoduplication  
S. Gerber, M. Goessel (University of Potsdam, Germany)

MLDD (Multi-Layered Design Diversity) architecture for achieving  
high design fault tolerance capabilities  
Aki Watanabe, Ken Sakamura (University of Tokyo, Japan)

12:30 Lunch

14:00 Session 9: Parallel Systems

Chair: Paulo Verissimo, INESC, Lisbon, Portugal

Reconfiguration and checkpointing in massively parallel systems  
Bernd Bieker, Erik Maehle (University of Paderborn, Germany), Geert  
Deconinck, Johan Vounckx (Catholic University of Leuven, Belgium)

An approach for hierarchical system level diagnosis of massively  
parallel computers combined with a simulation-based method for  
dependability analysis  
J. Altmann, F. Balbach, A. Hein (University of Erlangen-Nuernberg,  
Germany)

Hierarchical checking of multiprocessors using watchdog processors  
I. Majzik, A. Pataricza (Technical University of Budapest,  
Hungary), M. Dal Cin, W. Hohl, J. Hoenig, V. Sieh (University of  
Erlangen-Nuernberg, Germany)

15:30 Break

16.00 Panel Discussion:

Future directions in dependable computing

Moderator: Jean-Claude Laprie, LAAS-CNRS, Toulouse, France

Panelists:

Algirdas Avizienis, University of California, Los Angeles, USA

Jan Hlavicka, Czech Technical University, Prague, Czech Republic

Michele Morganti, ITALTEL Central Research Labs. Milano, Italy

Brian Randell, University of Newcastle-upon-Tyne, United Kingdom

Ernst Schmitter, Siemens AG, Munich, Germany

17.30 End

18.00 Boat Trip

20.30 Conference Dinner

Invited Speaker: David Talbot, Head of Division,  
Software and Advanced Information Processing,

DG III-Industry-ESPRIT, Commission of the European Commission

Thursday, October 6, 1994

08:30 Session 10: Fault Tolerance in VLSI

Chair: Jozsef Sziray, Computer Research and Innovation Center,  
Budapest, Hungary

An effective reconfiguration process for fault-tolerant VLSI/WSI  
array processors

Yung-Yuan Chen, C.-H. Cheng, Y.-C. Chou (Chung-Hua Polytechnic  
Institute, Hsin-Chu, Taiwan)

Concurrent error detection in fast FNT networks

Jamel M. Tamir, Satnam S. Dlay, Raouf N. Gorgui-Naguib, Oliver R.  
Hinton (University of Newcastle-upon-Tyne, United Kingdom)

Feasible regions quantify the configuration power of systems with  
multiple fault types

Laurence E. LaForge (University of Nevada, Reno, USA)

10:00 Session 11: Measurement

Chair: Tashko Nikolov, Technical University of Sofia, Bulgaria

Software reliability analysis of three successive generations of a switching system

M. Kaaniche, K. Kanoun, M. Cukier (LAAS-CNRS, Toulouse, France), M. Bastos Martini (CpQD-Telebras, Brazil)

Performance of consistent checkpointing a modular operating system: Results of the FTM experiment

Gilles Muller, Mireille Hue (IRISA/INRIA, Rennes, France), Nadine Peyrouze (Bull Research, France)

11:00 Break

11:30 Session 12: Switching Networks and Hypercubes

Chair: K. Iyoudou, Moscow Aviation Institute, Russia

Ring-Banyan network: a fault tolerant multistage interconnection network and its fault diagnosis

Jae-Hyun Park, Heung-Kyu Lee (Korea Advanced Institute of Science & Technology, Taejon, Korea)

Reconfiguration of faulty hypercubes

Dimitri R. Avresky, K.M. Altawil  
(Texas A&M University, College Station, USA)

Fault tolerance on Boolean n-cube architectures

Chu-Sing Yang, Shun-Yue Wu (National Sun Yat-Sen University, Kaohsiung, Taiwan)

13:00 Lunch

14:30 Session 13: Distributed Systems

Chair: Jan Torin, Chalmers University of Technology, Goteborg, Sweden

Relative signatures for fault tolerance and their implementation  
Martin Leu (University of Dortmund, Germany)

GATOSTAR: a fault tolerant load sharing facility for parallel applications

Bertil Folliot, Pierre Sens (MASI Laboratory, Paris, France)

A hierarchical membership protocol for synchronous distributed systems

P.D.V. van der Stok, M.M.M.P.J. Claessens, D. Alstein (Eindhoven University of Technology, The Netherlands)

16:00 Break

16:15 Joint meeting of European Dependable Computing and Fault Tolerance  
Working Groups - open to all EDCC-1 participants

Chairs:

E. Schmitter, J.C. Laprie. L. Simoncini

18.00 End



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 16: Issue 26

Wednesday 20 July 1994

## Contents

- [IRS](#)  
[Phil Agre](#)
- [Crashed bank teller](#)  
[Kees Goossens](#)
- [HEREF Vindication II](#)  
[Winn Schwartau](#)
- [The digital individual](#)  
[Phil Agre](#)
- [Victim on the infobahn](#)  
[Bill Donahue](#)
- [Benefits Agency Smart Payment Card](#)  
[Shaggy](#)
- [Risks of confusing "headlines" with "in depth news"](#)  
[Bob Estell](#)
- [Re: Aircraft Avionic Vulnerabilities](#)  
[A. Padgett Peterson](#)
- [Re: Inmates con jail computer](#)  
[Amos Shapir](#)
- ["Firewalls and Internet Security" by Cheswick/Bellovin](#)  
[review by Rob Slade](#)
- ["The Fool's Run" by Camp](#)  
[review by Rob Slade](#)
- [InfoWar II--First Call for Participation](#)  
[Mich Kabay](#)
- [Info on RISKS \(comp.risks\)](#)

---

## IRS

*Phil Agre <pagre@weber.ucsd.edu>*

*Wed, 20 Jul 1994 15:36:55 -0700*

The 19 August 1994 New York Times carries a long article about hundreds of IRS (Internal Revenue Service, the American tax collection people) employees being disciplined for peeking at tax returns that they shouldn't have been. The

IRS's investigations concluded that the employees' suspicious behavior ranged from out-and-out fraud to simple curiosity. The discovered the need for guidelines about which degrees of wrongdoing merited which punishments. The full reference is:

Robert D. Hershey, Jr., IRS staff is cited in snoopings, New York Times, 19 July 1994, pages C1, C12.

It's one of those stories that can be invoked as evidence for either of two contradictory positions: that employees' illicit use of personal files is a serious problem, or that it's not a real problem since the wrongdoers are getting caught. It's clear that private businesses have the same problems with illicit peeking at personal information. We might ask whether public or private organizations have a greater incentive to prevent this kind of thing. Since information can be copied readily, it's not like pilfering in a warehouse, where the organization loses capital in a straightforward sense and thus has a straightforward interest in preventing it. An exception would be information that is leaked to customers who would otherwise purchase the information from the organization, as opposed to being leaked to people whose status or purposes would not otherwise permit them to buy the information through the front door.

Instead, the organization's interest is generally more indirect, having primarily to do with its reputation and the reputations of its leaders. In a society without privacy activists or a free press serving a public that is aware that its privacy is threatened, I think organizations would have little incentive to do anything about leaks of personal information. In the society we have right now, I would suggest that the IRS has a greater incentive to prevent leaks of personal information than does a credit bureau or other private information holder, since it is politically much more practical for the legislature to make the IRS bureaucrats miserable than to make the officers of private firms miserable. Others may disagree, but the important thing is to understand the mechanisms which create, or *could* create, organizational interests in genuinely protecting private information. Fear of legislation is a good one, but others exist as well.

Phil Agre, UCSD

---

## Crashed bank teller

*Kees Goossens <kgg@dcs.ed.ac.uk>*

*Tue, 19 Jul 94 10:55:35 +0100*

[I presume you call a cash till that does not give cash a TELLER? KGG]

[Well, we might as well for the purposes of this message.

It is certainly not an ASKER! PGN]

Today, in my local branch of Banca di Roma, in central Rome, Italy I encountered a bank teller which had crashed. These machines allow you to obtain bank statements but do not dispense cash. The display I encountered contained a number of error messages (file not found, could not create file, etc) followed by the prompt (A>). Feeling somewhat guilty, I typed DIR, which

worked and listed a number of executables and some documents. I looked at one called "fine", meaning "end" in Italian, which contained instructions for the shutdown of the system. At this point I alerted the lady at the counter: "Are you aware that your system has crashed and that I can modify whatever I want in the system?". The latter to emphasise the gravity of the situation; I'm not sure how much I could have done in practice. This did indeed produce some alarm, and I was told that there was a systems person who'd take of the situation. I did not see this person arrive during my subsequent wait in the queue (which this teller is supposed to diminish btw). As for the cause of the crash, the computer terminals at the counters were dead at roughly the same time, perhaps due to a common cause.

Kees Goossens <kgg@dsi.uniroma1.it> <http://www.dcs.ed.ac.uk/staff/kgg>  
Dip. di Scienze dell'Informazione, Universita di Roma "La Sapienza", Italy

[A considerable risks would exist if there is a way to crash the system intentionally in order to reach that prompt... Knowing what we know about risks, we might suspect that to be the case. PGN]

---

## HERF Vindication II

"Winn Schwartau" <p00506@psilink.com>  
Mon, 18 Jul 94 11:58:19 -0500

As RISKS readers know, I have ruffled more than a few feathers here in the US and with foreign governments over the issue of HERF (High Energy Radio Frequency) interference as a potential weapon system. Recently, RISKS readers have seen mounting evidenced of anomalous electrical interference behavior at 37,000 feet. Boeing and Apple and others companies have tried to quantify the phenomenon but EMI and RFI interference is highly elusive.

Maybe the July 18, 1994 issue of the New York Times will shed additional light. The FBI mounted a whistle blower sting operation against General Electric with the assistance of one of their engineers who alleged that the company was improperly grounding its jet engines to the detriment of safety to both commercial and military aircraft. So alarmed was the Air Force One pilot that he refused to take off from Rome's airport with President Clinton until he was assured it was safe to do so.

The GE engineer and whistle blower Ian Johnson, said he discovered the problems with improper engine grounding in 1989 but was subsequently brushed aside by his concerns. Engine grounding is critical to proper electrical performance in the air, and the technique GE uses to insure a quality connection is called electrical bonding. Is it any coincidence that laptop EMI stories began about a year later when portable digital electronics became popular?

As any electrical engineer knows, any connection will introduce a given amount of electrical resistance (measured in ohms . . . Ohm's law, remember?) into a circuit. The goal is to approach zero resistance in any connection. Period. Poor connections not only change the values in the circuit thus changing the circuit performance, but can also become diode-like and act like

unpredictable rectifiers. Not good.

According to the article, GE engine's electrical bonding should result in an added impedance (resistance) of 2.5 milliohms (.0025 ohms) but were found to in some cases exceed 60,000 milliohms (60 ohms) and that is a lot: off by a factor of 24,000! In my former life as a circuit/systems designer, such an intolerable error would GUARANTEE a failure.

The need for adequate bonding is clear: make sure that stray electrical signals such as from lightning bolts or from laptop computers or other consumer electronic devices do not interfere with the safe and reliable operation of a 100 tons of metal hurtling through the atmosphere.

GE denies it (what else is new!) and there is bound to be a debate as to whether there really was an intentional cover-up as stated by Mr. Johnson.

In an interesting side note, the FBI had Mr. Johnson wear a wire (a tap recorder on his person) over a period of 6 months to get the goods on GE.

I guess this case will take over our minds and souls soon enough, on the "All O.J. Network."

---

## The digital individual

*Phil Agre <pagre@weber.ucsd.edu>*

*Sat, 16 Jul 1994 14:09:31 -0700*

An academic journal called *\_The Information Society\_* has just published a special issue (volume 10, number 2, April-June 1994) entitled "The Digital Individual". (I'm the issue's guest editor.) It includes five articles whose general theme is that people's activities increasingly cast "shadows" onto the insides of computers. As a result, the whole notion of a human individual is beginning to change. Everyone has their physical self and surroundings and possessions, but they also have an elaborate digital aspect to their selves which follows them around through life. People use their digital shadows in a variety of beneficial ways, for example in sending messages to mailing lists like Risks, but they are often managed and controlled through their digital shadows as well. Since the outcome of this ambivalent situation is neither all-good or all-bad, it helps to make distinctions and put things in contexts, and that's what the articles in this special issue try to do. If you would like to see the full contents and abstracts for the special issue, send a message that looks like this:

To: rre-request@weber.ucsd.edu

Subject: archive send tis-digital

Phil Agre, UCSD

[Remember to sniff it out. The shadow nose! PGN]

---

## Victim on the infobahn

Bill Donahue <74562.3064@compuserve.com>

18 Jul 94 21:08:20 EDT

I learned the other day that I am a victim on the information superhighway. It's a long story; I'll relate it in hopes that there are folks out there who have had similar experiences and can tell me about them.

My wife and I had been getting about 15 anonymous calls a day for the past three weeks. The caller would contact us at all hours, and would never say anything at all. We were quite rattled because, as it happened, the calls began coming just as I, a freelance journalist, began work on a murder story and just as we prepared for the birth of our first child. The unknown man on the other end of the line was, in our haunted imagination, a crazed murderer after our new child.

We tried to invoke "Caller ID" to catch our harasser, but this did not work. Next, we called our phone carrier, US West, and our local sheriff to get them to look into the matter. We kept a log of all the "harassing" calls, and asked ourselves who so hated us that they would spend the money to call us via long distance 15 times a day and hang up each time.

Finally, the other day we got an answer: A computer software firm had inadvertently entered our number into a database and prompted one of its modems to keep trying our number, over and over. The lawyer for the company called me today to apologize for the disturbance his firm had caused us. He said, "I guess you were just a victim on the information highway. I'm sorry," but I was quite struck how minimal this whole thing was on his end (a few misstrokes on the keyboard) and how massive the disturbance was on our end--getting woken in the middle of the night, etc.

I'm thinking now of writing a magazine article on our experience, and am posting for two reasons. First, I'd like to hear from people who, like me, have become "victims on the infobahn," and second, I'd like to get some broader perspective. Do people know of any groups which monitor modem-caused problems? Are you aware of any laws covering such matters, and do you know how frequently mishaps like mine occur?

Any input would be greatly appreciated. Thank you,

Bill Donahue 74562,3064@CompuServe.com

---

## Benefits Agency Smart Payment Card

Shag the Moose <Shaggy@moose.demon.co.uk>

Thu, 14 Jul 94 23:07:36 GMT

The Benefits Agency (the 65,000 strong government agency responsible for the administration and payment of welfare benefits in the UK) has announced a new method of payment system, to be introduced over the next three years throughout the UK.

Customers will present their personalised smart card to the Post Office, who will swipe it, do an (as yet unspecified) id check from info held electronically on the card, and check on-line to the BA office to find out how much money the person is due. This will replace Girocheques and order books;

a system of 'valuable paper' which has been essentially unchanged since 1948. The prototype uses a digitised photo and pressure-pad signature.

As the cards will have no inherent value, rough estimates are that payment-related benefit fraud will be reduced by approximately 90%.

The BA has some 23,000,000 customers at any given time; approximately half the adult population of the UK. Customers will have an alternative to the smart card, in the form of ACT payments to their bank.

Shaggy

---

## Risks of confusing "headlines" with "in depth news"

*Bob Estell - The Ancient Mariner <estell@fidler.chinalake.navy.mil>  
Tue, 19 Jul 1994 09:30:26 PDT*

One of the several RISKS of using computers is that ordinary people (i.e., NOT computer gurus) may tend to listen TOO much to computer gurus. Why? Probably for reasons akin to why we listen to our doctors or our auto mechanics: if they are good they know more than we do about something that is important to us.

OK so far. But we (too many of us) are spoiled to getting news in "sound bytes" (or their e-mail or paper memo or slide presentation equivalents). Too many of us do not appreciate the difference between CNN's Headline News and PBS's McNeil-Lehrer Report; or their computing equivalents, for example INFORMATIONWEEK and IEEE COMPUTER. Both valuable, but very different.

So we hear one week that ISDN (or some other recent technology) has been revised and is now thriving; and within a month we hear from some other guru that the same technology has not lived up to its promise. Promise? or just hype? not only that, but hype by those same gurus, perhaps a bit too eager for more clients? or just not reading each other's stuff? OK, gurus have only 24 hours a day, and can't keep up either.

In early Aug 94, I retire from 34 years of federal service; and will thus for a while at least be off the InterNet. I'll especially miss RISKS because it is one of the very few forums that is both current and thorough which is a tribute to its clients and especially its Moderator.

According to some of these same gurus I am an old dog not able to learn new tricks; but others say that people like me are a valuable resource. I believe the latter opinion, not only because it is flattering, but also because the former may misunderstand the difference between 30 years experience and 3 years repeated 10 times.

Bob Estell (542 Mary Ann Ave., Ridgecrest, CA 93555)

---

**Re: Aircraft Avionic Vulnerabilities ([RISKS-16.25](#))**

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>

Wed, 20 Jul 94 10:17:20 -0400

I have been wearing hearing aids for over twenty years and on numerous occasions have allowed me to listen to things most people are "deaf" to.

This is made possible by the inductive pickups in my hearing aids, throwing a switch turns off the microphone and on the inductive pickup & a whole new world appears.

Just as an example, once upon a time, many people in a particular section of the building I worked in began complaining of headaches though no reason could be found. I happened to walk through the area in inductive mode & began to hear a beeping. Turned out that a RADAR unit at the nearby airbase had become misaligned and was sweeping the corner of the building. Realignment cured the headaches.

Through the years I have had many such incidents of being able to identify electrical problems this way by characteristic "sounds". The point is that the interior of a commercial aircraft is one of the "noisiest" environments I have ever encountered with the 400 hz being almost "deafening" and a myriad of other jingles, jangles, and hums also apparent.

One cannot but think that there must be almost no shielding of any signals in a modern aircraft and to me the amazing part is not that instruments are affected by laptops (low amplitude but I can "hear" them) but that they manage to operate at all in such an electronic bedlam.

Padgett

ps I have no idea what the spectrum of my hearing aids is, just that they have enabled the detection of too many diverse things to be very limited. Once they determined that a "haunted" corner in a house was nothing more than a power box on the other side of the wall.

[Ah, Padgett is an auditory canary, similar to the canary the miners used to take down with them to provide an early warning on toxic gases! Think of it as a \*gift\*. PGN]

---

## Re: Inmates con jail computer (Ilieve, [RISKS-16.23](#))

Amos Shapir <amos@cs.huji.ac.il>

17 Jul 1994 13:29:47 +0300

Peter Ilieve <peter@memex.co.uk> writes:

>The sophisticated computerised security system was designed to end slopping  
>out by allowing one prisoner at a time from each landing to go to the toilet  
>during the night. [Sanitation is not the UK prison system's strong point,  
>prisoners usually have to make do with a bucket in the corner of the  
>cell (...)]

This incident demonstrates a far more important RISK than just subverting the computerized system; the real RISK is that such a system was installed to solve a problem which should have been solved by a better sewage system!

Amos Shapir, The Hebrew Univ. of Jerusalem, Dept. of Comp. Science.  
Givat-Ram, Jerusalem 91904, Israel +972 2 585706,586950 amos@cs.huji.ac.il

---

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">  
Mon, 18 Jul 1994 01:37:32 -0600 (MDT)

Subject: "Firewalls and Internet Security" by Cheswick/Bellovin

BKFRINSC.RVW 940502

Addison-Wesley Publishing Company

P.O. Box 520

26 Prince Andrew Place

Don Mills, Ontario

M3C 2T8

416-447-5101

fax: 416-443-0948

Heather Rignanesi, Marketing, x340, 73171.657@Compuserve.com

or

Tiffany Moore, Publicity tiffanym@aw.com

Bob Donegon bobd@aw.com

John Wait, Editor, Corporate and Professional Publishing johnw@aw.com

Tom Stone, Editor, Higher Education Division tomsto@aw.com

Philip Sutherland, Schulman Series 74640.2405@compuserve.com

Keith Wollman, Trade Computer Group keithw@aw.com

Lisa Roth Blackman, Trade Computer Group lisaro@aw.com

1 Jacob Way

Reading, MA 01867-9984

800-822-6339

617-944-3700

Fax: (617) 944-7273

5851 Guion Road

Indianapolis, IN 46254

800-447-2226

"Firewalls and Internet Security", Cheswick/Bellovin, 1994, 0-201-63357-4,  
US\$26.95.

firewall-book@research.att.com ches@research.att.com smb@research.att.com

The Internet has a reputation for a lack of security. Those books which mention security on the Internet generally suggest setting up a firewall machine in order to protect yourself, but stop short of giving anything resembling details of how to do such a thing. Cheswick and Bellovin not only give practical suggestions for firewall construction, they also address other aspects of Internet security, as well.

Part one gives a basic background, both of security, and of TCP/IP. If you didn't think you needed security before, you will after reading chapter two.

Part two details the construction of firewall gateways, as well as authentication, tools, traps, and cracking tools for use in testing the integrity of your system. Part three discusses attacks, and the logging and analysis, thereof. The book also looks at legal aspects, secure communication over insecure links, resources and various helpful information.

Although the book deals specifically with TCP/IP, the concepts, which are the parts stressed, are applicable to any network-connected systems. This is probably destined to become one of the security classics within its specialized field.

copyright Robert M. Slade, 1994 BKFRINSC.RVW 940502

=====

Vancouver Institute for Research into User Security Canada V7K 2G6  
ROBERTS@decus.ca Robert\_Slade@sfu.ca rslade@cue.bc.ca p1@CyberStore.ca

---

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">  
Wed, 20 Jul 1994 13:05:39 -0600 (MDT)

Subject: "The Fool's Run" by Camp

BKFLSRUN.RVW 940428

%A Camp, John  
%C 2801 John Street, Markham, Ontario, Canada L3R 1B4  
%D 1989  
%G 0-451-16712-0  
%I Penguin/Signet  
%O U\$4.95/C\$5.95  
%T "The Fool's Run"

I very strongly suspect that whoever wrote the screenplay for "Sneakers" read this first. There is a mob connected corporation. They wish to do some espionage. They hire a tiger team to do it for them. They try to betray, and possibly destroy, the tiger team. The team is then forced to "crack" their former client. There is the same paranoia about the National Security Agency.

I don't know who the technical consultant was for this book, but he, she or it did an even better job here than Captain Crunch did for the movie. We have insider information, phone phreaking, database surfing, social engineering and overconfident systems managers. Chapter thirteen introduces computer viral programs, and I had to go back and check the copyright date. At a time when the supposedly technical books were printing absolute garbage, this novel had the concepts down pat (although slightly shaky on the details).

Probably it won't become a classic in either literature or data security, but a reasonably fun read, and refreshingly accurate technical details.

copyright Robert M. Slade, 1994 BKFLSRUN.RVW 940428

=====

Vancouver Institute for Research into User Security Canada V7K 2G6  
ROBERTS@decus.ca Robert\_Slade@sfu.ca rslade@cue.bc.ca p1@CyberStore.ca

---

## InfoWar II--First Call for Participation

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
19 Jul 94 12:22:13 EDT*

[For further information, contact Mich at 75300.3232@compuserve.com. PGN]

### FIRST CALL FOR PARTICIPATION

Second International Conference on Information Warfare:  
"Chaos on the Electronic Superhighway"

Conference Date: Wed 18 January 1995  
Conference Locale: Dorval Airport Hilton Hotel  
Montreal, Canada

#### 1. INTRODUCTION

Cultures that depend on information systems are vulnerable to Information Warfare. Attacks on data confidentiality, data integrity and data availability will damage individuals, corporations and other private organizations, government departments and agencies, nation-states and supranational bodies.

It is essential to erect legal, organizational, and cultural defences against information warfare.

The Second International Conference on Information Warfare will focus on panel discussions of Winn Schwartau's new book, *Information Warfare: Chaos on the Electronic Superhighway*, published in 1994 by Thunder's Mouth Press (ISBN 1-56025-080-1).

This announcement serves as a request for participation by those wishing to appear on panels, those wishing to suggest speakers, and others wishing to be added to a mailing list (electronic and snailmail) for further details as they develop.

Panelists will be asked to analyze selected portions of *Information Warfare* and to present refutations or support for the author's statements, assertions, predictions, warnings and recommendations.

The Conference will serve the interests of information security specialists and strategic planners from the corporate world, military and government circles, and academia. The Press will be permitted to cover the event, providing opportunities for increased public awareness of vulnerabilities of the information infrastructure.

The Conference Proceedings will contribute to the national and

international debates about information warfare and the need for careful planning to avoid disruption by hostile forces as national and international information highways develop worldwide.

Following recommendations from last year's participants in the First International Conference on Information Warfare, we have scheduled more free time for the animated discussion among participants.

Informal discussions will be aided by Special Interest Group signs allowing people with specific interests to congregate.

The organizers are making a special effort to reach members of the defence establishments of Canada and the United States. In order to foster the greatest degree of serious and productive discussion, room has been reserved for no more than 100 participants.

## 2. PROGRAM:

- 07:30-08:30 Registration and Continental Breakfast
- 08:30-09:00 Keynote Address: Warfare and InfoSec
- 09:00-10:15 Class I InfoWar: Attacks on Personal Information
- 10:15-10:45 Break for informal discussions by topic:
  - Privacy, Cryptography, Laws, Law Enforcement
- 10:45-12:00 Class II InfoWar: Corporate InfoSec
- 12:00-13:30 Buffet lunch and informal discussions by sector:
  - Corporate, Government, Military, Academic
- 13:30-14:45 Class III InfoWar: Global InfoSec
- 14:45-15:30 Informal discussions by network technology:
  - PCs, LANs, WANs, Internet
- 15:30-16:15 General discussions among panelists and other participants
- 16:15-16:30 Closing comments

The official language of the Conference is English.

## 3. SUBMISSIONS

The Program Committee will select a suitable number of participants for the panel discussions. Selection will be based on subjective judgements of who is likely to offer the most thoughtful and stimulating expositions and analyses of the topics.

Once panelists have been selected, the Program Committee requests that they submit a brief written analysis of the topic they agreed to speak on. This one- to ten-page document will be published in the Conference Handbook and will then appear in the Conference Proceedings along with additional materials added during the Conference.

Deadline for consideration as a panelist: 30 Sep 1994.

Confirmation of panel participation: 15 Oct 1994.

Deadline for submissions for inclusion in Conference Handbook:

15 Nov 94.

[Rest deleted. Write Mich for full text. 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 16: Issue 27**

**Thursday 21 July 1994**

## Contents

- [Pentagon computers cracked](#)  
[Mich Kabay](#)
- [Chemical Bank ATM's go down after snafu](#)  
[Josh Rivel](#)
- [Re: Crashed Bank Teller](#)  
[William Hugh Murray](#)
- [EPIC on Gore Letter](#)  
[David Sobel](#)
- [Re: Victim on the infobahn](#)  
[Marc Horowitz](#)  
[Jeffrey I. Schiller](#)  
[Max Hadley](#)  
[Bob Rahe](#)  
[John W. Burgeson](#)  
[Mich Kabay](#)  
[Andrew Marc Greene](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Pentagon computers cracked

"*Mich Kabay [NCSA Sys\_Op]*" <75300.3232@compuserve.com>  
21 Jul 94 19:45:03 EDT

>From the Associated Press newswire (94.07.21 @ 12:15 EDST) via Executive News Service (GO ENS) on CompuServe:

Internet-Hackers

By JOHN DIAMOND, Associated Press Writer

"WASHINGTON (AP) -- Intruders have been tapping into the Pentagon's unclassified computer system through the Internet for the past seven months and some have stolen, altered and erased records, officials said today.

Investigators have found no indication that the hackers have entered

classified systems that control critical functions such as nuclear weapons and the movement of troops and ships."

The author provides the following key points:

- o "...Betsy McDonald, spokeswoman for the Defense Information Systems Agency, said the compromised systems include those used for ballistic weapons research, aircraft and ship design, military payroll, personnel records, procurement, electronic mail, supercomputer modeling of battlefield environments and computer security research."
- o The Pentagon is taking the attacks seriously: the intruders evidently breached data confidentiality, damaged information integrity and threatened system availability.
- o The US and foreign attackers were able "to guarantee their ability to gain later access and to keep tabs on passwords needed to get into the system."
- o Michael Higgins, Deputy Director for Information Security at DISA (Defense Information Systems Agency) is reported as having said that "'major portions" of the Defense Department's unclassified networks had been penetrated by hackers, "adversely affecting DOD military readiness."
- o The attacks are related to the February 1994 CERT alert about network sniffers trapping passwords.
- o Because of the nature of computer crime, the Pentagon admits that it is difficult or impossible to determine the extent of the security breaches.
- o The Senate Armed Services Committee has been echoing the warnings of analysts [such as Winn Schwartau] about systematic attacks on the information infrastructure: "With almost no security protections, the nation faces the prospect of potentially grievous assaults by even small groups with limited resources."
- o Pentagon sources pointed to "the inherent difficulty of security for a computer system that, by its very design, allows outside access and easy communication."

[Comments from MK: gosh, and only one day after the preliminary announcement of the Second International Conference on Information Warfare, too... <g>]

Michel E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

---

## Chemical Bank ATM's go down after snafu

*Josh Rivel <csfb1!phantom!jrivel@uunet.uu.net>*

*Thu, 21 Jul 1994 03:06:21 -0400 (EDT)*

Chemical Bank's ATMs were out of commission for more than five hours, beginning at 6:45 a.m. on 20 July 1994. A routine file update was botched,

overloading the computer system. This came six months after Chemical systematically [no pun intended] charged its customers twice for cash withdrawals. [PGN abstracting from a NY Post article by Paul Tharp, Wed 20 Jul 1994.]

---

**Re: Crashed bank teller (Goossens, [RISKS-16.26](#))**

*William Hugh Murray <0003158580@mcimail.com>*

*Thu, 21 Jul 94 18:56 EST*

> The display I encountered contained a number of error messages (file  
> not found, could not create file, etc) followed by the prompt (A>).

Users of operating systems, such as MS-DOS and Unix, in which the operating system is owned by or owns the "standard input" often believe that the normal way for an application to fail is to return control to the user. (I have had this discussion ad nauseam with our beloved moderator, who seems unable to believe in any other failure mode for more than a few minutes at a time.)

In fact, for the first 30 years of computing that was an unusual way of failing. With the exception of those running on Unix, most applications failed by doing nothing or by returning the user to logon. IBM's MVS, the successor to an operating system for processing punched paper input and producing printed paper output, did not even know about terminals and had no operating system prompt. The prompt that the users saw came from a subsystem such as CICS. CICS Applications failed in many mysterious and disruptive ways but almost never by giving a legitimate user of an application unintended operating system privileges.

Applications running on Unix, an operating system originally intended by programmers for programmers, usually fail by returning control to the user at the operating system prompt. To limit the exposures associated with this mode of failure, Unix was extended with the "setuid" (set user id) function. The intent was to have applications run with a special limited profile. This would permit a user to run an application with privileges that would not be appropriate with all of the generality of the operating system. In practice programmers use the function to have their programs run with either their privileges or with "root" privileges. Setuid has hurt instead of helped.

Modern operating systems, such as OS/400, often have a mechanism like setuid that permits a user to run an application with privileges that are unique to the application. However, they do not permit the user to retain those privileges across the failure of the application. (Indeed, one of the things that characterizes such operating systems is that they have very few failure modes.)

Application machines, such as ATMs or the Teller described by the poster, should normally fail by doing nothing. While it is appropriate for my program to fail by returning ME to the operating system, my program should not fail by returning YOU to the operating system prompt with privileges that are different from those that you have on your own.

Application machines should fail by doing nothing. PAC-MAN never fails by exposing either itself or its host environment.

William Hugh Murray, New Canaan, Connecticut

---

## EPIC on Gore Letter

David Sobel <dsobel@washofc.epic.org>

Thu, 21 Jul 1994 14:55:05 EST

[Reprinted with permission from EPIC ALERT, Volume 1.04 (special edition), July 21, 1994 Published by the Electronic Privacy Information Center (EPIC) Washington, DC (Alert@epic.org)

SPECIAL EDITION -- "SON OF CLIPPER" [excerpts]

[1] Administration "Reversal" on Clipper

[2] EPIC Statement

[3] Letter from Gore to Cantwell

[4] What You Can Do (Email the VP)

=====  
[1] Administration "Reversal" on Clipper  
=====

A letter from Vice President Al Gore to Representative Maria Cantwell (D-WA) sent this week during Congressional debate on the Export Administration Act has raised important questions about the current state of the Clipper proposal. Some have hailed the statement as a major reversal. Others say the letter seals a bad deal.

Below we have included the letter from the Vice President, a statement from EPIC, and recommendations for further action.

=====  
[2] EPIC Statement on Gore Letter to Cantwell  
=====

News reports that the Clinton Administration has reversed itself on encryption policy are not supported by the letter from Vice President Gore to Maria Cantwell regarding export control policy. In fact, the letter reiterates the White House's commitment to the NSA's key escrow proposal and calls on the private sector to develop products that will facilitate electronic surveillance.

The letter from the Vice President calls on the government and the industry to develop jointly systems for key escrow cryptography. Key escrow is the central feature of the Clipper chip and the NSA's recommended method for electronic surveillance of digital communications.

The letter also reaffirms the Administration's support for

Clipper Chip as the federal standard for voice networks. There is no indication that the White House will withdraw this proposal. Statements that Clipper is "dead" are absurd.

The letter offers no changes in export control policy. It recommends instead that the status quo be maintained and that more studies be conducted. (The White House already completed such a study earlier this year. The results were never disclosed to the public, despite EPIC's request for release of the findings under the Freedom of Information Act.)

This is a significant setback for groups expecting that export control laws would be revised this year.

The White House expresses a willingness to allow unclassified algorithms and to hold key escrow agents liable for misuse. These are the only provisions of the Gore letter favorable to the user community. But neither provision would even be necessary if the White House did not attempt to regulate cryptography in the first place.

The Administration's willingness to accept private sector alternatives to Clipper for data networks essentially ratifies an agreement to develop "wiretap ready" technologies for data networks.

We believe the letter from the Vice President is essentially a blueprint for electronic surveillance of digital networks. The government will set out the requirements for surveillance systems such as key escrow, and the industry will build complying systems.

The plan dovetails neatly with the FBI's Digital Telephony proposal, which will establish legal penalties for companies and users that design systems that cannot be wiretapped.

We do not believe this is in the interests of users of the information highway. Key escrow necessarily weakens the security and privacy of electronic communications. It makes networks vulnerable to tampering and confidential messages subject to compromise. It is the approach urged by organizations that specialize in electronic eavesdropping. No group of Internet users has ever called for key escrow encryption.

If this proposal goes forward, electronic surveillance will almost certainly increase, network security will be weakened, and people who design strong cryptography without key escrow could become criminals. This is not a victory for freedom or privacy.

We support unclassified standards and relaxation of export controls. We cannot support the premise that the government and industry should design key escrow systems. We also do not believe that Clipper is an appropriate standard for federal voice communications.

We are asking the Vice President to reconsider his position and urging network users to make known their concerns about the

proposal.

Electronic Privacy Information Center  
Washington, DC  
July 21, 1994

=====  
[3] Letter from Gore to Cantwell  
=====

THE VICE PRESIDENT  
WASHINGTON

July 20, 1994

The Honorable Maria Cantwell House of Representatives Washington, DC 20515

"Dear Maria,

"I write today to express my sincere appreciation of your efforts to move the national debate forward on the issue of information security and export controls. I share your strong conviction for the need to develop a comprehensive policy regarding encryption, incorporating an export policy that does not disadvantage American software companies in world markets while preserving our law enforcement and national security goals.

"As you know, the Administration disagrees with you on the extent to which existing controls are harming U.S. industry in the short run and the extent to which their immediate relaxation would affect national security. For that reason we have supported a five-month Presidential study. In conducting this study, I want to assure you that the Administration will use the best available resources of the federal government. This will include the active participation of the National Economic Council and the Department of Commerce. In addition, consistent with the Senate-passed language, the first study will be completed within 150 days of passage of the Export Administration Act reauthorization bill, with the second study to be completed within one year after the completion of the first. I want to personally assure you that we will reassess our existing export controls based on the results of these studies. Moreover, all programs with encryption that can be exported today will continue to be exportable.

"On the other hand, we agree that we need to take action this year to ensure that over time American companies are able to include information security features in their program in order to maintain their international competitiveness. We can achieve this by entering into a new phase of cooperation among government, industry representatives and privacy advocates with a goal of trying to develop a key escrow encryption system that will provide strong encryption, be acceptable to computer users worldwide, and address our national security needs as well.

"Key escrow encryption offers a very effective way to accomplish our mutual goals. That is why the Administration adopted the key escrow encryption standard in the "Clipper Chip" to provide very secure encryption for telephone communications while preserving the ability for law enforcement and national security. But the Clipper Chip is an approved federal standard for telephone communication and not for computer networks and video networks. For that reason, we are working with industry to investigate other technologies for these applications.

"The administration understands the concerns that industry has regarding the Clipper Chip. We welcome the opportunity to work with industry to design a more versatile, less expensive system. Such a key escrow scheme would be implementable in software, firmware or hardware, or any combination thereof, would not rely on a classified algorithm, would be voluntary, and would be exportable. While there are many severe challenges to developing such a system, we are committed to a diligent effort with industry and academics to achieve such a system. We welcome your offer to assist us in furthering this effort.

"We also want to assure users of key escrow encryption products that they will not be subject to unauthorized electronic surveillance. As we have done with the Clipper Chip, future key escrow schemes must contain safeguards to provide for key disclosure only under legal authorization and should have audit procedures to ensure the integrity of the system. Escrow holders should be strictly liable for releasing keys without legal authorization.

"We also recognize that a new key escrow encryption system must permit the use of private-sector key escrow agents as one option. It is also possible that as key escrow encryption technology spreads, companies may establish layered escrowing services for their own products. Having a number of escrow agents would give individuals and businesses more choice and flexibility in meeting their needs for secure communications.

"I assure you the President and I are acutely aware of the need to balance economic and privacy needs with law enforcement and national security. This is not an easy task, I think that our approach offers the best opportunity to strike an appropriate balance. I am looking forward to working with you and others who share our interest in developing a comprehensive national policy on encryption. I am convinced that our cooperative endeavors will open new creative solutions to this critical problems."

Sincerely  
/s/ Al Gore

=====  
[4] What You Can Do (Email the VP)  
=====

The Clipper debate has reached a critical juncture. The White House and industry are about to seal a deal to make key escrow the standard for encrypted communications. If you believe that individuals should have the right to make full use of new technologies to protect privacy, now is the time for your voice to be heard (and your email to be sent).

EMAIL the Vice President at [vice.president@whitehouse.gov](mailto:vice.president@whitehouse.gov)

- Thank him for the Administration's willingness to reconsider its views on Clipper.
- Express support for the decision to support unclassified algorithms and liability for key escrow agents.
- But urge him not to require key escrow as a standard for encryption products.
- Emphasize that key escrow is the soul of Clipper, the method for conducting electronic surveillance of digital communications.
- Call for extensive testing and studies before any key escrow system is deployed.

You should also:

- Urge him to withdraw Clipper as a standard for voice communications.
- Urge him to support relaxation of export controls.
- Ask for the public release of the earlier White House study on cryptography.
- Ask for the public release of White House documents reviewing the weaknesses of the key escrow proposal.

The Vice President has clearly shown a willingness to listen to the concerns of the user community on this issue. Your letter could make a difference.

[This message is included for your information. Whether you agree or disagree with David's recommendations, if you care to, write and tell the VP and cc: David Sobel <[dsobel@washofc.epic.org](mailto:dsobel@washofc.epic.org)>. PGN]

---

**Re: Victim on the infobahn (Donahue, [RISKS-16.26](#))**

Marc Horowitz <[marc@MIT.EDU](mailto:marc@MIT.EDU)>

Wed, 20 Jul 94 22:15:20 EDT

<> I'm thinking now of writing a magazine article on our  
<> experience, and am posting for two reasons. First, I'd like to hear

<> from people who, like me, have become "victims on the infobahn," and  
<> second, I'd like to get some broader perspective.

If this is a problem with the information superhighway, it's been  
around since the horse-and-buggy days the information dirt road.

This is not a new problem. I can recall similar incidents happening over a  
decade ago, and I'm only 23 years old. I suspect occurrences that this  
problem will increase for a short period of time, while networking gains  
popularity, but decrease soon after, as data telecommunications (ISDN, frame  
relay, ATM, etc) becomes more popular. It's really hard to wake somebody up  
in the middle of the night with a misdirected ATM packet! I've yet to have  
someone complain at an errant ICMP echo, myself.

Marc

---

### **Victim on the infobahn (Donahue, [RISKS-16.26](#))**

*Jeffrey I. Schiller <jis@mit.edu>*

*Thu, 21 Jul 94 00:28:35 -0400*

This sort of situation is not new. I remember a problem we had with a uucp  
dial-out line in 1983. Someone added a dial-out entry but transposed two  
digits in the destination telephone number. This meant that once an hour  
we were calling up some poor folks and annoying them all night long!

Luckily this only happened over one night. In the morning I investigated why  
none of our uucp connections to that host completed, and noticed the typo. I  
did call up the people who we had been bothering (sort of hoping that the  
number would be invalid and no one had been bothered!) and emphatically  
apologized for our error. They were understanding. I guess it helped that I  
was *\*not\** a lawyer and was able to empathize with their plight. In fact I felt  
good about the call afterwards... now I knew that these folks would know what  
had happened and would not fear that someone was after them!

Jeff

---

### **Re: Victim on the infobahn (Telephone protocols) (Donahue, 16.26)**

*Max Hadley <mrh@shl.co.uk>*

*Thu, 21 Jul 1994 11:25:10 +0100*

Mr Donahue's predicament is symptomatic of a wider problem which will grow  
over the next few years - 'semantic overload' of the telephone system. PTT's  
and Telco's are still stuck in a mode where a telephone line is used to allow  
one human being to talk to another. In fact, more and more phone lines are  
connected to machines, many of which can initiate as well as receive calls,  
and vary in levels of human compatibility. Examples range from answering  
machines, through voice mail systems, fax machines, 'smart boxes', pagers,  
alarm systems, modems, all the way up members of the International Union of  
Deaf-Mute Dyslexic Telephonists :-). The current telephone system is a mess -

it allows anything to connect to anything at any time, regardless of compatibility, and regardless of the consequences. Yet this proliferation of machines that use the telephone network has arisen precisely because of the flexibility of connection on the telephone network. People use the phone system to send text messages via fax and email, although the Telex system in theory provides most of the same facilities. It just wasn't flexible enough. To make the situation more bearable, without restricting connectivity, an extension of caller ID could be made, so the calling line can say 'I am a xxxx and I understand yyyy protocols'. Only once a 'speech' protocol is negotiated between the ends of the link does the phone actually ring. Of course, this requires Mr Donohue to purchase a phone with this facility. However, such a phone could also route calls around his fax, modem, answering machine & WHY, and would provide a better solution than the various 'smart boxes' currently on the market. Or we could sit back and wait for the Coming Of Broadband ISDN/ATM.

Max Hadley | Stewart Hughes Ltd.,  
Principal Consultant | School Lane, Chandlers Ford  
| Eastleigh, Hampshire SO53 4YG UK  
mrh@shl.co.uk | Tel: +44 (0) 703 270027 x215  
mrh@shluk.uucp | Fax: +44 (0) 703 270007

---

## Re: Victim on the infobahn (Bill Donahue)

*Bob Rahe <bob@hobbes.dtcc.edu>*

*Thu, 21 Jul 1994 08:28:37 EDT*

In [RISKS-16.26](#) Bill Donahue writes of an incident of a 'modem' dialing his home and giving him and his wife some apparent cause for worry for their safety.

I'm not so sure I'd call his experience a fatality on the info-bahn, maybe a pebble on the windshield(!).

I had a similar experience when a local school district put my home phone number into their FAX machine as the number for the local TV station. I'd get calls every 5 minutes for random amounts of time and random times of the day. By the time I'd run upstairs and get my fax software ready to go (faxes have a "chirp" from the calling to caller machines that make it easy to tell it was a fax) it would stop. Then it would quit for days or weeks...

I finally caught them, read the organization from the top of the fax, and called. They were profusely sorry but...

I wonder tho, most of the failure here was purely human - mis-setting the number and then failing to notice that the fax never got sent to its intended recipient. I'd assume the machine would somehow tell the operator that an automatic retry had failed after <x> attempts. But then again, when I called it took a bit to explain what the problem was to them....

Bob Rahe, Delaware Tech&Comm College, Computer Center, Dover, Delaware  
Internet: bob@hobbes.dtcc.edu

---

## Victim on the Autobahn

*"John W. Burgeson, 73531,1501 on Compuserve" <jburgeson@VNET.IBM.COM>  
Thu, 21 Jul 94 12:01:57 CDT*

Bill Donahue's experience at least happened "all at once." We had the misfortune to get a new phone number which had once been that of a genealogy BBS -- it took us a few weeks to realize that this number was being shared by genealogy buffs all over the world! For several reasons, we could not change our number. The calls continued at the rate of 2 to 3 a week for over a year! I put appeals on a number of FORUMS in PRODIGY & Compuserve (DO NOT CALL 512-250-xxxx) and after 18 months the calls are down to about one or two a month.

My TAD response, you might believe, is just a trifle surly!

John W. Burgeson, 73531,1501 on Compuserve

---

## Harassment by modem (Donahue, [RISKS-16.26](#))

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
21 Jul 94 08:33:55 EDT*

Thanks to Mr. Donahue for posting the interesting anecdote about the heavy-breathing modem.

Periodically over the years, people have set their fax machine to dialing my voice line instead of my fax line. Some of the fax machines have been quite persistent; usually the fax operator will notice the repeated failures and call up to complain that my fax machine isn't responding. However, in one case, the maddening thing dialed me up every ten minutes for over two hours. I fixed that one by hooking my fax machine to my voice line just before the next scheduled interruption and actually receiving the fax.

It would make sense for fax and modem manufacturers to distinguish between a non-responding telephone line (no answer or busy) and a non-responding device. Most modems can generate an error message (e.g., "VOICE") when appropriately programmed; it would be helpful if both fax machines and modems treated an answer-but-no-tone event by alerting the operator immediately instead of mindlessly redialing.

Michel E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

P.S. Two minor matters.

---

## Modems and faxes

*<Andrew\_Marc\_Greene@frankston.com>*

*Thu, 21 Jul 1994 12:50 -0400*

I've said it before and I'll say it again.

Modems and fax machines should be programmed that on an outgoing call, until they establish a connection, they play a digitized recording along the lines of "This is a modem call" -- and there should be an AT command to append "from xxx-xxx-xxxx" Of course, this isn't the kind of feature that will cause many potential customers to choose your line over someone else's.

- Andrew Greene

[Bob Frankston suggested once again that we should have some redundant check digits on phone numbers as well, to minimize wrong numbers. Our subsequent off-line discussion went into how knowledge of the algorithm would not prevent people from fabricating consistent but incorrect numbers. I just thought I'd mention it... 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 16: Issue 28

Friday 22 July 1994

## Contents

- [Hoods Hit the Highway](#)  
[Jon Loeliger](#)
- [Dutch police victim of phone-tapping criminals](#)  
[Ralph Moonen](#)
- [As the Worm Turns--Ant-icipating Problems](#)  
[Mich Kabay](#)
- [It's a real world out there, and the Internet is part of it.](#)  
[Phil Agre](#)
- [Automated mail listserver causes "Spamming" on the Internet](#)  
[Jean Renard Ward](#)
- [Leahy Statement on Gore Statement on Clipper](#)  
[Marc Rotenberg](#)
- [Privacy Journal this month](#)  
[Robert Ellis Smith](#)
- [CFP: IEEE Symposium on Security and Privacy](#)  
[Catherine A. Meadows](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Hoods Hit the Highway

*Jon Loeliger <jdl@healthcare.com>*

*Fri, 22 Jul 1994 09:49:25 -0500*

From Jon Loeliger, Healthcare Communications Inc. [jdl@healthcare.com](mailto:jdl@healthcare.com)

Hoods Hit the Highway; Computer users warned of scams

By Charlotte Anne Lucas

Austin Bureau of The Dallas Morning News

Dallas Morning News, 1 July 1994,

REPRINTED WITH PERMISSION OF THE DALLAS MORNING NEWS

AUSTIN -- Computer users, beware: Driving on the information highway,  
it's possible to get fleeced.

Scam artists have hit the cyberspace, offering high-tech ponzi schemes, sending illegal electronic chain letters and hyping virtually worthless stock, according to state securities regulators across the nation.

In Texas, regulators say an Austin retiree lost \$10,000 in a fake mutual fund deal sold by a man who promoted his "money managing" skills through an on-line computer service.

"The danger here is that cyberspace, which could be a beneficial way for consumers to do a better job of informing themselves, will instead be discredited as a haven for fast-buck artists," said Denise Voigt Crawford, the Texas Securities Commissioner.

In New Jersey and Missouri on Thursday, securities regulators filed cease and desist orders against promoters who used computer links to tout allegedly fraudulent deals. Texas regulators say it is likely that they will seek an indictment in the case of the nonexistent mutual fund.

But with nearly 4 million computer users nationwide linked into commercial computer services and 20 million people on the internet, a world-wide computer network, "it is almost too big to police effectively," said Jared Silverman, chief of the New Jersey Bureau of Securities and chairman of a multi-state team that investigates computer fraud.

In response, regulators in all 50 states issued a bulletin to investigators, describing the potential frauds and listing steps small investors can take to protect themselves. "We're trying to tell people to be careful," said Ms. Crawford, "there is a new fraud on the horizon."

Although regulators are concerned about the problem, Ms. Crawford acknowledges enforcement will be a challenge. Because electronic conversations, or E-mail, are considered private, "we don't know what difficulties we are going to have getting subpoenas enforced or what kind of cooperation we will get from (commercial bulletin board systems)." [sic]

Officials say promoters tend to advertise offers or stock tips on the financial bulletin board sections of on-line computer services such as CompuServe, America Online and Prodigy, or in the specialized discussion forums in the Internet.

Regulators said that of 75,000 messages posted on one computer service bulletin board during a recent two-week period, 5,600 were devoted to investment topics. While some commercial computer bulletin board services try to control the publicly posted investment tips, most do not try to control most communications on the service.

What begins as innocent E-mail can end with an unwary investor "getting cleaned out by high-tech schemers," said Ms. Crawford.

In Texas, the case under investigation began when an Austin retiree

posted a public note in a commercial bulletin board system looking for conversations about the stock market, according to John A. Peralta, deputy director of enforcement at the Texas Securities Board.

"He was contacted. It turned into a private E-mail conversation, a telephone conversation and then exchanges through the mail," said Mr. Peralta. But the person who promoted himself on the computer as a skilled money manager turned out to be unlicensed -- and the mutual fund the retiree invested in turned out to be nonexistent.

Mr. Peralta said at least one other person, not from Texas, invested \$90,000 in the same deal, "We are aware of two, but we don't really know," he said. "There may be dozens of victims."

Securities regulators began taking interest in on-line scams last fall, after Mr. Silverman -- a computer junkie -- raised the issue at a national meeting of regulators. "I heard stories about things going on on computer bulletin board services, and I have been monitoring these things for close to a year," he said.

In fact, the New Jersey case came from Mr. Silverman's off-hours cruising of an on-line service. "I sit at a keyboard two hours a day -- to the chagrin of my wife -- scanning these things," he said.

What he found was a promoter pushing an E-mail chain letter. The promoter, identified only as from San Antonio, claimed that in exchange for \$5, investors could earn \$60,000 in three to six weeks.

Regulators said participants were told to send \$1 to each of five people on a list in the computer bulletin board, add their own name to the list and post it on 10 different computer bulletin board sites.

That, regulators said in a statement, "amounted to a high-tech variation on the old pyramid scam, which is barred by federal and state laws."

In Missouri, regulators Thursday moved against an unlicensed stockbroker for touting his services and "making duubious [sic] claims for stocks not registered for sale in the state." Among other things, regulators said, the promoter falsely claimed that Donald Trump was a "major, behind-the-scenes player in a tiny cruise line" whose stock he pitched.

Ms. Crawford said that while computer users may be sophisticated in some ways, they still are attractive targets because they tend to have discretionary income and frequently are looking for ways to invest their money.

Some of the commercial services also allow users to use various aliases, making it all the more difficult for investigators to figure out who they are really communicating with.

---

## Dutch police victim of phone-tapping criminals

*Ralph Moonen <ralph@inter.nl.net>*

*Fri, 22 Jul 1994 11:59:33 +0200*

Usually law enforcement's arguments for regulated encryption center around their ability to tap criminal's conversations. In the Netherlands this discussion has taken a whole new twist when Dutch newspaper De Telegraaf laid hands on phone-tap recordings not from the police, but from criminals who had tapped various high police officials' home and work phones. Needless to say the newspaper published transcripts of the recordings which proved to be quite interesting. (Proving police used several illegal means of gathering evidence and revealing a lot of internal trouble in the police dept.)

Soon after publication police officials called for more funding to be able to buy encryption devices. Was this just naivety on the part of the police to assume criminals couldn't wire-tap or was it an isolated incident where the criminals got lucky? Evidence supports only the first assumption. Hopefully this incident will lead to more discussion on encryption technology. A while ago legislation was proposed to ban encryption without having a permit for such devices. This proposal was cut down in light of strong opposition from industry and commerce. After that, no-one in the Netherlands really took up the issue, which I think we all agree upon is one of the most important ones of the information age.

Oh, the RISK? I dunno, but I think it's obvious :-)

--Ralph

---

### **As the Worm Turns--Ant-icipating Problems**

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>*

*22 Jul 94 08:47:44 EDT*

>From the United Press International newswire (94.07.21 @ 12:17 EDST) via CompuServe's Executive News Service (GO ENS):

Ants help BT improve computers

By SIMONA de LOGU

"LONDON, July 21 (UPI) -- British Telecom scientists are exploring ways of making computer programs more robust and adaptable by using ant colonies as models for interactive programs that respond to changing conditions in computer networks.

A team of computer specialists based at BT's Martlesham Heath laboratories in Ipswich, east England, has been studying research material on ants for the past two years and using their findings on developing programs."

Key points from the article:

- o "Our system is made up of small, autonomous, reactive, mobile blocks of computer code that interact in a way derived from ant behavior," said scientist Simon Steward. "The control system that emerges from all of these mobile software agents working together is inherently adaptable and robust unlike normal computer programs."
- o The goal of the work is to prevent system crashes when an unanticipated [PGN, please forbear] condition occurs.
- o The distributed computing model uses message-passing to coordinate computation.
- o "The programs are mobile like ants, moving from one computer to another, when needed."
- o After making software or parameter changes, the "mobile programs" would "leave messages for other programs on how the system has been adapted."
- o Modules will display "a certain amount of random behavior...."
- o The system will display heuristic, goal-seeking behaviour.

[Comments from MK follow:]

Programs that move from system to system are usually called worms. The work described above is related to Von Neumann's concepts of cellular automata, and I guess would count as an example of "artificial life" or a-life. The idea that semi-autonomous computer programs would migrate from place to place reminds one of the debate about "useful viruses."

I was getting antsy about this (the idea was really bugging me), so I searched on "ant or ants" in the Ziff Computer Database Plus (GO COMPDB on CompuServe) and located an article in Computergram International (June 10, 1994), p. 15 entitled, "British Telecom's research lab claims to have found the fastest Travelling Salesman algorithm." In this application, which runs on a single RISC workstation, "The search algorithm is set in motion on a problem to find the shortest travelling distance between several cities, for example. In effect a whole series of `ants' are thrown on a map of the area and if the system doesn't find a destination city, it dies, whereas if it does find a chosen destination city it `gives birth' and grows." A path is then established between cities. The algorithm is very fast--two seconds for a 100-point optimization problem and 2.5 minutes for 1000 points.

All this is fascinating, and I naturally wondered about the implications for system reliability. Turning back to the UPI story, it seems to me that there must be a lot of work to include quality assurance principles into heuristic, semi-autonomous algorithms that change system or network configuration. The consequences of malfunction increase when the problems occur in control structures e.g., a hole in your hose can swamp your lawn, but a bug in your electronic shutoff valve that reverses inputs (off ->

on) can really put a bee in your bonnet.

One of the main objections to free-roaming software worms and viruses is that they (themselves) offer no opportunity for a system manager or owner to block their activity (one can usually do so with antivirus tools, though). When a system is seeded with these rogue programs, one never knows what will flower. Who wants untested software making changes in her computer system? Similarly, how do we cope with "genetic" algorithms that spontaneously make changes in, say, operating system tables or even executable code? How does one test a real-time change in the operating system?

It will be interesting to follow this work and see how concerns for reliability are worked into this evolving field.

Michel E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

---

### **It's a real world out there, and the Internet is part of it.**

*Phil Agre <pagre@weber.ucsd.edu>*

*Fri, 22 Jul 1994 14:21:17 -0700*

Many denizens of the Internet think of it as a place of untrammelled free speech and decentralized democracy. Evidence is accumulating that it's more complicated than that. Writing in the liberal journal *\_The Nation\_*, Jon Wiener (a historian at UC Irvine whose does a sort of investigative journalism) outlines some of the complications. The full reference is:

Jon Wiener, Free Speech on the Internet, *The Nation* 258(23), 13 June 1994, pages 825-828.

He describes the Karla Homolka trial in Canada, a group of Turks who swamp newsgroups with automatic messages denying the Armenian genocide, gun activists taking over alt.motherjones, libel suits provoked by on-line statements, gender imbalances, abusive behavior by unreformed net-guys, and more. None of which means the net is bad; it just means the net is part of reality. At one level the Risk is computer-related: bad stuff can happen on-line, just like in real life. But the real Risk comes from believing the hype: just because it's decentralized doesn't make it democratic. If we want democracy we have to actively make it. Just like in real life.

Phil Agre, UCSD

---

### **Automated mail listserver causes "Spamming" on the Internet**

*Jean Renard Ward <jrward@midget.ptltd.com>*

*Fri, 22 Jul 94 08:49:50 EDT*

The past week I have been getting filled-out copies of a survey form completed by beta users of the netsurf.com services. Each day up to a half-dozen of

these forms would show up in my Internet mailbox.

Evidently the problem caused by three factors: (1) the original survey form had in the "cc:" field the listserv address for mailing to the entire beta user group, (2) many of the beta users had "reply to all" set as the default for their mailer software, and (3) the folks at netsurf.com had configured their listserver to remail the incoming Emails with the completed forms back out to the addresses on their beta user list.

The only interesting thing about getting the completed survey forms is that most of the respondents to the survey seemed to be middle-aged males with "erotica" as one of their interests in using the Internet. Netsurf's questionnaire specifically stated that they had no interest in invading anyone's privacy, so that the questionnaire would be effectively confidential, even though they could not guarantee that formally.

Notes Emailed to netsurf.com had no effect. Finally, out of frustration, I did a "reply to all" on one of the incoming forms with a note about the problem back out to the same listserver. Although this was an act of "spamming" on its own, it did get the people at netsurf.com to address (intentional pun) the problem.

A last note: I got a note from netsurf.com blaming me and all those users who had set "reply to all" as the default in their mail software for spamming their beta user list, rather than admitting that they had overlooked the possible effects of their listserver and mailing configuration.

By the way -- this is being sent with a cc: to netsurf.com.

---

*Marc Rotenberg <rotenberg@washofc.epic.org>*

*Fri, 22 Jul 1994 15:48:32 EST*

Subject: Leahy Statement on Gore Statement on Clipper

U.S. SENATOR PATRICK LEAHY, Vermont

STATEMENT OF PATRICK LEAHY ON  
VICE PRESIDENT GORE'S CLIPPER CHIP LETTER

July 21, 1994

I have read the July 20th letter from the Vice President about the Administration's current thinking on Clipper Chip and, to my mind, it represents no change in policy. In fact, when this letter was sent, I would be surprised if the Administration even thought it was news.

The letter makes clear to me that the Administration continues to embrace key escrow encryption technology, and stands behind Clipper Chip as a federal standard for telephone communications. The official standard makes clear that this standard applies to any communications over telephone lines. Those communications include not only voice, but

also low-speed computer data and facsimile messages. The Administration is working on encryption technologies for higher-speed transmissions, such as for computer networks and video networks.

The Vice President says that they want to work with industry to design a key escrow system that could be implemented not just in hardware, but also in software, that would be voluntary, exportable and not rely upon a classified encoding formula. The Administration said all this last February when the federal standard was approved. Yet, when Administration witnesses were questioned about the progress they had made in this effort at my Judiciary subcommittee hearing in early May, I learned they had held only a few meetings.

Last week, the Appropriations Committee accepted strong Report language I suggested on Clipper Chip. The Attorney General is directed to report to Congress within four months on ten areas of concern about Clipper Chip.

I agree with the Vice President that balancing economic and privacy needs with law enforcement and national security is not always an easy task. But we can do better than Clipper Chip.

---

### **Privacy Journal this month**

*Robert Ellis Smith <0005101719@mcimail.com>*

*Fri, 22 Jul 94 14:38 EST*

Here are the headlines from the July 1994 PRIVACY JOURNAL:

DIVORCE LAWYERS FIND A SPOUSE'S PC A GOLD MINE

A TENTATIVE PROPOSAL FOR A NATIONAL ID CARD

AN ILLUSTRATION ON HOW MATT BLAZE DISCOVERED A HOLE IN CLIPPER

A NEW DATA BASE FOR BRADY GUN-CONTROL LAW

TWO PRIVACY CLEARINGHOUSES SEEK FUNDING

HOW VEGAS AND JERSEY KEEP A COMPUTERIZED EYE ON HIGH ROLLERS

A VICTIM OF E-MAIL PROFANITIES LOSES LAWSUIT

CALIFORNIA BEGINS NEW 'OPT-OUT' FOR CREDIT-CARD CUSTOMERS

Robert Ellis Smith/Publisher 401/274-7861, or 0005101719@mcimail.com

[The all-caps format makes it begin to sound like a weekly tabloid. PGN]

---

### **CFP: IEEE Symposium on Security and Privacy**

Catherine A. Meadows <meadows@itd.nrl.navy.mil>

Fri, 22 Jul 94 17:27:46 EDT

CALL FOR PAPERS

1995 IEEE Symposium on Security and Privacy  
May 8-10, 1995  
Oakland, California

sponsored by

IEEE Computer Society Technical Committee on Security and Privacy

in cooperation with

The International Association for Cryptologic Research (IACR)

The Symposium on Security and Privacy has for fifteen years been the premier forum for the presentation of developments in computer security, and for bringing together researchers and practitioners in the field.

This year, we seek to build on this tradition of excellence by re-emphasizing work on engineering and applications as well as theoretical advances. We also seek to broaden the scope of the Symposium by introducing new topics. We want to hear not only about new theoretical results, but also about work in the design and implementation of secure systems and work on policy relating to system security. We are particularly interested in papers on policy and technical issues relating to privacy in the context of the information infrastructure, papers that relate software and system engineering technology to the design of secure systems, and papers on hardware and architectural support for secure systems.

The symposium will focus on technical aspects of security and privacy as they arise in commercial and industrial applications, as well in government and military systems. It will address advances in the theory, design, implementation, analysis, and application of secure computer systems, and in the integration and reconciliation of security and privacy with other critical system properties such as reliability and safety.

Topics in which papers and panel session proposals are invited include, but are not limited to, the following:

Secure systems    Privacy Issues    Access controls  
Security verification    Network security    Policy modeling  
Information flow    Authentication    Database security  
Data integrity    Security Protocols    Viruses and worms  
Auditing    Biometrics    Smartcards  
Commercial and industrial security    Intrusion Detection  
Security and other critical system properties    Distributed systems

A new feature of the symposium this year will be a special session of very brief (5-minute) talks. Our goal is to make it possible for us to hear from people who are advancing the field in the areas of system design and implementation, and who would like to present their ideas to the symposium audience but may lack the time and resources needed to prepare a full paper. Submissions for this session will be accepted up to five weeks before the symposium, to permit us to hear of the most recent developments. Abstracts of these talks will be distributed at

the conference.

#### INSTRUCTIONS TO AUTHORS:

Send six copies of your paper and/or proposal for a panel session to Catherine Meadows, Program Co-Chair, at the address given below. Papers and panel proposals must be received by November 7, 1994. Papers, which should include an abstract, must not exceed 7500 words. The names and affiliations of the authors should appear on a separate cover page only, as a "blind" refereeing process is used. Authors must certify prior to December 25, 1994 that any and all necessary clearances for publication have been obtained.

Papers must report original work that has not been published previously, and is not under consideration for publication elsewhere. Abstracts, overlength papers, electronic submissions, late submissions, and papers that cannot be published in the proceedings will be rejected without review. Authors will be notified of acceptance by January 16, 1995. Camera-ready copies are due not later than March 6, 1995.

Panel proposals should describe, in two pages or less, the objective of the panel and the topic(s) to be addressed. Names and addresses of potential panelists (with position abstracts if possible) and of the moderator should also be included.

Submitters of abstracts for the special session of five-minute talks should submit one page abstracts to Catherine Meadows, program co-chair, at the address given below. Abstracts must be received by April 3, 1995. Authors will be notified of acceptance or rejection of abstracts by April 17. Submitted abstracts that are accepted will be distributed at the conference.

The Symposium will also include informal poster sessions where preliminary or speculative material, and descriptions or demonstrations of software, may be presented. Send one copy of your poster session paper to Carl Landwehr, at the address given below, by January 31, 1995, together with certification that any and all necessary clearances for presentation have been obtained.

Also for the first time this year, we will attempt to counsel prospective authors. If you have questions about whether or how to present your work to the symposium, please send e-mail to the Chair (landwehr@itd.nrl.navy.mil), and we will do our best to assist you.

Information about this conference will be also be available by anonymous ftp from chacs.itd.nrl.navy.mil in directory /pub/SP95, by World Wide Web from <http://www.itd.nrl.navy.mil/ITD/5540/announce/SP95.html>, or by sending email to sp95@itd.nrl.navy.mil.

#### PROGRAM COMMITTEE

Ross Anderson, Cambridge University, UK

Steve Bellovin, AT&T, USA  
Tom Berson, Anagram Laboratories, USA  
Oliver Costich, Independent Consultant, USA  
George Dinolt, Loral, USA  
Cristi Garvey, TRW, USA  
Li Gong, SRI, USA  
Sushil Jajodia, GMU, USA  
Steve Kent, BBN, USA  
Steve Lipner, TIS, USA  
Teresa Lunt, ARPA/CSTO, USA  
John McLean, NRL, USA  
Jonathan Millen, Mitre, USA  
Birgit Pfitzmann, Universit"at Hildesheim, Germany  
Sylvan Pinsky, DoD, USA  
Michael Reiter, AT&T, USA  
Jaisook Rho, TIS, USA  
Peter Ryan, DRA, UK  
Tom Schubert, Portland State University, USA  
Paul Syverson, NRL, USA  
Vijay Varadharajan, HP, UK  
Raphael Yahalom, Hebrew University, Israel

For further information concerning the symposium, contact:

Carl Landwehr, General Chair	Catherine Meadows, Program Co-Chair
Naval Research Lab., Code 5542	Naval Research Laboratory, Code 5543
4555 Overlook Ave., SW	4555 Overlook Ave., SW
Washington DC 20375, USA	Washington DC 20375, USA
Tel: +1 (202) 404-8888	Tel: +1 (202) 767-3490
FAX: +1 (202) 404-7942	FAX: +1 (202) 404-7942
landwehr@itd.nrl.navy.mil	meadows@itd.nrl.navy.mil

Dale Johnson, Vice Chair	John McHugh, Program Co-Chair
The MITRE Corporation	Computer Science Department
Mailstop A156	Portland State University
202 Burlington Rd	P.O. Box 751
Bedford, MA 01730-1420, USA	Portland OR 97207-0751, USA
Tel: +1 617-271-8894	Tel: +1 (503) 725-5842
Fax: +1 617-271-3816	Fax: +1 (503) 725-3211
dmj@mitre.org	mchugh@cs.pdx.edu

Charles Payne, Treasurer  
Naval Research Lab., Code 5542  
4555 Overlook Ave., SW  
Washington DC 20375, USA  
Tel: +1 (202) 404-8763  
FAX: +1 (202) 404-7942  
payne@itd.nrl.navy.mil

Peter Ryan, European Contact	Jim Gray, Asia/Pacific Contact
Defence Research Agency	Department of Computer Science
Room NX17	Hong Kong Univ. of Science & Technology
St Andrew's Rd	Clear Water Bay, Kowloon, Hong Kong
Malvern	Tel: +852 358-7012

Worcs WR14 3PS,UK  
Tel +44 (0684) 895845  
Fax +44 (0684) 894303  
ryan@rivers.dra.hmg.gb

Fax: +852 358-1477  
gray@cs.ust.hk



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 16: Issue 29**

**Tuesday 26 July 1994**

## Contents

- [Let me off the Information Superhighway!](#)  
[Nancy Leveson](#)
- [Risks of assuming standard interfaces](#)  
[Clive D.W. Feather](#)
- [Airport codes](#)  
[Clive D.W. Feather](#)
- [Embezzlement at Beijing Hotel](#)  
[Mich Kabay](#)
- [Remote reading of gas meters](#)  
[Mich Kabay](#)
- [Hack FAQ \(summary\)](#)  
[Martin Minow](#)
- [Risks of being unable to clear records](#)  
[Marcus J Ranum](#)
- [More inadvertent mail list "spamming"](#)  
[Phillip Finch](#)
- [Two kinds of risks](#)  
[Robert Morrell Jr.](#)
- [Risks of hot lines](#)  
[Philip H. Smith III](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Let me off the Information Superhighway!

*Nancy Leveson <[leveson@cs.washington.edu](mailto:leveson@cs.washington.edu)>  
Sat, 23 Jul 1994 18:56:17 PDT*

I have started to get strange email requests wanting to chat with me about security, DES encryption standards, and advice on how to get rid of hackers who are intruding on their machines. When I reply that I am not a security expert, the replies have been equally as weird. I found out that somebody has published a book called "Email Addresses of the Rich and Famous" (of which I am neither) and that I am listed on the center of page 8 as a security expert. Apparently, my entry is not the only error in this book.

Godin, Seth "E-MAIL addresses of the Rich & Famous"

Copyright 1994 by Seth Godin Productions, Inc.

Addison-Wesley Publishing Company Inc.

ISBN: 0201408937

This book appears to be on the same level as those who sell maps and addresses to the stars homes in Hollywood (and about as accurate), and I am appalled that a reputable publisher like Addison-Wesley would be involved in such an obviously unchecked invasion of privacy. The time involved in dealing with this unwanted mail is starting to interfere with my work. Can I sue? Is this happening to other readers of the RISKS Forum?

I wrote to the editor of my software safety book at Addison-Wesley and asked him to get me the name and email address of the \$!&^%# editor at Addison-Wesley responsible for this so I can post his/her address on the alt.sex.kinky bboard :-).

Nancy Leveson

---

### Risks of assuming standard interfaces

"Clive D.W. Feather" <clive@sco.com>

Mon, 25 Jul 1994 10:54:52 +0100 (BST)

[Taken from Ford UK's (free) magazine for drivers, without permission.]

Car thieves who broke into a Ford driving event at Oulton Park in Cheshire, has a nasty surprise when the car they pinched turned out to be a specialised reverse steer Fiesta equipped with an upside down steering rack.

Used normally to improve driver's co-ordination and concentration, it is an exceptionally difficult vehicle to drive, requiring the driver to think in opposites. However, the thieves were not to know this.

Attempting to turn left out of the main exit, they turned instead straight into a concrete bollard on the right. Dazed but unhurt they escaped on foot.

Clive D.W. Feather, Santa Cruz Operation, Croxley Centre, Hatters Lane, Watford WD1 8YN, United Kingdom clive@sco.com +44 923 816 344 Fax: +44 923 210 352

---

### Airport codes

"Clive D.W. Feather" <clive@sco.com>

Mon, 25 Jul 1994 11:13:52 +0100 (BST)

Seen on a BBC news item last night, a baggage tag with the code:

LUN - Port Armstrong, Moon

My database says that LUN is Lusaka, in Zambia. \*What\* an opportunity

for your luggage to get lost.

Clive D.W. Feather, Santa Cruz Operation, Croxley Centre, Hatters Lane, Watford  
WD1 8YN, United Kingdom clive@sco.com +44 923 816 344 Fax: +44 923 210 352

---

## Embezzlement at Beijing Hotel

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
26 Jul 94 10:00:52 EDT

Reuter (94.07.24 @ 23:19 EDST) via CompuServe's Executive News Service  
(GO ENS):

### CHINA JAILS FOUR FOR COMPUTER FRAUD

BEIJING, July 24 (Reuter) - In one of China's first officially reported cases of computer crime, four Beijing hoteliers have been jailed for cheating guests by manipulating computerised billing records.

Beijing Friendship Hotel managers Jiang Zheng and Du Yize, were sentenced to seven years, the state-run Legal Daily reported on Sunday. Two co-defendants were given three- and one-year terms."

Key points in the article:

- o Computer fraud a growing problem in China.
- o Two managers embezzled about U\$9,000 from guests from Feb-May 93.
- o "They connived to use the computer to cancel or change hotel accounts, alter the records of 39 cash receipts and make fraudulent reports of daily hotel accounts," the report said.

[MK: This is clearly a case where Peking at your hotel bill is a good idea before you pay.][Apologies to PGN.]

Michel E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

---

## Remote reading of gas meters

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
26 Jul 94 10:00:47 EDT

>From the Washington Post newswire (94.07.23) via CompuServe's Executive News Service:

D.C. Residents Shocked by Gas Bill for \$2,248  
By Daniel Southerland, Washington Post Staff Writer

Rachel Carlson, a law student on a tight budget, was shocked when she opened the mail recently and found a monthly gas bill for \$2,248.28. Carlson, 23, and four others sharing a brick house in the District had been

paying bills ranging from \$50 to \$60 a month."

The story continues with the explanation. Seems the gas-meter reader had been unable to get into the house to read the meter, so the Washington Gas estimated usage for three years. When they finally got a reading, they invoiced the tenants for the unpaid difference between reality and estimation.

The mildly interesting portion of story for RISKS and NCSAFORUM readers is that the company will be installing low-intensity FM transponders "by March 1995 in all of the homes that currently are receiving estimated bills.... A van drives by the house and sends a 'wake-up' signal to a unit attached to the gas meter. The meter reading is transmitted to the computer in the van and then to the company's billing department."

Now, this scenario brings up a couple of RISKS that correspondents in the Washington, DC area might like to investigate (and report back to RISKS or the NCSAFORUM):

1) Integrity: what is the reliability of the system? How is a low error-rate ensured in the transmissions?

2) Confidentiality: how easy would it be for Nasty People Interested in Robbing Houses to tap the gas-meter signals? For all the automated timers attempting to camouflage the residents' absence, a gas meter showing little or no usage would indicate that absence for extended periods. I think this is a minor threat, but fun to think about for a few seconds.

3) Robustness: how easy would it be for Nasty People Interested in General Havoc to jam / spoof / corrupt the data transmissions? For that matter, is there any other source of interference which might cause faulty readings? One can imagine bills for \$22,482.80 if Rotting Rotifer the local criminal hacker decides to have his bit of fun while the Gas Van is roaming about the neighbourhood.

RISKS readers tired of real-world security will seize the opportunity to have a gas investigating this new threat to world peace and prosperity <g>.

Michel E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

---

## Hack FAQ (summary)

*Martin Minow <minow@apple.com>  
Sat, 23 Jul 94 19:16:04 -0700*

A friend recently sent me a copy of the "Hacking FAQ" (Frequently Asked Questions) that was posted to alt.2600 on July 9, 1994. (I wasn't able to find it in our Usenet archives, but we purge often.) It was posted by "will@gnu.ai.mit.edu (Will Spencer). It's too long to include in Risks, but may be copied from the Risks ftp archives as [[\*\*\*]]. This note summarizes the 20 page, 30,000 byte original.

The FAQ has two main sections: hacking computers (mostly Unix) and telephone

systems.

#### Hacking Computers:

- A list of programs for guessing passwords for Unix and VMS (both store passwords in a one-way encrypted fashion).
- Getting the list of encrypted passwords, even if they are shadowed or otherwise hidden on Unix. Getting the list of encrypted passwords from VMS.
- Breaking out of restricted Unix shells. Becoming root on Unix (an 8 line program), erasing yourself from the Unix logs (a 1 1/2 page program).
- Faking mail by using Telnet. Faking News postings.

#### Phone system hacking:

- Description of red, blue, and black boxes. These are (traditionally), small boxes with components that defeat telephone security, letting you make calls for free. For example, a red box mimics the sounds that money makes when coins are deposited in a pay phone. You can make one by changing the crystal in a tone dialer, or by recording the tones on a Hallmark "record your message" greeting card.
- A list of every "box" color, and a brief description of what it does.
- Finding the number of the telephone you're calling from. Traditionally, this is done by calling telephone-company provided services that were created for phone workers. The new method is to use the ANI service that delivers the calling phone number to 800 and 900 service providers: call (800) 471-8859. "It is an 800 phone sex line. The system will give you an account number. The first 10 digits of the account number will be the telephone number from which you are calling." (I haven't tested this since I don't particularly want my home phone number in their database.)
- Ringback numbers: these ring the phone from which it's called.
- Loop numbers: a loop is two telephone numbers linked together. if you call one number and your colleague calls the other number, you will be able to talk to each other.
- Reverse directory numbers: given a (listed) number, it returns the subscribers name and address. Two companies provide this information via 900 numbers, charging about one dollar per minute.

#### Internet sites of interest:

- FTP sites; many seem to have encryption software.
- Usenet newsgroups. alt.2600, alt.dcom.telecom, alt.hackers, etc. comp.risks is not mentioned, but perhaps we're not that interesting.
- WWW sites, including what appears to be two belonging to Gene Spafford, who is a computer security expert.
- IRC (Internet Relay Chat) sites. IRC is an internet broadcast facility.
- Hacking IRC to hide your username, and to hack ChanOp.
- one BBS site

I don't think that giving the Hack FAQ greater publicity in Risks is a serious risk in itself: the bad guys know this stuff, and it is useful for the rest of us to realize just how limited, for example, Unix security really is. For example, I hadn't realized that it was so easy to get the encrypted password list on VMS, and that it was so easy to get system privileges on Unix.

Martin Minow minow@apple.com

---

## Risks of being unable to clear records

Marcus J Ranum <mjr@tis.com>

Mon, 25 Jul 94 14:27:35 EDT

[From the Baltimore Sun, July 23, 1994]

This scares me a lot. We all know the power of innuendo -- when it's combined with computer databases (which never "lie") it is even worse. I've edited out the noise/filler with [...].

----Article Begins----

Couple mistakenly listed as abusers lost in court

No rights violation found by judges

By Anne Haddad, Sun Staff Writer

David and Marsha Hodge were mistakenly listed as child molesters in a state database for two years without a chance to know it or to correct the error.

But that did not violate the Taylorsville family's civil rights or invade its privacy, three judges in the 4th US Circuit Court of Appeals in Richmond, VA., ruled this week.

The decision overturns one by Judge Herbert F. Murray in US District Court in Baltimore in September, 1992.

"While it is true that such records may be expunged," the appeals court ruled, "there is no \*automatic\* right to expunction once an individual's name has been cleared."

Mr. Hodge says he plans to appeal the ruling.

[...]

"There is no constitutional right to have the state destroy records of an investigation," Ms. Cannon [MD Attorney General's Office] said. "The fact that the records exist does not hurt them. That's the key." [...]

In January, 1989, a misdiagnosis of 3-month-old Joseph Hodge's swollen arm led a pediatrician to report possible child abuse. The doctor thought it was a fracture, but the swelling was a bone infection later diagnosed and treated surgically at Union Memorial Hospital in Baltimore. [...]

David and Marsha Hodge, both scientists who hold national security clearances for their jobs, said the listing in the state database could harm them, but the court said that claim was not tangible.

The judge said that because of the confidentiality of records in abuse investigations, "we see no avenue by which a stigma or defamation labelling the Hodges as child abusers could attach."

----Article Ends----

The judge's finding is particularly amusing in the light of recent revelations of widespread accesses of IRS databases by curious employees [Sen Glenn announced some 1300 IRS employees are being disciplined for "browsing" databases.] -- any database that is not properly secured, which contains personal information, can cause someone problems. What's frustrating about these stories is that the technologies exist today to provide "need to know"

access and good audit trail for confidential databases. Moral: Don't trust someone else to keep their facts about you straight.

mjr.

---

## More inadvertent mail list "spamming"

*Phillip Finch <pffinch@CERF.NET>*

*Fri, 22 Jul 1994 20:32:34 -0700*

Here's another instance of how careless use of a listserver produced an unintended deluge in subscribers' mailboxes.

An associate editor of the American Journalism Review (a paper magazine) was researching an article about the plagiaristic practice known as "rip-and-read"; i.e., radio reporters reading print articles over the air, sometimes verbatim, without giving credit. The AJR editor posted a message on a professional journalists' mail list called SPJ-Online, asking print reporters to send him "rip-and-read" anecdotes.

However, the editor neglected to include a private address for replies. Apparently, many respondents sent their messages to the SPJ-Online listserver, which dutifully posted them to every subscriber.

I ran across this story in a humorous weekly on-line newsletter, BONG BULL (Bulletin of the Burnt-Out Newspapercreatures' Guild), which described the spamming as "an avalanche" and added this comment:

> Which is no way to protect a scoop.  
> But that's AJR's problem, isn't it?

Phillip Finch (pffinch@cerfnet.com)

---

## Two kinds of risks

*"Robert Morrell Jr." <bmorrell@isnet.is.wfu.edu>*

*Mon, 25 Jul 1994 11:26:39 -0400 (EDT)*

Bill Donahue harassment by an automated caller is simply a new version of the old problem of bad data inputs attached to systems that did not take into account the possibility of such erroneous inputs. Workers in hospitals have long been aware that the tiniest of erroneous keystrokes can have grave consequences, as have (though with less concern, apparently) workers in large bureaucracies (the old stories of people who had "died" in the Social Security System comes to mind).

I recently had the idea that any output "downstream" of a manual input be presented to all user interfaces in cursive script, so that the user is aware that keystroke errors are a possibility.

A separate kind of computer risk is represented in several threads in RISKS is the use of expert systems or near expert systems in scenarios not

envisioned by the designers (auto-pilots, safety and anti-theft systems linked to airbag deployment, and others). Here is a much newer kind of risk that will become more apparent as AI enters the mainstream, particularly as the mainstream seems oblivious to the differences between standard computer programs and AI. In one, all possible scenarios are supposedly thought out by the programmer, and errors generally result from inputs. Proper escape mechanisms (un-decreasing a Social Security number, for instance) can be anticipated by simply analyzing input error possibilities. In the other, all possible scenarios by definition cannot be thought out. Yet more global escape routines or even better, systems that automatically question human users about unusual scenarios it finds itself in, have not been added to make the system sensitive to its limitations. That is, people are designing, using and trusting AI and quasi AI systems in the same way they have dealt with standard computer programs.

In the case of Mr. Donahue's tele-nightmare a convergent solution might be an expert system that alerts autocaller users to any phone number that results in a certain number of failure to connect.

While readers of RISKS will continue to call for such common sense measures, the real problem remains a public that has inappropriate expectations and understanding of modern computer systems. We are still in the era where chainsaws have been handed out without any clear explanation of how they differ from axes.

Bob Morrell

---

## Risks of hot lines

*703) 506-0500 <PHILS@RELAY.RELAY.COM (Philip H. Smith III),>  
Fri, 22 Jul 94 08:38:50 EDT*

At our old building, we had a non-PBX line into the computer room. It was hooked to a Radio Shack environmental monitor, which would detect high temp, noise, etc. and call a list of phone numbers until someone responded. That part worked fine. But we started getting wrong numbers -- we'd be in the room and hear the phone ring, and the robot would pick up and start talking, but nobody who worked there would own up to it. This happened several times per day -- too many even for telemarketing -- and we couldn't figure it out for the longest time. Then one day I was driving home and heard an ad on the radio for a suicide hotline, in nearby Maryland -- at number (301) 685-0525. Our robot's line was (703) 685-0525! So some poor depressed person would get it together enough to call the number, but without the 301, and would get a robot saying "This is telephone number 6 8 5 0 5 2 5, the time is xx:yy, temperature is OK, noise level is OK, alert 1 is OK, alert 2 is OK, listen to the surrounding area for 15 seconds", after which it would switch on a microphone so they could either uninterrupted hear machine room noise or machine room noise with people saying "Hey, the robot's talking" "Yeah, it does that" "Wow, weird" and the like.

I shudder to think of whether there were any lasting ill effects of this problem. The good news is that shortly after discovering it, we moved to a new building with a new number.

...phsiii

---

**Re: As the Worm Turns--Ant-icipating Problems (Kabay, [RISKS-16.28](#))**

*Pete Mellor <pm@csr.city.ac.uk>*

*Sun, 24 Jul 94 19:09:44 BST*

On what species of ant are they modelling their software automata?

A few possibilities occurred to me:-

Army ants: These form nice quiet little colonies for a while, then (when population pressure builds up to a certain level) they change their life-style, and go on a random march through the jungle (read "usenet"? :-) devouring everything in their path.

Leaf-cutter ants: These carve up leaves and take them back to their colonies where they chew them into a mulch on which they grow an edible fungus.

Honey-pot ants: Some individuals "volunteer" (i.e., are "programmed" in BT's terms) to hang from the roof of the nest and be fed by the others. Their abdomens become grossly distended with the digested food, which the other members of the colony then suck out of them.

Pharoah's ant: A small variety emanating (as its name suggests) from Egypt, which is notorious for being able to get into \*anything\*. There are reports of surgeons opening sealed sterile dressings in the operating theatre, only to be confronted by a cute little ant waving its feelers.

The common British black ant: This forms neat little nests, usually under a crack in your kitchen floor, from where they make daily raids on your larder. According to entomologists (see ref. [1] below), these follow well-trodden trails each day, except that 10% of the individuals are more adventurous than the others, and persist in discovering new places to find food, instead of just following the rest. Every year, a set of winged fertile females is hatched and fly off at random to mate and found new colonies in totally unpredictable places (but probably under that other crack in your kitchen floor! :-).

The red ant: Similar to the black ant, but capable of biting through the skin and injecting painful amounts of formic acid if disturbed. Members of a colony recognise each other by smell. A colony that gets too large splits in two, and the members of the break-away colony develop a different smell, so that, if they come across members of the parent colony, there is a fight to the death.

The termite (and before any entomologist jumps down my throat, let me say I am well aware that termites, although colloquially referred to as "white ants" are not "ants" at all): This builds truly impressive hills of chewed and

hardened mud up to 20 feet tall. They are averse to light, and very skillful at building covered tunnels to get to where they want to be, i.e., to the nearest available source of cellulose (read "software library"? :-)) which they devour with unbelievable voracity. When my father served in India during the war, everything had to be kept in steel trunks, otherwise the little darlings would make short work of your spare uniform! :-)) Termites come in various forms: the queen is an enormous sluggish thing whose sole function is to lay eggs to make new termites. The soldiers are ferocious things with big jaws which rush to any breach in the nest and fight off the attacker. The workers are sterile females whose job is to tend the eggs and larvae and build the nest and tunnels by chewing and piling up pellets of mud which harden like concrete when mixed with their secretions.

QUESTION: Which species could BT be thinking of?

Returning to the key points from the article (as presented by Mich):-

- > o "Our system is made up of small, autonomous, reactive, mobile
- > blocks of computer code that interact in a way derived from ant behavior,"
- > said scientist Simon Steward. "The control system that emerges from all of
- > these mobile software agents working together is inherently adaptable and
- > robust unlike normal computer programs."

Must be worker termites. Entomologists have developed models of termite building behaviour which allow for the construction of large nests from very simple rules, e.g., "pile up mud pellets on top of one another, unless the worker nearest to you has made a taller pile than you have, in which case, stop working on your pile and help her to build hers".

OK, termites don't need to be too bright to build fancy nests, but is the resulting structure of any use to humans? If the requirement for the overall system is simply "I want big towers of chewed mud stuck at random over the landscape", then the "termite worker" model might just be the one we want.

- > o The goal of the work is to prevent system crashes when an
- > unanticipated [...] condition occurs.

Must be modelled on warrior termites. Simply rush to the hole in the nest (read "system") and chew the head off anything in sight!

- > o The distributed computing model uses message-passing to coordinate
- > computation.

Like using smell to communicate messages such as "Follow me to the food!"?

- > o "The programs are mobile like ants, moving from one computer to
- > another, when needed."

Army ants? The flying form of the common black ant?

- > o After making software or parameter changes, the "mobile programs"
- > would "leave messages for other programs on how the system has been
- > adapted."

"The fungus garden is over here!" "Nip up that rose-bush and milk those aphids!"

> o Modules will display "a certain amount of random behavior...."

Really? There's a surprise! :-)

> o The system will display heuristic, goal-seeking behaviour.

Whose goals? The statement is correct. An ant colony *does* display exactly such behaviour, and the behaviour of the colony is more complex than the behaviour of the individual. A colony of social insects behaves more like a single organism than a collection of individuals. This is due to the distribution of genes among the colony (all workers are half-sisters of the queen [ref. 2 below]). Next time you dig a wasps' nest out of a pile of garden rubbish (as I once made the mistake of doing) you could make sense of the consequences by reflecting that you have just been attacked by an animal the size of a small dog with 3,000 venomous teeth! :-)

The "goals" of an insect colony [ref. 2], however, are:-

1. Feed 2. Breed (or vice versa)

Can we be sure that our software "ant colony" would stick to *our* goals?

> All this is fascinating, and I naturally wondered about the implications  
> for system reliability.

So did I! :-)

Reliability is defined as: The probability that the system (i.e., the environment in which the "ant colony" "lives") will perform a required function for a given period of time under given conditions.

If the system is continually modified by software "ants" the implications are not obvious, and my gut reaction is that chaotic behaviour could manifest itself. Could the ants actually modify the required system behaviour? If so, will they also rewrite the functional spec.? :-)

> It will be interesting to follow this work and see how concerns for  
> reliability are worked into this evolving field.

I agree that the implications for reliability are interesting, but that is all that I can be adam-ant about at the moment! :-)

References:-

[1] For general ant behaviour: Derek Wragge-Morley: "The Book of the Ant", Penguin, 1958 (?)

[2] For the genetic basis of behaviour of social insects:  
Richard Dawkins: "The Selfish Gene"

Peter Mellor, Centre for Software Reliability, City Univ., Northampton Square,  
London EC1V 0HB +44 (71) 477-8422, p.mellor@csr.city.ac.uk



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 16: Issue 30**

**Tuesday 2 August 1994**

## Contents

- [Squirrels again bring down Nasdaq](#)  
[PGN](#)
- [MCI inbound internet gateways choked](#)  
[Mich Kabay](#)
- [RISKS of electrical wiring](#)  
[Robert Rose](#)
- [How to clean out a checking account](#)  
[Paul Dineen](#)
- [FBI hunting for Agent Steal, flashy computer hacker](#)  
[Mich Kabay](#)
- [PCMCIA cards](#)  
[Mich Kabay](#)
- [Progress on RFI in aircraft](#)  
[Mich Kabay](#)
- [Porn Peddlers Convicted in Memphis](#)  
[Mich Kabay](#)
- [Re: Video Cameras](#)  
[Nap van Zuuren](#)
- [Computer telephony](#)  
[Phil Agre](#)
- [Re: Crashed bank teller](#)  
[Ted Lemon](#)  
[Patrick O'Callaghan](#)
- [The Cult of Information by Ted Roszak](#)  
[WN Peters](#)
- [Report Released on Public Key Law and Policy](#)  
[Michael S Baum](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Squirrels again bring down Nasdaq

"Peter G. Neumann" <[neumann@chiron.csl.sri.com](mailto:neumann@chiron.csl.sri.com)>

Tue, 2 Aug 94 7:55:36 PDT

Nasdaq once again was shut down by an energetic squirrel who apparently chomped on a power line near the stock market's computer center in Trumbull, Connecticut, yesterday. The system failed to perform the automatic switchover to the temporary backup power supply (designed to last until the backup system in Rockville, Maryland, could be brought up), and consequently the market was down for 34 minutes. A similar problem occurred in December 1987. (A 2.5-hour outage on 15 July was reported in [RISKS-16.25](#), due to risky software upgrades.)

---

## MCI inbound internet gateways choked

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
01 Aug 94 10:47:51 EDT*

According to the Washington Post newswire (94.08.01 via CompuServe's Executive News Service), MCI's inbound Internet gateways were saturated last month, resulting in days of delay in delivery to MCI customers.

M. E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

---

## RISKS of electrical wiring

*<robert\_rose@VNET.IBM.COM>  
Mon, 1 Aug 94 17:47:37 EDT*

I had a really interesting experience in one of our labs today, an electrician was adding a new outlet into an office and tied the outlet into a junction point in the dropped ceiling. While tying in the neutral line he let the 'home-run' neutral line (the one going back to the main 3-phase distribution I assume) come loose from the junction. After a minute he discovered this at reconnected it... he didn't notice a thing. All of us in our offices however were really charged up.... There was smoke, sparks and crackling belching from numerous PCs, X terminals, surge protectors and fluorescent lamps.

One of our programmers who is an EE figured that when he dropped the main neutral the current instead started to flow between two branches of the three phase and that one office had very little equipment turned on and the other had great gobs of stuff powered up so that the office with everything turned on had almost the full 220V across its outlets. Total body count: 2 surge protectors, a fan, and one Gateway 2000 (which was spewing sparks out of the fan opening!) [I'm not a EE-minded person so hopefully I haven't botched this description too bad]

Lessons:

1. Don't trust your surge protectors blindly, the Gateway that got fried was plugged into one.
2. Its worth the money to buy an autoswitching 110/220 power supply, the Gateway was right next to an RS/6000 that has an autoswitching supply. We figure the RS/6000 was running until the breakers blew... it just thought it had made a quick trip to Europe. Another IBM machine with an auto

supply made it too.

I would have thought that some type of automatic device could prevent these type of overvoltages, but given the electrician's actions I guess not. (This electrical contractor was \*real\* happy when we discovered the RS/6000 wasn't toast!)

--Rob Rose OS/2 Development IBM Boca Raton

---

## How to clean out a checking account

Paul Dineen <pld@swttools.fc.hp.com>

Fri, 29 Jul 1994 18:01:45 -0600

I lost my checkbook a couple of weeks ago. Despite turning the house inside out that evening, I couldn't find it. So, I called the bank and had them put a watch on the account. Yesterday, I found the checkbook. (Wedge behind the seat of the lawn mower, must have fallen when I was cleaning the garage.) I called the bank to cancel the watch, needing to tell them only the account number and my name (printed on the check, naturally). They didn't ask me my mother's maiden name or anything. Obviously, what's to stop a finder or thief from making the same call? I didn't raise this question then because I didn't want to raise suspicion and have to go through some trouble to get the watch lifted, but I will raise it with them on the next working day.

Paul Dineen, pld@fc.hp.com

---

## FBI hunting for Agent Steal, flashy computer hacker

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>

01 Aug 94 10:47:38 EDT

>From the Reuter newswire (94.07.31 @ 21:10 EDST) via CompuServe's Executive News Service:

"FBI HUNTING FOR AGENT STEAL, FLASHY COMPUTER HACKER.

"LOS ANGELES, July 31 (Reuter) - The FBI is searching for a computer hacker suspected of committing high-tech crimes at the same time he allegedly worked undercover for the bureau catching other computer hackers, the Los Angeles Times reported Sunday.

The hacker, who goes by the moniker "Agent Steal" and whose real name is Justin Tanner Petersen, vanished last October and is on the run from the very federal agency -- the Federal Bureau of Investigation -- he told friends was paying his rent and flying him to computer conferences to spy on other hackers, the paper said."

Key points from the article:

- o Petersen admitted having committed computer crimes even while working with federal prosecutors.

- o He is alleged to have cracked federal computers and stolen information from a credit card information bureau.
- o He was involved in Kevin Poulson's fraudulent successes in radio phone-in contests in L.A.
- o Petersen claimed to have been responsible for "nailing" Kevin Mitnick, the infamous criminal hacker who is sought by authorities for breaking into police computers and impersonating a police officer.
- o J. Michael Gibbons, an FBI computer crime specialist, is sceptical that his agency ever hired Petersen: "It's not safe. Across the board, hackers cannot be trusted to work -- they play both sides against the middle."
- o "Petersen was arrested in Texas in 1991, where a grand jury returned an eight-count indictment accusing him of assuming false names, accessing a computer without authorisation, possessing stolen mail and fraudulently obtaining and using credit cards."
- o Convicted of six counts after pleading guilty, Petersen faces imprisonment for up to 40 years plus a fine of \$1.5 million.
- o "...[O]n Oct. 18, 1993, 15 months after entering his first guilty plea, Petersen was confronted outside federal court by Assistant U.S. Attorney David Schindler, who asked if Agent Steal had committed any crimes while free on bail.  
"Petersen said he had, according to the federal prosecutor. Petersen fled immediately after that meeting."

M. E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

---

## PCMCIA Cards

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
01 Aug 94 10:47:47 EDT*

The Washington Post newswire (94.08.01; via CompuServe's Executive News Service) provides an analysis of PCMCIA card problems:

"Add-In Card Standard: Good Plan, Bad Execution," by Brit Hume.

Hume summarizes the situation when the Personal Computer Memory Card International Association (PCMCIA) was founded in 1990: lack of slot standards made it difficult for manufacturers and users to have economical add-in devices. The new association devised three standards, but unfortunately the bugs are not quite out yet.

The author describes the problems trying to work with a new PCMCIA fax/modem card. It worked OK with PC-DOS 6.1 but the drivers failed with DOS 6.2.

Even on 6.1, after resuming from both the "suspend" and "hibernate"

operations, the operating system had lost track of its PCMCIA port. After extensive discussion with IBM support, the writer got function back after resuming from "suspend" but still lost the I/O port after "hibernate."

M. E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

---

## Progress on RFI in aircraft

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
01 Aug 94 11:51:35 EDT*

>From the NIST UPDATE for 94.08.01:

### ELECTROMAGNETIC FIELDS

#### Paper Details EMF Shielding Theory

In work supported by the Federal Aviation Administration, NIST researchers have developed a mathematical model and theory for predicting the electromagnetic field shielding effectiveness of large metal enclosures with apertures and interior loading. The model also should allow for estimations of the average field strength inside enclosures such as electronic equipment cases and aircraft bodies. It can be used for any enclosure regardless of size, shape, type of material and number of apertures, as well as for any frequency above a lower limit related to the dimensions of the enclosure. The model was experimentally evaluated using a rectangular aluminum cavity of about 0.57 cubic meter (approximately 20 cubic feet), with one aperture, and for a microwave frequency range from 1 gigahertz to 18 gigahertz. The agreement between model and actual measurement was within 20 percent after a number of additional sources of loss were incorporated into the original model. A report, "Aperture Excitation of Electrically Large, Lossy Cavities" (NIST Technical Note 1361), is available from the National Technical Information Service, Springfield, Va. 22161, (703) 487-4650, for \$19.50 prepaid. Order by PB 94-145711.

Media Contact: Collier Smith (Boulder), (303) 497-3198  
smithcn@micf.nist.gov

M. E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

---

## Porn Peddlers Convicted in Memphis

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
31 Jul 94 19:54:57 EDT*

The Associated Press newswire (94.07.28 and 29) via CompuServe's Executive News Service) reported on the recent conviction of Internet porn peddlers

The following summary is based on reports by WOODY BAIRD and ELIZABETH WEISE, Associated Press Writers. The first, by Baird, deals with the legal issues.

"MEMPHIS, Tenn. (AP) -- A husband and wife were convicted of distributing pornography via computer Thursday in a case that raised questions about how to apply federal obscenity law to the information superhighway.

Robert and Carleen Thomas, both 38, of Milpitas, Calif., were each convicted of 11 counts of transmitting obscenity through interstate phone lines via their members-only computer bulletin board. Each count carries up to five years in prison and \$250,000 fine."

Apparently the Thomases sold pornographic graphics files on their BBS. A Memphis postal inspector deliberately joined the BBS under an assumed name, downloaded some of the pics to his system and then complained to law enforcement authorities.

There's discussion of just what it means to try someone on the Internet under local pornography laws which refer to "community standards." "The opinion was designed to let local citizens say whether they want X-rated bookstores or movie theaters in their communities and get judges out of the business of deciding what is obscene, said Stephen Bates, a senior fellow with the Annenberg Washington Program, a communications think tank."

However, if this approach is applied to the Internet, "federal juries in the most conservative parts of the country could decide what sexually explicit images and words get on the information superhighway, Bates said."

Weise's article covers reactions on the Internet:

"SAN FRANCISCO (AP) -- Hours after a couple were convicted of sending images of bestiality and sexual fetishes over a computer bulletin board, the Internet was humming with warnings and protests.

"If this case stands, you can bet there will be a hell of a lot more prosecutions on the same basis in extremely short order," Karl Denninger of Chicago wrote Friday on the computer network."

The EFF's Mike Godwin is reported as saying, "This case ... has one community attempting to dictate standards for the whole country."

At least one BBS operator has stated that he'll quit as a result of the ruling, although he didn't explain what kind of files his BBS stocks....

Michel E. Kabay, Ph.D. / Dir Education / Natl Computer Security Assn

---

## Re: Video Cameras ([RISKS-16.20](#))

*Nap & Erik van Zuuren <100042.3164@compuserve.com>  
29 Jul 94 05:44:02 EDT*

Assume, that we need a 'balance' in the RISK Digest, the balance between "benefits" of certain techniques against their "risks"

I have to react, as we are in a limbo on this issue. As a Dutchman, living in Belgium, I follow the outcome of a weekly T.V. program, called "Opsporing

verzocht" (Help sought on Criminal Investigation), a program in which the Police Forces try to get necessary input for solving serious crimes. In that program, the presence of video-material from shopping malls and within shops has proven to be a big help in getting required input, and so we have to accept that we are "video-ed" when we are, for example, shopping; also for our "own" protection.

- Would not you feel better, with a camera 'at your shoulder', as e.g. a cashier in a petrol station at a highway ?

So: Benefits appear to outweigh risk !

Note: Apparently the Dutch Police Forces, and related Forces, are still considered -- in general -- to be the "friends" of the population by the Dutch population.

I thought that the same attitude towards the Police Forces was true for the U.K.; the relation to the "Bobbie". (As the original "risks message" originated in the U.K., I also refer to the "Bobbie")

I wish, this would be the case in other countries as well; but the requirements for reaching such a relation with the 'public' are:

- to be "of assistance to the public"
- to be trustworthy, accompanied by a free press and political will
- to be supported by the judicial apparatus, for the Forces to stay motivated
- a "quality of life" worth defending it

We will need a lot of "trustworthy" energy to protect us -- and our children -- against the "criminal" energy.

Do NOT get me wrong:

- I also fell victim to injustice (in my opinion) in a case versus an 'official'
- I even have been insulted in writing by a member of the Council of Ministers

But, we have to trust (and at the same time: control) the forces which should protect the "law-abiding" (or = sullen ?) citizen, and are paid by that same citizen to do so ! Might the price of "democracy".

Nap van Zuuren, CompuServe 100042,3164

---

## Computer telephony

*Phil Agre <pagre@weber.ucsd.edu>*

*Sun, 24 Jul 1994 14:09:10 -0700*

The July issue of Byte has a good technical review of systems for integrating

PC's and telephones. The full reference is:

Jon Udell, Computer telephony, Byte 19(7), 1994, pages 80-96.

The applications are still pretty primitive, since the necessary capabilities within the phone system itself don't quite exist yet, are just coming on-line, or are just receiving regulatory approval. Still, enough stuff is just over the horizon that non-trivial architectures are being built. Many of them use Caller-ID, for which the FCC just set US national standards over the dead bodies of several state utilities commissions; and despite the strange idea that Caller-ID is mostly for residential use, the article makes clear that developers see a world of commercial applications. In general, as the article points out in the case of sales and collections systems,

"As these tools find their way into the hands of smaller, more mainstream businesses, you can expect better service in some cases and more efficient harassment in others."

Indeed.

Phil Agre, UCSD

---

### **Re: Crashed bank teller (Murray, [RISKS-16.27](#))**

*Ted Lemon <mellon@ncd.com>*

*Thu, 21 Jul 94 18:03:51 PDT*

> [...] Setuid has hurt instead of helped. [...] While it is  
> appropriate for my program to fail by returning ME to the operating  
> system, my program should not fail by returning YOU to the operating  
> system prompt with privileges that are different from those that you  
> have on your own.

Mr. Murray's article on the behaviour of various historical systems is interesting, but makes a rather bizarre claim about the behaviour of setuid under Unix. In fact, a setuid program only has privileges in the process in which it is running and any child processes that it creates without first disabling the setuid privilege.

The problems we've seen on the Internet with setuid programs generally are the result of poor coding which leaves loopholes in the executing setuid program that a clever cracker can exploit. I don't see any reason to believe that OS/400 setuid-like programs are any safer from this sort of exploitation. The proper solution to this problem is probably either to program more carefully, or to set up an environment in which it's harder to make mistakes like this.

\_MelloN\_

---

### **Re: Crashed bank teller (Murray, [RISKS-16.27](#))**

"Patrick O'Callaghan" <poc@usb.ve>

Fri, 22 Jul 1994 08:14:13 -0400

From his description, Mr. Murray appears to think that setuid was introduced in order to restrict access rights, and has been abused by lazy programmers. Quite the contrary. The purpose of the `setuid' bit is to allow a program to run with the permissions afforded to the program's owner, rather than those of the user. To say that `setuid has hurt rather than helped' is like saying `electricity has hurt rather than helped'. Setuid is *\*fundamental\** to how Unix operates and its invention by Dennis Ritchie has been described as the only genuinely original idea in the Unix design (which is not to say it doesn't have problems).

William> ... However, they do not permit the user to retain  
William> those privileges across the failure of the application.

Neither does Unix. If my setuid program fails, I fall back to whatever invoked it, usually a Shell. I do *\*not\** retain setuid privileges.

Prof. Patrick O'Callaghan, Departamento de Computacion, Universidad Simon Bolivar, Caracas, Venezuela poc@usb.ve +058 (2) 906-{3241,3242,3254}

---

## The Cult of Information

<WN\_PETERS@wmich.edu>

Fri, 29 Jul 1994 11:17:37 -0400 (EDT)

I highly recommend a book entitled The Cult of Information: a Neo-Luddite Treatise on High-Tech, Artificial intelligence, and the True Art of Thinking, by Theodore Roszak (second edition, c1994). Roszak, in this book, is not attacking the idea of computerization, but he is warning our society against equating information with knowledge (the idea that if one can access information one, therefore, has knowledge on that given subject) and against over-computerization of our society. I found it to be a very readable book and quite illuminating.

University of California Press, ISBN: 0-520-08584-1

---

## Report Released on Public Key Law and Policy

Michael S Baum <baum@world.std.com>

Sun, 31 Jul 1994 08:51:33 -0400 (EDT)

**\*\*NEW INFO. SECURITY BOOK ON PUBLIC KEY LAW & POLICY\*\***

TITLE: FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY --  
Law and Policy of Certificate-Based Public Key and Digital Signatures

AUTHOR: MICHAEL S. BAUM, J.D., M.B.A.  
Independent Monitoring

Report No. NIST-GCR-94-654

450+ pages, highly annotated; multiple appendices; indexed.

U.S. DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Produced in support of the Federal Government's public key infrastructure study, this book identifies diverse technical, legal and policy issues affecting a certificate-based public key cryptographic infrastructure utilizing digital signatures supported by "trusted entities." It examines potential legal implications, surveys existing legal paradigms and the structures and roles of relevant governmental agencies and presents various institutional approaches to controlling liability. It considers the underpinnings of a legal and policy framework which might serve as a foundation for security policies and their implementation and concludes with a series of recommendations, both general and specific concerning certificate-based public key. Both public and private sector issues are addressed.

This publication is the result of legal, business and security management research, as well as interviews and analysis predominantly with public- and private-sector lawyers, policy makers, managers and management information system and security professionals in the United States and abroad.

SUMMARY OF CONTENTS:

- PREFACE
- ACKNOWLEDGMENTS
- TABLE OF CONTENTS
- I. INTRODUCTION
- II. SCOPE
- III. DEFINITIONS
- IV. ASSUMPTIONS
- V. SURVEY OF FCA ACTIVITIES CREATING LIABILITY EXPOSURE
- VI. LEGAL CONSIDERATIONS
- VII. FCA INFRASTRUCTURE - PROPOSALS AND PARADIGMS
- VIII. SURVEY OF, AND APPROACHES TO, TRUSTED ENTITY LIABILITY
- IX. OTHER APPROACHES TO MITIGATE LIABILITY
- X. CONCLUSIONS AND RECOMMENDATIONS
- XI. APPENDICES
- XII. GLOSSARY
- XIII. INDEX

OBTAINING COPIES: Copies may be purchased through the National Technical Information Service, Springfield, Virginia 22161, U.S.A., Phone +1 (703) 487-4650 or 1-800-553-6847. Request NTIS Document No: PB94-191-202. Cost: \$61.00

ABOUT THE AUTHOR: Michael S. Baum is Principal of Independent Monitoring, a consultancy focused on electronic commerce and information security law. He serves as a Delegate from the International Chamber of Commerce (ICC) to the United Nations Commission on International Trade Law (UNCITRAL); Chair of the EDI and Information Technology Division, Section of Science and Technology, American Bar Association (ABA) and its Information Security Committee; and Chairman of the ICC Working Party on Legal Aspects of Electronic Commerce.

Michael S. Baum, Independent Monitoring, Cambridge, Massachusetts [baum@im.com](mailto:baum@im.com)

[RISKS normally does not run advertising for books. However, this is a NIST/NTIS report. (Yes, NITS, ISN'T, SNIT are also anagrams.) It is also fair game for a review, in case someone wants to submit one. 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 16: Issue 31**

**Tuesday 9 August 1994**

## Contents

- [Unda\(u\)nted exploration: DANTE II](#)  
[PGN](#)
- [Denver "solves" hi-tech baggage handling problems](#)  
[Lauren Weinstein](#)
- [Re: Squirrels again bring down Nasdaq](#)  
[Joe Morris](#)  
[Bob Frankston](#)
- [More than squirrels: Newbridge Networks](#)  
[Bob Frankston](#)
- [Re: RISKS of electrical wiring](#)  
[Lauren Weinstein](#)
- [Re: The Cult of Information](#)  
[Steven Tepper](#)
- [Rapid Application Development \(RAD\)](#)  
[Rebecca Mercuri](#)
- [Intel plant in Albuquerque](#)  
[Phil Agre](#)
- [Madcap world of modern banking](#)  
[Ross Anderson](#)
- [A330 Crash investigation report: Pilot error blamed for crash](#)  
[Erik Hollnagel](#)
- [Workshop Announcements PDCS2 and SCSC](#)  
[Barry Hodgson](#)
- [CSR Software Reliability & Metrics Club - Meeting Announcement](#)  
[Pete Mellor](#)
- [Washington DC ACM Seminar](#)  
[John Sheckler](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Unda(u)nted exploration: DANTE II

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Tue, 9 Aug 94 7:41:18 PDT

The Dante II robot (successor to Dante I, whose fiber cable snapped only 21 feet down into Mt Erebus in 1993) has been exploring the volcanic crater of Mt Spurr in Alaska, apparently with great success in gathering information in a human-risky environment after the 1992 eruption. En route to the bottom, Dante II survived being hit by rocks and slopping through mud and snow; prior to its descent its satellite dish antenna was chewed on by a bear. However, the last few days have provided grist for the RISKS mill as to what can go wrong going wrong. Last Wednesday (3 Aug 1994) the robot lost power, and then its transmitter went dead. On Thursday, a short-circuit (due to condensation) was fixed in a connector to the 1000-volt power and communications cable. The robot then was able to begin its ascent (at three feet per minute). On Friday night, the 1700-pound Dante II lost its footing when one of its eight legs malfunctioned, and it toppled over. Plans are now afoot (no pun intended) to hoist it out by helicopter, or if that fails for a geologist (John Laskeivitch of the Alaska Volcano Observatory) to climb down and attach a tether -- using the knowledge obtained from Dante II that there are lots of rocks but that the expected hot gases are no longer present. The robotic software seems to have functioned well throughout. [SOURCES: PGN News Service from articles by Charles Petit in the San Francisco Chronicle, 4-5 Aug 1994, and AP items, 7 and 9 Aug 1994.]

---

## Denver "solves" hi-tech baggage handling problems

*Lauren Weinstein <lauren@vortex.com>*

*Thu, 4 Aug 94 23:40:23 PDT*

It looks as if the folks in Denver have figured out what they need to do to finally get their new airport open. As you may recall, it has failed to open for quite sometime because the amazing, computer-controlled, \$200 million baggage handling system simply doesn't work. Nor does it appear that there is much hope of making it work quickly. The more deeply the system is inspected, the more problems are found.

Videos of the failing system under test are great fun to watch. Bags being flung at carts that aren't where they're supposed to be, carts flying off tracks, bags flying through the air smashing into the ground, and so on. Quite a show.

So how to open the airport? Simple! They've apparently decided to spend more bucks and build \*another\* baggage handling system--the conventional kind with conveyer belts. After they build this new, old-style system, they'll finally be able to open the airport, which is currently losing something like \$1 million/day just sitting there.

The plan is to shift back to the computerized system when (if?) they get all the bugs out of it.

--Lauren--

---

**Re: Squirrels again bring down Nasdaq (Neumann, [RISKS 16.30](#) )**

Joe Morris <jcmorris@mwunix.mitre.org>

Tue, 02 Aug 94 12:15:04 -0400

>Nasdaq once again was shut down by an energetic squirrel ...

To many people interested in commercial power (including computer center managers such as yours truly was at one time) the word "squirrel" is often defined as "a self-propelled short circuit".

Joe Morris / MITRE

---

## Re: Squirrels again bring down Nasdaq

<Bob\_Frankston@frankston.com>

Sat, 6 Aug 1994 14:54 -0400

There was a followup article (which I don't have handy) in the times noting that this the outage caused trade reconciliation algorithms to fail.

A general problem is cascading failures when interacting timeouts start going off.

---

## More than squirrels: Newbridge Networks

<Bob\_Frankston@frankston.com>

Mon, 8 Aug 1994 14:20 -0400

Squirrels aren't Nasdaq's only problem. According to an article in New York Times, there are also some race conditions in their procedures.

The article describes attempts to stop trading in Newbridge Networks stock. Apparently the attempt to stop trading was entered at 9:32 instead of 9:30 due to an error entering a command. Many options (more highly leveraged than shares) got through and were confirmed. They were retroactively cancelled.

There are two basic problems. One, as the article noted, is that a confirmation is not a confirmation. The other is the contrast between human speeds and computer speeds. Two minutes is a very very long time.

---

## Re: RISks of electrical wiring

Lauren Weinstein <lauren@vortex.com>

Tue, 2 Aug 94 11:01 PDT

Regarding the electrician who blew out some equipment by dropping the neutral from a circuit, causing a power leg to go to around 220V (about double the North American standard of ~117V). One might suggest that (even though it can be inconvenient) turning \*off\* the power to areas that could be directly affected by ongoing electrical work would be a simple and mandated procedure.

No fancy protective gear is needed in this case. Just turn off the breakers until the work is done.

--Lauren--

---

## **The Cult of Information ([RISKS-16.30](#))**

*Steven Tepper <greet@datatools.com>*

*Tue, 2 Aug 94 14:41:50 PDT*

> Roszak, in this book, is not attacking the idea of computerization

He already did that in a novel called "Bugs".

---

## **Rapid Application Development (RAD)**

*Rebecca Mercuri <mercuri@gradient.cis.upenn.edu>*

*Fri, 5 Aug 1994 17:49:27 +0500*

I am writing an article on Rapid Application Development (RAD) and would like to include a risky horror story or two, if anyone has one they want to share. If you can BRIEFLY describe a project where RAD techniques were used to develop a system or software which resulted in quantifiable losses (in terms of time, money, etc.) to an individual or organization, I will consider quoting you (with proper citation of course). The anecdote must be traceable to an organization or individual involved (there can be some anonymity, but some person or group must be identifiable so the story can be verified).

Please send replies DIRECTLY to mercuri@gradient.cis.upenn.edu

Sorry, I don't have time to address other matters (like "what is RAD?" -- if you don't know then you probably weren't using it).

BTW, I'm especially interested in projects where an outside consulting team came in, used RAD, developed something and left it either unfinished, undocumented, untested, and/or unsupportable. Hope someone wants to go on the record with their experience(s).

Thanks in advance, Rebecca Mercuri

---

## **Intel plant in Albuquerque**

*Phil Agre <pagre@weber.ucsd.edu>*

*Fri, 5 Aug 1994 16:27:24 -0700*

The SouthWest Organizing Project is engaged in a campaign against the Intel chip fabrication plant in Albuquerque, New Mexico. They allege excessive water use, chemical hazards to workers, and large expenditures of public funds for small numbers of jobs for local people. Their report is available from

them (US\$10 plus \$1.50 p/h) at SWOP, 211 10th St SW, Albuquerque NM 87102, USA.

Phil Agre, UCSD

---

## Madcap world of modern banking

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

*Sun, 7 Aug 1994 16:36:01 +0100*

The Sunday Times reports on 7th August that one of its readers in Hertfordshire, England, paid a cheque for a thousand pounds into her account with Barclays Bank in June. The cheque bounced, and Barclays did not credit it to her account; but for no reason they also removed a further thousand, causing her to go overdrawn.

After writing letters and waiting for weeks, she got a letter from Barclays explaining that the loss was "a quirk in our accounts processing system which is effectively debiting twice the amount of a customer's unpaid in cheque". It goes on: "Your helpful comments are valuable to us in prioritising the resolution of difficulties such as those experienced by you".

I suspect that many firms only fix software bugs when enough customers have complained about them. But how many make a virtue out of it?

Ross Anderson Cambridge University Computer Laboratory rja14@cl.cam.ac.uk

---

## A330 Crash investigation report: Pilot error blamed for crash

*Erik Hollnagel HRA <M575@eurokom.ie>*

*Fri, 05 Aug 1994 10:45 +0200*

[Erik provided an article from the U.K. *\*Times\**, 3 Aug 1994, p.7, which is omitted here. The article noted confusion on the flight deck and three seconds of hesitation by a tired chief pilot as being responsible for seven deaths on the test-flight takeoff of an Airbus A330. PGN]

My comment is that in the absence of an obvious single fault in the hardware (which in this case mostly is software) the default explanation is "human error". It looks rather as if the combination of automation, ill-defined tasks, and an unsupportive organisation were the real causes. But I would not expect Airbus to ever acknowledge that.

erik.hollnagel.hra@eurokom.ie

Erik Hollnagel, Technical Director, Human Reliability Associates Ltd.,  
School House, Higher Lane, Dalton, Lancs. WN8 7RP, UK +44.257.463.121

---

## Workshop Announcement



The Safety-critical Systems Club was formed in 1991 with support from the DTI and SERC. It provides a regular forum for presentations and interaction on a wide range of topics concerning the use of computing systems in safety-critical applications. The majority of participants are practitioners and users of such systems, but developers and research workers are also represented in the membership of almost 2,000. Each year the club holds a series of meetings and seminars, circulates a regular newsletter and organises a three day conference on the theme of safety-critical systems.

PDCS2 - ESPRIT Basic Research Project 6362  
Predictably Dependable Computing Systems

## 2ND PDCS2 OPEN WORKSHOP

### WORKSHOP PROGRAMME

19-21 September 1994  
University of Newcastle upon Tyne

#### MONDAY 19 SEPTEMBER

12.30-14.00 Registration and Lunch

14.00-14.15 INTRODUCTION  
Brian Randell (Univ. Newcastle)

14.15-15.45 FAULT PREVENTION &  
FAULT TOLERANCE:ARCHITECTURAL ISSUES  
A Systematic Approach for the Analysis of Safety  
Requirements for Process Control Systems  
- Tom Anderson  
(Univ. Newcastle)  
A TTP Solution to an Automotive Control System  
Benchmark  
- Hermann Kopetz (TU Wien)

15.45-16.10 COFFEE

16.10-18.00 DEMONSTRATIONS

- - -

#### TUESDAY 20 SEPTEMBER

09.00-10.30 INVITED SPEAKERS FROM INDUSTRY

10.30-11.00 COFFEE

11.00-12.30 FAULT TOLERANCE: LANGUAGE ISSUES  
Implementing Fault-tolerant Applications: an  
approach based on reflective object-oriented  
programming  
- Jean-Charles Fabre (LAAS-CNRS, Toulouse)

Object-Oriented Environmental Fault Tolerance

- Cecilia Calsavara (Univ. Newcastle)

12.30-14.00 LUNCH

14.00-15.30 FAULT FORECASTING: METHODOLOGY ISSUES AND MARKOV MODELS

Engineering Judgement about Dependability: pitfalls and defences

- Lorenzo Strigini (CNR, Pisa)

Availability Bounds for Large Markovian Models of Fault Tolerant Systems

- Pierre-Jacques Courtois (UC Louvain)

15.30-16.00 COFFEE

16.00-18.00 DEMONSTRATIONS

20.00 WORKSHOP BANQUET

- - -

WEDNESDAY 21 SEPTEMBER

09.00-10.30 FAULT FORECASTING: RELIABILITY AND AVAILABILITY MODELLING

Software Reliability Analysis of Three Successive Generations of a Switching System

- Karama Kanoun (LAAS-CNRS, Toulouse)

Relativistic Reliability Modelling for Highly Reliable Systems

- Bernard de Neumann (City Univ., London)

10.30-11.00 COFFEE

11.00-12.30 FAULT FORECASTING: FAULT INJECTION

Comparison of Two Fault Injection Techniques Supported by the MEFISTO Tool

- Marcus Rimen (Chalmers UT, Goeteborg)

Comparison and Integration of Three Diverse Physical Fault Injection Techniques

- Johan Karlsson (Chalmers UT, Goeteborg)

12.30-14.00 LUNCH

14.00-15.30 INVITED SPEAKERS FROM INDUSTRY AND CONCLUSION

Including closing address

by Jean-Claude Laprie (LAAS-CNRS, Toulouse)

[PLEASE CONTACT BARRY DIRECTLY FOR THE FULL ANNOUNCEMENT.  
IT IS TOO LONG FOR RISKS. PGN]

Dept. of Computing Science, Claremont Tower, University of Newcastle,  
Newcastle upon Tyne, NE1 7RU, UK

EMAIL = j.b.hodgson@newcastle.ac.uk PHONE = +44 91 222 7948

FAX = +44 91 222 8232

---

## CSR Software Reliability & Metrics Club - Meeting Announcement

*Pete Mellor <pm@csr.city.ac.uk>*

*Tue, 9 Aug 94 13:40:05 BST*

CSR  
Software Reliability & Metrics Club  
announces its forty-second meeting,  
to be held at Brighton on 12th October 1994,  
a seminar on

=====  
|| Process Improvement ||  
=====

### Learn from the practitioners

The morning session will be devoted to talks by leading experts in the increasingly important field of software process improvement, dealing with significant practical issues:

- \* How to measure software process improvement
- \* Identifying opportunities for process improvement
- \* Defining and describing processes
- \* Reasoning about process effectiveness
- \* Achieving and quantitatively demonstrating improvement

### Explore the key issues

After meeting with their peers over lunch, groups of delegates will work together, sharing their collective experience, and discussing some of the topical issues in the field of process improvement:

- \* Bottom-up or top-down?
- \* How to get started
- \* Which comes first - the process or measurement?

Delegates are encouraged to suggest other topics for discussion in this part of the meeting; to do so, fill in the relevant part of the tear-off slip on the next page. The working session will be followed by reports back to the main meeting, and an open discussion of the issues raised.

### Discover the future

Following informal discussion over tea, the final session of the day will be led by one of the key players in determining the future development of this important field. This perspective will be important for all who are planning to be, or are already, involved in the software process improvement area.

### Who should attend

This meeting is aimed at anyone with a professional interest in improving software development processes, including:

- \* software engineers, project managers and quality personnel wishing to learn about the practice of process improvement
- \* experienced process improvers who wish to broaden their knowledge and keep in touch with the latest developments
- \* researchers wishing to learn from the practical application of process improvement ideas.

Why you should attend

The benefits of attendance at this meeting include:

- \* exposure to the practical experience of other professionals who have successfully applied software process improvement within their companies and for the benefit of their clients
- \* opportunities to share your experiences and problems with other professionals, both during the formal sessions and informally during the breaks
- \* updating on the practice of the leaders in the process improvement field, and on likely short term future developments which will have implications for the whole industry.

Where, when and how to attend

The meeting will be held in Brighton, at the Bedford Hotel, on 12 October 1994, starting at 10.30 am, with registration from 10.00 am onwards. The cost of this one day meeting will be L.165.50 which covers lunch and refreshments during the day and includes L.60 Club membership fee with L.10.50 VAT; if you are already a Club member the charge is only L.90. If you would like to attend, please complete the tear-off slip below and return with your remittance; early registration would be much appreciated and may help to avoid disappointment. Maps and suggested train times will be sent to registered delegates, who are responsible for arranging their own accommodation (if required).

FOR FURTHER INFORMATION, CONTACT

Joan Atkinson, Centre for Software Reliability, Bedson Building,  
University, Newcastle upon Tyne, NE1 7RU  
Tel: 091 221 2222; Fax: 091 222 7995;  
e-mail: csr@newcastle.ac.uk

---

## Washington DC ACM Seminar

*John Sheckler, ATSC, 301/805-3258 <ndqajds@atscv1.atsc.allied.com>  
4 Aug 1994 12:20 EST*

The next Washington DC ACM Professional Development Seminar series is scheduled for November 14 through November 18, 1994. The following topics and presenters have been scheduled.

Monday, November 14

- Mr. Allen S. Perper - Business Process Engineering/Reengineering
- Mr. Will Tracz - Domain-Specific Software Architectures  
-- Process, Products, and Infrastructure

Tuesday, November 15

- Dr. Cy Svoboda - Information Engineering
- Mr. Mike Gorman - Managing the Development  
of Client/Server Applications

Wednesday, November 16

- Mr. Ed Krol - The Whole Internet -- Archie, Veronica and  
the Gopher Explore the World Wide Web
- Mr. William Durell - Data Administration and Management

Thursday, November 17

- Dr. Robert N.Charette - Profiting from Risk Management
- Mr. Watts S. Humphrey - Personal Process Improvement

Friday, November 18

- Dr. Robert S. Arnold - Legacy System Migration
- Mr. Edward V. Berard - Testing Object-Oriented Software

In addition to the regular twice yearly seminar series, the WDC-ACM also hosts a distinguished international lecturer. This year, Mr. Philip Zimmerman, developer of the well known Pretty Good Privacy encryption algorithm, will discuss Public Key Cryptography on Thursday November 10, 1994.

The seminar series and international known lecturer presentation are held at the University of Maryland Adult Education Center on the campus near the intersection of Adelphi Road and University Boulevard (Route 193).

REGISTRATION

Category	Advance Cash, Check, Credit Card	Walk-in Cash, Check, Credit Card	Purchase Orders Training Requests
ACM Chapter Member	\$170	\$205	\$230
Non-Member	\$175	\$205	\$230
Full-Time Student	\$ 80	\$110	\$230
Sr. Citizen (age 60 or over)	\$ 80	\$110	\$230

Attendance at each course will be limited to the capacity of the room being used (check with the ACM/PDC answering machine, (202) 462-1215, for availability). We are planning on using the largest rooms available for Mr. Krol, Zimmerman and Humphrey. Detailed registration information and assistance can be obtained by calling Mrs. Nora Taylor at (301)229-2588.



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 16: Issue 32**

**Tuesday 16 August 1994**

## Contents

- [Pin the tail on the Dante?](#)  
[PGN](#)
- [Adventures in Debugging](#)  
[Michael J. Stern](#)
- [Commercial identity on the Internet](#)  
[Mich Kabay](#)
- [Desktop check forgery](#)  
[Phil Agre](#)
- [Burglary suspects caught by Caller ID](#)  
[Jonathan I. Kamens](#)
- [National Guard payment problems](#)  
[Mich Kabay](#)
- [Escrowed keys vulnerable to chosen contraband attacks](#)  
[Stephen R. Savitzky](#)
- [The Danger of Six-Digit Dates](#)  
[Mike Sullivan](#)
- [A Minor Risk for Centenarians](#)  
[Bruce Scott](#)
- [IRC bug](#)  
[Andrew David Tinkham](#)
- [Privacy Conference](#)  
[Dave Banisar](#)
- [Intrusion Detection Workshop announcement](#)  
[Debra Anderson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Pin the tail on the Dante?

*"Peter G. Neumann" <neumann@chiron.csl.sri.com>  
Tue, 16 Aug 94 7:58:42 PDT*

On 9 Aug 1994, an attempt was made to rescue Dante II (see [RISKS-16.31](#)) from the Mt. Spurr crater. A helicopter tried to lift Dante II by its half-inch Kevlar-reinforced tether, but the tether snapped from the force of the

attempted liftoff. The tether had survived earlier tests that demonstrated it had sufficient strength to lift the 1700-pound robot; however, the tether may have been wrapped around one of the VW-sized boulders as a result of Dante's earlier movements. (Tim Hegadorn, a CMU grad student, was injured in the process.)

And, finally, on 12 Aug 1994, David Bares (civil engineer, and leader of the CMU robot development effort) and an Army ``pathfinder'' climbed into the Mt. Spurr volcano. David removed the computer and electronics module, which were then helicoptered out of the crater. They then hooked up a sling so that the robot itself could be hauled out. Six of the robot's legs had been ``badly dented'' --- but otherwise the robot appears ready for another mission. [From what may be the final article in this series, by Charles Petit in the *\*San Francisco Chronicle\** on 16 Aug 1994, p. 2.]

---

## Adventures in Debugging

*Michael J. Stern <stern@panix.com>  
10 Aug 1994 10:37:18 -0400*

This is from *\*New Scientist\**, 2 Jul 1994.

'Tis just 40 years since North American TV stations started broadcasting in colour, using the NTSC system. Officially NTSC was named after the National Television System Committee which chose it. Unofficially NTSC has often been called Never Thrice the Same Colour.

A journalist who used to cover the NTSC told us recently of a lighter moment at the laboratories of the record company RCA in Princeton, New Jersey, where the system was developed. Team leader George Brown laid on a final transmission test. A colour camera was focused on a bowl of colourful fruit in one lab, and the received signal was displayed in another lab on a prototype colour tube. Just before the test Brown took a banana from the bowl and painted it blue.

For the rest of the day the engineers at the receiving end struggled desperately to find out how their new system was faithfully reproducing the colour of red apples, orange oranges and green grapes, but resolutely converting yellow into blue.

---

## Commercial identity on the Internet

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
15 Aug 94 11:05:05 EDT*

[Source: Address for Success: Internet Name Game; Individuals Snap Up Potentially Valuable Corporate E-Mail IDs, By Stewart Ugelow, *\*The Washington Post\**, 11 Aug 1994, PGN abstracting from MK abstracting]

Jim Cashel has registered at least 17 E-mail addresses, including esquire.com, hertz.com, trump.com. Registration applications are honored in the order of

their requests. If YOUR name has already been taken, you can choose another name, or you can buy the rights, or you can try legal proceedings. Adam Curry is being sued for registering mtc.com. Also registered are names such as coke.com, nasdaq.com, and windows.com. However, the laws are as yet unclear on net addresses. [This RISKS item should not be construed as an invitation to run out and get into the name-registering lottery. PGN]

---

## Desktop check forgery

*Phil Agre <pagre@weber.ucsd.edu>  
Mon, 15 Aug 1994 19:04:59 -0700*

Saul Hansell, New breed of check forgers exploits desktop publishing,  
\*The New York Times\*, 15 August 1994, pages A1, C3.

This article reports that it's easy to manufacture fake checks with widely available desktop publishing software. You need an original check, which you can get from the trash, from a paid insider (usually a low-level employee), or by standing outside check-cashing shops and paying people to let you photocopy their payroll checks. Then you need a scanner, and software to manipulate the image. Then you need check paper and a check printer (both of which are readily obtained). Finally, you need someone to pass the check -- someone who'll take a cut to risk getting arrested.

The forgers and the banks are engaged in a technological arms race. Tellers can run checks through scanners to make sure they've got the right kind of magnetic ink on them, but then magnetic-ink printers are widely available. Image manipulation programs allow for "authenticating" stamps and signatures to be forged as well. When forged checks are discovered, some banks fax the pertinent information to every other bank branch in the same region of the country, figuring that the forgers have made several copies of the check and are driving around cashing them as fast as they can before the alarm is sounded. And so on.

This story illustrates one of the many subterranean interactions between computer technology and social institutions -- the tendency of applied computing to change physical objects into hybrid things that have one foot planted in cyberspace. We've always relied on the relative immutability of physical objects to do various kinds of work for us. Computers make it easier to synthesize many kinds of objects, including mutated copies of originals. The obvious solution -- at least, the solution that's obvious within the conventions of computer design -- is to give every check a digital "shadow". For example, when an employer issues a payroll check, the check number and amount might be registered digitally and made available on a server. When a check is presented for payment, the teller feeds the check into a scanner that recovers the check number and payment amount from the magnetic ink and then, rather like credit cards now, consults that server to see if the check has been presented yet.

This is only one of the many social mechanisms through which people, places, and things acquire digital shadows. Each mechanism has a seemingly inexorable logic through which the shadows cast by human artifacts and activities grow

more expansive and more detailed. This process might be planned out in advance or it might proceed through a reaction to unanticipated holes in the system. When the trends that precipitate further growth in the shadow system are bad, or at least stigmatized, little attention is paid to alternatives that might minimize the amount of personal information that is being gathered while still providing genuine benefits and helping to prevent genuine ills.

What's your shadow like?

Phil Agre, UCSD

[The ability to cloud men's minds also helps. But sniffing out forgeries is itself an art: The Digital Shadow Nose! <Shadowy laugh> PGN]

---

## **Boston Globe: Burglary suspects caught by Caller ID**

*"Jonathan I. Kamens" <jik@cam.ov.com>*

*Wed, 10 Aug 1994 17:47:26 -0400*

From the "New England News In Brief" section of the August 10, 1994 edition of \*The Boston Globe\*, here's a description of a situation in which a technological innovation had a positive but unanticipated side-effect:

Suspects dial ahead, are caught

Naugatuck, Conn. - Telephone technology has helped nab two burglary suspects who had allegedly called ahead to see if anyone was home. Police said one of the suspects called Sunday and left a message on an answering machine asking if anyone was there. The burglars rewound the answering machine when they arrived at the home, but did not notice that their number was recorded on a Caller ID device. Police traced the call to the apartment of Gregory Alves, 23, and his roommate, Gary Ingham, 19. (AP)

Jonathan Kamens | OpenVision Technologies, Inc. | jik@cam.ov.com

---

## **National Guard payment problems**

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>*

*15 Aug 94 11:05:11 EDT*

A software bug in the cutover to a new computer system at the Defense Finance and Accounting Center at Fort Benjamin Harrison in Indianapolis resulted in 900 Army National Guard members and over 7000 vendors suffering from almost \$100 million in delayed payments for a year. The National Guard also wound up with excessive payments. No fraud implied. [Source: An Associated Press item by John Diamond, from Washington, D.C., 15 Aug 1994]

---

## **Escrowed keys vulnerable to chosen contraband attacks**

Stephen R. Savitzky <steve@cache.crc.ricoh.com>

Tue, 9 Aug 94 14:25:13 -0700

Given a class of data that it is unlawful to possess (e.g. child pornography in the US, government secrets almost anywhere), escrowed encryption keys can be forced out of escrow by simultaneously transmitting such data to a site (e.g. via e-mail or anonymous FTP), and asserting to the appropriate authorities that there is probable cause to believe that such data is present at the site.

Even if evidence obtained in this way cannot be used in court, it still puts the victim through the (perhaps considerable) expense of replacing the compromised key (which may be embedded in hardware) and of tracking down anything else that may have been affected, as well as opening the door to a generalized fishing expedition that may well turn up something that \*can\* be used.

A user at the site can easily be tricked into requesting the data, for example by means of a URL that simultaneously transmits the data to the user, and notifies the appropriate authorities. This attack can easily be used against a selected set of users, e.g. those on a mailing list or subscribers to a Usenet news group.

Steve Savitzky \ <http://www.crc.ricoh.com/people/steve/steve.html>  
steve@crc.ricoh.COM \ Cyberspace: an alternate universe where magic works.

---

## The Danger of Six-Digit Dates

Mike Sullivan <74160.1134@compuserve.com>

15 Aug 94 23:05:00 EDT

I came upon this excellent warning about the dangers of six-digit dates (with the year represented by two decimal digits) recently on USENET and have reproduced it here for the readers of RISKS digest with permission:

>From: Problem Reporting Service <PROBLEMS@TDR.COM>  
>Newsgroups: tdr.problems  
>Subject: 0026 - Exactly. What do we do? (Six Digit Dates)  
>Date: Fri, 11 Aug 1994 23:00:58 -0500 (EST)  
>Organization: Tansin A. Darcos & Company, Silver Spring MD  
>Lines: 179  
>Approved: PROBLEMS@TDR.COM  
>Message-ID: <94-0026.PROBLEMS@TDR.COM>  
>NNTP-Posting-Host: access3.digex.net

Please excuse the long delay between the prior posting and this one, I have been busy with a number of very critical issues.

I've been trying to think of a way to solve the problem. I - and probably many of you - have been trying to figure out what to do about it.

At the end of "The Andromeda Strain" the Senator asks Dr. Stone what they

can do if another biological emergency occurs. "What do we do then?" he asks. "Exactly, " responds Dr. Stone, "What do we do?"

The problem is the issue of six-digit dates and the turn of the century, now less than six years away.

The problem is probably not as bad as it was, because with the introduction of IBM PCs which support dates past the year 2100, the issue isn't a problem except to the extent of programs that still use six-digit dates.

Some of you might not understand why this is a serious issue. I'll explain.

Much software which is still in use - especially on mainframes - was written ten, fifteen, even twenty years ago for use in the solving of current problems at that time.

Some of that software survives, even twenty years later. As I once pointed out in a posting on the newsgroup alt.cobol, a large company might have a massive 2,000,000 line cobol program with 500 modules that requires 50 programmers for its constant maintenance, care and feeding, and that over the years the company has probably spent in excess of fifteen million dollars.

These applications are the "bet the company" applications that are used every day to keep it in business. They are the "crown jewels" that if anything goes wrong with the application, the company might actually go into Chapter 11 or suffer massive customer backlash.

These applications cannot be rewritten because it would be too expensive, and the company can't afford to be without them. Thus, unless something happens to encourage the company to change its systems, they will continue running these old, maintenance-heavy applications.

In some cases, the program is so huge and so complicated nobody knows everything it does; it is beyond the capacity of any one person to know every function and interface and module.

Therefore it can't be said with certainty what the different sections are doing with each other. Thus finding where things are happening can be frustratingly difficult.

Which comes to the issue at hand. Many of these programs were written to use dates which are six digits in length. Three days from now it will be August 14, 1994. You can write that as 08/14/94 or 14/8/94 depending on which way your system codes dates.

Figuring out the difference between 8/14/94 and 8/15/94 is no problem, and figuring out that 8/13/95 is after 8/14/94 is also no problem.

The last date of this century is Friday, December 31, 1999. 12-31-99. Want to tell me what the next date after that is? Saturday, January 1, 2000. 01-01-00.

Which date is earlier, 01/01/99 or 01/03/00? What is the difference between 12/15/99 and 12/31/99? About two weeks. What is the difference

between 12/15/99 and 01/03/00? About 99 years.

Hypothetical Example #1. I use my Visa Card to charge \$15.00 on December 15, 1999, and the bill is calculated on Monday, January 3, 2000.

99 years of 21% compounded interest on \$15 can be over a billion dollars. Depending on where the minus sign is, either the company is going to think I haven't paid them for 99 years, and freeze my account, send me a bill for \$1 billion in interest, or roll over into positive numbers, and tell me my account has \$1 billion in available credit.

Or it simply dumps every account with outstanding balances for manual handling as the numbers are outrageous, which effectively stops automatic billing. Or the system simply crashes.

Scenario #2. A major petrochemical processing plant has a system that cooks a batch of chemicals for a certain period of time, before pushing that load out to the next process. The plant runs continuously, and batches are cooked according to time.

A plant computer shoves a load in to cook for one hour beginning at 11:45 pm on December 31, 1999. At Midnight, one of these things happens:

(1) the system notices that the batch has been in the oven too long, and pushes a batch of molten chemicals into the next process, where the process of spraying them causes an explosion.

(2) the clock counter overflows and shuts down the whole system.

(3) the system counter overflows and the batch isn't released, so it overcooks in the oven and perhaps explodes under high heat.

(4) the batch stays in the oven while a new batch is shoved in, overloading the oven and causing an explosion.

(5) any of these explosions carries back through the utilities and supplies, causing gas line explosions or power surges, as a plant that is eating perhaps 2 megawatts of power suddenly drops off the grid, causing an instant overflow and shutting down power for several areas.

Scenario #3. Several power plants go into maintenance shutdown because they've been running continuously for 98 years and 7 months longer than the maximum 90 day operating maximum. Some Nuclear Power plant goes critical or shuts down because the system believes that the rods have been installed too long.

So having looked at this issue, what can we do about it?

I got thinking about this. In some systems, there's little or no room to expand their data files and the ability to remove running applications is impossible. Therefore any method that changes the system must allow their applications to continue running.

And I thought of a method.

By coding the date into a character field, effectively in base 32, it would be possible to encode a larger date and still only use 6 characters. By encoding the year to use the letters of the alphabet, e.g. AA through

ZZ plus A0 through Z0, it is possible to cover more than 900 years, e.g. start counting with 1400 through 2300, thus covering any date that could have occurred during civilization.

In fact, if one wants to encode the month and day - Month encoded to add A,B and C and day encoded as 0-9 and A-U, it is possible to use 4 digits for the year and still fit everything into 6 bytes. Or use both and fit everything into 4 bytes.

This would also then work for places using packed decimal for the six-digit year and thus only allowing 4 bytes.

One of the things that is necessary is to make programs expecting numbers fail so that they can be changed. Programs that read these records will have to expect both old and new format records, while programs that write them should only output the new format.

The point is that with many sites having hundreds or even thousands of programs, the effort could be equivalent to three full-time people over a three year period at some sites. (Some companies have thousands or tens of thousands of programs in their libraries.) This is extra and additional maintenance on top of current maintenance. Expensive overhead that will get worse in the future as it needs to be more urgently done.

What is needed are automated searching and checking facilities to find programs that manipulate dates and change those programs to handle a new date format.

If we do not make the changes, we could be looking at failed programs, massive errors, disasters and setbacks that could produce serious, perhaps even fatal problems. It can't be done in a hurry in the last 6 months of 1999.

Let us not forget the amount of time needed to do updates, which could be days or weeks, depending on how good the automated tools are and how many applications they have.

What do we need to do?

- (1). If your site has in-house applications, and lots of source files, you need to push for the acquisition of automated checking tools.
- (2). You need to push for the manpower and resources necessary to do the work now rather than later, because "later" won't be budgeted for.
- (3). You need to push for the updating of databases to allow full 8-digit dates.
- (4). Push for all reports to eliminate use of 6-digit dates, even in display fields.
- (5). Find out what your vendor is doing if you use canned applications.

If we work on the problem now while there is time, we can do this with less error and better control, then trying to rush fixes in November of 1999 when errors could spell disaster.

If you have better ideas on how to solve the six-digit problem, please

write back.

----

To Reply to this message, write to <PROBLEMS@TDR.COM>; for private replies or subscriptions use <problems-request@tdr.com>; or use newsgroup <tdr.problems>. Please feel free to redistribute this article widely.

This message is file ftp.digex.net:/pub/access/tdarcos/0026

[This message was also forwarded by Monty Solomon <monty@roscom.com>.

By the way, I also am a subscriber to PROBLEMS.

Note that this topic has been the source of many discussions in RISKS, an Inside Risks column (January 1991), and a more recent summary of the most interesting RISKS cases that will appear in the RISKS book, Computer-Related Risks, scheduled for publication in about five weeks.

Also, see the following item, which is "old" news to gray-RISKers. PGN]

---

## A Minor Risk for Centenarians

*Bruce Scott TK <bds@ipp-garching.mpg.de>*

*Wed, 10 Aug 94 21:21:35 +0200*

The following was reported in the News of the Last Page section of the German News regularly posted by germnews@vm.gmd.de:

Babies and young children need their check-ups. One Erna Schnoor also received an invitation to the "U6" for her first birthday: "Dear Erna, now you are already suuuuch a big girl..." was how the letter from the insurance company AOK Marne of Schleswig Holstein began. Unfortunately, the computer only saves the last two digits of each person's birthday. Erna Schnoor, at 101 the oldest city's oldest inhabitant, took it in good humor.

The poster adds that he is looking forward to the turn of the Millenium...

Dr Bruce Scott Max-Planck-Institut fuer Plasmaphysik bds@ipp-garching.mpg.de

---

## IRC bug

*Andrew David Tinkham <tinkha@alkaid.dartmouth.edu>*

*Wed, 10 Aug 94 10:38:54 EDT*

A friend told me I should mention this bug here, so here goes....

In some ircII (Internet Relay Chat) clients (v2.2.9, I believe but possibly other versions as well), there is a bug called the GROK or JUKE bug which allows other people to take over your client. Irc clients have functions built in by default that allow access to an account, most notably the ability to run shell commands and such, and as long as the only person accessing the client is the one whose account it is, these commands have their uses. When someone with malicious intent gets control of a client, they can cause major

troubles such as deleting the entire account or compromising system security.

This bug seems to have been in copies of the code that was available last spring. Personally, I got a client compiled through the auto-compiler at sci.dixie.edu sometime last April or early May, I believe, and that client had the bug. I believe that since then however, they have fixed their code as have the people at cs.bu.edu and the bug no longer appears.

To determine if the bug is present in your client, login to irc and then type:

/ctcp <http://caligari.dartmouth.edu/~tinkha/andy.html>

---

## Privacy Conference

*Dave Banisar <banisar@washofc.epic.org>*

*Wed, 10 Aug 1994 17:21:49 EST*

ANNOUNCEMENT: TECHNOLOGIES OF SURVEILLANCE, TECHNOLOGIES OF PROTECTION

Sponsored by Privacy International, The University of Eindhoven, and  
The Electronic Privacy Information Center

Friday, September 9, 1994

Nieuws Poort International Press Centre, The Hague, The Netherlands

The conference will bring together experts in law, privacy, human rights, telecommunications and technology to discuss new technological developments that affect personal privacy. The sessions will be interactive, starting with introductions to the subjects by leading experts, followed by questions and discussion led by the moderators.

8:45 Introduction

Simon Davies, Chairman, Privacy International

9:00 Information Infrastructures

Marc Rotenberg, Electronic Privacy Information Center (US), Stephanie Perrin, Industry Canada

10:00 European Government Information Sharing Networks

Jos Dumatier, professor of law and director of the Interdisciplinary Centre for Law and Information Technology (ICRI) at K.U.Leuven

11:00 Cryptography Policy

David Banisar, Electronic Privacy Information Center, Jan Smiths, University of Eindhoven

12:00 Lunch

1:00 Smart Cards and Anonymous Digital Transactions

David Chaum, Digicash

2:00 Wrap up

[SPACE IS LIMITED. For the application form or more information, contact David Banisar, 1+202-544-9240(voice), 1+202-547-5482(fax) banisar@epic.org (email) or Privacy International, Washington Office, Attn: Conference Registration 666 Pennsylvania Ave, SE, Suite 301, Washington, DC 20003]

---

## **Intrusion Detection Workshop announcement for interested people**

*Debra Anderson <debra@csl.sri.com>*

*Mon, 15 Aug 94 15:24:43 -0700*

I am writing to invite you to attend a one-day workshop on intrusion detection to be held at the Baltimore Convention Center in Baltimore MD on Thursday, October 13, 1994, in conjunction with the 17th National Computer Security Conference. Because of your interest in this field, your ideas and experience will be valuable to the discussion.

The NCS Conference organizers have kindly provided us with a room at the convention center. We need know if you and/or your colleagues will attend by returning the attached reply form. For other questions, please call Liz Luntzel at 415-859-3285 or send us a fax at 415-859-2844 or email at luntzel@csl.sri.com.

The workshop will consist of several short presentations as well as discussion periods. To help me in preparing the agenda, I would be interested in knowing whether you have any progress to report on an intrusion-detection project or some related work that would be appropriate for a brief presentation. If so, please indicate the title and a paragraph describing your proposed talk on the attached form. Please also indicate there your suggestions for discussion topics.

Please respond to me, [debra@csl.sri.com](mailto:debra@csl.sri.com)

Debra Anderson, Room EL-223

SRI International

Computer Science Laboratory

333 Ravenswood Avenue

Menlo Park, California 94025

There will be no charge for the workshop, and meals will not be included. There are numerous places in the surrounding Baltimore Harbor area for breakfast and lunch. The workshop will begin at 9am and will conclude at 4pm.

I look forward to seeing you at the workshop!

Fourteenth Intrusion-Detection Workshop

Yes! I will attend the Intrusion-Detection Workshop October 13 at the Baltimore Convention Center.

Please complete the following:

Name:

Title:

Affiliation:

Address:

Check one:

I am interested in presenting a talk.

I am not interested in presenting a talk.

Title of Talk:

Abstract:

Suggestions for Discussion Topics:



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 16: Issue 33

Tuesday 23 August 1994

## Contents

- [Program Information: 17th National Computer Security Conference long](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Program Information: 17th National Computer Security Conference (long)

<Borodkin@DOCKMASTER.NCSC.MIL>

Tue, 16 Aug 94 15:06 EDT

[There is a 9 Sep 1994 deadline coming up for advance reg (saves \$45, but there is no student reduction) and conference hotel rates. As usual, RISKS runs only the program info (and in this case the full file is 42K). PLEASE E-mail Borodkin@DOCKMASTER.NCSC.MIL for full brochure. OR, you may FTP [risks-16.33](#)ncs from the RISKS: archive directory on CRVAX.SRI.COM for the full brochure, or [risks-16.33](#)ncsx for just the missing stuff. PGN]

17th NATIONAL COMPUTER SECURITY CONFERENCE

October 11-14, 1994

Baltimore Convention Center

Baltimore, Maryland

CONFERENCE PROGRAM and REGISTRATION

Tuesday, October 11, 1994 10:00a.m. - 12:00 p.m.

OPENING PLENARY

Opening: George B. Mitchell and Irene Gilbert Perry

Welcome to Baltimore: Dennis Lego, Bureau of Management  
Information Systems, City of Baltimore

Welcome to the Conference: James H. Burrows & Patrick R. Gallagher, Jr.

Keynote Address: The Honorable Sally Katzen

Administrator, Office of Information and Regulatory Affairs  
Office of Management and Budget

Systems Security Award: Patrick R. Gallagher, Jr. and James H. Burrows

Award Address: Distinguished Awardee  
Best Paper Awards: Dennis Gilbert and Christopher Bythewood  
Close: Irene Gilbert Perry and George B. Mitchell

Tuesday, 2:00-3:30 p.m.

Track A - Intrusion Detection      Chair: R.Bace, NSA  
Testing Intrusion Detection Systems: Design Methodologies and Results from an  
Early Prototype

N. Puketza, University of California, Davis  
A Pattern Matching Model for Misuse Intrusion Detection  
S. Kumar, Purdue University  
Artificial Intelligence and Intrusion Detection: Current and Future Directions  
J. Frank, University of California, Davis

Track B - Panel - The Development of Generally Accepted System Security  
Principles (GSSP)

Chair: M. Swanson, NIST  
Panelists: W. Ozier, ISSA GSSP Committee Chair  
E. Roback, NIST  
B. Guttman, NIST

This panel discusses the GSSP that NIST is developing under the auspices of  
Information Systems Security Association (ISSA) in coordination with OMB and  
with technical assistance from NSA.

Track C - Panel - Can Your Net Work Securely?

Chair: P. Neumann, SRI  
Panelists: E. Boebert, Secure Computing Corp.  
A. Goldstein, Digital Equipment Corp.  
W. Diffie, SUN Microsystems  
C. Neuman, USC-Information Sciences Institute  
Distributed systems must often rely on components whose trustworthiness cannot  
be assured. This panel explores related issues.

Track D - Panel - Model Information Security Programs

Chair: R.Owen,Jr., Texas Office of the Attorney General  
Panelists: G. Burns, Monsanto Co.  
S. Green, University of Houston  
P. Sibert, Dept. of Energy  
J. Wright, Information Resources Comm. Florida

This panel presents Information Security Programs from the state, federal,  
private, and academic sectors, highlighting their similarities and differences:  
requirements; security organizational structure; security management process;  
and methods of security awareness.

Track E Tutorial - Security in the Future

Speakers: LtCdr A. Liddle, Royal Navy, Information Resources Management College  
J. Sachs, Arca Systems, Inc.

This tutorial takes a view forward to security and its role in enterprises,  
applications, and information infrastructures; with general threats to  
information systems; and with the roles of security disciplines.

Special Session - Panel: International Harmonization, the Common Criteria -

## Progress & Status

Chair: E. Troy, NIST

Panelists: C. Ketley, European Commission (UK)

Y. Klein, European Commission (France)

H. Kreutz, European Commission (Germany)

A. Robison, CSE, Canada

M. Tinto, NSA, US

This panel discusses the Common Criteria Project, the input documents, the timetable, and the public review process. Panelists provide the first public overview of the draft Common Criteria document contents.

Tuesday 4:00-5:30 p.m.

## Track A - Panel - Fuzzy Security: Formalizing Security as Risk Management

Chair: R. Nelson, Information Systems Security

Panelists: H. Hosmer, Data Security, Inc.

J. McLean, Naval Research Lab

S. Ovchinnikov, San Francisco State University

This panel explores strategies for building flexibility into the formal aspects of computer security to produce more functional trusted systems. Panelists present views radically different from the conventional security approach.

## Track B - Security Standards and Taxonomic Structures Chair: W.Jansen, NIST

A Taxonomy for Security Standards

W. Jansen, NIST

The Graphical Display of a Domain Model of Information Systems Security (INFOSEC) Through Semantic Networks

T. Smith, NSA

A New Attack on Random Pronounceable Password Generators

R. Ganesan, Bell Atlantic

## Track C - Operational Security Enhancements Chair: D. Dodson, NIST

Controlled Execution UNIX

L. Badger, TIS

Architectures for C2 DOS/Windows-Based Personal Computers

J. Epstein, Cordant, Inc.

A Practical Hardware Device for System and Data Integrity as well as Malicious Code Protection

T.E. Elliott, CSE

## Track D - Panel - Interdisciplinary Perspectives on INFOSEC

Chair: M.E. Kabay, National Computer Security Assn.

An Anthropological View: Totem and Taboo in Cyberspace

M.E. Kabay, National Computer Security Assn.

Panelists: J. Craft, Systems Research and Applications Group

V. Black, Pace Univ.

P. Black, Pace Univ.

E. Martin, Organization & Education Consultants

INFOSEC, like other areas of human endeavor, can benefit from the insights of other disciplines. This panel, a diverse group of academics and practitioners, present their insights.

Track E - Tutorial - Risk Management

Speaker: LtCdr A. Liddle, Royal Navy, Information Resources Management College

This tutorial focuses on the importance of an overall risk management perspective to information system security, stressing risk tolerance as opposed to risk avoidance. Topics include: risk models and differentiation; asset, threat, vulnerability, and risk analysis; and technical vs. operational decisions.

Special Session - Panel: Security Requirements for Distributed Systems

Chair: R. Dobry, NSA

Panelists: J. Cugini, NIST

V. Gligor, University of Maryland

T. Mayfield, Institute of Defense Analysis

The panelists describe what is entailed in providing security for distributed systems and how they see their efforts fitting into the Common Criteria.

Wednesday, 9:00 - 10:30a.m.

Track A - Access Control Chair: D. Cooper Unisys

A Three Tier Architecture for Role Based Access Control

R. Sandhu, SETA Corp.

Using THETA to Implement Access Controls for Separation of Duties

R. Pascale, Odyssey Research Associates

Implementing Role Based, Clark-Wilson Enforcement Rules on a B1 On-Line Transaction Processing System

B. Smith-Thomas, AT&T Bell Laboratories

Track B - Criteria Chair: G. Wagner, NSA

Development History for Procurement Guidance Using the Trusted Computer System Evaluation Criteria (TCSEC)

Maj M. DeVilbiss, USA, NSA

Exporting Evaluation: An Analysis of US and Canadian Criteria for Trust

P. Olson, NSA

What Color is Your Assurance?

D. Wichers, Arca Systems, Inc.

Track C - Panel - Internet Firewalls

Chair: J.Wack NIST

Panelists: M. Ranum, TIS

B. McConnell, The MITRE Corp.

This panel discusses how firewalls work, policies that can be implemented by firewalls, and updates on different firewall configurations to support restricted access.

Track D - Panel - Ethical Issues in the National Information Infrastructure

Chair: J. Williams, MITRE Corp.

Panelists: D. Denning, Georgetown University

G. Hammonds, National Council of Negro Women

H. Hosmer, Data Security Inc.

E. Leighninger, Andover-Newton Seminary

M. Rotenberg, EPIC

Social, legal, and ethical values reflected in the design, implementation, and management of the NII will be highly visible in the security policies supported

by the NII. This panel addresses broad issues such as equity vs. risk, privacy vs. accountability, privacy vs. surveillance, and the international ramifications.

#### Track E - Tutorial - Trust Concepts

Speaker: C. Abzug, Information Resources Management College

This tutorial focuses on the fundamental concepts and terminology of trust technology. It includes descriptions of the Trusted Computer Systems Evaluation Criteria (TCSEC) classes, how these classes differ and how to determine the appropriate class for your operational environment.

Wednesday, 11:00a.m. - 12:30 p.m.

#### Track A - Panel - The Future of Role Based Access Control: Its Structure, Mechanisms, and Environment

Chair: H. Feinstein, SETA Corp.

Panelists: M. Abrams, MITRE Corp.

D. Denning, Georgetown University

D. Ferraiolo, NIST

R. Sandhu, George Mason University

This panel addresses the various definitions of role based security and how they differ from the traditional Bell-Lapadula model. Panelists represent researchers and the user community.

#### Track B - Panel - Product and System Certification in Europe

Chair: K. Keus, BSI, Germany

Panelists: M. Ohlin, Swedish Defense Materiel Admin.

P. Cambell-Burns, Admiral Mngt. Services Ltd., UK

H. Kersten, BSI, Germany

A.C. Jennen, BSI, Germany

P. Overbeek, TNO Physics and Electronic Lab, NL

J. Wilde, Logica, UK

L. Borowski, CR2A, France

This panel, representing Certification bodies of the European Community, discusses their experiences with the European Criteria.

#### Track C - Panel - Proven Detection Tools For Intrusion Prevention

Chair: M. Higgins, DISA/CISS

Panelists: E. Dehart, Carnegie Mellon University

S. Weeber, Lawrence Livermore National Lab

F. Avolio, Trusted Information Systems

D. Slade, Bell Communications Corp.

This panel addresses the uses, implementation, features, and lessons learned of protection tools. Panelists will take audience through detection scenarios and lessons learned from operational implementation.

#### Track D - Panel - Medical Information Privacy Current Legislative And Standards Activities

Chair: M. Schwartz Summit Medical Systems, Inc.

Privacy and the Handling of Patient Related Information in the Public Swedish Health Care System

T. Olhede, Swedish Institute for Health Services

Panelists: R. Gellman, U.S. House of Representatives  
M. Donaldson, National Academy of Sciences  
D. Miller, Irongate, Inc.  
C. Waagemann, Medical Records Institute  
G. Lang, The Harrison Avenue Corp.

This panel addresses the technical and human issues generated by the currently available technology in the medical arena.

Track E - Tutorial - Trusted Networks

Speaker: R.K. Bauer, Arca Systems, Inc.

This tutorial focuses on basic points in network security and gives an overview of the Trusted Network Interpretation (TNI). Topics include: network security concerns and services, trusted network components, the TNI and its Evaluation Classes, system composition and interconnection, and cascading.

Wednesday 2:00 - 3:30 p.m.

Track A - Database Developments      Chair: M. Schaefer, Arca Systems, Inc.

Virtual View Model to Design a Secure Object-Oriented Database

F. Cuppens, ONERA/CERT

Achieving Database Security Through Data Replication: The SINTRA Prototype

M. Kang, Naval Research Lab

The SeaView Prototype: Project Summary

T. Lunt, SRI International

Track B - Panel - New Concepts in Assurance

Chair: P.Toth, NIST

Panelists: L. Ambuel, NSA

D. Kimpton, CSE - Canada

K. Rochon, NSA

K. Ferraiolo, ARCA Systems

This panel discusses new concepts in the area of assurance for IT security products and systems. Presentations include results of two workshops on assurance: The Invitational Workshop on Information Technology Assurance and Trustworthiness and the International Workshop on Development Assurance.

Track C - Panel - MLS System Solutions-A Continuing Debate Among the Critical Players

Chair: J. Sachs, Arca Systems, Inc.

Panelists: J. Adams, SecureWare

M. Askew, GTE

G. Evans, ARCA

P. Klein, DISA

A. Leisenring, NSA

K. Thompson, USACOM

J. Seymour, Joint Staff

This panel debates issues associated with acquiring an MLS system.

Track D - Detecting and Deterring Computer Crime      Chair: J. Holleran, NSA

The Electronic Intrusion Threat to National Security & Emergency Preparedness

Telecommunications: An Awareness Document

T. Phillips, Booz Allen & Hamilton, Inc.

Using Application Profiles to Detect Computer Misuse

N. Kelem, Trusted Information Systems

Can Computer Crime Be Deterred?

S. Sherizan, Ph.D, Data Security Systems, Inc.

Track E - Tutorial - Trusted Databases

Speaker: G.Smith, Arca Systems, Inc.

This tutorial focuses on security from a "database view" and gives an overview of the Trusted Database Interpretation (TDI). Topics include: DBMS specific security requirements, vulnerabilities, and challenges; database design considerations; implementation issues; and use issues.

Wednesday 4:00 - 5:30 p.m

Track A - Panel - Inference Problem in Secure Database Systems

Chair: B. Thuraisingham, MITRE Corp.

An Inference Paradigm

D. Marks, NSA

Panelists: D. Marks, NSA

T. Lunt, SRI Intl.

T. Hinke, University of Alabama

M. Collins, MITRE Corp.

L. Kerschberg, George Mason University

This panel focuses on the practical developments made on the inference problem over the past three years and provides direction for further work on this problem.

Track B - Panel - New Challenges for C&A: The Price of Interconnectivity and Interoperability

Chairs: Ellen Flahavin, NIST

Joel Sachs, ARCA

Panelists: A. Lee MITRE

E. O'Connor, IRS

H. Ruiz, DISA

S. Schanzer, CIA

E. Springer, OMB

This panel focuses on new challenges for certification and accreditation from a variety of government perspectives including civil, defense, intelligence, and multi-agency.

Track C - Putting Trusted Products Together

Chair: B. Burnham, NSA

Partitioning the Security Analysis of Complex Systems

H. Holm, NSA

The Composition Problem: An Analysis

G. King, Computer Science Corp.

Making Do With What You've Got

J. Jerryman, The Boeing Co.

Modern Multilevel Security (MLS): Practical Approaches for Integration, Certification, and Accreditation

B. Neugent, The MITRE Corp.

Track D - Panel - Computer Crime on the Internet

Chair: C. Axsmith, Esq., ManTech Strategies Associates

Panelists: D. Parker, SRI Intl.

M. Pollitt, FBI

T. Chambers, Food & Drug Admin.

B. Fraser, CERT, Carnegie Mellon Univ.

M. Schoffstall, Performance Systems International

M. Fedor, Performance Systems International

This panel addresses computer crime issues related to Internet connections. The issue will be dealt with from many angles to provide a practical and wellrounded overview.

Track E - Tutorial - Criteria Comparisons

Speaker: C. Abzug, Information Resources Management College

This tutorial focuses on the differences and similarities of the national and international criteria of Canada, the United States, and Europe. They are compared and considered, both in the context of value to security engineering today, and as foundations for the Common Criteria.

Wednesday, 7:00p.m. Conference Banquet at the Hyatt Regency Inner Harbor Hotel

Harry B. DeMaio, Deloitte & Touche

Thursday, 9:00 - 10:30 a.m.

Track A - Panel - Key Escrowing: Today and Tomorrow

Chair: M. Smid, NIST

Panelists: J. Manning, NSA

M. Glimore, FBI

D. Denning, Georgetown University

This panel provides an in-depth technical view of the key escrow system developed in conjunction with FIPS 185.

Track B - Panel - The Department of Defense Goal Security Architecture

Chair: W.T. Polk, NIST

Panelists: R. McAllister, NSA

C. Deutsch, NSA

J. Schafer, DISA

J. Coyle, Booz.Allen & Hamilton

This panel discusses the DGSA. The DGSA is derived from DoD Information System Security Policy and reflects requirements for the support of multiple security policies, distributed information processing, conductivity by common carriers, users with different security attributes, and resources with varying degrees of security protection.

Track C - Panel - Trusted Systems Interoperability Group

Chair: S. Wisseman, Arca Systems, Inc.

Panelists: P. Cummings, Digital Equipment Corp.

R. Sharp, AT&T Bell Laboratories

J. Edelheit, The MITRE Corp.

C. Watt, SecureWare, Inc.

G. Mitchell, NSA

This panel, discussing TSIG work since 1989, addresses problem progress in providing multi-vendor interoperability among security enhanced and traditional UNIX systems.

Track D - Risks and Threats Chair: D. Gambel, Northrup Grumman

Demonstrating the Elements of Information Security With Threats

D. Parker, SRI International

The Aerospace Risk Evaluation System (ARIES): Implementation of a Quantitative Risk Analysis Methodology for Critical Systems

C. Lavine, The Aerospace Corp.

The Security-Specific Eight Stage Risk Assessment Methodology

D. Drake, Science Applications International Corp.

Track E - Tutorial - UNIX Security

Speaker: E. Schultz, Arca Systems, Inc.

This tutorial focuses on operational security with systems in an internetworked environment, using UNIX as an example. It includes security weaknesses, methods for improving security, and ways to detect and respond to attacks on UNIX systems.

Thursday, 11:00a.m.- 12:30p.m.

Track A - Panel - The Security Association Management Protocol (SAMP)

Chair: Maj T. Hewitt, USAF NSA

Panelists: D. Walters, NIST

D. Wheeler, Motorola

M. White, Booz. Allen & Hamilton

A. Reiss, NSA

J. Leppke, Harris Corporation

A security association is an agreement between two or more entities that resolves all of the options (negotiable parameters) of the security mechanisms that perform security services for communication. This panel addresses some of the questions, design considerations, and requirements for security associations.

Track B - Network Architecture Chair: H.Weiss, SPARTA, Inc.

BFE Applicability to LAN Environments

T. Benkart, ACC Network Systems

The Architecture of Triad: A Distributed, Real Time, Trusted System

E.J. Sebes, TIS

Constructing a High Assurance Mail Guard

R. Smith, Secure Computing

Track C - Panel - NSA Concurrent Systems Security Engineering Support To The MLS TECNET Program

Chair: B. Hildreth, NSA

Panelists: M. Mayonado, Eagan, McAllister Assoc.

T. Acevedo, Pulse Engineering, Inc.

J. Himes, NSA

G. Wessel, NSA

R. Blair, NSA

R. White, Air Intelligence Agency

G. Hurlburt, Naval Air Warfare Center

This panel discusses the Concurrent System Security Engineering initiative that NSA is applying to aid TECNET, the Test & Evaluation Community Network. TECNET

must evolve the capability for simultaneously processing unclassified and classified data while supporting both cleared and uncleared users.

Track D - Panel - Current Issues & Trends in Trusted Product Evaluations

Chair: K. Bruso, NSA

Panelists: P. Toth, NIST

J. Arnold, NSA

C. McBride, NSA

L. King, NSA

M. Hale, NSA

J. Pedersen, NSA

This panel will highlight the significant accomplishments of trusted product evaluations during the past year. Process improvements will be discussed with particular attention given to the Trust Technology Assessment Program and the Trusted Products Evaluation Program.

Track E - Tutorial - Windows NT Security

Speaker: J. Williams, Arca Systems, Inc.

This tutorial focuses on operational security with distributed PC- based computing, using Windows NT as an example. It discusses security from the perspectives of both clients and servers: exposures and vulnerability, appropriate control measures, and recommended policies and practices.

Thursday, 2:00-3:30 p.m.

Track A - Networks and Distributed Systems

Chair: D. Schnackenberg, Boeing Defense & Space Group

Towards a Formal Verification of a Secure and Distributed System and its Applications

K. Levitt University of California at Davis

Making Secure Dependencies Over a LAN Architecture - for Security Needs

B. d'Ausbourg, CERT/ONERA

Automatic Generation of High Assurance Security Guard Filters

V. Swarup, The MITRE Corp.

Track B - Panel - Multilevel Security (MLS) - Current Applications and Future Directions I

Chair: Col. J. Sheldon, USA, DISA/CISS

Panelists: J. Wiand, USSOCOM

R. Myers, USACOM

E. Klutz, USACOM

LTC T. Surface, USPACOM

Maj K. Newland, USSPACECOM

P. Woodie, NSA

C. West, DISA

This panel covers applications and use of multilevel security (MLS) solutions fielded at the US Unified Commands by the Department of Defense MLS Program, and an overview of the NSA Multilevel Information System Security Initiative (MISSI).

Track C - Security Implementations Chair: J.Anderson, J.P. Anderson Co.

Applying COMPUSEC to the Battlefield

S. Arkley, Computer Sciences Corp.

Security Requirements for Customer Network Management in Telecommunications

V. Varadharajan, Hewlett-Packard Labs.

Support for Security in Distributed Systems Using MESSIAHS

S. Chapin, Kent State University

Track D - Panel - Do You Have the Skills to be a Future INFOSEC Professionals?

Chair: V. Maconachy, DISA/CISS

Panelists: C. Schou, Idaho State University

R. Morris

G. Burns, Monsanto Corp.

This panel examines the types of skills that will be needed to cope with the changing work environment and what types of individual initiatives are required to keep up with advancing technologies and management challenges.

Track E - Tutorial - System Security Engineering, Certification, and Accreditation

Speaker: J. Sachs, Arca Systems, Inc.

This tutorial focuses on engineering and assessment issues in integrating MLS solutions using trusted products, developing the certification evidence, and the accreditation process. Topics include: system security, assurance, trade-offs, and methodologies.

Thursday, 4:00- 5:30p.m.

Track A - Formal Methods and Modeling Chair: S. Jajodia, George Mason University

Belief in Correctness

M. Abrams, The MITRE Corp.

Towards a Privacy-Friendly Design and Use of IT-Security Mechanisms

S. Fischer-Hubner, University of Hamburg

Using a Semiformal Security Policy Model 2C a C2 Better

M. Schaefer, Arca Systems, Inc.

Track B - Panel - Multilevel Security (MLS) - Current Applications and Future Direction II

Chair: Col. J. Sheldon, DISA/CISS

Panelists: J. Wiand, USSOCOM

R. Myers, USACOM

E. Klutz, USACOM

LTC T. Surface, USPACOM

Maj K. Newland, USSPACECOM

P. Woodie, NSA

C. West, DISA

This panel covers applications and use of multilevel security (MLS) solutions fielded at the US Unified Commands by the Department of Defense MLS Program, and an overview of the NSA Multilevel Information System Security Initiative (MISSI).

Track C - Views on Vulnerability Chair: R. Wood, NSA

A Technical Approach for Determining the Importance of Information in Computerized Alarm Systems

J. Lim, Lim & Orzechowski Assoc.

ASAM: A Security Certification and Accreditation Support Tool for DoD Automated Information Systems

L. Remorca, Secure Solutions, Inc.

A Financial Management Approach for Selecting Optimal, Cost-Effective Safeguards Upgrades for Computer- and Information- Security Risk Management

S.T. Smith, Barracana, Inc.

Track D - Real Lessons      Chair: J. Campbell, NSA  
Security Awareness and the Persuasion of Managers

D. Poindexter, CISS

The Network Memorandum of Agreement (MOA) Process: Lessons Learned

L. Jaworski, TIS

Independent Validation and Verification of Automated Information Systems the Department of Energy

W. Huntzman, Los Alamos National Laboratory

Track E - Tutorial - Information System Security Officer's Challenges

Speaker: C. Bressinger, DoD Security Institute

This tutorial focuses on the continued protection and accreditation of operational information systems. Topics include: virus prevention and eradication; access control evaluation and configuration; media clearing and purging; intrusion detection and handling; and dealing with risk.

Thursday, 6:00 p.m. Awards Ceremony followed by Awards Reception  
at the Baltimore Convention Center

Friday, 9:00 - 10:30 a.m.

Track A - Panel - Highlights of the New Security Paradigms '94 Workshop

Chair: E. Leighninger, Co-Program Chair

Formal Semantics of Confidentiality in Multilevel Logic Databases

A. Spalka, University of Bonn

Healthcare Information Architecture: Elements of a New Paradigm

D.Essin & T. Lincoln

Communication, Information Security and Value

J. Dobson, University of Newcastle

Fuzzy Patterns In Data

T.Y. Lin, San Jose State University

Track B - Panel - Prominent Industry-Sponsored Security Architectures Currently Under Development

Chair: M. McChesney, SecureWare

Panelists: R. Schell, Novell, GSA

B. Dwyer, Hewlett-Packard, DCE

This panel discusses the Distributed Computing Environment Security Servicing, the Novell Global Security Architecture, and the Extended Global Security Architecture; how they relate to one another and how they might evolve in the future to provide compatible security functionality.

Track C - Panel - Provisions to Improve Security on the Internet

Chair: H. Highland

Panelists: F. Avolio, Trusted Information Systems, Inc.

S. Bellovin AT&T Bell Laboratories  
M. Bishop, University of California, Davis  
W. Cheswick, AT&T Bell Laboratories  
Dr. J. David, The Fortress  
Colonel F. Kolbrener  
A. P. Peterson, P.E., Martin Marietta

This panel discusses what Internet has done to promote net security the specific risks of operating under TCP/IP, and what can be done quickly and easily to promote net security.

#### Track D - Panel - Computers at Risk (CAR) Recommendations: Are They Still Valid?

Chair: H.Tipton, CISSP, Member of the CAR Committee, Member of the GSSP Committee

Panelists: W. Ozier, Ozier Peterse & Assoc.

S. Walker, Trusted Information Systems

E. Boebert, Secure Computing Corp.

Panelists revisit the CAR committee recommendations in view of the information security environment today.

#### Track E - Panel - IT Security Resources

Panelists: K. Everhart, NIST

M. Swanson, NIST

B. Lau, NSA

N. Lynch, NIST

This session presents an overview of major sources of information on IT security and a model for acquiring, disseminating, and managing security-relevant information resources.

Friday, 11:00 a.m. - 12:30 p.m. CLOSING PLENARY

"Security, Privacy, and Protection issues in Emerging Information Infrastructures"

Distinguished Panel:

Professor Anthony Oettinger (Co-Chair)

Chairman

Program on Information Resources Policy

Harvard University

Dr. Brian Kahin (Co-Chair)

Director

Information Infrastructure Project

Science, Technology and Public Policy Program

Harvard University

Robert Lucky

Vice President

Applied Research

Bellcore

Fred M. Briggs

Senior Vice-President and Chief Engineering Officer

MCI



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 16: Issue 34**

**Weds 24 August 1994**

## Contents

- [Bug in Microsoft Word](#)  
[Chris Norloff](#)
- [Report on the 1993 Gatwick near-miss](#)  
[Peter Ladkin](#)
- [The new Cray and Unix passwords...](#)  
[Peter Wayner](#)
- [Most home security alarms are false](#)  
[Mich Kabay](#)
- [Misconceptions about PGP 2.6 from MIT](#)  
[Philip Zimmermann](#)
- ["Secrets of a Super Hacker" by Fiery](#)  
[Rob Slade](#)
- [International Cryptography Institute](#)  
[Dorothy Denning](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Bug in Microsoft Word

<[cnorloff@tecnnet1.jcte.jcs.mil](mailto:cnorloff@tecnnet1.jcte.jcs.mil)>

Wed Aug 24 14:55:07 1994

There's a bug in Microsoft Word 6.0 and 6.0a: what you see is not what you get. I saw this in *\_Windows Magazine\_*, May 1994 (Fred Langa's column "Win.INI", pages 11 and 14). I checked the problem with a copy of Word 6.0a, and confirmed it exists. I'm surprised I haven't seen it in RISKS, and checked the archive, but could find no mention of it in volumes 15 or 16.

### THE BUG:

Word has a summary info area, for each document, that cannot be turned off. If you do not enter information in the summary (which is the default setting) then Word will lift sentences out of the beginning of your document and place them in the summary, without telling you. Even if you then change the summary info, the lifted sentences may still remain hidden in the document, visible to

any text editor (but not visible in Word).

If all you use is printed copies, you're okay. However, if you give somebody the file on disk or send it by email, then there may be unintended information in the file -- not great for people working with sensitive, competition sensitive, or classified information.

According to the *\_Windows Magazine\_* article, Microsoft denies this is a problem. For the time being, you can:

1. Turn on the "Prompt for Summary Info" in the Tools/Options/Save menu (this requires you to enter summary information, or accept what you've already entered, each time you save the document. This way Word will not lift sentences out of the text.)

-or-

2. Block copy all your text to another document before transferring the file.

-and-

3. Notify Microsoft if you believe this is a problem, to encourage them to fix it.

The RISKS? well ...

1. You start to write a flame-o-gram, but later tone it down. Those first sentences may still be buried in the document.

2. You're involved with sensitive information (competition sensitive, source selection sensitive), or classified information. You don't see anything sensitive or classified so the document goes out. But those first sentences may still be there.

3. A software company sets their product to do something without telling you, particularly something that uses information from you, in ways unintended by you, without your knowledge or permission.

Chris Norloff

---

## Report on the 1993 Gatwick near-miss

*Peter Ladkin <Peter.Ladkin@loria.fr>*

*Wed, 24 Aug 1994 20:42:35 +0200*

[NOTE: PGN introduced an error in the original copy of this, 1992 instead of 1993. That is corrected here. PGN]

The accident report is now in on the February 1993 off-course Continental Airlines Boeing 747 with 233 people aboard that flew within 500 feet of the Gatwick passenger terminal during a landing attempt at Gatwick Airport. Apparently computer failure prevented the automatic pilot from locking on to the radio beams that would have guided the plane to the runway. A manual landing followed. The crew had expressed doubts as to the accuracy of the instruments. [Source: A Close Call for U.S. Jet at Gatwick, excerpted by PGN from The International Herald Tribune, 24 Aug 1994, p.2]

It sounds as though there was a failure to capture the localiser. But that happens. And how on earth were they following it if they hadn't captured it? I'd also guess there was some discrepancy amongst the instruments that they were busy trying to troubleshoot. Maybe one of the UK people can grab the report? Peter Ladkin

[Also noted by Olivier M.J. Crepin-Leblond <o.crepin-leblond@ic.ac.uk>. PGN]

---

## The new Cray and Unix passwords...

*Peter Wayner <pcw@access.digex.net>*

*Fri, 19 Aug 1994 19:29:19 -0400*

There has been a bit of news in the business sections about the new NSA contract given to Cray to develop a hybrid machine that combined the best of the old Cray vector approach with the best of the old Thinking Machine CM-1/CM-2 architecture. It is somewhat ironic that this was released in the same time frame that Thinking Machines went into Chapter 11, but it may turn out that this marriage really brings out the best in both approaches. Some of the news stories concentrated on the quasi-Chrysler-like bailout of an important technological treasure, but that is a question for political scientists who cleave to moldy debates about the relationship between private enterprise and the state.

The biggest question for citizens of the techno-tribe of cyberspace, though, is what does this mean for digital privacy. Will the NSA be able to crack passwords with abandon? Will they be able to cut through the protection of DES like it was butter? Any speculation is, of course, pure speculation. But it is possible to make some educated guesses about the machine.

News reports and other research states that this machine will include 512,000 processors that contain 256 bits of memory apiece. Each processor contains an ALU and three one bit registers. It really isn't a processor as much as a programmable logic gate that will take three inputs and spit out one of the 8 possible outputs. The architecture is supposed to borrow heavily from a neat machine called the Processor-In-Memory (PIM aka TeraSys) developed by the Supercomputer Research Center, a semi-public branch of the NSA.

I happened to play with a very similar architecture several years ago developed by a company called Coherent Research Inc in Syracuse, NY. It turns out that it does a pretty good job of breaking DES. One hypothetical machine with 1 billion processors should be able to test all  $2^{55}$  possible keys for DES in 1 day.

How long should it take the Cray/SRC? The Cray/SRC processors are supposed to run at 2.08 ns/cycle. The Coherent Chips ran at 50MHz or 20 ns/cycle. This means the Cray/SRC is about 10 times faster. This is a very rough estimate, though, because it is not clear how many cycles it takes the Cray to complete each operation. The Coherent Processor took 2-4 cycles per operation. This would imply that the Cray/SRC could knock off all  $2^{55}$  possible keys in 100 days.

Given that DES may still be used extensively in financial transactions that move billions of dollars, it becomes clear that it might be worth it to spend \$10 or so million on a machine and let it crank for a bit. (That's my wild estimate on the price. I think it could be as low as \$2-3 million).

But even if most of us don't have \$100 million to steal, we still have reason to wonder about the effects of this machine. UNIX security systems use DES to encrypt the passwords 25 times before comparing them to a encrypted version stored in the central password file. A popular attack on the systems is to grab this central file and encrypt all of the words in the dictionary looking for a match. This is easy to do with a garden variety RISC machine today which is why many decent system administrators require gibberish passwords with numbers.

How long would it take to attack gibberish passwords with this new Cray/SRC? I extrapolated some earlier work of David Feldmeirer and Phil Karn to show that a 64k processor version could knock off all 6 character passwords in about half of a day. (6 characters drawn from the set A-Z,a-z,0-9) If the 512k processor Cray/SRC can really run 10 times faster, then it could knock off these 6 character passwords in less than 15 minutes. All seven character UNIX-style passwords would take less than 2 days and all eight could be searched in less than four months.

There is one interesting side-effect of this approach. It takes about the same amount of time to attack 1000 passwords as it does to attack 1. After the 512k processors complete their encryption, they check to see if they've got a match. The encryption process was about 10,000 times slower than the matching on my design. So if you could grab a password file for a computer with 1000 users it would still take you about 15 minutes to find the one sucker with a 6 digit password.

This means that even the maximum-sized 8-character UNIX-style passwords are really on the edge of obsolescence. It is really time for a new system to be developed. 16 characters might be best. But who can remember that many? Sure some know millions of digits of pi, but a bunch of politicians tried to shorten it to plain 3. This means we need to rethink many of the modes of protecting machines.

[I presume that when Peter wrote "a plain 3" he was implying just 3 digits, as opposed to the old mathematical physicists' joke about pi being equal to 3 for small values of pi and large values of 3. PGN]

All of what I've written falls into the realm of informed speculation. You can read about my design in a paper which was presented at Crypto 92. Mail me if you want a TeX version of it. I suggest that you dig up conference proceedings about the PIM/Terasys machine to get a better estimate of the new Cray/SRC's machine's performance.

---

## Most home security alarms are false

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
16 Aug 94 07:44:52 EDT*

>From the Associated Press newswire (94.08.16 @ 00:00 EDST) via CompuServe's Executive News Service (GO ENS):

"Home Security", By WILL LESTER, Associated Press Writer

The author describes the current problems caused by home security systems.

Key points:

- o Burglars can easily disable some home security system control panels.
- o Estimates of false alarms from these systems range from 70% to 90% and even higher.
- o "The false alarms are astronomical," says Sgt. Steve Emmons, spokesman for the Tulsa, Okla., Police Department. "It ties up two officers every time we get one, and 98 percent of our alarms are false. It is causing our call load to grow to an extreme level."
- o Dallas police field 140,000 alarms/year, "most of them false."
- o Los Angeles charges \$80 per false alarm after the first four free false alarms per location.
- o Miami tolerates five false alarms but then charge increasing fines.
- o Portland, OR. impose escalating fines and provide training.
- o "Security specialists advise buying a more sophisticated system that can provide protection for windows, motion detectors and a control system not easily disabled. Sirens are useful to shorten the burglars' stay."

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn

---

<Philip Zimmermann, creator of PGP>

18 Aug 94

[NOTE: PGN removed PZ's PGP signing, for brevity. Besides, I corrected a few typos, which would blow the integrity check. PGN]

I'd like to clear up some widely held misconceptions about PGP version 2.6 from MIT. I get a lot of email and phone calls from people who report a lot of misinformation on many Internet newsgroups about this MIT version of PGP.

(For those of you who need an introduction to Pretty Good Privacy (PGP), it is a free software package that encrypts email. PGP is the worldwide defacto standard for email encryption. It's available via FTP from net-dist.mit.edu, in the pub/PGP directory. But then, if you haven't heard of PGP, you don't need to read this letter.)

Here is a list of misconceptions:

Myth #1: PGP 2.6 is incompatible with previous versions.

Myth #2: PGP 2.6 is weaker than previous versions, with a back door.

Myth #3: PGP 2.6 was released without Zimmermann's cooperation.

All of these misconceptions would be cleared up if you read the PGP User's Guide that comes with PGP 2.6, but a lot of people seem to be spreading and believing these myths without looking into the matter empirically and getting the new PGP and reading the manual. Let's go over these myths in detail.

-----  
Myth #1: PGP 2.6 is incompatible with previous versions.  
-----

This is untrue. PGP 2.6 will ALWAYS be able to read stuff from earlier versions.

PGP version 2.6 can read anything produced by versions 2.3, 2.3a, 2.4, or 2.5. However, because of a negotiated agreement between MIT and RSA Data Security, PGP 2.6 will change its behavior slightly on 1 September 1994, triggered by a built-in software timer. On that date, version 2.6 will start producing a new and slightly different data format for messages, signatures and keys. PGP 2.6 will still be able to read and process messages, signatures, and keys produced under the old format, but it will generate the new format. This change is intended to discourage people from continuing to use the older (2.3a and earlier) versions of PGP, which Public Key Partners contends infringes its RSA patent (see the section on Legal Issues). PGP 2.4, distributed by Viacrypt (see the section Where to Get a Commercial Version of PGP) avoids infringement through Viacrypt's license arrangement with Public Key Partners. PGP 2.5 and 2.6 avoid infringement by using the RSAREF(TM) Cryptographic Toolkit, under license from RSA Data Security, Inc.

According to ViaCrypt, which sells a commercial version of PGP, ViaCrypt PGP will evolve to maintain interoperability with new freeware versions of PGP, beginning with ViaCrypt PGP 2.7.

It appears that PGP 2.6 has spread to Europe, despite the best efforts of MIT and myself to prevent its export. Since Europeans now seem to be using version 2.6 in Europe, they will have no problems maintaining compatibility with the Americans.

Outside the United States, the RSA patent is not in force, so PGP users there are free to use implementations of PGP that do not rely on RSAREF and its restrictions. Canadians may use PGP without using RSAREF, and there are legal ways to export PGP to Canada. In environments where RSAREF is not required, it is possible to recompile the same PGP source code to perform the RSA calculations without using the RSAREF library, and re-release it under the identical licensing terms as the current standard freeware PGP release, but without the RSAREF-specific restrictions. The licensing restrictions imposed by my agreement with ViaCrypt apply only inside the USA and Canada. It seems likely that any versions of PGP prepared outside the US will follow the new format, whose detailed description is available from MIT. If everyone upgrades before September 1994, no one will experience any discontinuity in interoperability.

Some people are attracted to PGP because it appeals to their rebellious nature, and this also makes them resent anything that smacks of "giving in" to authority. So they want to somehow circumvent this change in PGP. Even though the change doesn't hurt them at all. I'd like to urge them to think this one through, and see that there is absolutely no good reason to try to get around it. This new version is not "crippled" -- in fact, it is the old versions that are now crippled. I hope that PGP's "legalization" does not undermine its popularity.

This format change beginning with 2.6 is similar to the process that naturally happens when new features are added, causing older versions of PGP to be unable to read stuff from the newer PGP, while the newer version can still read the old stuff. All software evolves this way. The only difference is that this is a "legal upgrade", instead of a technical one. It's a worthwhile change, if it can achieve peace in our time.

Future versions of PGP now under development will have really cool new features, some of which can only be implemented if there are new data format changes to support them. Like 2.6, the newer versions will still read the older stuff, but will generate new stuff that the old versions can't read. Anyone who clings to the old versions, just to be rebellious, will miss out on these cool new features.

There is another change that effects interoperability with earlier versions of PGP. Unfortunately, due to data format limitations imposed by RSAREF, PGP 2.5 and 2.6 cannot interpret any messages or signatures made with PGP version 2.2 or earlier. Since we had no choice but to use the new data formats, because of the legal requirement to switch to RSAREF, we can't do anything about this problem for now. Not many people are still using version 2.2 or older, so it won't hurt much.

Beginning with version 2.4 (which was ViaCrypt's first version) through at least 2.6, PGP does not allow you to generate RSA keys bigger than 1024 bits. The upper limit was always intended to be 1024 bits -- there had to be some kind of upper limit, for performance and interoperability reasons. But because of a bug in earlier versions of PGP, it was possible to generate keys larger than 1024 bits. These larger keys caused interoperability problems between different older versions of PGP that used different arithmetic algorithms with different native word sizes. On some platforms, PGP choked on the larger keys. In addition to these older key size problems, the 1024-bit limit is now enforced by RSAREF. A 1024-bit key is very likely to be well out of reach of attacks by major governments. In some future version, PGP will support bigger keys. This will require a carefully phased software release approach, with a new release that accepts larger keys, but still only generates 1024-bit keys, then a later release that generates larger keys.

-----  
Myth #2: PGP 2.6 is weaker than previous versions, with a back door.  
-----

This is not true. I would not allow MIT or anyone else to weaken PGP

or put a back door in. Anyone who knows me will tell you that.

This is not to say that PGP doesn't have any bugs. All versions have had bugs. But PGP 2.6 has no known bugs that have any net effect on security. And MIT should be releasing a bug-fixed version of PGP 2.6 Real Soon Now.

-----  
Myth #3: PGP 2.6 was released without Zimmermann's cooperation.  
-----

Well, that's not true, either. Or I wouldn't be telling you all this.

MIT did not steal PGP from me. This was a joint venture by MIT and myself, to solve PGP's legal problems. It took a lot of maneuvering by me and my lawyers and by my friends at MIT and MIT's lawyers to pull this off. It worked. We should all be glad this came off the way it did. This is a major advance in our efforts to chip away at the formidable legal and political obstacles placed in front of PGP; we will continue to chip away at the remaining obstacles.

I hope this clears up the myths about PGP 2.6. I urge all PGP users to upgrade to the new version before September. And I urge you all to use the official 2.6 release, not anyone else's incompatible bastardized mutant strain of PGP. Please pass the word around, and help dispel these misguided rumors. This letter may be (and should be) quickly reposted to BBS's and all appropriate newsgroups.

--Philip Zimmermann

---

<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067">  
Thu, 18 Aug 1994 14:25:22 -0600 (MDT)

Subject: "Secrets of a Super Hacker" by Fiery

BKSCSUHK.RVW 940609

Loompanics Unlimited  
P.O. Box 1197  
Port Townsend, WA 98368  
206/385-5087  
fax 206/385-7785  
loompanx@pt.olympus.net  
"Secrets of a Super Hacker", Fiery, 1994, 1-55950-106-5, U\$19.95

Despite Loompanics' reputation as a "dark side" publisher, this may be a very good book. It deals primarily with social engineering, despite the purported coverage of other topics. It would therefore be valuable reading material around corporate lunchrooms, since forewarned is just a little bit more

paranoid and, therefore, forearmed. As those involved with data security in the real world well know, cracking is basically a con job. Thus, The Knightmare, if he really is "super", is a con artist par excellence--and is pulling off a really great con here!

Revealing the secrets of social engineering poses very little threat to security. Con men already exist and will continue to exist. Cracker wannabes are unlikely to be able to carry off a successful con if they need to rely on canned advice like this. On the other hand, it is much more likely to shock naive and non-technical users into an awareness of the need for suspicion and proper procedures--albeit possibly only temporarily. Thus, this information is almost inherently of more use in data protection than in data penetration.

As for technical help for the cracker; well, are you really expecting great technical revelations from someone who knows there is a difference between baud and bits per second--and gets it backwards? Or, who thinks 140 and 19,900 baud are standard modem speeds? Who thinks Robert Morris' worm found "original" bugs? (And who doesn't know the difference between "downgrade" and "denigrate"?) All the successful hacks in the book rely on social engineering rather than technology. Lots of jargon is thrown in along the lines of, "You need X," but without saying what X really is, where to get it, or how to use it.

The official definition of a hacker in the book is of the "good side" seeker after knowledge. As it is stated early on, a hacker *could* do lots of mischief--but doesn't. In the course of the text, though, the image is much more convoluted. The book almost seems to be written by two people; one who is within the culture and has the standard confused cracker viewpoint, and another, sardonically aware of pulling the wool over all the wannabes' eyes. The chapter on contacting the *true* hacker community is EST-like in its refusal to define when you might have made it, or how.

Like I said, buy it for the corporate or institutional lunchroom. Make sure that the non-techies get first crack at it. If you'll pardon the expression.

copyright Robert M. Slade, 1994 BKSCSUHK.RVW 940609

=====

DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733  
DECUS Symposium '95, Toronto, ON, February 13-17, 1995, contact: rulag@decus.ca

---

## International Cryptography Institute

*Dorothy Denning <denning@chair.cosc.georgetown.edu>*  
*Tue, 16 Aug 94 17:26:10 EDT*

International Cryptography Institute 1994: Global Challenges

September 22-23, 1994  
Ritz Carlton, Washington, DC

Presented by  
The National Intellectual Property Law Institute

The International Cryptography Institute will focus on problems and challenges associated with the use of cryptography within nations and for international communications. The Institute will address such questions as: What are the different national policies and regulations governing cryptography and how might these evolve? What cryptographic technologies are on the market in different countries, what is being used, and what is it being used for? What problems is cryptography causing law enforcement? What are the requirements of businesses and other organizations? What are the new trends in cryptography and what will be their impact on society? What efforts are leading toward an international cryptography framework? The Institute is for government officials, industry leaders, policy makers and analysts, researchers, and users of cryptographic technologies.

#### Program

September 22

8:45-9:00 Opening Remarks

Dorothy E. Denning, Chair of Program

James Chandler, President, National Intellectual Property Law Institute

9:00-9:30

The Challenges of International Cryptography

Edward J. O'Malley, The OSO Group

9:30-10:00

Cryptography in the European Community

Christopher E. Sundt, ICL Secure Systems

10:00-10:30

Cryptography in the German Governmental Area

Ansgar Heuser, BSI

10:30-10:45 Break

10:45-11:15

Cryptography in Belgium

Els Lemmens, Belgian Office for Scientific, Technical and Cultural Affairs

11:15-11:45

The Use of Cryptography in Singapore

Kwok-Yan Lam, National University of Singapore

Seow-Hiong Goh, John Yong, National Computer Board

11:45-12:15

An Australian and South-East Asian View of Cryptography

William J. Caelli, Queensland University of Technology

12:15-1:45 Lunch with Keynote TBA

1:45-2:15

GSM: Security for World-Wide Mobil Radio

Charles B. Brookston, British Telecomm

2:15-2:45

International Exchange of Digital Signatures in a Diversified World

Jean-Jacques Quisquater, University of Louvain

2:45-3:15

Creating Global Cryptographic Infrastructures

Sead Muftic, Stockholm University

3:15-3:30 Break

3:30-4:00

An International Cryptography Framework

Keith S. Klemba and Jim Schindler, Hewlett-Packard Co.

4:00-4:30

Experiments in International Cryptography and Software Key Escrow

Stephen T. Walker, Trusted Information Systems, Inc.

4:30-5:00

International Escrowed Encryption

Dorothy E. Denning, Georgetown University

John Droge, Mykotronx, Inc.

5:00-6:00 Reception

September 23

9:00-9:30

U.S. Government Cryptography Policy

Michael R. Nelson, Office of Science and Technology Policy

9:30-10:00

Domestic Regulation of the Exportation of Cryptography

James Chandler, National Intellectual Property Law Institute

10:00-10:30

Sue E. Eckert, U.S. Department of Commerce

10:30-10:45 Break

10:45-11:30

Rose Biancaniello, U.S. Department of State (invited)

11:30-12:00

World-Wide Availability of Cryptography Products

David Balenson, Trusted Information Systems, Inc.

12:00-1:30 Lunch with Keynote

Louis J. Freeh, Director, Federal Bureau of Investigation

1:30-2:45

International Regulation of Cryptography

James Chandler, National Intellectual Property Law Institute

Alexander Patijn, Ministry of Justice, The Netherlands

William Wolfowicz, Fondazione Ugo Bordoni

2:45-3:00 Break

3:00-4:00

Cryptography in the Financial Industry

Mr. Mitsuru Iwamura, The Bank of Japan

Dr. Victor Panchenko, SignalRox, Russia (invited)

others TBA

[Hotel and Registration info deleted. Ritz Carlton has a SPECIAL CONF RATE of only \$225 per night! Tuition is \$595. E-mail Dorothy for 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 16: Issue 35

Thursday 25 August 1994

## Contents

- [Fraud and Identity](#)  
[Mich Kabay](#)
- [Summary of Der Spiegel interview with Airbus' Bernard Ziegler](#)  
[Peter Ladkin](#)
- [CORRECTION, Report on the \\*1993\\* Gatwick near-miss](#)  
[PGN](#)
- [Re: pi = 3](#)  
[James Dudley](#)  
[L. P. Levine](#)
- [Re: The new Cray and Unix passwords...](#)  
[Chris Ransom](#)

---

## Fraud and Identity

"*Mich Kabay [NCSA Sys\_Op]*" <75300.3232@compuserve.com>  
20 Aug 94 17:13:41 EDT

According to the U.K. Press Association newswire (94.08.10), the final culprit has been jailed for defrauding the British social security administration of a small fortune:

### LAWYER'S DAUGHTER JAILED FOR BENEFITS FRAUD

By Melvyn Howe, PA News

'The daughter of a wealthy and respected lawyer was jailed for three and a half years today for her part in a massive countrywide social security fraud.

Public school educated Olu Atobatele, regarded as a "pariah" by her "shamed" family, took a leading role in a highly sophisticated operation which involved 2,000 false identities and was the largest benefits conspiracy of its kind in Britain.'

Key points from the article:

- o Part of a gang of 11 who defrauded the Crown of 1 million pounds.
- o She herself stole 90,000 pounds in 20 months.
- o The gang members used "details of students' identities" and fabricated identities using information "from the Death Register at St Katherine's House, as well as identities from the British and African edition of Who's Who to make more than 240 bogus claims for income support between early 1992 and August last year."
- o The Department of Social Security "has instituted new procedures" to reduce fraud as a result of this scam.

[Comments from MK:

Please skip on to the next message if you're not in the mood for a leisurely stroll through some speculation. I got to thinking about this case of a Saturday afternoon and wrote down this little essay on identity in the real world and in cyberspace.

Impersonation is one of the techniques used by criminals, including criminal hackers, to acquire goods and services belonging to or due to others. Many people will be familiar with the techniques of "social engineering" (properly called "lying, cheating and extorting") used by criminal hackers to obtain information need in penetrating restricted systems. Such techniques include impersonating journalists, technicians and high-ranking personnel. High-resolution colour scanners, photocopiers, printers and image-processing software, have been turned to evil effect by high-tech forgers of currency and of authenticating documents.

In the case above, criminals were able to bamboozle human beings into entering false information into computerized systems--a kind of data diddling at one remove.

Disproportionate public outrage over much-publicized social services fraud by immigrants is pushing many jurisdictions towards insisting on biometric pattern recognition (e.g., fingerprints) to authenticate claims on social entitlements. Such a system would preclude inventing identities to be claimed by the same human being, since the "different" people would all have the same fingerprints.

However, biometric systems do not solve the fundamental problem: the difficulty of authentication of identity in today's world of fragmented communities and highly mobile individuals. Consider the true story underlying the film "Le Retour de Martin Guerre" (severely distorted in the US remake called "Sommersby"). A young man in mid-Renaissance France is forced to marry an even younger woman against their wishes because of family pressures. After seven years of unconsummated marriage, he runs away, only to reappear many years later. With his detailed knowledge of everything he ought to know as Martin Guerre, he is re-integrated into his village despite oddities like the wrong shoe size and hostility from his own dog. Even his wife welcomes him back to the conjugal bed. However, envious relatives eventually challenged him as an imposter. The real Martin Guerre reappears and the imposter is hanged.

This story has been part of French history for centuries precisely because successful imposture was so unusual in agrarian Europe. Most people never travelled more than a day's journey from their place of birth in their entire lives. They married the people they had known all their lives; they were no more likely to take on other identities than to learn to read.

Now contrast today's world: there would be nothing unusual about being born in Tucson, growing up in San Francisco, going to college in Boston, taking the first job in Chicago, moving to Denver, and ending up in Syracuse with a spouse from Edmonton. In such a society it's a wonder that there aren't \_more\_ impersonations--and who knows, maybe there are lots but they're real successful <g>.

Benjamin Wright, author of The Law of Electronic Commerce and instructor in the National Computer Security Association's online seminar on EDI Security has often commented that we seem to demand more of identity in cyberspace than we do in reality. Suppose Able Baker carries on a discussion with Charlie Delta; does it matter to either "who" the other is in another context? What would matter is for an imposter to pretend to be Able or Charlie and interfere in their communication by inserting fraudulent messages or intercepting legitimate messages.

Real-world authentication fails because of reliance on paper documents which are just too easy to falsify; perhaps computer-based authentication could reduce such fraud. Despite relatively poor reliability for any one biometric technique, the error rates for combinations are very low. Combining any two of, say, fingerprints, retinal scans and signature dynamics, for example, would provide trustworthy authentication. The question will be cost-effectiveness; would the enormous expense of installing huge numbers of biometric input devices and the network and database infrastructure be seen as justified? And would the costs of protecting the "cyberspace shadow" (as some writers are calling it) against tampering exceed the reduction in fraud?

The remaining difficulty is the bridge between social identity and identity in cyberspace. How does one ensure that the person registering as Echo Foxtrot really is Echo Foxtrot in other aspects of his life? And how much do we care? Enough to implant a non-forgable device in the person's body at birth or upon receiving legal immigration status? Yuk! Sounds like the basis for a police state, doesn't it?

I predict that under the increasing pressures of immigration (legal and illegal), increasing economic disparities, and continuing entitlement programs, the occurrence of impersonation will increase. At some point, fingerprinting will become mandatory for all claims on the social welfare systems; eventually, pressures will mount for authentication even in the initial claims for entitlements. At that point, societies will turn to mechanisms of authentication familiar to computer system users. Will the time come when microprocessors will be implanted under people's skin to transfer their cryptographically-sound identifiers on demand? And what will the consequences of such institutionalized scepticism be on social relations? Will people meeting in person for the first time press their wrists together to exchange public keys? Will those who refuse to participate in rituals of

authentication be frowned upon? And will such tokens become valuable commodities--valuable enough to steal and trade in the underworld? Sounds like the subject for an interesting science fiction novel.]

M.E.Kabay/DirEd/Natl Computer Security Assn (Carlisle, PA)

---

## Summary of Der Spiegel interview with Bernard Ziegler, Airbus Ind.

*Peter Ladkin <Peter.Ladkin@loria.fr>*

*Sat, 20 Aug 1994 21:32:45 +0200*

The German newsweekly Der Spiegel, issue 33 (1994) dated 15 Aug 94, contains an interview with Bernard Ziegler, described as Technical Director of Airbus Industrie, responsible for flight test and certification ('Zulassung') of all Airbus aircraft. There is a short background statement concerning the accidents on pp160-161, and the interview is on pp161-164.

The interview focuses on the reliability of Airbus aircraft, in the light of the following crashes: Bangalore, Feb 90 (A320: landed short of the runway in clear weather, 92 dead); Strasbourg, Jan 92 (A320 descended into a hill in clouds on a backcourse approach to the airport, 87 dead); Warsaw, Sep 93 (A320, landing in a thunderstorm, overran the runway, 2 dead, many injured); Nagoya, Apr 94 (A300, copilot and autopilot in control conflict, eventually nose rose at an extreme angle and the plane stalled, crashing tail first onto the ground, 246 dead); Toulouse-Blagnac Jun 94 (A330, testing engine-out go-arounds, stalled and crashed, 7 dead including the Airbus chief test pilot). The Habsheim A320 accident is not mentioned. The header to the intro says:

"Airbus Industrie is under pressure. Twelve total-losses since 1987 with 815 dead have awakened doubts about the concept of airplanes dependent on electronics ['elektronisch hochgeruesteten Flugzeuge']. Do technical failures contribute to the series of accidents? Or are pilots overextended by the 'flying computers'?"

Here is a summary of what I surmise are the salient parts of the interview for RISKS readers.

[begin summary]

Ziegler says they've had a lot of bad luck recently, contrasted with the first 14 accident-free years (except for the Iranian Airbus shot down by the US Navy). But he suggests comparing the record of the A320 with that of the B727, B737 or DC9 when they were introduced. He says that Airbus is 30 per cent better than the average of all builders - but he wants to be 100 per cent better. He says there's no reason to change the Airbus 'philosophy' of taking over some of the pilot's tasks by computer, pointing out that all of the new technology developed by Airbus, from 'glass cockpit' to new types of autopilot, has been followed by 'all the others'. And, '[..] the pilot still has the last decision. Whoever suggests the contrary doesn't know what they're talking about.'

They discuss the problems in Warsaw concerning the late deployment of airbrakes and thrust reverse, concerning which he points out that (a) it's a requirement for all modern airplanes that deployment is not enabled until the plane is firmly on the ground; and (b) there are particular limits on landing, for example not when a tailwind is stronger than 10 knots, or when the landing speed is too high. In Warsaw, these boundaries, which were carefully ascertained in test flights, were crossed. Also, runway overrun is one of the 'classical' airplane accidents, regardless of type. When asked why the Polish investigators singled out late deployment of airbrakes and reversers, he noted that the report also misses important details, including the problem with the false weather information given to the pilots, and notes that many of the Polish recommendations contradict various requirements of the air transport supervisory authorities. He said that the level of the compression sensors on the landing gear, and the landing logic, has been changed for Lufthansa at the request of the client, but that only an expert can tell the difference between the old and the new landing logic.

There follows a discussion about computers vs other kinds of flight control, during which he says that there is in principle no difference between more traditional methods of control and the fly-by-wire of the A320, and that it's an illusion to believe that there's ever a direct connection between the pilot's hand and the behavior of an airplane - flying is in this sense something artificial.

He says that there are always ways to improve airplanes, and they remain in close contact with the clients to make such improvements.

He is asked about the involvement of the autopilot in Nagoya, and about a prima facie similar problem with an autopilot in 1991 in Moscow (an A310), and why Airbus had not modified all the autopilots of these types. He replies that requiring expensive modifications is not a simple matter, and must first be thoroughly investigated to see if they cause more problems than they solve [not his phrase - I am paraphrasing. pbl]. He notes that Boeing has waited twelve years before recommending modifications in one case. He says that in conjunction with the certification authorities, Airbus had developed an autopilot modification and recommended that A300-600 clients perform it, and after the Moscow incident had notified everyone officially of the correct use of the autopilot [there are standard procedures for doing these things - he's pointing out that the standard procedures for clarification of operating procedure were vigorously pursued. pbl] After the Nagoya accident, Airbus decided that the modifications they had recommended to A300-600 and A310 aircraft should be mandatory. It will take about 2 years and \$60m to alter the fleet.

When asked about the 'spectacular crashes' in India, he rejects the categorisation and points out the statistics for India show that it's a difficult environment for airlines, and that the A320 crash happened right after two B737 crashes. There's then some discussion of pilot training and capabilities.

Concerning the A330 test flight crash in Toulouse, he points out that it was a difficult but not dangerous test, and in response to a question concerning entering the right autopilot 'flight level', he points out that it was mistakenly left at 2000ft but should have been at 7000ft according to the

checklist. He says that the fundamental error was that the crew let the nose-high, low-speed situation persist too long, and speculates why: because they took the nose-high situation for an anomaly and they wanted to see what would develop [according to the preliminary report, it was pilot commanded. They were confused as to which mode the flight control was in. pbl]; because the test engineer trusted the pilot to know when to return to normal; and Nick Warner [the chief test pilot of Airbus, one of the two pilots. pbl] had been criticised before by test engineers for retaking control too quickly, and maybe was sensitive to potential criticism in this case also. It was a question just of two seconds delay.

The consequences, he says, will be that automatic protection will be developed that will rule out such extremely unlikely accidents, and that the A330 and A340 will be the first aircraft to be protected automatically against the development of such a flight condition ('entsprechend ueberzogenen Flugzustand').

[end summary]

A few comments -

Warsaw: Ziegler correctly points out regulations concerning thrust reverse and airbrakes. However, no mention was made by the interviewer or Ziegler of the wheel brakes themselves. The wheels did not spin up on landing to the required speed to allow the anti-skid system to function as designed. Ziegler's selection of the tailwind for commentary raises some hypothetical considerations. At the given landing speed, with the tail wind, the wings were developing less lift than they would have been without the tail wind, making it more likely that the braking functions would have been enabled by the sensors. On the other hand, had there been no tailwind, the pilots would have landed at the same indicated airspeed, which would have given them 10 kts slower ground speed, but the same amount of lift preventing the sensors from indicating ground contact. For similar problems not to have occurred in this situation, the wheels would have not to have aquaplaned at this slower landing speed. But in the accident situation, they did not appear to spin up to speed until the ground speed was well below this, and much more of the airplane weight was on the wheels.

It's a simple consequence of the landing logic that braking systems did not deploy under the landing condition in Warsaw, as may be seen from an inspection of the description of the logic in the Flight Crew Operating Manual. The sensor settings and landing logic has apparently been changed sufficiently so that A320s landing in similar conditions, in a similar manner to the accident airplane, will not suffer a lengthy delay in activation of braking systems (brakes, airbrakes, thrust reversers). The logic is written in the Flight Crew Operating Manual which your local A320 pilot might be happy to show you.

Bangalore: it appears the pilots were confused as to which control mode the airplane was in. Under the particular conditions of flight, the engines went to flight-idle and the airplane descended rapidly into the ground while the pilots were trying to figure out what was going on.

Nagoya: The autopilot appears to have been engaged and in 'go-around' mode ('abort landing, gain altitude quickly'). The copilot, who was flying, was pushing hard forward on the control column trying to land the airplane. The autopilot was counteracting this by configuring the airplane aerodynamically for full nose-up (this 'trim' feature is a standard control in all airplanes). When the copilot eventually let go of the column, the airplane's nose rapidly rotated upwards to an extremely high angle (given the trim condition, this is what one would expect) and the speed decayed severely, causing the aircraft to stall nose-high, close to the ground. It hit the ground tail-first. The standard procedure in which pilots are trained (on this and all other transport airplanes) is to disconnect the autopilot and ensure it is disconnected if they want to hand-fly the plane onto the runway. There are numerous puzzles concerning this accident.

Toulouse: Under the correct checklist settings, the pitch (nose-upward angle) of the aircraft on takeoff would have been automatically controlled when the autopilot was engaged. The co-pilot who was flying rotated on take-off to a high angle. Meanwhile, Warner engaged the autopilot (which took three tries) and 'failed' the left engine. It's surmised they were expecting the autopilot to return the aircraft to a precise pitch as it handled the situation, as planned. The aircraft was flying in a different control regime than planned due to the mistaken altitude-capture setting of 2000ft rather than 7000ft on the autopilot. Pitch was not 'protected' by the autopilot in this regime. Speed decayed rapidly since the nose did not go down, the aircraft was unable to maintain lateral control when it was below the airspeed required to do so, and yawed and rolled. After this situation had developed, Warner throttled back the right engine to regain lateral control, as well as regaining wings-level and nose-level. When control was regained, the ground was just a little too close. There are a couple of important reports on this accident in Flight International for 10-16 Aug and 17-23 Aug.

The Strasbourg crash was reported in [RISKS-13.06](#), with follow-ups in numerous immediately following RISKS-13 numbers. The official verdict was reported in [RISKS-14.74](#), with follow-ups in 14.76 and 14.77. Warsaw, Nagoya and Toulouse accidents have been discussed in [RISKS-15.13](#), 15.30, 15.31, 15.32, 15.36, 16.07, 16.13, 16.14, 16.15, 16.16, 16.22 and 16.23. For a survey of these accidents (except for the A330), see RISKS contributor Peter Mellor's paper: 'CAD: Computer-Aided Disaster'.

Additional comments on Airbus aircraft may also be found in RISKS-13 numbers 06,07,08,09,11,12,16,19,20,21,22,23,24,27,64,67; and RISKS-14 numbers 01,07,74,76,77.

Peter Ladkin

---

### **CORRECTION, Report on the 1993 Gatwick near-miss (Ladkin, [RISKS-16.34](#))**

*"Peter G. Neumann" <neumann@csl.sri.com>  
Thu, 25 Aug 94 10:23:10 PDT*

I must apologize for an overzealous attempt to correct what appeared to be an error. Peter Ladkin's message explicitly referred to the \*1993\* Gatwick

near-miss. I was reading some out-of-band communications in which there had been a date error that made it appear that the \*1993\* was incorrect, so I miscorrected it miscorrectly. Sorry. Mea culpa. PGN

---

**pi = 3 (Re: Wayner, [RISKS-16.34](#))**

*James Dudley <james@cssnps.com>*

*Wed, 24 Aug 94 20:52:40 EST*

Actually, my home state of Indiana did try to legislate that the value of pi should be 3. Here is some information from the alt.folklore.urban archives from an article written by Mark Bader (msb@sq.com) (Further information can be found in "Mathematical Cranks", Underwood Dudley, The Mathematical Association of America, Washington D.C.). James Dudley

THE STORY

The author of the bill was Dr. Edwin J. Goodwin, an M.D., of Solitude, Indiana. It seems that he was a crank mathematician. He contacted his Representative, one Taylor I. Record, with his epoch-making suggestion: if the State would pass an Act recognizing his discovery, he would allow all Indiana textbooks to use it without paying him a royalty.

Nobody in the Indiana Legislature knew enough mathematics to know that the "discovery" was nonsense. In due course the bill had its third House reading, and passed 67-0. At this point the text of the bill was published "and, of course, became the target for ridicule", "in this and other states".

By this time a real mathematician, Prof. C. A. Waldo, had learned what was going on. In fact, he was present when the bill was read on February 5, 1897. ("...imagine [the author's] surprise when he discovered that he was in the midst of a debate upon a piece of mathematical legislation. An ex-teacher was saying ... 'The case is perfectly simple. If we pass this bill which establishes a new and correct value for Pi, the author offers ... its free publication in our school text books, while everyone else must pay him a royalty'", Waldo wrote in a 1916 article.) But the House had passed the bill.

Fortunately, Indiana has a bicameral legislature. The bill came up for first reading in the Senate on Thursday, February 11. Apparently in fun, they referred it to the Committee on Temperance. The Committee reported back on Friday, February 12, approving the bill, which then had its second reading.

The Indianapolis Journal reported what happened: "The Senators made bad puns about it, ridiculed it, and laughed over it. The fun lasted half an hour. Senator Hubbell said that it was not meet for the Senate, which was costing the State \$250 a day [!], to waste its time in such frivolity ... He moved the indefinite postponement of the bill, and the motion carried. ... All of the senators who spoke on the bill admitted that they were ignorant of the merits of the proposition. [In the end,] it was simply regarded as not being a subject for legislation."

## ANNOTATED TEXT OF THE BILL

/\* Following is the text of Indiana House Bill #246 of 1897, with my  
\* own annotations (in comment signs and exdented, like this text).  
\* In my annotations, A, r, d, c, and s are respectively the circle's  
\* area, radius, diameter, circumference, and the side of the inscribed  
\* square. \*/

A bill for an act introducing a new mathematical truth and offered as a contribution to education to be used only by the State of Indiana free of cost by paying any royalties whatever on the same, provided it is accepted and adopted by the official action of the legislature of 1897.

/\* You normally have to pay royalties on mathematical truths?  
\* The Pythagoras estate must be doing well by now... \*/

### SECTION 1.

Be it enacted by the General Assembly of the State of Indiana: It has been found that a circular area is to the square on a line equal to the quadrant of the circumference, as the area of an equilateral rectangle is to the square on one side.

/\* The part after the last comma is a remarkable way of saying  
\* "as 1 is to 1". In other words, this says  $A = (c/4)^2$ , which  
\* is the same as  $A = (\pi*r/2)^2 = (\pi^2/4)*r^2$  instead of the  
\* actual  $A = \pi*r^2$ . \*/

The diameter employed as the linear unit according to the present rule in computing the circle's area is entirely wrong, as it represents the circle's area one and one-fifth times the area of a square whose perimeter is equal to the circumference of the circle.

/\* The formula  $A = \pi*r^2$  is interpreted as  $A = d*(c/4)$ , which is correct.  
\* The author claims that the d factor should be  $c/4$ , so the ratio of  
\* the area by the author's formula to the area by the real formula  
\* is  $c/(4*d)$ , that is,  $\pi/4$ . Since he believes  $\pi = 3.2$ , this ratio  
\* is  $3.2/4$ , which is  $4/5$ . Therefore the area by the author's rule  
\* is  $1/5$  smaller than the actual area. Now he apparently thinks that  
\* the reciprocal of  $1-1/5$  is  $1+1/5$ , and thus that the other area is  
\*  $1/5$  larger than his area, which of course would actually require  
\* the ratio to be  $5/6$ . \*/

This is because one-fifth of the diameter fails to be represented four times in the circle's circumference.

/\* In other words,  $c = (1-1/5) * (4*d)$ ; consistent with  $\pi = 3.2$ . \*/

For example: if we multiply the perimeter of a square by one-fourth of any line one-fifth greater than one side, we can in like manner make the square's area to appear one fifth greater than the fact, as is done by taking the diameter for the linear unit instead of the quadrant of the circle's circumference.

/\* He says that if we consider the area of a square of side x to be  
 \*  $(4*x)*(x/4)$  and we replace the second x by  $(1+1/5)*x$ , we get an  
 \* area 1/5 too large, and this is analogous to using d in place of  
 \*  $c/4$  with the circle. \*/

## SECTION 2.

It is impossible to compute the area of a circle on the diameter as the linear unit without trespassing upon the area outside the circle to the extent of including one-fifth more area than is contained within the circle's circumference, because the square on the diameter produces the side of a square which equals nine when the arc of ninety degrees equals eight.

/\* I can only assume that "nine" is a mistake for "ten". See also  
 \* the annotation after the next one. \*/

By taking the quadrant of the circle's circumference for the linear unit, we fulfill the requirements of both quadrature and rectification of the circle's circumference.

/\* Getting repetitive here... \*/

Furthermore, it has revealed the ratio of the chord and arc of ninety degrees, which is as seven to eight, and also the ratio of the diagonal and one side of a square which is as ten to seven, disclosing the fourth important fact, that the ratio of the diameter and circumference is as five-fourths to four; and because of these facts and the further fact that the rule in present use fails to work both ways mathematically, it should be discarded as wholly wanting and misleading in its practical applications.

/\* The meat of the bill. He says that  $s/(c/4) = 7/8$ , and  $d/s = 10/7$ ,  
 \* therefore  $d/c = (10/7)*(7/8)/4$ , which he reduces only as far as  
 \*  $(5/4)/4$ . Of course this is  $5/16$ , and gives  $\pi = c/d = 16/5 = 3.2$ .  
 \* It also implies that the square root of 2 is  $10/7$ . \*/

## SECTION 3.

In further proof of the value of the author's proposed contribution to education, and offered as a gift

to the State of Indiana, is the fact of his solutions of the trisection of the angle, duplication of the cube and quadrature of the circle having been already accepted as contributions to science by the American Mathematical Monthly, the leading exponent of mathematical thought in this country.

/\* When I first posted this I assumed that the A.M.M. must have had a  
\* policy of politely acknowledging crankish submissions, but apparently  
\* at one time they simply printed whatever they were sent. I haven't  
\* checked this out. \*/

And be it remembered that these noted problems had been long since given up by scientific bodies as unsolvable mysteries and above man's ability to comprehend.

/\* "Given up" is not the same as "proved insoluble"! \*/

[Also noted by

pcw@access.digex.net (Peter Wayner),  
"Tom Zmudzinski" <zmudzint@cc.ims.disa.mil>, who suggests using 355/113,  
mhaynes@bgsu.edu (Michael F. Haynes),  
clark@cpd125.cpd.ford.com (Andrew Clark),  
nhy@panix.com (Nina H. Yuan),  
George Jansen <gjansen@seas.gwu.edu>,  
dalamb@qucis.queensu.ca (David Lamb), and  
cc32859@vantage.fmrco.com (Donald Sharp), who wonders  
``how many other technically flawed ideas have actually been codified  
into law because not enough people in the legislature understood  
flaw? And what is the risk involved in trying to implement laws that  
contradict the fundamental truths of nature?''.

(However, two of those remembered the state incorrectly.) I am delighted to have this urban nonlegend put to rest. Thanks. PGN]

---

### PI = 3

*"Prof. L. P. Levine" <levine@blatz.cs.uwm.edu>  
Thu, 25 Aug 1994 06:56:54 -0500 (CDT)*

There are two biblical verses that show PI to have a value of three. They seem to be the same information repeated, but from the King James version as reported in the Library of the Future CDROM, which seems to be filled with texts from the past:

Kings-1 verse 7:23 And he made a molten sea, ten cubits from the one brim to the other: [it was] round all about, and his height [was] five cubits and a line of thirty cubits did compass it round about.

Chronicles-2 verse 4:2 Also he made a molten sea of ten cubits from brim to brim, round in compass, and five cubits the height thereof; and a line of thirty cubits did compass it round about.

Leonard P. Levine, Professor, Computer Science, Univ. of Wisconsin-Milwaukee  
Box 784, Milwaukee, WI 53201 levine@cs.uwm.edu 1-414-229-5170

---

## Re: The new Cray and Unix passwords...

"Chris Ransom" <chris@quests.com>

Thu, 25 Aug 94 09:45:13 PDT

Mr. Wayner neglects to consider the "salt" values used to hash the passwords which prevent this type of attack. All 1000 passwords would likely require independent encryption with unique salt values.

Chris Ransom chris@quests.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 16: Issue 36

Monday 29 August 1994

## Contents

- [Vandals Cut Cable, Slow MCI Service](#)  
[Mich Kabay](#)
- [Mexican election computers](#)  
[John Sullivan](#)
- [Attack of the killer spellcheckers...](#)  
[Valdis Kletnieks](#)
- [U.S. Mail causes ZIP-code problem](#)  
[Al Stangenberger](#)
- [Re: Bug in Microsoft Word](#)  
[Dave Moore](#)
- [Salt in wounds \(Re: New Cray and Unix Passwords...\)](#)  
[Peter Wayner](#)
- [Re: Fraud and Identity -- SCI-FI](#)  
[Andrew Marchant-Shapiro](#)
- [Politicians Join the Internet](#)  
[Mich Kabay](#)
- [Re: pi = 3](#)  
[Mark Stalzer](#)  
[Rob Boudrie](#)
- [System makes bank check forgery easy](#)  
[Christopher Klaus](#)
- [CFP: 2nd ACM Conference on Computer and Communications Security](#)  
[Li Gong](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Vandals Cut Cable, Slow MCI Service

"*Mich Kabay [NCSA Sys\_Op]*" <75300.3232@compuserve.com>  
28 Aug 94 13:12:43 EDT

>From the Washington Post newswire (94.08.27):

VANDALS CUT CABLE, SLOW MCI SERVICE

By Elizabeth Corcoran  
Washington Post Staff Writer

"Telephone calls between New York City and Washington on the MCI network encountered traffic jams yesterday afternoon after vandals removed a segment of cable in Newark. The problems began just before 2 p.m. and lasted until 5:45 p.m.

"MCI Communications Corp. spokesman Jim Collins said vandals 'neatly cut' out a 20-foot segment of fiber-optic cable that ran along a railroad overpass above a street in Newark. The cable, which was wrapped in a thin plastic casing, was not easy to reach."

The article continues with the following key points:

- o Repairs took about an hour after the break was located.
- o NJ residents, in particular, got many busy signals when alternative routes were saturated.
- o Brokers on the NASDAQ exchange, including Dow Jones, were affected.
- o Motives for the theft of 20 feet of fiber optic cable are unknown.

[Comments by MK: could this be a dry run for a class-3 (international) information warfare attack? "Let's see what happens when we deliberately interfere with one of the major carriers...."]

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn

---

## Mexican election computers

*<sullivan@geom.umn.edu>*

*Fri, 26 Aug 94 13:21:42 -0500*

RISKS readers will recall that six years ago, the Mexican ruling party PRI evidently stole the presidential election through tricks with the vote-counting computer.

Last month, the Economist had an article about preparations for the elections this year in Mexico. Their reporter interviewed a government official in charge of elections; when he asked about the computer irregularities six years ago, the interview was abruptly ended.

It seems that the elections this year were more open and fair than those six years ago. But there have been some questions raised again about the computer system. The IFE (Federal Electoral Institute) has delayed releasing the final vote totals. PRI representatives say the delay is because the PRD (opposition party) is demanding recounts of each ballot box. But, according to Reuters, PRD representatives to the IFE claim instead that the delays were "due to suspicious problems with the official computer system". The Reuters report continues to say that:

IFE officials denied Thursday there were any problems with the computer system but said an investigation was continuing into an apparent effort by unknown individuals to infiltrate a computer virus into the main electoral computer.

Interior Minister Jorge Carpizo said Wednesday that investigators had found some clues indicating who might have been responsible for the effort but did not say who they were or whether the effort was politically motivated or not.

John Sullivan sullivan@geom.umn.edu

---

## Attack of the killer spellcheckers...

*Valdis Kletnieks <valdis@black-ice.cc.vt.edu>  
26 Aug 1994 18:53:21 GMT*

Seen on page 2 of the New River Valley Current section of the Roanoke Times & World-News, Aug 24, 1994:

Corrections:

Because of an overzealous computer spellchecker, a number of names in a story on Radford University sports in the Welcome Students section appeared incorrectly and were not caught by a sports-ignorant editor.

Phil Leftwich is the former Highlander now in the pros. Chris Connolly plays ball in Wllmington, Del., not Laminating, Del., and there's no such place as Educator, Ga. -- Eric Parker is from Decatur. Chibi Johnson is not in the least bit Chubby, and Done Staley is legendary, not Don Stellae. Meanwhile, Paul Beckwith, who is no relation to Paul Backwash, departed for Cornell.

Because of a reporter's error, a story in Saturday's New River Current incorrectly reported a July 20 vote by the Montgomery County Planning Commission on a Price Mountain tower proposal. The vote only recommended the proposal for a public hearing. But by a 5-4 vote, the commission recommended approval of the tower Monday. The Board of Supervisors will consider it next month.

.....

The obvious first-order RISK is of course not keeping your spellchecker in line. However, the following should also be noted:

1) The correction contained the Wllmington with an upper-case 'l' - there's nothing like having a typo in an apology for an errant spellchecker.

2) The first 2 paragraphs have an unusual amount of levity - the third is reprinted as a sample of their usual correction style. One almost needs to wonder if in fact, the original error never happened, and that the retraction is itself a creation of an AI gone amuck... ;)

Valdis Kletnieks, Computer Systems Engineer

---

## U.S. Mail causes ZIP-code problem

Al Stangenberger <forags@nature.Berkeley.EDU>

Sat, 27 Aug 1994 13:37:23 -0700

Residents of Oak Avenue in San Rafael, CA, are victims of a burgeoning mail problem caused when their street was "inadvertently" deleted from the Postal Service's national ZIP code database. San Rafael has several ZIP codes for various areas; two of these (94901 and 94904) have Oak Avenues with similar street numbers. Somehow the Oak Avenue in 94901 was deleted from the master database of streets, and this deletion was propagated to all commercial mailers in the USA who subscribe to the Post Office's ZIP code update service. The result of the deletion was that commercial mail programs automatically changed all Oak Avenue addresses in code 94901 to the Oak Avenue in 94904. The resulting flood of misdirected mail has caused the usual problems associated with missing bills, mortgage statements, etc. Further, any ZIP code changes back to 94901 requested when residents discovered this error were automatically "corrected" back to 94904 by the programs which relied on the Post Office's bad data. This situation will persist until the next revision tapes for the national ZIP database are distributed.

The article I saw (Marin Independent-Journal, 12 August 1994) did not explain how a record was "inadvertently" deleted from the national database. I checked a printed ZIP code directory for San Rafael, and saw at least four other pairs of streets which could also have fallen victim to the problem. Fortunately, they did not.

Until the problem is fixed, Oak Avenue mail is being manually sorted.

Al Stangenberger Univ. of Calif Berkeley Dept. of Env. Sci., Policy, & Mgt.  
forags@nature.berkeley.edu

---

## Re: Bug in Microsoft Word

Dave Moore <davem@garnet.spawar.navy.mil>

Thu, 25 Aug 1994 14:20:37 -0400 (EDT)

<>Word has a summary info area, for each document, that cannot be turned off.

I wasn't aware of this specifically, but there is a much more substantial but similar feature that I encountered in version 4.x & 5.x of Word for the Mac. I suspect that it exists in the PC versions as well but have not checked. Fortunately, it's easy to test it yourself. Just create a Word file. Save it with "Fast Save". Re-open the file, delete something and save again with fast-save. Now use any external file viewer and look for your deleted text.

The following is an internal memo I sent out a couple of years ago:

-----

Do you send WORD files via e-mail ? If so, be aware that you may be accidentally sending out your underwear along with your intended message.

<Dramatic pause for puzzlement and underwear checking>

The default configuration in WORD for file saving is "Fast Save". The way this works is it only saves a list of edits and appends them to the existing file. When this file is opened, only the end result is displayed. However when you send this file via e-mail, the entire file is sent.

So what does this mean ? It means that if you use Word to delete stuff that you change or that you don't intend to send or be seen; the supposedly deleted stuff may still be present in the file. The recipient of that file may be able to recover some or all of the deleted information.

Under ordinary usage, this is not a problem. Recovery of deleted text by the recipient requires some specific knowledge and time. For obvious reasons, I won't explain the method.

If you have some specific reason to be sure that no deleted text can be recovered, turn off Fast Save prior to saving for transmittal. Otherwise, your underwear may be visible.

-----

Actually recovery is not difficult at all, but the above was intended for a non-technical audience.

---

### **Salt in wounds (Followup to new Cray and Unix Passwords...)**

*Peter Wayner <pcw@access.digex.net>*

*Fri, 26 Aug 1994 09:54:31 -0400*

One should be careful pushing the envelope while calculating on the back of it. I made one misstep in my piece in [RISKS-16.34](#) when I stated that 1000 passwords could be attacked as easily as one. I neglected to take account of the Salt, which is a neat part of the UNIX password system that effectively increases the size of the password space by a factor of 1024.

If you are attacking one password, then the time limits from the earlier piece still hold if you're able to guess the salt ahead of time. This may not be possible and it certainly isn't possible if you're trying to use the "neat" trick of compare 1000 passwords in one swell FLOP.

There are additional weaknesses that should be pointed out. If people only use lower-case characters and numbers, then the size of the key space is even smaller. This is only  $36^8$  possible choices which is about 1/76th the size of the space made up of {A-Z,a-z,0-9}.

But who uses digits? Many don't. The number of 8 character passwords made up of just lower-case letters can be searched about 1026 times faster. That's

less than an hour given the rough estimates. This pretty close to the size of the salt so the two cancel each other out and the running times from the previous post would apply here. This emphasizes the need for using different cases, numbers and punctuation in the password.

When people use DES manually, they often just type in the key like a password. (Many of the automatic systems choose keys randomly from the entire key space.) If this is the case, then all of the estimates from the earlier piece in 16.34 also apply to this case without having to worry about the salt. Clearly, any new standard encryption algorithm should include a method for hashing a longer phrase down to a shorter key in such a way that the entire keyspace is covered.

Finally, some have asked about shadow password files, a common UNIX system hack that prevents ordinary users from access to the password file that used to be kept open for all to read. It is unclear how common these are, but this problem is really independent of the problem of attacking encrypted passwords. People can get at encrypted passwords by sniffing the network as well as a variety of other file system hacks. If the users could never get at encrypted passwords, we wouldn't need to encrypt the passwords anymore.

I should point out again that my estimates of about the Cray came from thin air. I have no direct knowledge of the exact architecture of the machine or many of the small and medium sized details that could impose factors of 2 or 4 on the results.

There are several other details. Although most focus their paranoia on the NSA, there are many others who might come to own such a machine. The Cray computer eventually emerging from this project should be available on the open market. It will undoubtedly have many uses in many arenas. The memory architecture may grow to be popular in desktop machines because it can be used to do ray tracing, CAD applications and many other computational projects. Other Cray innovations are now common on desktop machines. That may be well into the future, but concentrating on that is one way to keep from getting mired in the past.

---

### **Re: Fraud and Identity -- SCI-FI (Kabay, [RISKS-16.35](#))**

*"MARCHANT-SHAPIRO, ANDREW" <MARCHANA@gar.union.edu>  
25 Aug 94 14:58:00 EST*

MK writes:

>And will such tokens become valuable  
>commodities--valuable enough to steal and trade in the underworld? Sounds  
>like the subject for an interesting science fiction novel.]

I recall at least once SciFi story in which eyeballs are removed to trick retinal scanners (that is, you remove someone ELSE's eyeball, and hold it up to the scanner...not at all nice!).

Andrew Marchant-Shapiro, Depts of Sociology and Political Science, Union College, Schenectady NY 12308 (518) 388-6225 marchana@gar.union.edu

---

## Politicians Join the Internet

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
29 Aug 94 07:42:27 EDT*

The Washington Post newswire (94.08.29) reports on the growing use of Internet services by the US Congress and Senate:

"E-Mail Puts Congress At Voters' Fingertips; House, Senate Venturing Onto the Internet"

By Elizabeth Corcoran  
Washington Post Staff Writer

"When the House of Representatives was weighing an amendment to a bill on education earlier this year, constituents swamped Rep. Elizabeth Furse's office with questions and concerns.

"The Oregon Democrat took to the information highway: Along with conventional interviews, she posted soothing explanations on various computer bulletin boards. The uproar died down, and the bill passed."

The author makes the following key points:

- o Growing use of Internet access throughout the US government, including legislators, support staff, and government employees.
- o White House plans to put multimedia documents online by mid-September.
- o "...about 40 representatives and 30 senators have acquired Internet addresses; about that many more members and committees in both houses have requested access."
- o Enthusiasts praise the immediacy of the electronic communications channel.
- o Voters can obtain detailed information online about legislation.
- o Congressional staffers are working on security measures "to protect its paths onto the Internet from hackers bent on disrupting databases."
- o Remote voting by legislators is a possibility under discussion for the long term.

[Comments by MK:

### 1) Disproportionate weight

In social psychology, one of the observations about how people form judgements about issues ("social cognition") is that *\_salience\_* influences judgement. That is, the unusual, the exceptional, the striking--these factors insensibly lead us to overestimate their importance. In experimental work over many years, psychologists have found that anyone who is noticeably different in a

group picture is assumed unconsciously by observers to have special importance.

Until Internet access becomes more widespread, anyone sending E-mail to a Congresscritter is likely to be considered with greater interest than someone sending snailmail--simply because of the novelty.

## 2) Spoofs

Congresscritters naturally weigh public comments with an eye to voter preferences. If there 20,000 messages supporting a particular initiative and 500 opposing it, the recipient may be influenced in favour of the proposal.

And how will the congressional staff judge how many people sent the 20,000 messages if there is no authentication of the identity of the senders? Yes, fraudsters could go to the trouble of generating thousands of printed messages and mailing them from the appropriate district (so the postmark would fit). Mind you, it would be quite a job, what with using different fonts, margins and wording to simulate the contributions of individual voters.

What a contrast with E-mail! Without public key signatures, a computer program could generate thousands of E-mail messages using randomizers for the text and a list of fraudulent identifiers. Even with public keys, if the Bad Guys chose to certify thousands of their own pseudonyms, nobody could stop them--and it is unlikely that Congresscritters would know which keys had been certified by criminals.

## 3) Representative democracy

Each letter and phone call to a legislative office is assumed to represent the opinions of many others who have not taken the time to communicate with their representatives. The practice of allowing free mail to representatives is supposed to increase the availability of such communications.

What assumptions will legislators make about E-mail? And what will be the demographic attributes of E-mail senders? I think there's scope for some pretty intensive research here before anyone draws conclusions about the population sending political E-mail.

Legislators must analyze issues, not merely tally indices of popularity. And with electronic communications, they must be especially wary of taking the easy path of vote-counting. Some of those "voters" may be phantoms, and the rest may be very different from "normal" voters.

Many commentators have suggested that access to the Internet may widen the gap between the enfranchised intelligentsia and the disenfranchised masses. As E-mail links to legislators increase, it will be important to monitor the gap. If it becomes intolerable, that gap will have to be closed by widening access to the proposed National Information Infrastructure.]

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn

---

**Re: pi = 3 ([RISKS-16.34,35](#))**

<stalzer@macaw.hrl.hac.com>

Thu, 25 Aug 1994 12:49:39 +0800

It doesn't take a law to make pi = 3. On some old versions of Basic for PDP-11s, you could assign any value to the "constant" pi. The constant was contained in a shared run-time system (with write permission!), and changing it in one program changed it for all Basic programs (until the rts was reloaded).

Mark Stalzer, mas@acm.org

---

**More on Pi ([RISKS-16.34,35](#))**

Rob Boudrie <rboudrie@chpc.org>

Thu, 25 Aug 94 14:39:41 EDT

[The Indiana Pi-throwing] is covered in detail in Peter Beckmann's book "A History of Pi", in which he points out both the incomprehensibility of that Indiana law, as well as the difficulty in finding Pi=3 in it. That volume (available in paperback) is absolute must reading for all of those who at one time knew Pi to over 200 digits.

rob boudrie

[Also noted by Hal Lewis (hlewis@voodoo.physics.ucsb.edu):  
the book "has lots of other great stories about this remarkable  
number." PGN]

---

**system makes bank check forgery easy**

Christopher Klaus <cklaus@shadow.net>

Mon, 29 Aug 94 12:42:54 EDT

Here's an obvious risk that I am not sure exists for all banks but here's the deal:

I use to live in dorms and when I opened an account with a local bank, they sent 3 or 4 packets of checks. I put the extra packets in my desk. Unfortunately, my roommates were less than honest and forged a check for some pizza. I noticed 1 or 2 packets missing so I had the bank stop payment for all the packets of checks that were missing. More than 6 months later, after I moved, I grabbed a packet of checks, and wanted to verify these were good ones and not ones I had previously stopped payment on.

I called up the bank and the lady told me , if the checks had been stopped payment for more than 6 months, it is automatically purged from the system , and are good again. I asked her, 'If I stole a few packets of blank checks from someone, I could just wait 6 months for the stop payment to roll over in your system, and begin forging again?' And she said, 'Yea, but not a lot of people know that.' Well, gee, that makes me feel safer.

I am not sure if this is true for most banks, but I wouldn't be surprised if it were so.

Christopher William Klaus <cklaus@shadow.net> <iss@shadow.net>  
Internet Security Systems, Inc. Computer Security Consulting  
2209 Summit Place Drive, Penetration Analysis of Networks  
Atlanta,GA 30350-2430. (404)998-5871.

---

## **CFP: 2nd ACM Conference on Computer and Communications Security**

*Li Gong <gong@csl.sri.com>  
Thu, 25 Aug 94 12:18:21 -0700*

This is the first announcement of the upcoming ACM conference [RISKS-pruned]. You can access the full registration information online by E-mail to [acmccs2@isse.gmu.edu](mailto:acmccs2@isse.gmu.edu) or by www file <http://www.csl.sri.com/acm-ccs/ccs.html>

Call For Participation  
2nd ACM Conference on Computer and Communications Security  
Nov 2-4 1994, Fairfax, Virginia  
Sponsored by: ACM SIGSAC

Hosted by: Bell Atlantic and George Mason University

In cooperation and participation from  
International Association of Cryptologic Research  
IEEE Communication Society TC on Network Operations and Management  
IEEE Computer Society TC on Security and Privacy

### Conference Highlights

Building on last year's highly successful inaugural conference, we are pleased to invite your participation in this year's conference. The purpose of the conference is to bring together researchers and practitioners of computer and communications security. As evidenced by the program, the conference offers a unique blend of cryptography and security, theory and practice, with emphasis on the practical. The conference will be held in the Holiday Inn, Fair Oaks, in Fairfax, Virginia; minutes from the Nation's Capital. We welcome you to enjoy an informative and invigorating program, and Washington's pleasant mid-fall sight-seeing weather.

Advance Technical Program  
(Subject to Change)

November 2

8:45 - 9:00 Welcome, D. Denning and R. Pyle

9:00 - 10:30 Applications, R. Sandhu  
- Support for the File System Security Requirements of Computational  
E-Mail Systems, A. Prakash and T. Jaeger

- Secure Wireless LANs, V. Bhargavan
- The Design and Implementation of Tripwire: A File System Integrity Checker, G. Kim and E. Spafford

11:00 - 12:30 Emerging Areas, S. Lee

- Exchange of Patient Records: Prototype Implementation of a Security Attribute Service in X.500, M. Jurecic and H. Bunz
- A Process-Oriented Methodology for Assessing and Improving Software Trustworthiness, E. Amoroso, C. Taylor, J. Watson and J. Weiss
- Panel: To be announced

2:00 - 4:00 Key Escrow, C. Neuman

- Clipper Repair Kit - Towards Acceptable Key Escrow Systems, T. Beth, H. Knobloch, M. Otten, G. Simmons and P. Wichmann
- Protocol Failure in the Escrowed Encryption Standard, M. Blaze
- Panel: Corporate Key Escrow, R. Ganesan

4:30 - 6:00 Cryptography -1, J. Feigenbaum

- Secure Agreement Protocols: Reliable and Atomic Group Multicast in Rampart, M. Reiter
- Key Distribution via True Broadcasting, M. Just, E. Kranakis, D. Krizanc, P. Van Oorschot
- Conditionally Secure Secret Sharing Scheme with Disenrollment Capability, C. Charney and J. Pieprzyk
- Meta-ElGamal Signature Schemes, P. Horster, H. Petersen and M. Michels
- Anonymous Credit Cards, S. Low, N. Maxemchuk and S. Paul

November 3

9:00 -10:30 Database Security, Carl Landwehr

- An Efficient Multiversion Algorithm for Secure Servicing of Transaction Reads, P. Ammann and S. Jajodia
- A Temporal Authorization Model, E. Bertino, C. Bettini and P. Samarati
- Propagation of Authorizations in Distributed Database Systems, P. Samarati, P. Ammann and S. Jajodia

11:00 - 12:30 Cryptography-2, J. Stern

- Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis, H. Heys and S. Tavares
- Information Leakage of Boolean Functions and its Relationship to Other Cryptographic Criteria, M. Zhang, S. Tavares and L. Campbell
- Authentication Codes that are r-fold Secure Against Spoofing, R. Safavi-Naini

2:00 - 4:00 Electronic Commerce Security - R. Ganesan

- The Role of Licensing, Insurance and Endorsements in Evaluating Trust of Distributed System Services, C. Lai, G. Medvinsky and C. Neuman
- To be announced
- Panel: Security Issues in Electronic Commerce, C. Neuman

4:30 - 6:00 Cryptographic Protocols, P. Van Oorschot

- New Protocols for Third-Party-Based Authentication and Secure Broadcast, L. Gong
- How to Simultaneously Exchange Secrets by General Assumptions,

T. Okamoto and K. Ohta

- A Key Distribution Method for Object-Based Protection, W. Ford and M. Wiener

November 4

9:00 - 10:30 Cryptanalysis, L. Gong

- On the difficulty of factoring, A. Lenstra
- How to Break Gifford's Cipher, T. Cain and A. Sherman
- Parallel Collision Search with Application to Hash Functions and Discrete Logarithms, P. Van Oorschot and M. Wiener

11:00 - 12:30 Firewalls, S. Bellovin

- Application Access Control at Network Level, R. Molva and E. Rutsche
- Network Security Probe , P. Rolin, L. Toutain and S. Gombault
- Panel: Firewalls, S. Bellovin

2:00 - 3:00 Experience, R.Graveman

- Security Modelling for Organizations, A. Anderson, L. Kwok and D. Longley
- Mainstreaming Automated Information Systems Security Engineering, J. Coyne and N. Kluksdahl

3:30 - 5: 00 Multilevel Security, V. Gligor

- The Compatibility of Composable Policies, H. Hinton and S. Lee
- An Entropy Conservation Law for Testing the Completeness of Covert Channel Analysis, R. Browne
- Prerequisite Confidentiality, J. Nestor and S. Lee

General Chairs: Dorothy Denning (Georgetown University), Raymond Pyle (Bell Atlantic)

Program Chairs: Ravi Ganesan (Bell Atlantic), Ravi Sandhu (George Mason Univ.)

Treasurer and Local Arrangements: Richard Graveman (Bellcore)

Proceedings: Jacques Stern (ENS/DMI)

Publicity: Li Gong (SRI)

[Program Committee distinguished, but deleted for space, along with registration info. 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 16: Issue 37**

**Weds 31 August 1994**

## Contents

- [Risks of spread-spectrum cordless phones](#)  
[Don Alvarez](#)
- [St. Louis water mishap](#)  
[David G. Himrich](#)
- [Satellite imaging for targeted marketing?](#)  
[Denis Haskin](#)
- [Millennium goes to prison](#)  
[Henry Troup](#)
- [Breakdown of police emergency number](#)  
[John Colville](#)
- [Risks of client search tools \(the WWWorm turns, and returns,...\)](#)  
[Rob Slade](#)
- [Changeable `constants'](#)  
[James Ashton](#)
- [Re: vandals Cut Cable, Slow MCI Service](#)  
[C. Paul Ferroni](#)
- [Unintended document contents](#)  
[Walter Smith](#)
- [Re: Bug in Microsoft Word](#)  
[Steen Hansen](#)  
[Pete Ferris](#)  
[Anthony E. Siegman](#)
- [Re: system makes bank check forgery easy](#)  
[Paul Gloger](#)
- [More on Real World/Cyberspace ID matching](#)  
[Paul Green](#)
- [Re: pi = 3](#)  
[Mark Brader](#)
- [New indecency rules proposed for all online services](#)  
[Daniel J. Weitzner](#)
- [Info on RISKS \(comp.risks\)](#)

---

**Risks of spread-spectrum cordless phones**

*Don Alvarez <dla@cmb.rphys.cmu.edu>*

*Tue, 30 Aug 1994 09:36:01 -0400*

I just purchased a 900Mhz spread spectrum phone from Escort (the radar detector people). They don't take P/O's, so I had to order with a credit card. I'm not sure I want to show the following credit card receipt to the ladies down in purchasing...

ESCORT PHONE, WHITE \$299  
ADULT SIGNATURE REQUIRED

(Thank goodness they didn't name the thing after a Cobra or an English Sheepdog or mention the "rubber-duckie" antenna... at least this way I only look like your run-of-the-mill degenerate).

---

### **St. Louis water mishap**

*"David G. Himrich" <76270.1257@compuserve.com>*

*30 Aug 94 10:56:16 EDT*

A pressure valve in the St. Louis city water system opened inadvertently and the resulting pressure spike damaged water mains in 15 locations throughout the City. It also tripped 14 fire alarms by disrupting sprinkler systems.

The city water division suspects that a Southwestern Bell Telephone Company repair crew caused an "errant electronic command" which opened the 66-inch (168 cm) diameter valve. The crew was working on a data transmission line at the pressure control room at the Chain of Rocks water works in St. Louis. Southwestern Bell is not officially aware of any link between the repair and the mishap but will "be happy to work with the city to determine if there is any link." [Source: Article by Tim O'Neil and Melanie Robinson in the St. Louis Post-Dispatch, 30 August 1994.]

- David Himrich

---

### **Satellite imaging for targeted marketing?**

*Denis Haskin <DWH@epub.ziff.com>*

*Tue, 30 Aug 1994 13:18:31 -0500 (EST)*

A 25 Aug 1994 article in the \*San Jose Mercury News\* discusses BADGER (Bay Area Digital GeoResource), an "electronic library of maps, census data, property lines and environmental features."

This is a project funded by NASA and involves Bay Area cities+towns, a company called Smart Valley, NASA Ames, Lockheed, and other companies to "create a shared data base of geographic information about the Bay Area and the software to help cities use it to identify polluters, prevent power failures or plan land-use policies."

Sounds pretty benign until you get to the discussion of use of this data by

private companies for identifying potential customers, to wit:

Organizers say private companies might make use of the mapping service as well. For example, a satellite photo that located swimming pools could be cross-referenced to a property-tax map to create a data base of pool owners. That could be useful to pool-cleaning services.

With high-resolution satellite images, roofers might be able to locate homeowners with aging wood shake roofs.

The risks to personal privacy are, I think, obvious.

Denis Haskin, Sr. Mgr., Production Engineering, Information Access Company,  
10 Presidents' Landing, Medford, MA 02155 dwh@epub.ziff.com 617 393 3649

---

## Millennium goes to prison

*"henry (h.w.) troupe" <hwt@bnr.ca>  
Wed, 31 Aug 1994 15:07:00 -0400*

KINGSTON, Ontario -- The success of a recent trial of the Northern Telecom Millennium pay phone at Collins Bay Prison in Kingston, Ontario, may mean the system is set to go to prison for life.

Northern Telecom partnered with the Canadian Federal Correctional Services, telephone consortium Stentor, and Bell Canada, to customize the flexible Millennium system architecture to fit the unique demands of a prison setting. The resulting "Millennium Inmate Solution" includes real-time management of inmate phone traffic to allow or restrict numbers, and enhance fraud control.

Production on the Millennium Inmate Solution is slated to begin in Calgary by year-end, after final reviews by Stentor and the federal government. Roll out to federal prisons coast to coast is planned for the first quarter of 1995. The new prison phone system was also very well received by the American Correctional Association when it was shown at their conference this month in St. Louis, Missouri.

---

## Breakdown of police emergency number

*John Colville <colville@socs.uts.edu.au>  
Wed, 31 Aug 1994 13:49:15 +1000 (EST)*

[Based on radio reports]

Last night (Tue Aug 30), callers to the NSW Police's emergency 000 phone number in Sydney could not get through for a period of about five hours from 7.30 pm. Emergency calls to fire and ambulance, which are also reached by 000, were not affected. One caller, who was reporting a robbery in progress, was asked to call the local police station. 000 calls in other areas e.g. Newcastle and Wollongong were not affected.

The State Commander [Officer in charge of day to day operations for NSW] said that nothing like this had ever happen before, to his knowledge.

Police are investigating the failure.

John Colville, School of Computing Sciences, University of Technology, Sydney  
Broadway, NSW, Australia, 2007 colville@socs.uts.edu.au +61-2-330-1854

---

## Risks of client search tools (the WWWorm turns, and returns, ...)

*"Rob Slade, the famous sleep deprivation experiment" <ROBERTS@decus.ca>  
Tue, 30 Aug 1994 12:45:46 -0600 (MDT)*

I noticed the following on net-happenings as an explanation of why a promised World Wide Web search tool was not released. It doesn't give full details, but, for those who can read between the lines, you can see that such a local client search tool would consume enormous amounts of bandwidth. I'm glad that the developer had the good sense not to pursue it. "Some searches were not meant to be meddled with, Dr. Lemieux!" :-)

(btw, for those without W3 who want to access the document cited, send mail to listproc@www0.cern.ch with the command:

www <http://web.nexor.co.uk/mak/doc/robots/robots.html>  
in the body of the message.)

----- Forwarded message -----

Date: Sun, 28 Aug 1994 19:03:53 -0400 (EDT)  
SENDER: Mac WWW Worm <lemieuse@ere.umontreal.ca>  
Subject: [announce] Mac WWW Worm

First, sorry for my french colleagues for this english answer. I just didn't want to write it twice...

-----

Here are my presents thoughts about that:

- 1- Due to the net traffic that would be produce by such an easy-to-use 'bot, I first decided that it should never be widely released.
- 2- My Mac WWW worm was an engine designed to search for specific topics. He was downloading lots of pages, but kept informations only about a little portion of them. This way there's a lot of wasting in net resource.  
  
So, if you were striving to get such a tool, you should consider using one of the publicly accessible WWW Database.
- 3- Everyone running a bot without letting other people acces the data is wasting resources, and should not be permitted to do that...

Anyone interested in the subject of WWW Robot should consider reading the following document:

<http://web.nexor.co.uk/mak/doc/robots/robots.html>

Before flaming me for not releasing the 'bot, read every thing you can find under that URL.

-----

Beside that, the MacWWW worm program still contains lots of neat HyperCard script that can be easily recycled for any internet based material... I would accept to share all this material with any other HC-minded people.

Be aware that building net program is not a little thing. Even if HC permit it to be really easy, you should always keep in mind that the internet is a \_public\_ network. Don't waste other's resources...

Anyway, thanks for your interest.

Sebastien Lemieux, dept. biol. lemieuse@alize.ERE.UMontreal.CA  
<http://alize.ere.umontreal.ca:8001/~lemieuse/>

Ce message a ete reposté par le reposteur TCL  
Pour info: lemieuse@ere.umontreal.ca

[Very lemieusing! PGN]

---

### Changeable `constants'

"James Ashton" <jaa@deakin.anu.edu.au>  
Wed, 31 Aug 1994 13:41:00 +1000 (EST)

In [RISKS-16.36](#) it was noted that 'On some old versions of Basic for PDP-11s, you could assign any value to the "constant" pi.' I believe that on some versions of FORTRAN you could do even better. You could assign any value to numerical constants. While I never tried it, our FORTRAN lecturer told us that (at least in the local implementation of the time) numerical constants were collected by the compiler and stored in writable memory. Statements like `3=4' could then cause the chaos that you might expect.

James Ashton, Department of Systems Engineering, Australian National Univ.  
Canberra ACT 0200 Australia +61 6 249 0681 James.Ashton@anu.edu.au

---

### Re: vandals Cut Cable, Slow MCI Service (Kabay, [RISKS-16.36](#))

"C. Paul Ferroni" <cpferron@cle.ab.com>  
Tue, 30 Aug 1994 08:15:46 -0400

I would suggest that another plausible explanation is that the cut was designed to allow for insertion of <something> into the line at another point,

while the first cut was being fixed. While the line was down for repairs, such an insertion wouldn't be noticed... I hope someone at MCI is thinking.

-cpf Paul.Ferroni@ab.com

---

## Unintended document contents

*Walter Smith <wrs@newton.apple.com>*

*Mon, 29 Aug 1994 21:37:36 -0700*

> If all you use is printed copies, you're okay. However, if you give somebody > the file on disk or send it by E-mail, then there may be unintended info...

This problem is not at all limited to Microsoft Word--there is another way in which a file can end up containing unintentional disclosures visible to a raw data editor. Checking my own disk, I have found several instances of this.

There are many applications that don't write to every byte of their files. On the Macintosh (and presumably some other systems), when file space is allocated, the system doesn't zero the allocated blocks. Whatever data was written there previously remains. Thus, documents can end up with bits of other--completely unrelated, perhaps sensitive--documents trapped inside them.

It's a particularly insidious problem, because once the old bits are trapped in the new document, they remain with the document forever. Even if you prepare your CD-ROM (or whatever) on a pristine, newly formatted hard disk, you may be copying little excerpts from the disks of all the machines the documents originated from.

- Walter Smith / Newton Software / Apple Computer, Inc.

---

## Re: Bug in Microsoft Word

*Steen Hansen <steen@kiwi.swhs.ohio-state.edu>*

*Tue, 30 Aug 94 08:03:27 -0400*

In the August issue of Byte Magazine, columnist Pournelle (Chaos Manor) recommends turning Fast-Save off - he reported losing hours of work because of it.

Steen Hansen, Computer Specialist, Ohio State University hansen+@osu.edu

---

## Re: Bug in Microsoft Word (Moore, [RISKS-16.36](#))

*<pferris%[mohawk.uucp@drd.com](#)>*

*Tue, 30 Aug 94 00:04:35 -0600*

Gadzooks! You (and the fellow that originally reported it!) are correct. The problem also exists on the Mac - though I don't see the "Summary" problem as

he stated for Windows. Norton revealed the truth of the matter on the Mac. Still, I don't consider this *\_fatal\_* by any means. I just won't send out any Word (Fast Saved - which I keep don't use / disable, BTW!) discs. Thanks to both of you for the warning(s).

I thought MS fixed the Fast Save bugs in 5.1a (note the "a"! ). Evidently not this one! Hullo Mr. Gates, are you there?

Tell me, do you know if this is a problem in Word 5.1a for Macintosh? I haven't encountered it yet, but I seldom rip into Word files with anything but Word. I'm curious, if this might not be used for a (future?) "restore to previously saved version" type thing... but again, why just on "Fast Save"?! Hmmm... I'd like to hear MS explain/correct this one (making a note to call tomorrow!).

Bullwinkle sez: "Watch this Rocky! Now I'll use CPS Tools to do a Word file recover operation and see which variation of the file it prefers... " I suspect I know... :-<

Pete Ferris, N5KBD pferris%*mohawk.uucp@drd.com*

P.S.: To other readers: I stand corrected here... also: FYI: I use a Mac so not all Windows stuff is applicable here...

[Another response from Pete, to Norloff, is omitted here. PGN]

---

## Re: Bug in Microsoft Word (something similar in WriteNow?)

*"Anthony E. Siegman" <siegman@Sierra.Stanford.EDU>  
Tue, 30 Aug 94 10:14:37 PDT*

>Word summary info area for each document that cannot be turned off.

I was using On Location (an excellent Mac utility which builds indices and enables you to find every document on your hard disk containing a given text string) to look for a letter to "Richard Jones" I had written 2 years ago. OL found such a document -- a WriteNow template letterhead I employ -- but when I opened this document the contents appeared to be a later letter to someone else.

On a hunch I tried the WriteNow "Revert to Saved" menu command, and the original letter to Richard Jones appeared.

Whether this could be a security hole if I sent the later letter by file transfer or over a net to someone else who also had WriteNow, I can't say. Maybe I had only printed the later letter and not Saved it; maybe I typed it in and did a "Save As", leaving the Jones letter still hidden in the template's hidden backup area.

--AES siegman@sierra.stanford.edu

---

## **Re: system makes bank check forgery easy**

*<Paul\_Gloger.es\_xfc@xerox.com>*

*Tue, 30 Aug 1994 02:53:02 PDT*

I believe I can explain the reported 6-month auto. purge on check stops, in a way which precludes the obvious risk in the usual check-stop case, although not in the actual case reported by Christopher Klaus.

There is a U.S. federal banking regulation which says that a check dated more than 6 months ago is deemed "stale," relieving the maker of the check of obligation to honor it. (The banks don't however themselves generally monitor the currency of this date, any more than they generally verify that the signature is valid. Instead, they generally accept the check only with recourse to the payee, and subject to collection from the maker; and they send the maker, their account holder, a periodic checking account statement saying that he has 10 days [or whatever] to protest, after which he is deemed to have accepted the checks for payment. Thus the banks mostly leave it to you to know and claim your rights, while making very sure that they don't get caught in the middle. Thus the only time the bank will actually fully vet a check is when they're cashing it without recourse back to the payee.)

Anyway, the 6-month-stale rule was presumably established in pre-current-computer-technology days, to bound the records and balances which must be maintained for outstanding checks, by the maker for all such checks, by the maker and the bank for stopped checks.

In conjunction with this rule, a 6-month check stop works fine for checks which have been made and dated and issued and then stopped for some reason.

In contrast, a check stop doesn't hold up beyond 6 months for blank checks which have been lost or stolen. However, you've got the right to simply refuse a forged check on your account, per the discussion above, so technically you're still protected; but the bank may make you sweat to exercise that right. In this case, I believe the only response that's secure against even attempted forgery is to close the account, which is what most banks would push for here.

Paul Gloger *<Paul\_Gloger.es\_xfc@xerox.com>*

---

## **More on Real World/Cyberspace ID matching (Kabay, [RISKS-16.35](#))**

*<Paul\_Green@vos.stratus.com>*

*Tue, 30 Aug 94 11:35 EDT*

Regarding Mich Kabay's article that reports the welfare benefits fraud case in the UK and then goes on to make some interesting speculations regarding the larger issues raised...

If it is indeed true that we can take approximate measurements of multiple body characteristics and combine them to get a reliable indicator of identify (passes the common sense test; has any authority written on this

subject?), then why not measure attributes of the face?

>From what I have read of genetics and inheritance, and of course from my own observations, the human face is highly variable. We can speculate why random variation and natural selection has given our species this characteristic (reliably bonding parents and children?), but given that it is there, we can also take advantage of it. For example, we already measure head size (for hats) and inter-eye distance (for glasses). Other advantages are that it is noninvasive, fairly permanent, always at hand, difficult to forge, and well-established as an acceptable, nontechnical means of identification. Some difficulties would be separating identical twins (and someday, perhaps, clones), and accounting for the effects of injury, disease, and aging.

As a footnote, I read recently that people whose faces are considered beautiful have facial measurements that are close to the average. Measuring faces could be fairly compute-intensive. If so, in the future, Helen of Troy could be the face that launched a thousand chips.

(Gotcha!)

Paul Green, Sr. Technical Consultant, Stratus Computer, Inc., Marlboro, MA  
01752 (508) 460-2557 Paul\_Green@vos.stratus.com; PaulGreen@aol.com

---

**Re: pi = 3 (Dudley, Bible, [RISKS-16.35](#))**

<msb@sq.com>

Fri, 26 Aug 1994 19:04:12 -0400

> Actually, my home state of Indiana did try to legislate that the value of pi  
> should be 3. Here is some information from the alt.folklore.urban archives  
> from an article written by Mark Bader (msb@sq.com)

There are three important corrections to be made here. First, the act did not assign pi the value 3; this is quite clear if you actually read my article. Taking the term "pi" to mean the ratio of circumference to diameter, the bill assigned the reciprocal of this ratio the value  $(5/4)/4$ , or in other words,  $\pi = 3.2$ .

Second, my name is not Bader.

Third, "try to legislate ... the value of pi" is not really accurate. A closer description of the legislation was that it attempted to \*recognize\* a better value for pi. However, because of the wording used, if passed it would, as a side-effect, have assigned that value. The intent is fairly clear from the description in...

> (Further information can be found in "Mathematical Cranks", Underwood  
> Dudley, The Mathematical Association of America, Washington D.C.).

Two additional references are:

\* Edington, Will E.: "House Bill No. 246, Indiana State Legislature, 1897",  
Proceedings of the Indiana Academy of Science (PIAS), 1935.

\* Singmaster, David: "The Legal Values of Pi",  
Mathematical Intelligencer, vol. 7 (1985) #2, p.69-72.

As to the Kings-1 and Chronicles-2 items, one need only murmur the phrase "to one significant digit".

[Incidentally several folks noted that the structure need not be circular to satisfy the stated conditions; an oval would do just fine. PGN]

Mark Brader, msb@sq.com            "But I want credit for all the words  
SoftQuad Inc., Toronto            I spelled \*right\*!" -- BEETLE BAILEY

---

## New indecency rules proposed for all online services

*Daniel J. Weitzner <djw@eff.org>*  
*Thu, 25 Aug 1994 14:32:40 -0600*

(900#s in cyberspace)

### I. Overview

During the final hours before the Senate telecommunications bill (S.1822) was marked-up by the Senate Commerce Committee, a provision was added which would expand the current FCC regulation on obscene and indecent audiotext (900 number) services to virtually all electronic information services, including commercial online service providers, the Internet, and BBS operators. This proposal, introduced by Senator Exon, would require all information service providers and all other electronic communication service providers, to take steps to assure that minors do not have access to obscene or indecent material through the services offered by the service provider.

Placing the onus, and criminal liability, on the carrier, as opposed to the originator of the content, threatens to limit the free flow of all kinds of information in the online world. If carriers are operating under the threat of criminal liability for all of the content on their services, they will be forced to pre-screen all messages and limit both the privacy and free expression of the users of these services. Senator Exon's amendment raises fundamental questions about the locus on liability for harm done from content in new digital communications media. These questions must be discussed in a way that assures the free flow of information and holds content originators responsible for their actions.

### II. Summary of Exon Amendment

The Exon amendment which is now part of S.1822, expands section of the Communications Act to cover anyone who "makes, transmits, or otherwise makes available" obscene or indecent communication. It makes no distinction between those entities which transmit the communications from those which create, process, or use the communication. This section of the Communications Act was

originally intended to criminalize harassment accomplished over interstate telephone lines, and to require telephone companies that offer indecent 900 number services to prevent minors from having access to such services. The 900 number portions are known as the Helms Amendments, having been championed by Senator Jesse Helms. These sections have been the subject of extension constitutional litigation.

If enacted into law, these amendments would require that anyone who "makes, transmits, or otherwise makes available" indecent communication take prescribed steps to assure that minors are prevented from having access to these communications. In the case of 900 numbers, acceptable procedures include written verification of a subscriber's age, payment by credit card, or use of a scrambling device given to the subscriber after having verified his or her age. Failure to do so would result in up to a \$100,000 fine or up to two years imprisonment.

### III. Carrier Liability and Threats to the Free Flow of Information

These provisions raise serious First Amendment concerns. (Note that we use the term 'carrier' here to refer to a wide range of information and communication service providers. This does not suggest that these entities are, or should be, common carriers in the traditional sense of the term.)

Overbroad carrier liability forces carriers to stifle the free flow of information on their systems and to act as private censors

If carriers are responsible for the content of all information and communication on their systems, then they will be forced to attempt to screen all content before it is allowed to enter the system. In many cases, this would be simply impossible. But even where it is possible, such pre-screening can severely limit the diversity and free flow of information in the online world. To be sure, some system operators will want to offer services that pre-screen content. However, if all systems were forced to do so, the usefulness of digital media as communication and information dissemination systems would be drastically limited. Where possible, we must avoid legal structures which force those who merely carry messages to screen their content.

Carriers are often legally prohibited from screening messages

In fact, under the Electronic Communications Privacy Act of 1986, electronic communication service providers are generally prohibited from examining the contents of messages or information carrier from one subscriber to another.

Extension of the 900 number rules to all electronic information services may be unconstitutional

The regulation of indecent 900 number programming was only accomplished after nearly a decade of constitutional litigation, with rules being overturned by the Supreme Court. The regulations were finally found constitutional only after being substantially narrowed to meet First Amendment scrutiny. Since the access methods offered by online service providers are significantly different than simple telephone access to 900 services, we doubt

that the same constitutional justifications would support the newly expanded rules. This issue requires considerable study and analysis.

Content creators, or those who represent the content as their own, should be responsible for liability arising out of the content

In sum, it should be content originators, not carriers, who are responsible for their content. Any other approach will stifle the free flow of information in the new digital media.

#### IV. Next Steps

Having only just received the language offered by Senator Exon, EFF still needs to do further analysis, and consult with others in the online community. We also hope to speak with Senator Exon's staff to understand their intent. Another important hearing will be held on S.1822 in mid-September by the Senate Judiciary Committee. By that time, we hope to have this issue resolved. While we agree that these carrier liability problems are in need of Congressional consideration, we do not believe that the time is ripe to act. Before any action is taken, hearings must be held and careful evaluation of all the issues, not just indecency, must be undertaken.

Daniel J. Weitzner, Deputy Policy Director, Electronic Frontier Foundation,  
1001 G St. NW Suite 950 East, Washington, DC 20001 +1 202-347-5400(v)



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 16: Issue 38**

**Friday 2 September 1994**

## Contents

- [Football interference without penalty?](#)  
[PGN](#)
- [RFI and "winchcraft"](#)  
[Mich Kabay](#)
- [Drawbridge controls -- fail-safe?](#)  
[Steve Summit](#)
- [Chile: "Multicarrier" telephone system collapses](#)  
[Patricio Poblete](#)
- [Anarchist files linked to child mutilation](#)  
[Mich Kabay](#)
- [Poulson Pal Pinched](#)  
[Mich Kabay](#)
- [Barclays Bank's new computer system](#)  
[Steve\\_Kilbane](#)
- [Risks of living abroad](#)  
[DelleraK](#)
- [Re: Changeable `constants'](#)  
[George W Dinolt](#)  
[Joseph H Presley](#)  
[Mark Brader](#)  
[Bob Frankston](#)  
[Steve Kilbane](#)  
[Lars-Henrik Eriksson](#)  
[James Cottrell](#)  
[James Carlson](#)  
[Mark Nelson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Football interference without penalty?

*"Peter G. Neumann" <neumann@csl.sri.com>*  
*Fri, 2 Sep 94 8:47:48 PDT*

National Football League coaches will have radio transmitters this year to

send plays in to their quarterbacks. RISKS readers may suspect that unless the communications are encrypted, the opposing coaches will be able to listen in. However, a different security problem must also be solved. The last time this was tried in the World Football League, quarterbacks sporadically picked up signals from local radio stations and air traffic controllers. You can imagine a situation in which the flight instruction just happened to coincide with the name of a play. Well, apparently the NFL techies believe they have solved the interference problem this time around; perhaps they resorted to the Playfair Cipher. [Thanks to Tom FitzGerald in the San Francisco Chronicle, 2 Sep 1994, p. E6, for reminding me of this risk.]

---

## **RFI and "winchcraft"**

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
02 Sep 94 07:40:26 EDT*

The *\_Globe and Mail\_* newspaper in Canada for 94.09.02 (p. A8) reports on radio-frequency interference with building-construction cranes and other devices:

Breaking the spell of 'winchcraft'  
by Mary Gooderham, Applied Science Reporter

...Without warning--and with no obvious electrical or mechanical fault--the Kroll K-154 crane would shut itself off, sometimes while hoisting a bucket filled with a couple of thousand kilograms of concrete. Two transmissions blew, their gears suffering when the machine's emergency braking system stopped the bucket in mid-air. The crane sputtered, losing power last week to the point where it could lift loads only slowly, only a few metres off the top of the building.

The article explains that these problems caused major delays in the construction site at Simcoe Place in Toronto. Investigation revealed that the equipment was being disrupted by radio-frequency interference (RFI), probably from nearby microwave relay dishes and broadcasting stations.

Workers with experience at the Scotia Plaza site built during the late 1980s recalled similar problems there; intermittent problems began once cranes were raised above the 60th story and depended on the orientation of the cranes--apparently because the cranes acted like antennas. In that case, engineers figured out that the RFI was disturbing "the wiring on the cranes' direct-current motors."

Significantly, the Simcoe Place crane also has a new DC motor, whereas the other, unaffected crane uses an AC motor.

The engineers installed some metal-coated foam usually applied to ductwork. The problems stopped. A lead shield is now being installed for more secure isolation.

According to the contractors erecting the outer walls of Simcoe Place, their laser level "started acting funny when it was used above the 20th floor."

The receiver that picks up the laser signal beeped when the laser was off-target or wasn't even turned on. Wrapping all but its tiny electronic eye with the aluminum foil that usually keeps sandwiches fresh in the workers' lunch boxes seemed to solve the problem.

M.E.Kabay, Ph.D./DirEd/Natl Computer Security Assn (Carlisle, PA)

---

### **Drawbridge controls -- fail-safe?**

*Steve Summit <scs@eskimo.com>*

*Fri, 2 Sep 1994 08:59:31 -0700*

The Evergreen Point Floating Bridge across Lake Washington in Seattle (SR 520) has been notorious for its control problems -- either it gets stuck open or stuck closed, or opens partially for no reason (which has led to one death and one serious injury, on two separate occasions). The draw span has been rebuilt this summer, although the following account (from the Seattle Times of September 1) of the new controls will perhaps not be as reassuring to RISKS readers:

To ensure that the center lift span never again pops up accidentally, the old mechanical system has been replaced and is now controlled by a computer with a series of safety features that must be overseen by the bridge operator.

"You have to push buttons to make the gates go down, the lights come on and the [actuating hydraulic] pumps to start," [project engineer Jay] LaVassar said. "Every step has to be completed before you can go to the next step."

Steve Summit   scs@eskimo.com

---

### **Chile: "Multicarrier" telephone system collapses**

*Patricio Poblete <ppoblete@dcc.uchile.cl>*

*Fri, 2 Sep 1994 18:15:07 GMT*

MULTICARRIER TELEPHONE SYSTEM COLLAPSES AFTER 4 DAYS--  
A telecommunications system that allows callers to choose their own long-distance telephone company, called the multicarrier, collapsed only 4 days after its inauguration. The system failed because callers were using codes obsolete with the start-up of the multicarrier, confusing the system. Talca and Curico, the first cities to have the multicarrier installed, were the first to experience problems. The entire country will be hooked up by late October. (La Epoca, p. B6)

---

## Anarchist files linked to child mutilation

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>

02 Sep 94 07:40:34 EDT

The Montreal Gazette for 94.09.01 reports on page E1 about a pipe-bomb explosion related to computer bulletin board anarchist files:

Boy loses 3 fingers in pipe-bomb explosion:  
Kirkland youngster, 13 and 15-year-old friend  
were following instructions on a computer.

by Ann Carroll, The Gazette

A 13-year-old Kirkland boy lost three fingers on  
one hand and his 15-year-old friend was seriously  
injured last week when a pipe bomb they were making  
--following instructions on a home computer disk--  
accidentally exploded.

The article states that the boys had "decided to try an experiment they had  
picked up from a computer information network." The little idiots ignited the  
"high-powered flare" and it exploded in the hands of the 13-year-old. The other  
boy is undergoing continuing treatment to remove shrapnel from his hand.

The mutilated victim's mother destroyed the diskette containing the instructions  
but does not know the information's source.

{Comments by MK:

Discussion at HoHoCon 94 in Austin, Texas:

Q: "What about the Alansky case in Hartford where the cops  
are attacking a BBS for having bomb-making info?"

A: [Deth Vegetable answers] I wrote those files when I was  
15; and the files are in the news again in Montreal.  
Some kids used my files and blew up their fingers.  
I feel bad about that. However, anyone stupid enough  
to use the files to make bombs deserves what they get.  
It's like Darwin, you know? In Canada they don't have  
guaranteed free speech, so the cops are taking boards  
down for having this stuff on them. Alansky got 28  
onths in jail. His lawyer said he didn't want to get  
involved with the First Amendment. So Alansky  
plea-bargained and then went to jail. There were other  
irregularities; e.g., they didn't inform the lawyer of  
the location for the indictment.

Q: [MK, loudly] "Why publish such files at all?"

[Furious faces circle on me from all quarters;  
people recite, "Information Wants to be Free" and snarl,

"There was nothing illegal about it" and "He had a right to post it."]

A: [Someone hands me a note written by Voyageur]

"We provide the files in order to protest our rights to the freedom of information. If we voluntarily censor ourselves, we do as much as if the government were doing it itself. We maintain our rights through the exercise and use of our rights. In addition, many adults enjoy pyrotechnics as a recreational activity. Quality information provided at low or no cost greatly reduces the risk of pyrotechnic experimentation resulting in unfortunate accidents."

....

Discussion about posting bomb files with Deth Vegetable and others:

[Would you like to be called Mr Deth or Mr Vegetable?]

Most people call me, "Veggie."

[Why did you post the bomb-making files?]

"The government has the power; so publishing the anarchy files is important. It's as if one day the revolution will come and these files will arm the masses to rise up against the establishment. Anyway, it was funny to me at the time [when he was 15, 4 years ago]".

[What about now?]

"I wouldn't do it now. I can't say exactly why. I'm a different person now.... Anyway, who's to say if it's right or wrong?"

[MK, seizing D.V.'s shirtfront and slowly drawing him to an inter-nose distance of 1 inch: "Who's to say if it's right or wrong? \_YOU\_ are. \_I\_ am. [sweeping arm to indicate entire room] \_We\_ are. We live in a society of human beings who have responsibilities to each other. We don't live in an anarchic paradise where you can ignore the consequences of your actions by appealing to a vapid ideology of non-involvement."]

\set disgust = on

I wonder if the fools who posted the pipe-bomb information have any shred of self-respect. "If it's legal it must be OK" is a prescription for amoral anomie. The National Computer Ethics and Responsibility Campaign sponsored by the National Computer Security Association and the Computer Ethics Institute includes a discussion of this attitude; we call it the "video-game syndrome." The syndrome entails assuming that if something is feasible it must be

acceptable; "after all, if the game designers meant to forbid pressing CTL-ALT-7 to shortcut to the winning frame, they should have programmed the game to prevent it." The next stage is, "If the system administrator wanted to keep us out of the medical records, she should have put up better security." And then "If it were wrong to [name of reprehensible act], it should be impossible to accomplish it.

set disgust = off\

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn (Carlisle, PA)

---

## **Poulson Pal Pinched**

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
01 Sep 94 13:22:37 EDT*

The Reuter newswire for 30 Aug 1994 issued a report on the capture of Justin Petersen, a criminal hacker involved in Kevin Poulson's radio-station contest fraud in Los Angeles:

### HACKER NABBED AFTER NEARLY A YEAR ON THE LAM

LOS ANGELES, Aug 30, (Reuter) - After nearly a year of searching, the FBI nabbed a computer hacker who pleaded guilty to tapping radio station phone lines to win contest prizes, a federal prosecutor said Tuesday.

Justin Petersen, 34, was arrested after an agent spotted him getting out of a car in West Los Angeles on Monday, Assistant U.S. Attorney David Schindler said. Petersen tried to flee, but was apprehended after a brief foot pursuit.

The article explains that Petersen admitted June 1993 to having committed "computer fraud, conspiracy and illegally accessing computer files of a credit rating agency...." in connection with his nefarious deeds as a close collaborator of the notorious Kevin Poulson.

At his October 31 sentencing, he could receive 40 years of jail and be fined up to \$1.5 million.

Although he cooperated with law enforcement officials in tracking down other criminal hackers, Petersen disappeared from view and an arrest warrant was issued for him.

Petersen called himself "Agent Steal" and boasted about how much he was being paid by the FBI to inform on his pals at hacker conferences.

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn (Carlisle, PA)

---

## **Barclays Bank's new computer system**

*Steve\_Kilbane <steve@cegeleproj.co.uk>*

*Wed, 31 Aug 1994 14:51:00 +0000*

Barclays Bank in the UK have a new computer system, and are currently inviting customers to check their records, in groups. This week, customers with surnames beginning with J-M are asked to check their records. So I did.

I gave my surname and postcode to the assistant, who promptly brought up my records on a pretty Motif interface (used to be Windows, as I recall). Numerous records needed updating. Some were rather dubious. The first recorded how long I had held an account with them. This hadn't been altered since the last time I gave them this information, two years ago. It's bad enough telling them how long they'd had a record of me when they first got the earlier system going, but they don't seem to update this information at all, and it doesn't seem to be a time reference. sigh.

The other dubious field was my salary, which occurred in two places (general form, and employment form), and needed updating in both places. Why is there this duplication?

A couple of other things bothered me about all this. The first was that I wasn't asked for any more proof of identity other than my surname and postcode, and I got to play with all the fun figures that affect my life. I know this information about at least one friend who banks with Barclays, and their surname's further down the alphabet. :-> More seriously, this information is pretty easy to obtain. I raised it with the assistant, and she informed me that these two pieces of information were considered more secure than an account number. Sigh. I wasn't even asked to produce a physical ID.

The other problem didn't occur to me until I started writing this. The assistant turned the screen towards me, and away from all the other people in the bank. Unfortunately, this also means that she turned it towards the large wall-like window, and all the people in the street. :-(

*Steve\_Kilbane@cegeleproj.co.uk*

---

## **Risks of living abroad**

*Dellerak <dellerak@rferl.org>*

*Fri, 02 Sep 1994 18:08:48 +0100*

I have discovered that living outside the US puts you in the database-never-never-land of People with Foreign Addresses.

I now expect to have to follow up several times after giving my address to just about any US business: the first time to be told "we can't mail out of the country" (read: "we can't make the computer mail out of the country"); the second time to talk to a supervisor, who checks the procedure and tries to enter the address; the third time to call back and discover it was somehow mixed up (frequently as an American address with the German postal code as the ZIP); the fourth time to request a resend with the correct additional postage, which often must be hand-carried to the mail room... you get the picture.

With luck, I eventually receive a tattered envelope bearing several layers of metered postage stickers, US postal reject stamps and some handwriting from the Bundespost employee who managed to successfully interpret the address once the letter finally crossed the ocean.

Then there are the firms like the credit reporting agency that told me the only way to fix my garbled address was to contact each of the companies listed on my credit report...which of course couldn't be mailed out of the country.

The risks? As usual, computerization can greatly streamline handling of the routine, but can also eliminate the flexibility to handle exceptions. And, in an increasingly international world, not everybody has a ZIP code.

---

**Re: Changeable `constants' ([RISKS-16.37](#))**

*George W Dinolt <dinolt@wdl.loral.com>*

*Thu, 1 Sep 1994 19:10:07 +0800*

Re James Ashton's comments in [RISKS-16.37](#) on changing the value of constants in Fortran compilers, it was indeed possible to do so on some Fortran and other compilers. I demonstrated this to my students in the fall of 1972 using one of the Fortran (I think it was either G or H) compilers on MTS (the Michigan Terminal System, a time sharing system using IBM 360 tools).

The compiler would not let you assign a new value to a constant directly. One had to pass the constant as an argument to a subroutine. Inside the subroutine, one referenced the argument as a variable and hence one could assign new values to it. Since subroutine arguments were passed by reference, the value was changed by the assignment and subsequent references to the constant at any later time and in any procedure reflected the new value.

My guess is that this trick would have worked on any IBM 360 system using the same compiler. Other compilers would flag the assignment line in the called subroutine, complaining that one was changing the value of an argument of the subroutine.

The issues arising from overwriting supposedly constant memory with new and ``useful" information have been discussed many times in Risks. This example is more insidious than some because both the calling and called procedure appear to be ``correct" as stand-alone modules. It is the glue (calling mechanism) which causes the problem. My application of this particular compiler ``feature" is just another example of what happens when the ``equivalence" between algorithms and implementations fails in obscure and hidden ways.

George Dinolt, Loral WDL

[The rest of this issue continues this thread. My inconstant moderation allowed me to let the following items through the filter. PGN]

**Re: Changeable `constants' (Ashton, [Risks-16.37](#))**

Joseph H Presley <presley@astra.mh.att.com>

Thu, 1 Sep 94 15:24:08 EDT

On the IBM 1130 system (circa 1970 for me), constants were kept in memory. The following would output  $1 + 1 = 4$  as the answer:

```
CALL X(1)
I = 1 + 1
WRITE (6, 10) I
10 FORMAT (1H1, 7H1 + 1 =, I2)
STOP
END
SUBROUTINE X(I)
I = 2
RETURN
END
```

Additionally, floating point operations were done via subroutines. One night during "student time", I exchanged the + and - subroutines (actually entry points in one routine) on the system disk for about an hour.

Joe Presley j.h.presley@att.com

---

**Re: Changeable `constants' (Ashton, [Risks-16.37](#))**

<msb@sq.com>

Thu, 1 Sep 1994 16:30:49 -0400

Some years ago when I was at university I heard about a student who had tried a similar statement in whatever language they were working in at the time (I think it was a COBOL dialect) and it had worked. The student showed the program to a more knowledgeable person with great concern -- in case the program had "broken the 3 in the computer."

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

---

**Re: Changeable `constants'**

<Bob\_Frankston@frankston.com>

Thu, 1 Sep 1994 21:24 -0400

Fortran wasn't so bad as to allow "4=3". The problem is that parameters were always passed by reference, including constants. so that if you had a subroutine that incremented its parameter, calling it would increment the constant. This was worse than "4=3" since you couldn't tell by inspection that

```
CALL SCORE1(3)
```

would change the constant. There would normally be a single copy of the constant in memory since machines like the IBM 7094 didn't have inline constants.

---

## Re: Changeable `constants'

Steve\_Kilbane <steve@cegelecproj.co.uk>

Thu, 1 Sep 1994 08:18:41 +0000

Believe it or not, there *is* a useful application for this sort of thing. The IEC1131-3 compiler generates object code where all data objects are stored in a lookup table, with constants and variables being virtually indistinguishable. One reason for this is that while commissioning control systems at site, field engineers often have to tune "constant" values to get maximum results from the system. The object file format allows the engineer to change what the programmer originally considered as a constant.

Ok, so I'm talking about changing the constants after compilation is complete - the compiler won't allow the programmer to write to a constant - but it's near enough.

steve <Steve\_Kilbane@cegelecproj.co.uk>

---

## Changeable `constants' (Ashton, [RISKS-16.36](#))

<lhe@sics.se>

Thu, 1 Sep 1994

... Statements like `3=4' could then cause the chaos that you might expect.

This is syntactically incorrect and should not work. However, the following fragment could have the effect of changing 3 to 4.

```
CALL ASSIGN(3,4)
.....
SUBROUTINE ASSIGN(I,J)
  I=J
END
```

Lars-Henrik Eriksson, Swedish Institute of Computer Science  
Box 1263 S-164 28 KISTA, SWEDEN lhe@sics.se +46 8 752 15 09

---

## Changeable `constants'

"James Cottrell" <James\_Cottrell@qmbase.mitre.org>

1 Sep 1994 09:03:51 -0500

While at RCA in the early 80's I was developing Fortran code for PDP/11-70's and showed a colleague an example of what you described. I believe the example you cite is incorrect since the compiler could determine that the left hand side of the equation contained a constant making the statement illegal. The procedure that would work, turning the constant '3' into any

other value is as follows.

Subroutine Foo

call change (3)

printf (I5)3

return

Subroutine Change (I)

Integer I

c change the value of 3 for routine Foo

I=4

Return

In subroutine Foo after the call to change, the compile time constant '3' would be equal to the value assigned in subroutine change. This change occurs because PDP Fortran parameter passing was call by address. I believe, and with age my memory is getting dimmer on the technical details, the PDP Fortran compiler would gather all constant declarations in a subroutine and allocate memory for the constants and load the constants in the memory. I don't remember if this memory was in the code space of the routine or in the data space. If the memory was allocated in the code space, the modification of '3' would remain until the subroutine was overlayed. If the memory was allocated in the data space, the modification of '3' would remain until the program stopped.

This problem would not modify the value of the constant '3' in other subroutines, since the compiler would generate a new (local) copy of all constants for each subroutine.

!The opinions expressed here are mine and may conflict with my employer, !wife or any other person.

---

## Changeable "constants" in Fortran

*James Carlson <carlson@xylogics.com>*

*Thu, 1 Sep 94 10:55:54 EDT*

Close -- the actual problem was a bit more obscure. I know; I've been bitten by it.

Years ago (about 1983), I worked on Finite Element Analysis software at a small company in Pittsburgh. Of course, all of this stuff is done in Fortran since the original public-domain SAP-IV and PLOT-10 packages were in highly condensed and uncommented Fortran.

We ran into a problem with the "constant" zero occasionally assuming other values in one particular module on a Prime 750 running PRIMOS. The problem was caused by a sequence of statements of the form:

```
call somefunction(iargument,0)
```

```
...
call anotherfunction(0)
```

The first callee looked something like this:

```
subroutine somefunction(iarg,icount)
integer*4 iarg,icount
...
icount = icount + 1
...
return
end
```

Of course, Fortran uses call-by-reference rather than call-by-value, so it has to push an address on a stack instead of a literal value. To do this with a constant, like 0, it has to dump the constant into a literal pool and pass the address of the literal pool entry to the subroutine. The compiler "optimized" the other zero-value references in the same module to refer to this "convenient" constant. Then, when the subroutine modified the value of zero in the literal pool, the optimized references were then subtly wrong. The following call passed a value of 1 instead of 0 to the next function, resulting in a skipped element in an array.

Fortunately for my sanity, PRIMOS had a superb debugger, and I knew enough assembly to figure out what had happened. (Playing with memory- to-memory only architectures like the Westinghouse W2500 -- a machine with core memory and a RAM scratchpad -- in my misspent youth also helped. ;-))

James Carlson <carlson@xylogics.com> Annex Software Support / Xylogics, Inc.  
53 Third Avenue / Burlington MA 01803-4491 +1 617 272 8140

## Re: Changeable `constants'

Mark Nelson <mnelson@cis.udel.edu>

Thu, 1 Sep 94 18:20:57 EDT

I've never seen a Fortran compiler that allowed assignments of this form, as this should be easily detected by the parser. However, code similar to the following has worked on every Fortran I've ever tested it on (various DEC, CDC, Cray, and Sun compilers, at least);

```
program modify

c  attempt to modify the value of a constant
c  output will probably be 987.654, not the expected 123.456

call modif(123.456)

print *,123.456

stop
end
```

```
subroutine modif(x)
```

```
real x
```

```
x = 987.654
```

```
return
```

```
end
```

Tricks like this generally don't work with small (absolute value) integer constants, as most machines provide instructions to load such values into registers without accessing memory. But as Mr. Ashton noted, other constants are often stored as literals in memory, with the compiler efficiently reusing the same location for each use of a particular value.

Mark Nelson, Department of Computer and Information Sciences,  
University of Delaware [mnelson@cis.udel.edu](mailto:mnelson@cis.udel.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 16: Issue 39**

**Tuesday 6 September 1994**

## Contents

- [PKZIP encryption broken \(known plaintext attack\)](#)  
[Paul Carl Kocher](#)
- [Some privacy notes](#)  
[Phil Agre](#)
- [Database Marketing \(privacy in \\*Business Week\\*\)](#)  
[Mark Stalzer](#)
- [Backspace Problems](#)  
[John Vilkaitis](#)
- [Backspace Failure](#)  
[John Vilkaitis](#)
- [Re: Millenium goes to prison](#)  
[Jim Hiller](#)
- [\\_Modern\\_ risks of call by reference](#)  
[Mike Albaugh](#)
- [Some comments on the A330 accident](#)  
[Peter Ladkin](#)
- [ESORICS 94 Program](#)  
[Yves Deswarte](#)
- [Info on RISKS \(comp.risks\)](#)

---

### PKZIP encryption broken (known plaintext attack)

*Paul Carl Kocher <kocherp@leland.Stanford.EDU>  
Sun, 4 Sep 1994 17:31:28 -0700*

I finally found time to take a closer look at the encryption algorithm by Roger Schlafly that is used in PKZIP and have developed a practical known plaintext attack that can find the entire 96-bit internal state.

The basic encryption algorithm has four steps, two of which are based on linear shift registers, one is like a linear congruential, and the final converts the contents of an internal state register into an 8-bit value to XOR onto a plaintext byte. A complete description of the algorithm is included in the file APPNOTE.TXT, which is included with PKZIP version 1.1 (check Archie

for "pkz110.exe").

Although the algorithm is substantially better than the toy ciphers used in many products, I have developed a practical known plaintext attack that finds the 96 bit internal state. Unlike the ZipCrack program I released a couple years ago, this attack finds the internal state registers directly and does not involve a brute-force attack on the password. If adequate known plaintext is available, my attack will find the state, regardless of the password's size or content.

My attack is an improvement on a known plaintext attack described in a paper by Biham (unpublished work) that takes  $2^{38}$  operations. My improvements reduce the amount of work required by approximately a factor of 1500 with 200 bytes of plaintext. With less plaintext the attack will take somewhat more time, but just 40 bytes should be enough to be practical. I've written code for all steps of the attack; a version written in C with a few optimizations in inline assembly runs in less than a day on my '486. The attack will work with versions 1.1 or 2.xx of PKZIP and other programs using the same algorithm.

A more in-depth description of the attack will be made available soon, but I wanted to let people using PKZIP (and any other programs that use the same algorithm) know immediately about the weakness.

Paul C. Kocher [kocherp@leland.stanford.edu](mailto:kocherp@leland.stanford.edu) Independent data security consultant/contractor. 415-323-7634 [Disclaimers removed. PGN]

---

## Some privacy notes

*Phil Agre <[pagre@weber.ucsd.edu](mailto:pagre@weber.ucsd.edu)>  
Mon, 5 Sep 1994 18:37:31 -0700*

The September issue of *Smithsonian* magazine includes a long article on "ubiquitous computing" research at Xerox, with some attention to the moral issues relating to tracking and monitoring.

The 5 Sep 1994 issue of *Business Week* has a cover story on database marketing. Like most *Business Week* cover stories it's a superficial rehash of items you might have seen elsewhere. But it might be useful as a summary.

Finally, here is a wonderful quotation from a much longer article by Edwin McDowell, "The scrambling is on for off-season tourism" (*The New York Times*, 5 Sep 1994, business section, pp. 17-18) on off-season tourism marketing:

"Another reason for the growing success of off-season strategies is that states have become a lot more sophisticated with their data bases", said James V. Cammisa Jr., a travel industry consultant in Miami. "They know where the peaks and valleys in their tourism operations are, and they know how to market the off-season effectively.

"Kentucky's data base showed that only 350,000 of the 2.5 million Canadians

who drove through the state last year stayed overnight.

"Our research showed that 83 percent of them come from January to June, headed for Florida, South Carolina and the beaches of Alabama and Mississippi", said Robert Stewart, the Commissioner of Travel Development for Kentucky. To entice more of them, Kentucky officials will soon hold a press conference in Toronto and Canadians will be offered a card giving them discounts at hotels, restaurants and attractions along three of Kentucky's interstate highways.

"Also for the first time, Kentucky is using direct mail to bolster anemic winter occupancy rates in its 15 resort parks that offer overnight accommodations year-round." (page 18)

This kind of database marketing is worth thinking about in the context of rapidly advancing proposals for thoroughgoing instrumentation of cars and roads under the rubric of "intelligent vehicle-highway systems", particularly given that most of the marketing organizations mentioned in the article are in fact government agencies using commercial methods for the benefit of private businesses.

Phil Agre, UCSD

---

## Database Marketing

*<stalzer@macaw.hrl.hac.com>*

*Tue, 6 Sep 1994 13:44:22 +0800*

The cover story of the current issue of Business Week (5 Sep 1994), a conservative business magazine (sorry, Phil), is on Database Marketing. The goal of Database Marketing is to build detailed customer profiles so that a company can target advertisements to specific customers for products and services. This approach is highly successful: response rates are double digit as opposed to 2%--3% for junk mail.

The data collection process starts with a customer's past purchases. Other sources include surveys, rebate requests, and warranty cards. American Express scans a customer's individual transactions to find patterns and to suggest local places that take the card. Many hospitals sell the names and addresses of families with newborns. The data is then combined with public records, such as drivers' licenses, auto registrations, and property tax rolls. Ohio sold its drivers' license and car registration lists for \$375,000 to TRW. What results is a detailed profile of each customer.

The computing technology used to mine a database for prospects includes parallel processing and neural networks. Neural nets are trained to look for people likely to buy a product or service given the parameters in the database, e.g.,

what combination of income level, investment activity, and credit-card spending is most likely to be seen among people who are in the market for mortgages?

The net is applied against each profile in a process called "drilling down." This is a compute intensive operation and companies are starting to resort to parallel processing or workstation clusters. Indeed, it's estimated that a large portion of the projected growth in commercial parallel processing, from \$400M today to \$5B in 98, will be for database marketing applications.

When asked about the privacy issues, one marketer responded that the loss of privacy is offset by the convenience to the customer of highly selective advertising. I'll forgo the commentary and simply refer the interested reader to the original source for more details and anecdotes.

Mark Stalzer, mas@acm.org

---

## Backspace Problems

*Javilk <javilk@netcom.com>*

*Sat, 3 Sep 1994 04:28:10 -0700 (PDT)*

I subscribe to the NETCOM Internet service provider. Although new to UNIX, I have been using computers for over 25 years, and had once worked for one of the largest timesharing service providers in the world. I currently work as a consultant in the areas of software development on PC's and mainframes.

On a number of occasions while writing E-mail using NETCOM's MAIL utility, I was chagrined to discover that my backspace/DEL key has been disabled, yielding a "^?" rather than deleting the previous character. This problem also occurs at the UNIX command level, yet utilities, such as the PICO editor and slower to use ELM E-mail utility interpret the backspace/DEL key correctly. (Except for the subject line!)

Further investigation suggests the once this failure occurs on a server, it remains till corrected by the staff. Reloading my telecom package changes nothing, getting another server does; but there is no means of selecting which server will answer my call. My E-mail complaints to NETCOM yielded various responses from a rather insistent and unfriendly person regarding a "^H" in the text, and flaming me as incompetent when I tried to point out that I neither typed a "^H" in the E-mail, nor see it on my screen, and do not find it consistent across servers; to several more gentle statements by other persons to the effect that there are some differences between servers but that is "Not a Problem", "not a bug" -- if you see a "^H", go fix your terminal program. I have even had one E-mail me that if I was not satisfied, I should change to another internet service company.

(For the last time, I see a "^?", NOT a "^H"! And not on every server! If it is MY problem, how is it that their staff fixes it on their end every once in a while -- even when I don't complain?)

The RISK of not reading E-mailed complaints is finding it in RISKS.

The RISK at command level is entering unintended ambiguities when attempting to correct parameters.

The RISK is sending out correspondence with garbage characters and unmeant words. (As in earlier correspondence with the Moderator.)

And as a person who started in the field on a help desk in 1970, the GAIN in LISTENING to what customers say, ESPECIALY when everyone else is telling them to go away, is making good friends. Their problems usually turn out to be Very Simple!

-JVV- (javilk@netcom.com) John V. Vilkaitis, Senior Consultant  
Software General Corp. Field Office: 408-983-0518 (Voice/Fax)

---

## Backspace Failure

*Javilk <javilk@netcom.com>  
Sat, 3 Sep 1994 04:53:00 -0700 (PDT)*

This problem reminds me of another problem I had as a student working on the old IBM 360, where I would occasionally see this error on my ONLINE-OS 2250(?) video terminal:

(IBM-ese number) ILLEGAL ERROR.

whereupon my partitioned data set would be trashed. There would be NO hardcopy of the message. The center staff would tell me, with varying degrees of politeness, that I was "working too hard" or "staying up too late".

Finally, after months of occasional problems, I spent one night looking through A LOT of manuals to find the explanation that the error routine had found an illegal pointer in the traceback chain, and thus it was the error information that was "illegal".

The first step in solving a problem, is listening to the person having the problem. How can you solve a problem, when you don't know what it is?

-JVV- Javilk@netcom.com John V. Vilkaitis, Senior Consultant  
Software General Corp. Field Office: 408-983-0518 (Voice/FAX)

---

## Re: Millenium goes to prison ([RISKS-16.37](#))

*<JHILLER@lancer.afit.af.mil>  
Tue, 6 Sep 1994 21:05:48 -0400 (EDT)*

I have to wonder whether there was any intended marketing connection between the name chosen for the above-referenced communication system (Millenium Inmate System) and the resulting acronym...

One can derive a lot of humor envisioning a Millenium press release extolling the virtues of the system, but using only the acronym, and then applying the discussion out of context in a community of automators!

The RISK here isn't entirely intuitive, but smells something like the risk of choosing a product name without regard for semantics that might be invoked by a segment of the product's potential market...

Jim Hiller

[Something is aMISs? In this case, a MIS is as good as a smile  
(from a .MIL source, at that!). PGN]

---

## **\_Modern\_ risks of call by reference**

*Mike Albaugh <albaugh@agames.com>*

*Tue, 6 Sep 1994 10:16:53 -0700 (pdt)*

I realize you are probably sick to death of the "3=4" thread, but the thing that struck me was that all the contributions were of the "When I was a kid we had to walk ten miles through the snow and use a compiler that could bung up its constants" form. What saddens me is that the introduction of the "reference" operator in C++ indicates that computer science has apparently not learned the lesson taught by the earlier and very well documented problems. It is simply not advisable to have a single character buried in a 1000+ line "include" file radically change the behavior of:

```
{
  double my_angle,result1,result2;

  /* we can't make my_angle const, because it needs to be
   * "tweaked" on a per-run basis, so neither prototypes
   * nor MMU's can save us...
   */
  my_angle = get_current_operating_assumptions();

  result1 = some_library_function(1,my_angle);
  result2 = some_library_function(2,my_angle);
}
```

In C, one can be confident that no matter what else may be wrong with some\_library\_function(), it will NOT damage my\_angle. In C++, the addition of a single '&' character destroys the basis of that confidence. I can forgive Backus for "changeable constants", but Stroustrup should have known better :-)

The average sailor will not spit into the wind a second time. The average computer scientist does not, apparently, learn from experience.

Mike Albaugh, Atari Games Corp (Arcade Games, soon Time Warner Interactive)  
675 Sycamore Dr. Milpitas, CA 95035 (408)434-1709 albaugh@agames.com

---

## **Some comments on the A330 accident**

Peter Ladkin <Peter.Ladkin@loria.fr>

Sat, 27 Aug 1994 19:02:00 +0200

There are a few points worth emphasising which follow from the Air et Cosmos issue 1482 summary of the A330 accident preliminary report, along with the 1480/1 AeC summary of the preliminary-preliminary findings from the telemetry data.

The A330 preliminary accident report singles out lack of pitch protection with the autopilot in ALT\* mode as a determining factor.

According to the report by Casamayou in Air et Cosmos 1480 (11-16 July), the copilot rotated to 28deg to hold 150kts of speed (the airplane actually went to 29deg), and the autopilot was engaged by Warner, who also retarded the left engine and cut the left hydraulic pump to simulate an engine failure: 'As planned, the pitch of the aircraft started to diminish and passed from 29deg to 25deg, the [pitch] limit authorised by the [flight] envelope protection system FMGES (flight management guidance and envelope system).'

It is presumed that the pilots were expecting that the autopilot was to remain in SRS mode ('Speed Reference System') under which there is automatic pitch protection. However, because the altitude was set too low (2000ft) in the flight director (FCU), the autopilot reverted almost immediately to ALT\* mode, under which there is no pitch protection. However, it was non-obvious for the pilots to know they were in ALT\* mode since it wasn't displayed on the PFD under those flight conditions - mode info disappears from the PFD at 25deg, \*\*the same point to which pitch is protected by the FMGES\*\*.

The preliminary report noted the lack of PFD display of mode as a contributing factor, but not a cause. Bernard Ziegler, technical director of Airbus, singled out in interviews the action of achieving 25deg of pitch as one of his main contributing factors [[RISKS-16.35](#), also the specific figure of 25deg, a 'particularly high pitch angle' is found in Flight International, 17-23 Aug 1994, p4]. (The other two factors mentioned in the Speigel interview were the 2000ft altitude setting and that the pilots waited too long to recover.)

However, if you want to test pitch protection it follows you have to put the airplane into more than 25deg of pitch, which is what the pilots did. But this is a flight condition such that you can't tell on the PFD what AP mode you're in, and hence whether pitch is actually protected! This info might be available, but it is not displayed on the PFD.

Contributory factors that were also noted by the report: the full-aft center of gravity, and the TOGA thrust on the engines. However, the airplane may be legally loaded to full-aft CG, and if a go-around is needed on an automatic landing, that's what TOGA thrust is for. TOGA conditions are statistically the most likely conditions under which there is an engine failure.

All of the above is a matter of record, or of common knowledge. I'd like to add a few comments and questions of my own.

Firstly, the report implies that autopilot mode confusion played a role in the late reaction of the pilots to the flight condition. They were expecting SRS mode and got ALT\* (for whatever reason) - they were expecting pitch protection

when there was none - they were waiting for something that wouldn't happen, and they couldn't tell from the PFD. Pete Mellor, in his article 'CAD: Computer Aided Disaster' and Robert Dorsett have noted that mode- or control-law-confusion seems to have played a role in many of the A320 accidents as well.

Secondly, this airplane was loaded to within legal limits and was using thrust appropriate to a go-around situation. There are US airports at which commercial flights take place at which the missed-approach procedure requires one to climb-and-maintain altitudes in the region of 2000ft. So, one might consider the possibility that these three of the identified 'causes' of the accident were plausible, although maybe unusual, operating conditions. The airplane was pitched up by the copilot to 28 deg, in order (I would surmise) to activate the automatic pitch protection mechanism, under conditions of engine failure. Under these conditions, under autopilot control, the airplane flew itself into an flight condition from which an experienced test pilot was unable to recover in time. I wonder why more attention is not paid to this feature of the accident?

The trim setting was singled out as a cause, but the report also says that the accelerated rotation caused by this was controlled by the copilot, so I don't see how it figures as a cause, unless it was seen as one-task-too-many.

For comparison and discussion in RISKS, I'd like to mention a possible point of view different from that provided by Airbus [Ziegler interviews, Der Spiegel 15.8.94, [RISKS-16.35](#), and Flight International, 17-23 Aug 1994, p4]. Namely: if the airplane had not crashed, seven more people would be alive - but we also wouldn't have known that an A330 with full aft CofG is unable to fly itself out of an engine-out-during-go-around situation if the altitude-select on the AP is set at or near 2000ft and the pitch is slightly above its 25deg limit of protection.

Is this computer-related? I'm sure the A330 software will be changed. If only because the Commission of Inquiry recommended it.

Peter Ladkin

---

## ESORICS 94 Program

*Yves Deswarte <deswarte@laas.fr>*

*Tue, 6 Sep 1994 14:17:01 +0100*

THE INSTITUTE OF MATHEMATICS AND ITS APPLICATIONS

Catherine Richards House, 16 Nelson Street, Southend-on-Sea, Essex, SS1 1EF.

Tel: (0702) 354020 Fax (0702) 354111

EMAIL: IMACRH@V-E.ANGLIA.AC.UK

PROVISIONAL PROGRAM ESORICS-94  
(European Symposium on Research in Computer Security)

THE OLD SHIP HOTEL, BRIGHTON, UKO

7TH - 9TH NOVEMBER, 1994

ESORICS-94 is organised by the IMA in co-operation with AFCET (creator),  
BCS Computer Security Specialist Group, CERT-ONERA, AICA and GI

ESORICS-94  
Provisional Program

Monday, 7th November, 1994

9.15 - 9.30 a.m. Introduction - Roger Needham and Gerard Eizenberg

9.30 - 10.30 a.m. Session 1 - Measures (Chair: Dieter Gollmann)

Valuation of Trust in Open Networks  
T. Beth, M. Borchering, B. Klein

Performance Requirements in Data Communication Systems  
V. Zorkadis

11.00 - 12.30 p.m. Session 2 - High Assurance Software  
(Chair: John McLean)

Non-interference through Determinism  
A.W. Roscoe, J.C.P. Woodcock, L. Wulf

Mechanical Proof of Security Properties  
J.P. Banatre, C. Bryce, D. Le Metayer

Security through Types  
C. O'Halloran, C.T. Sennett

2.00 - 3.00 p.m. Session 3 - Key Management I (Chair: Einar Snekkenes)

Designing Secure Key Exchange Protocols  
C. Boyd

Robust and Secure Password and Key Change Method  
R. Hauser, P. Jansson, R. Molva, G. Tsudik,  
E. Van Herreweghen

3.30 - 5.00 p.m. Session 4 - Authentication (Chair: Emilio Montolivo)

Beacon Based Authentication  
A. Jiwa, J. Seberry, Y.L. Zheng

Authentication via Multi-Service Tickets in the  
Kuperee Server  
T. Hardjono, J. Seberry

Oblivious Signatures  
L. Chen

POSTERS

Tuesday, 8th November, 1994

9.00 - 10.00 a.m. Session 5 - Key Management II (Chair: Chris Mitchell)

A Model for Establishing Secure Channels in Open Networks

U.M. Maurer, P.E. Schmid

On Strengthening Authentication Protocols to Foil Cryptanalysis

W. Mao, C. Boyd

10.00 - 10.30 a.m. Session 6 - Invited Talk (presented by Chris Mitchell)

Security Research for the Financial Sector

H. Beker

11.00 - 12.30 p.m. Session 7 - Digital Payment  
(Chair: Jean-Jacques Quisquater)

Efficient Electronic Payment Systems Protecting Privacy

J.L. Camenisch, J.M. Piveteau, M.A. Stadler

The ESPRIT Project CAFE - High Security Digital Payment Systems

J.P. Boly, A. Bosselaers, R. Cramer, R. Michelsen,  
S. Mjolsnes, F. Muller, T. Pedersen, B. Pfitzmann,  
P. de Rooj, B. Schoenmakers, M. Schunter, L. Vallee,  
M. Waidner

Liability and Computer Security: Nine Principles

R.J. Anderson

2.00 - 3.15 p.m. Session 8 - Distributed Systems  
(Chair: Peter Bottomley)

Implementing Secure Dependencies over a Network by Designing a Distributed Secure SubSystem

B. d'Ausbourg

A Secure Medium Access Control Protocol:

Security vs Performances

P. Siron, B. d'Ausbourg

Distributed File Systems over a Multilevel Secure Architecture, Problems and Solutions

C. Calas

3.45 - 5.15 p.m. Session 9 - Panel Session (Chair: Helmut Kurth)

Security Evaluation in Practice

POSTERS

Wednesday, 9th November, 1994

9.00 - 10.30 a.m. Session 10 - Access Controls  
(Chair: Vijay Varadharajan)

On the Expressive Power of the Unary Transformation  
Model  
R.S. Sandhu, S. Ganta

Privilege Graph: an Extension to the Typed Access  
Matrix Model  
M. Dacier, Y. Deswarte

A Consideration of the Modes of Operation for Secure  
Systems  
C. Robinson, S.R. Wiseman

11.00 - 12.30 p.m. Session 11 - Database I (Chair: Catherine Meadows)

Mark-and-Sweep Garbage Collection in Multilevel Secure  
Object-Oriented Database System  
A. Ciampichetti, L. Mancini, E. Bertino

Decomposition of Multi-level Objects in an  
Object-Oriented Database  
N. Boulahia-Cuppens, F. Cuppens, A. Gabillon,  
K. Yazdanian

Supporting Object-based High-assurance Write-up in  
Multilevel Databases for Replicated Architecture  
R. Thomas, R.S. Sandhu

2.00 - 3.00 p.m. Session 12 - Database II (Chair: Joachim Biskup)

Aggregation in Relational Databases:  
Controlled Disclosure of Sensitive Information  
A. Motro, D.G. Marks, S. Jajodia

Information Flow Controls vs Interference Controls:  
An Integrated Approach  
F. Cuppens, G. Trouessin

3.00 - 3.15 p.m. Conclusion - Roger Needham

GENERAL CHAIR: Roger Needham (University of Cambridge).

REQUEST REGISTRATION INFORMATION FROM

Miss Pamela Irving, The Conference Officer, The Institute of Mathematics  
and its Applications, Catherine Richards House, 16 Nelson Street,  
Southend-on-Sea, Essex, SS1 1EF. Tel. (0702) 354020. Fax. (0702) 354111.  
EMAIL: IMACRH@V-E.ANGLIA.AC.UK

:::: Yves Deswarte - LAAS-CNRS & INRIA - 31077 Toulouse (France) ::::  
:::: E-mail:deswarte@laas.fr - Tel:+33/61336288 - Fax:+33/61336411 ::::



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 16: Issue 40**

**Monday 12 September 1994**

## Contents

- [Highest Quality Company Logos for Inclusion in Software](#)  
[Dennis Lawrence](#)
- [German Parking Violators Accused of War Crimes](#)  
[Scott Mincey](#)
- [Enola Gay: Another text substitution \(from alt.folklore.urban\)](#)  
[Henry Troup](#)
- [More daring tales of address disasters!](#)  
[Peter Ladkin](#)
- [Risks of duality in electronic media](#)  
[Bob Mehlman](#)
- [Unique way to find bugs: be investigated for breaking the rules \[McLaren Peugeot Formula One\]](#)  
[Bjorn Freeman-Benson](#)
- [Neural Redlining == Plausible Deniability ?](#)  
[Fred Baube](#)
- [Reply to New indecency rules proposed for all online services](#)  
[Julian Meadow](#)
- [CPSR Annual Meeting](#)  
[Phil Agre](#)
- [Proceedings on Assurance and Trustworthiness](#)  
[Marshall D. Abrams](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Highest Quality Company Logos for Inclusion in Software

*Dennis Lawrence* <[LAWRENCE@advax.llnl.gov](mailto:LAWRENCE@advax.llnl.gov)>

*Wed, 7 Sep 1994 08:05 PST*

I received an ad from TigerDirect, Florida, offering a set of "650 High-Quality Logos" of major corporations. The ad suggests using "these logos in newspaper and yellow page ads, brochures and cross-promotions." It goes on to say "all images displayed are the registered trademarks or trademarks of their respective companies." Can be used by Macintoshes or Windows applications.

What a wonderful gift for con artists!

-- Dennis Lawrence

---

### German Parking Violators Accused of War Crimes

Scott\_Mincey <scottm@dorsai.dorsai.org>

Sat, 10 Sep 1994 22:47:31 -0400 (edt)

Bayreuth, Germany - Three violators of the municipal parking code became war criminals when an official entered the wrong code number. According to the "Nordbayerischen Kurier" the three Bayreuth residents received summonses for "Conspiracy to prepare aggressive warfare," when they should have only received citations for parking violations. According to the paper, the official, who had just served ten hours on the night shift, filled out the forms relating to the minor offenses and incorrectly entered the code number of the violation. (Deutsche Presse Agentur)

---

### Enola Gay: Another text substitution (found in alt.folklore.urban)

"henry (h.w.) troupe" <hwt@bnr.ca>

Wed, 7 Sep 1994 11:55:00 -0400

(amusing, not very new)

The Dragon De Monsyne (dragondm@netcom.com) wrote:

...

:Well, I can vouch for it REALLY happening. In today's (Sept. 5, 1994, Final  
:Edition) Northwest Herald (a local paper in the far northwest Chicago Suburbs  
:(McHenry County, for those who know where that is), on pg 3, bottom, left hand  
:corner, I found this gem.

: "Atomic bombers criticize Enola homosexual exhibit"

Nicely documented, for UL hunters.

Henry Troup - H.Troup@BNR.CA (Canada)

---

### More daring tales of address disasters!

Peter Ladkin <Peter.Ladkin@loria.fr>

Thu, 8 Sep 1994 18:32:55 +0200

A colleague, Paul Gibson, arrived at INRIA Lorraine in France from Scotland at the beginning of July. He set up an account with a local branch of the Banque Populaire de Lorraine in Haussonville, a district of Villers in the Nancy conurbation. The address on his account is that of our host, who lives in a tiny village 75km from here. The bank put a false postal code on his address, consequently his mail from the bank arrives either very late or, in the case

of important items such as his bankcard PIN code and checkbook, not at all (I wonder if the important mail has a 'Do Not Forward' instruction on the envelope?). However, whenever he notifies the branch and they check, the correct postal code appears with his account information. The bank employees claim not to understand how the two addresses can be different and seem to be at a loss to rectify the situation, even though he's been physically to see them about it three times in the last two months.

There's an easy fix. Close the account and open another one. But there should be an easier fix - ensure the right address. Either way, the bank lacks effective procedures for troubleshooting. He still has no checkbook and no functioning cash card.

Peter Ladkin

---

### Risks of duality in electronic media

*<rmehlman%grumpy.decnnet@UCLASP.IGPP.UCLA.EDU>  
Sat, 10 Sep 1994 14:29:50 PDT*

A new teleconferencing system installed at JPL still has some bugs. Participants are told to dial into the telecon themselves. Two numbers are provided: an area 818 local number, and an 800 number for distant callers. I dialed the local number for a NASA/Galileo project telecon which turned out to be seriously depleted; half the expected participants, including the convener, were missing. Attempts to reach the convener by phone failed; the line was always busy. We went ahead and had our discussion anyway, only to learn later that a dual telecon, among the people who had dialed the 800 number, had taken place simultaneously.

This reminds me of a curiously similar situation on Telemail about ten years ago. A user complained of often missing important mail. Months later, investigation showed him to have two accounts, differing only by the appended organization. His default login went to one of these, but the group mail distribution list went to the other. About a hundred messages were there waiting for him. "The Black Hole of Telemail", we always called it.

Bob Mehlman, UCLA/IGPP

---

### Unique way to find bugs: be investigated for breaking the rules

*Bjorn Freeman-Benson <bnfb@ursaminor.scs.carleton.ca>  
Fri, 9 Sep 94 13:04:45 EDT*

Here's an interesting positive-risk (rather than negative-risk)...

The McLaren Peugeot Formula One racing team was investigated for breaking the rule against computerized driver aids. During the investigation, the governing body (FIA) contracted with LDRA Ltd to decode McLaren's software and determine if the rules were broken. According to the press release:

PRESS RELEASE FROM THE FEDERATION INTERNATIONALE DE L'AUTOMOBILE (FIA)

...lots of stuff...and then the interesting paragraph...

The World Council noted that during the course of the investigation, LDRA Ltd discovered a bug (fault) in the McLaren software which was producing a power loss in the engine (due to a faulty signal from the gearbox control unit to the engine control unit). McLaren will now be able to correct this problem.

Paris 7 September 1994

Bjorn N. Freeman-Benson

---

### Neural Redlining == Plausible Deniability ?

*F.Baube[tm] <flb@flb.optiplan.fi>  
Sun, 11 Sep 94 18:15:52 EET*

My understanding of neural nets is hazy, so someone please correct me if I'm way off-base.

Neural nets are being used more and more in commercial applications, for example in evaluating mortgage applications.

It occurs to me that since the internal state of a neural net, and its decision-making "process", is essentially opaque, a lender could depend on a neural net to implement redlining in a manner such that, if the bank were in fact to be accused of redlining, the bank could reply, "We don't redline, we rely on objective computer programs to evaluate applications."

The training set for the net could itself contain redlining, and the net would learn it. Then the training set is discarded, and there is no proof of intent to evade the law.

Any applications receives a final yes/no from a live human being, but how easy is it for the lending officer to let a neural net do his or her "dirty work" ?

\* Fred Baube(tm) GU/MSFS/88 baube@optiplan.fi

---

### Reply to New indecency rules proposed for all online services

*Julian Meadow <jmeadow@craycom.co.nz>  
Wed, 07 Sep 1994 17:17:42 +0000 (GMT)*

Don't you just love it when you read about something that might happen, happens! After reading Daniel J. Weitzner's comments about the proposed new indecency rules, I read the following article on the front page of this weeks New Zealand COMPUTERWORLD (dated Sept 5, 1994):

INTERNET SEX GOES OFF-LINE, by Rob Hosking

The prospect of being the target of an indecency test case has caused Internet service provider ICONZ (Internet Company of New Zealand) to pull its pornographic news groups and bulletin boards off line.

"We've pumped hundreds of thousands of dollars into ICONZ and I'm not going to see that go in a test case," says systems administrator Jon Clarke. The company pre-empted the impending litigation after hearing "through the grapevine" that an Auckland religious group was planning a lawsuit following an item on television news about the Internet. Approximately 20 news groups were taken off the wire, out of about 440, and only two users had complained since their removal, says Clarke. "To put it into some sort of perspective, it's effectively stopped us transmitting 100Kb out of 150Mb a day," he says.

The action would have been under the Films, Videos and Publications Classifications Act, passed earlier this year. There is some doubt as to whether the Internet is covered by the act, and the issue has yet to be decided in court.

Clarke says the material being carried is tamer than that available over the counter in most dairies (<JM comment - read cornerstore, newsagent, etc.), and he queries what he sees as a double standard involved. Network users in the US have formed a group to lobby against restrictive legislation and, with the Howick MP Trevour Rogers' Technology and Crimes private members bill currently before Parliament, Clarke says it could be time for the information of such a group here.

The material is still coming into New Zealand but is now "being put in the great big bit bin", as far as ICONZ is concerned. Clarke believes the material will be available - "there are millions of sites worldwide you can go to for this kind of stuff, the only thing is you'll have to pay for it".

<<< JM's comments follow >>>

This article raises several interesting questions:

1. Do we really want local network providers to become our censors?
2. How does the network provider filter 150Mb of data a day, especially when he doesn't know what the law states is and isn't allowed?
3. If a network provider, whilst censoring the days 150Mb of information, reads that a "religious group" was planning a lawsuit against him because they didn't agree with one of his services, what should he do?

The internet provider doesn't lose either way, since as Jon Clarke points out himself, his users just have to go further afield, and I'm sure he'll be happy to charge for this.

---

## **CPSR Annual Meeting**

*Phil Agre <pagre@weber.ucsd.edu>*

*Tue, 6 Sep 1994 19:02:42 -0700*

The 1994 CPSR Annual Meeting will be held on the weekend of October 8th and 9th at UC San Diego. One focus of the meeting this year is teaching people how to actually do something about computer-related Risks to privacy and the like. We'll have a workshop on privacy activism by Christine Harbs from the Privacy Rights Clearinghouse and Dave Redell from CPSR's Civil Liberties Working Group. We'll also have a workshop on legal issues for BBS operators from Mike Godwin of EFF, and a panel discussion on the issues that arise when protecting privacy and intellectual freedom in various professions. Everyone is welcome to attend.

The Annual Meeting Web pages are now ready to go. Just aim your Web client at <http://www.cpsr.org/dox/am/program.html> and look around. Or, if you prefer, you can get the program and registration information from an autoresponder by sending a message to [cpsr-annmtg@cpsr.org](mailto:cpsr-annmtg@cpsr.org).

Phil Agre, UCSD

---

## **Proceedings on Assurance and Trustworthiness**

*Marshall D. Abrams <[abrams@mwunix.mitre.org](mailto:abrams@mwunix.mitre.org)>*

*Wed, 7 Sep 1994 10:47:43 -0500*

Announcing the availability of the Proceedings of an Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness held March 21-23, 1994 at George Washington Inn Williamsburg, Virginia.

The proceedings are available by FTP as an ASCII document from [csrc.nist.gov](http://csrc.nist.gov). The path is `/pub/nistir/assure.txt` Hardcopy was published by the National Institute of Standards and Technology numbered NISTIR 5472.

### **ABSTRACT**

The purpose of the 1994 Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness was to identify crucial issues on assurance in IT systems and to provide input into the development of policy guidance on determining the type and level of assurance appropriate in a given environment. The readers of these proceedings include those who handle sensitive information involving national security, privacy, commercial value, integrity, and availability.

Existing IT security policy guidance is based on computer and communications architectures of the early 1980s. Technological changes since that time mandate a review and revision of policy guidance on assurance and trustworthiness, especially since the changes encompass such technologies as distributed systems, local area networks, the worldwide Internet, policy-enforcing applications, and public key cryptography.

### **1995 WORKSHOP**

A call for participation for the 1995 workshop will be available in October.

You may request a copy by sending e-mail to [witat-info@cs.umd.edu](mailto:witat-info@cs.umd.edu).

Marshall D. Abrams, Info Systems Security Division, The MITRE Corporation,  
7525 Colshire Drive, McLean, VA 22102-3481 703.883.6938 [abrams@mitre.org](mailto:abrams@mitre.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 16: Issue 41**

**Thus 22 September 1994**

## Contents

- [Computer disk crash causes misprinted ballots](#)  
[Lani Teshima-Miller](#)
- [Internet Gets First False Ad Charge](#)  
[PGN](#)
- [Uninterruptable thought patterns](#)  
[Phil Agre](#)
- [Re: Digital Logos](#)  
[Peter J. Denning](#)
- [Reason 55: National Security and the FBI Wiretap Bill](#)  
[Marc Rotenberg](#)
- [Yet More daring tales of address disasters!](#)  
[Paul T. Keener](#)
- [High Security Digital Payment Systems](#)  
[Michael Waidner](#)
- [The Fuzzy Systems Handbook](#)  
[Rob Slade](#)
- [Neural redlining](#)  
[Andrew W. Kowalczyk](#)  
[Peter J. Denning](#)  
[Fernando Pereira](#)  
[Thomas E. Janzen](#)  
[Jan Vorbrueggen](#)  
[Bob Frankston](#)  
[John Turnbull](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Computer disk crash causes misprinted ballots

*Lani Teshima-Miller <teshima@uhunix.uhcc.Hawaii.Edu>*  
*Tue, 13 Sep 1994 18:14:35 -1000*

(As reported on KHON-TV2).

The Hawaii Republican Party was up in arms today when it was discovered that a

"hard disk crash" caused a number of absentee ballots on the island of Maui (state of Hawaii) to inadvertently omit two candidates running for state legislature.

The crash, which reportedly occurred at a California company which had been contracted to print the ballots, means that over 140 Maui residents are now being asked to go in and re-cast their ballots. This printing error was discovered when friends couldn't find their friend's name on the ballot.

The security risks are obvious--if the printing of ballots is so dependent on a single hard drive, it would seem fairly straightforward that people could sabotage elections this way.

Lani Teshima-Miller (teshima@uhunix.uhcc.Hawaii.edu) "Sea Hare"  
UH School of Library & Info Studies.

---

### Internet Gets First False Ad Charge

*"Peter G. Neumann" <neumann@csl.sri.com>  
Thu, 22 Sep 94 9:25:34 PDT*

An AP item from 15 Sep 1994 (e.g., San Francisco Chronicle, D3) noted that the Federal Trade Commission filed a false-advertising complaint against Brian Corzine of Sacramento, California, for making false claims in promoting a credit-repair program. A federal court ordered the promotion stopped. Corzine maintained he was merely a reseller.

---

### Uninterruptable thought patterns

*Phil Agre <pagre@weber.ucsd.edu>  
Fri, 16 Sep 1994 15:41:19 -0700*

In his famous paper "The relation of habitual thought and behavior to language" (published in his collected papers, "Language, Thought, and Reality" by MIT Press), the American linguist Benjamin Lee Whorf began with some tales from his day job as an insurance risk expert, in which he described the lapses of reasoning that led to accidents that his company had to pay for. He says, for example, that people often assume that an "empty barrel" is wholly innocuous -- even if it recently contained gasoline and can thus be reasonably expected to be exhaling flammable vapors. He suggests that part of the problem is with the word "empty", which derives from a particular folk model of objects and materials that unfortunately does not correspond accurately enough to reality.

I am sure that Whorf is cringing in his grave at the power outage that hit O'Hare Airport this past Wednesday morning, which is described in a brief article in the Wall Street Journal:

Daniel Pearl, A power outage snarls air traffic in Chicago region,  
Wall Street Journal, 15 September 1994, page A4.

It would seem that power was lost for two hours when someone shorted out the power system for the Aurora air traffic control center while testing the uninterruptable power supply.

"There are certainly some additional precautionary measures that have to be taken to make sure this doesn't happen again", said Stan Rivers, the FAA's deputy associate administrator for airway facilities.

One precaution, he said, is not to perform the work when air traffic is at its peak. The power outage occurred at 8:45am CDT at the Aurora, Ill., facility, which serves traffic to and from the world's busiest airport, Chicago O'Hare International Airport.

Now, I have no first-hand knowledge of this event, but I do think it is legitimate to ask what could possibly have possessed someone to mess with the power supply for O'Hare Airport's traffic control at 8:45 in the morning. I would like to suggest that, just maybe, it has to do with the phrase "uninterruptable power system". Says the Journal,

It was the second time this year that the installation of an "uninterruptable power system" interrupted power at an air-traffic center.

Granted the first occurrence was more freakish than the second (a falling ladder a hit "break glass and hit button" button). But do you suppose that these things would happen during the morning rush hour, as opposed to 4AM, if uninterruptable power supplies were called "back-up kludges for highly sensitive and fragile power supplies"?

Where do hubristic terms like "uninterruptable" come from? They come from a very narrow understanding of "the system" -- if the power supply can overcome those mishaps that can happen within the narrow technical conception of the system that is found in box-and-arrow type diagrams, then it's "uninterruptable" so long as the world outside remains totally pure and safe.

And if you don't believe me, I've got an "inherently safe nuclear reactor" to sell you -- I kid you not!

Phil Agre, UCSD

---

## Re: Digital Logos (Lawrence, [RISKS-16.40](#))

*Peter J. Denning < [pjd@cne.gmu.edu](mailto:pjd@cne.gmu.edu) >  
Mon, 12 Sep 94 12:33:12 EDT*

Dennis Lawrence reported on an ad from TigerDirect, Florida, offering a set of 650 high-quality logos of major corporations. Logos are copyright by their owners and in many cases trade marked. This means that the copyright owner has sole rights to control who gets copies and who distributes. If TigerDirect has the explicit permission of the owners of the logos, all is well. If not, then not only they, but anyone else using the logo without authorization, is breaking the law. Anyone who would use a logo, authorization or no, to commit a fraud is also breaking the law.

Peter Denning

---

## Reason 55: National Security and the FBI Wiretap Bill

Marc Rotenberg <rotenberg@washofc.epic.org>

Tue, 13 Sep 1994 22:48:15 EST

100 Reasons to Oppose the FBI Wiretap Bill

Reason 55: The largest purchaser of telecommunications equipment in the federal government said the FBI wiretap plan would have an *\*adverse impact\** on national security.

In 1992 the General Services Administration wrote that the FBI wiretap plan would make it "easier for criminals, terrorists, foreign intelligence (spies) and computer hackers to electronically penetrate the phone network and pry into areas previously not open to snooping." The confidential memo was obtained as a result of a Freedom of Information Act request.

What To Do: Fax Rep. Jack Brooks (202-225-1584).  
Express your concerns about the FBI Wiretap proposal.

100 Reasons is a project of the Electronic Privacy Information Center (EPIC) in Washington, DC. For more information: 100.Reasons@epic.org.

---

## Yet More daring tales of address disasters!

Paul T. Keener <keener@upenn5.hep.upenn.edu>

Sat, 17 Sep 94 14:11:32 EDT

Reading Peter Ladkin's account of his colleague's address woes brought to mind an incident that occurred to my friend recently. He moved and sent an address correction to a company in which he holds some stock. The company acknowledged his change of address, but sent it to his *\*old\** address. One wonders if the database update occurred after the letter was generated or if it never happened. He has not received any mail since.

Paul T. Keener keener@upenn5.hep.upenn.edu

---

## High Security Digital Payment Systems

Michael Waidner <waidner@ira.uka.de>

Fri, 16 Sep 94 17:24:04 EDT

The following is the abstract of a paper that will be presented at ESORICS 94. The full text is available via anonymous ftp from ftp.uni-hildesheim.de in /pub/publications/Sirene/publications, file

BBCM1\_94CafeEsorics.ps.

The ESPRIT Project CAFE:  
High Security Digital Payment Systems

Jean-Paul Boly, Antoon Bosselaers, Ronald Cramer, Rolf Michelsen,  
Stig Mjolsnes, Frank Muller, Torben Pedersen, Birgit Pfitzmann,  
Peter de Rooij, Berry Schoenmakers, Matthias Schunter, Luc Vallee,  
Michael Waidner

CAFE (Conditional Access for Europe) is an ongoing project in the European Community's ESPRIT program. The goal of CAFE is to develop innovative systems for conditional access, and in particular, digital payment systems. An important aspect of CAFE is high security of all parties concerned, with the least possible requirements that they are forced to trust other parties (so-called multi-party security). This should give legal certainty to everybody at all times. Moreover, both the electronic money issuer and the individual users are less dependent on the tamper-resistance of devices than in usual digital payment systems. Since CAFE aims at the market of small everyday payments that is currently dominated by cash, payments are offline, and privacy is an important issue.

The basic devices used in CAFE are so-called electronic wallets, whose outlook is quite similar to pocket calculators or PDAs (Personal Digital Assistant). Particular advantages of the electronic wallets are that PINs can be entered directly, so that fake-terminal attacks are prevented. Other features are:

- \* Loss tolerance: If a user loses an electronic wallet, or the wallet breaks or is stolen, the user can be given the money back, although it is a prepaid payment system.
- \* Different currencies.
- \* Open architecture and system.

The aim is to demonstrate a set of the systems developed in one or more field trials at the end of the project. Note that these will be real hardware systems, suitable for mass production. This paper concentrates on the basic techniques used in the CAFE protocols.

Michael Waidner, Universit"at Karlsruhe  
(currently on leave to IBM Zurich Research, email: wmi@zurich.ibm.com)

---

## The Fuzzy Systems Handbook

*"Rob Slade, Ed. DECrypt & ComNet" <roberts@mukluk.decus.ca>  
Sat, 17 Sep 1994 20:12:47 EST*

BKFUZHKB.RVW 940616

Academic Press, Inc.  
955 Massachusetts Avenue  
Cambridge, MA 02139  
Josh Mills, Marketing, jmills@acad.com

[publisher@igc.org](mailto:publisher@igc.org)

"The Fuzzy Systems Handbook", Cox, 1994, 0-12-194270-8

We dinosaurs of procedural programming language orientation tend to have problems with functional programming languages such as Prolog. It is difficult to reorganize your thinking into the existential model of the expert systems programmer. We have similar problems with object oriented programming. The difficulties we have with fuzzy logic are probably for the same reason. Take heart, fellow dinosaurs. At the very least, this book explains *\*why\** we find fuzzy systems so troublesome. They are simply expert systems with a better conceptual grasp of probabilities.

The trade media has hyped fuzzy systems as the new and coming thing. Information systems professionals, who have lived through a great number of "coming things" still know little more, basically, than the fact that control systems are supposed to be better with fuzzy logic, and that close now counts in both horseshoes and fuzzy systems.

The reason for the confidence in this science of imprecision can, in part, be demonstrated in the control realm. Suppose you are building an automatic collision avoidance system for cars. It is fairly straightforward to program in the sequence of actions to be taken to slow the car as it approaches another object. If, however, the system fails, then what happens if you do hit the object? Will the "distance" become a negative number? If so, will the brakes bind or release? Will the drive train stop, accelerate, or go into reverse? This situation is simplistic, but the outcome, in a procedural language, must be accounted for, prepared and tested. Fuzzy systems deal with ranges, and it is much easier to see and understand that the concept of "close" should also include "hit" -- even before you start to build the actions to be taken.

The potential disasters associated with systems that would flip planes upside down when they flew over the equator are not confined to control systems, as IS professionals are all too well aware. Financial disasters can be precipitated by "decision support" software which can generate market crashes. Similar damage can be done on a smaller scale by specialized programs which may have undiscovered, and unintended, assumptions. As with control systems, working with ranges may make the pitfalls more obvious than working with static and sterile values.

Even so, it is difficult for the programmer to translate the concepts of fuzzy logic into code to play with. Cox has, therefore, given you code to play with. A high density MS-DOS format floppy contains C++ source code to mess around with. (C programmers should be able to work with most of it, and, since it is source code, Mac devotees should be able to use it, as well.)

For those wishing to explore this new field "hands-on", a slightly high-toned, but very useful, introduction.

copyright Robert M. Slade, 1994 BKFUZHKB.RVW 940616

---

**Re: Neural nets and redlining (Baube, [RISKS-16.40](#))**

*Andrew W Kowalczyk <AKOWALCZ+aLIFDR1%Allstate\_Corp+p@mcimail.com>  
Mon, 12 Sep 94 15:26 EST*

I have attended several presentations from neural net software vendors. If these sales pitches are any indications, then neural nets are being used for just the opposite of the dark purposes Fred Baube fears.

Successful lenders (and insurance companies) are driven by two basic business rules: avoid "bad" risks and sell more product (increase market size). Very broadly applied underwriting rules (don't write mortgages in ZIP codes with high default rates, don't insure Corvettes driven by young males) support the first rule but run counter to the second.

There is only so much market share that can be taken from the competition. What used to be considered a marginal market needs to be reconsidered in order to fuel the business growth that Wall Street demands. Many companies are essentially saying: "on first blush you sound like a bad risk - find me an excuse to sell to you" - and neural nets help find that excuse (maybe 23 year old male Corvette drivers who are Ph.D. candidates residing in a rural area are excellent risks).

The initial "training set" for the neural net may be current underwriting practices. This would be the same starting point as a rules-based, inference engine driven expert system. Neural nets promise to gain the advantage over this because more factors can be considered and the "model" is self correcting based on actual sales results and loss experience.

Andy Kowalczyk

---

### **Re: Neural nets and redlining (Baube, [RISKS-16.40](#))**

*Peter J. Denning <pjd@cne.gmu.edu>  
Mon, 12 Sep 94 12:41:10 EDT*

F. Baube speculates that a neural net might hide an unlawful decision-process. Two comments on this:

1. A neural net -- indeed any other machine whether in black box or not -- cannot "be responsible" for actions that break the law. In Baube's example, it is the loan officer who makes the declaration that the loan is granted (or not), not the neural net. It is on the loan-officer's authority that the loan is granted; the machine has no authority at all.
2. It is easy enough to test whether a black box machine (e.g., a neural net) is breaking the law. One subjects it to a battery of test cases and sees what it is advising. In Baube's example, it would be statistically easy to determine if there is probable cause to believe the loan officer is engaging in redlining by relying on the advice of the machine. Such tests can be performed even if the "training set" has been lost.

Peter Denning

## neural redlining

*Fernando Pereira <pereira@research.att.com>*

*Mon, 12 Sep 1994 19:14:34 -0400*

Fred's comments will hold not only of neural nets but of any decision model trained from data (eg. Bayesian models, decision trees). It's just an instance of the old "gigo" phenomenon in statistical modeling. It is true that with neural nets is that they typically have so many parameters that it is difficult to "blame" a particular parameter setting for particular decisions. However, proper evaluation of complex statistical models cannot depend on examining particular parameter values anyway. Instead, evaluation requires the behavior of the model on held-out test data to be documented, and the test data to be made available for verification and certification purposes.

If the model has acquired biases from its training data, those should be inferrable from its performance on its test data or new test sets, and the original developer should be held responsible for those biases. In the same way as ignorance of the law is not an excuse for breaking it, bad choice of training data is not an excuse. For example, if the data comes from the decisions of human beings (eg. loan officers) on particular cases, a lot of care must be exercised to ensure that those decisions are not affected by prejudice or confusion, rather than by examination of outcomes. On the other hand, if the data is derived from outcomes (eg., for loans, cases that ended in default vs cases that didn't, for loans with similar terms) and there is reasonable statistical coverage of all relevant case types, the model developer may be able to reasonably certify that any hidden correlations that the system discovers (eg. between location and default rates) are not demonstrations of intent to discriminate.

Overall, the whole issue of evaluation, let alone certification and legal standing, of complex statistical models is still very much open. The traditional machinery of linear or log-linear statistics does not apply directly to nonlinear models such as neural nets or decision trees, so for example it is difficult in general to compute model error estimates, and thus the only source of such estimates is performance on test data. Unfortunately, these difficulties are often swept under the carpet in the hype that surrounds neural nets and allied methods.

(This reminds me of a possibly apocryphal story of problems with biased data in neural net training. Some US defense contractor had supposedly trained a neural net to find tanks in scenes. The reported performance was excellent, with even camouflaged tanks mostly hidden in vegetation being spotted. However, when the net was tested on yet a new set of images supplied by the client, the net did not do better than chance. After an embarrassing investigation, it turned out that all the tank images in the original training and test sets had very different average intensity than the non-tank images, and thus the net had just learned to discriminate between two image intensity levels. Does anyone know if this actually happened, is it just in the neural net "urban folklore"?)

Fernando Pereira 2D-447, AT&T Bell Laboratories 600 Mountain Ave, PO Box 636  
Murray Hill, NJ 07974-0636 pereira@research.att.com

---

## RE: Neural Redlining == Plausible Deniability ?

"Thomas E. Janzen" <tej@world.std.com>  
Mon, 12 Sep 1994 19:40:52 +0059 (EDT)

F. Baube was concerned that a disingenuous bank might use a neural network trained to redline loans, and then destroy the training materials to hide the intent.

Why would artificial neural networks have this advantage over the biological ones that banks have used to redline mortgages with for years? A human loan officer could be trained with redline-based materials which were later destroyed. Human neural nets are also opaque, although they often seem transparent.

Tom

Tom Janzen - tej@world.std.com Real-time C, unix, VMS, AmigaDOS, Musical software, writer. See my video Dilettante at the DeCordova near Boston.

---

## Re: Neural Redlining == Plausible Deniability ? ([RISKS-16.40](#))

Jan Vorbrueggen <jan@neuroinformatik.ruhr-uni-bochum.de>  
Tue, 13 Sep 1994 12:25:34 +0200

The decision-making process isn't really opaque. There are techniques for running a standard, feed-forward net "backwards", which will tell you what types of input are required in order to get the desired output. If you do this systematically, you can easily evaluate which areas of the input space result in a certain decision.

Sure, if the training set contained redlining, the net would learn it - but that's part of the job, isn't it? Any other statistical technique (and in this case, a net trained by, e.g., backpropagation is just a non-parametric estimator) would suffer from the exact same problem. In both cases, the original data of which rules or weights are based could be hidden or destroyed.

Jan Vorbrueggen, Institut f. Neuroinformatik, Ruhr-Universität Bochum  
jan@neuroinformatik.ruhr-uni-bochum.de

---

## Re: Neural Redlining == Plausible Deniability ?

<Bob\_Frankston@frankston.com>  
Fri, 16 Sep 1994 11:12 -0400

But we already use a neural net for redlining -- the human brain which can hide all sorts of reasoning and, more likely, alternatives to reasoning. One

of the big issues in red-lining and other areas where social policy meets business policy is that the argument is often over results and premises. More to the to the point the same issue occurs when business policy meets business policy.

The opacity of neural nets reasoning is still an issue. Though, perhaps, more of an issue when trying to build systems with reproducible results. In general, however opacity can be a result of any complex system.

---

### **Re: Neural Redlining == Plausible Deniability ?**

*John Turnbull <turnbull@turnbull.wariat.org>*

*Sun, 18 Sep 94 20:27 EDT*

I remember a case similar to this coming to light in England about 7 years ago. It was in relation to a medical school that was using some form of artificial intelligence program to screen applicants. One item of data that was not available to the program was the race of the applicant, which should have helped ensure a relatively unbiased decision. However after complaints and some investigation it was determined that length of last name did have an effect on the outcome, and it was deemed that it was there because many students of, among others, Indian descent have significantly longer last names than the Anglo-Saxon applicants. So, it seems even this method can be caught, but obviously requires careful study to determine.

John Turnbull



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 16: Issue 42

Friday 23 September 1994

## Contents

- [Power Outage in Russia?](#)  
[Bradford Wetmore](#)
  - [The Future of the Internet is Secure: Press Conference](#)  
[Winn Schwartau](#)
  - [Telephone background noise RISKS](#)  
[Michael P. Gerlek](#)
  - [Re: Uninterruptable Thought Patterns](#)  
[A. Padgett Peterson](#)
  - [Re: Computer disk crash causes misprinted ballots](#)  
[Douglas W. Jones](#)
  - [Re: Yet More daring tales of address disasters!](#)  
[Steve Bellovin et al.](#)
  - [Re: Address disasters](#)  
[John Cantrell](#)  
[Martin Ewing](#)
  - [Re: Highest Quality Company Logos](#)  
[Jim Prall](#)  
[Gary Greene](#)  
[Ray T. Stevens](#)
  - [Call For Papers: 8th IEEE Computer Security Foundations Workshop 1994](#)  
[Li Gong](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

### Power Outage in Russia?

*Brad R. Wetmore <[Bradford.Wetmore@ebay.sun.com](mailto:Bradford.Wetmore@ebay.sun.com)>*

*Fri, 23 Sep 1994 13:10:08 -0700*

Did you hear about the plug getting pulled in Russia at a major missile site not too long ago? Apparently, the folks in charge didn't pay their electric bill, so the company cut them off...backup generators took over. One wonders what happens if they also don't pay their rent...? :)

It was in The New York Times not too long ago, and in the San Jose Murky News

this morning, Fri the 23rd.

Brad R. Wetmore, Computer Security Engineer, Sun Federal, Inc. MS UMIL06-94  
2550 Garcia Ave., Mountain View, CA 94043-1100 (408) 276-5557 ext, x35557 int

[The answer to Brad's wonder: rent asunder instead of rent us under. PGN]

---

## The Future of the Internet is Secure: Press Conference

"Winn Schwartau" <p00506@psilink.com>

Fri, 23 Sep 94 12:58:12 -0500

The Future of the Internet is Secure!  
On October 11, 1994, The Internet Will Become  
A Safe Place To Do Business.

Sidewinder:  
Internet Security That Strikes Back

The Internet is a dangerous place. Ask anyone.

- \* Between 85-97% of all computer break-ins go undetected.
- \* Industrial espionage is up 400% since the late 1980's.
- \* Hacker attacks increase exponentially.
- \* Over 1 million computer break-ins last year alone.
- \* Theft of confidential information costs billions to America's financial infrastructure.
- \* Privacy is almost nonexistent.

Yet, the Internet is the fastest growing segment of the National Information Infrastructure. Over 20 million users and businesses conduct global affairs on the Internet today, and over 125 million will by the year 2000.

Join us to witness the technological breakthrough in internetworking that finally makes the Internet a safe place to be.

The future of the Internet is secure.  
Come see how.

October 11, 1994  
10:00 AM  
National Press Club  
Zenger Room  
529 14St. NW  
Washington, DC 20045  
\_Continental Breakfast\_  
RSVP

Presented by:  
Secure Computing Corporation  
2675 Long Lake Road

Roseville, MN 55112

For more information contact:

Interpact, Inc., Winn Schwartau, 813.393.6600 P00506@Psilink.Com

Secure Computing: Kevin Sorensen, 1.612.627.2800, 1.800.692.LOCK  
Sorensen@Sctc.Com

---

## telephone background noise RISKS

"Michael P. Gerlek" <gerlek@dat.cse.ogi.edu>

Thu, 22 Sep 1994 13:57:26 -0700

Just another horror story:

I called a major airline the other day to make reservations. In the course of my dialog with the agent she put me on hold for a minute or so while she checked something, and I listened to the usual canned music interspersed with promos for the airline. Then, after more dialog with the agent, again she put me on hold... but this time didn't switch on the music.

As I waited, I could clearly make out another reservations agent working in the background: "yes, Mr. Smith, flight 234 from Portland to San Francisco..."

---

## Re: Uninterruptable Thought Patterns (Agre, [RISKS-16.41](#))

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>

Fri, 23 Sep 94 15:23:12 -0400

The falling ladder problem reminded me of something that happened at a facility I was working at in Texas a number of years ago. Disaster planning was taken very seriously and the facility had an emergency diesel generator \*and\* backup battery supplies to hold the data center up in case the diesel was hard to start.

Except for the dump truck that lost control while descending a rise, left the road and slammed into the adjacent power pole.

The pole broke off at the base and fell onto the generator building, doing grievous damage to the generator. The broken engine cooling & fuel lines added to broken water mains to flood the battery room with a noxious mess (the engine bay had a fuel loss containment system but it was not designed to cope with a water main). Along the way, the fire control system triggered adding to the mayhem.

Needless to say, the data center lost power rather suddenly.

Padgett

[Rube Goldberg Strikes Again! PGN]

---

## **Re: Computer disk crash causes misprinted ballots**

*Douglas W. Jones <jones@pyrite.cs.uiowa.edu>*

*22 Sep 1994 19:10:18 GMT*

Lani Teshima-Miller, writing on Tue, 13 Sep 1994, commented on a computer crash that led to misprinted ballots. I'm a member of the Iowa State Commission on Electronic Voting Machines (actually, the name is longer) -- we oversee the approval by the state of voting systems. Anyway ...

Last night, as it happens, I was reading the Federal Election Commission standards document for electronic voting machinery, and I note that these standards are generally very well thought out. There were a few places where, if anything, they seemed to require excessively expensive solutions to problems, but few places where they seemed to be open to failures.

The standards mandate considerable fault tolerance in the systems actually installed in polling places, whether they be mark-sense machines, punched card machines, or direct recording computerized voting systems. These have a serious real-time response requirement -- they must work on election day, all day.

The standards do not mandate a similar degree of fault-tolerance in off-line systems, such as those used to prepare ballots. What they do mandate is a clear audit trail and strong safeguards against tampering. In addition, they mandate provisions for many manual checks. It is in the latter area where the system in Hawaii clearly failed!

On taking delivery of a shipment of printed ballots, they should have been inspected -- this means examining a sample ballot from every press run, preferably from both ends of the run! (Different press runs may have required different ballot layouts, for example, by permuting the orders of candidate names, as required in some contexts). Furthermore, the workers at the polling places, at setup time, are required to perform certain inspection tasks, for example, by assuring themselves that the voting machine counters are all reset to zero.

The system seems to be designed well; this error in Hawaii seems to be a human error. The risk we face is complacency "it's all computerized, these checks in the system are just bureaucratic requirements, nothing ever goes wrong, so we can skip this". One of the fundamental requirements of a democratic system is a corps of election workers who take the requirements for running an honest election very seriously! I cannot imagine any way to use automation to eliminate this requirement.

Doug Jones jones@cs.uiowa.edu

---

## **Re: Yet More daring tales of address disasters!**

*<smb@research.att.com>*

Thu, 22 Sep 94 13:46:14 EDT

[...] He moved and sent an address correction to a company in which he holds some stock. The company acknowledged his change of address, but sent it to his \*old\* address. [...]

In fact, in this case the company did exactly the right thing. This is their mechanism for discovering forged address changes. If the request is false, the true owner will receive a notice, and can take corrective action. If the request is genuine, the Post Office will forward the acknowledgment to the proper place.

--Steve Bellovin

[This was also noted by

Jim Horning <horning@src.dec.com>,  
Alan Miller <millera@mcs.com>,  
Craig\_Everhart@transarc.com,  
Martin Ewing <martin.ewing@yale.edu>,  
Robert.L.Drysdale@dartmouth.edu,  
Patricia Shanahan <pats@equalizer.cray.com>,  
Nevin Liber <nevin@cs.arizona.edu>,  
James E. Leinweber <jiml@stovall.slh.wisc.edu>,  
ROBINSON\_PAUL@tandem.com,  
Crystal Linn Trexel <ct2f+@andrew.cmu.edu>,  
Clark <MERRILL@stsci.edu>,  
John Sullivan <sullivan@geom.umn.edu>,  
Jim Berets <jberets@bbn.com>,  
Geoff Kuenning <geoff@ficus.cs.ucla.edu>,

and they are still coming in... But thus far NO ONE remarked on the problem that a bogus Change of Address form previously sent to the local Post Office would result in the acknowledgment being forwarded to the imposter instead of the victim. Correction:

Just after I wrote the above lines, I found a note from

Charles Reichley <creichley@VNET.IBM.COM>,  
who suggested that the acknowledgement should be sent to BOTH the OLD and NEW addresses. Congratulations to Charles, who gets the RISKS-ALERTNESS prize for today. PGN]

---

## Re: Address disasters

John Cantrell <cantrell@sparky1.aero.org>

Thu, 22 Sep 94 12:21:31 PDT

After reading Paul T. Keener's comment about a friend's receiving a change of address acknowledgement from a company that was sent to his \*old\* address, I was overcome with *deja vu*.

Wasn't it here in RISKS that I read about the scam of changing the address for your credit-card bills so a thief could run up \$\$\$\$ without your ever knowing about it (until it was too late, that is)?

I would rather get the info at the old address and then forwarded by the post

office than run the risk of having to correct an "unauthorized" change of address with the trouble that goes with it.

cantrell@aero.org

---

## Postal address disasters

*Martin Ewing <martin.ewing@yale.edu>*

*Thu, 22 Sep 1994 15:22:27 -0400*

[...] We had a related problem recently, when the US Post Office decided on its own to return all our mail with a yellow computer-printed sticker saying "Addressee moved - no forwarding address". We only found out when my parents called up to ask where we had gone. Of course, our mail box being empty for several days was definitely suspicious. Our credit card company thought we'd absconded, when they got their statement back, and there were other unpleasant effects.

The P.O. was non-repentant, saying only they had had a new man on the route. At least they didn't blame it on the computer.

-Martin Ewing (martin.ewing@yale.edu) Yale University

---

## Re: Highest Quality Company Logos (Lawrence, [RISKS-16.41](#))

*Jim Prall <sq!trigraph!jimp@uunet.uu.net>*

*Fri, 16 Sep 1994 14:15:09 -0400*

>What a wonderful gift for con artists!

Well, it's not as crazy as it sound. Lots of stores use the logos and company identities of their suppliers in advertising. E.g. if WalMart sells, say, Timex watches, their flyer uses the official Timex logo on ads on the watch page.

Service bureaus can get a substantial amount of work creating good, clean, accurate electronic versions of such corporate identities for such advertisers. Once in a while a corporation actually supplies its corporate identity in electronic form, but so far this is rare. More common is a printed identity book with specs and samples for several fixed sizes, vertical and horizontal arrangement, and the Pantone color specs for corporate colors. Also common is trying to get by working from old output; this makes a lot harder to get a clean electronic logo.

Heaven help the creative director who starts to get creative with a supplier's corporate identity. This is greatly frowned upon. The one risk is not knowing the trade standards. If you display another company's identity, you better match it 100%.

Jim Prall, Trigraph, Inc., Toronto, CANADA [jimp%trigraph.uucp@csri.utoronto.ca](mailto:jimp%trigraph.uucp@csri.utoronto.ca)

---

**Re: Digital Logos (Denning [RISKS-16.41](#) on Lawrence, [RISKS-16.40](#))**

Gary Greene <garyg@unity.sj.unisys.com>  
23 Sep 1994 17:11:02 GMT

Peter Denning writes:

> ... If TigerDirect has the explicit permission of the owners of  
>the logos, all is well. If not, then not only they, but anyone else using  
>the logo without authorization, is breaking the law. Anyone who would use  
>a logo, authorization or no, to commit a fraud is also breaking the law.

What Peter says is technically true but ignores the doctrine of "fair use."  
I've been a graphic artist for over 25 years. Throughout that time there have  
been clip-art books, either print and lately digital that provide libraries of  
such logos for use in authorized situations. Virtually all such books I am  
aware of get their material directly from the trademark owners and therefore  
are authorized, but a few have not.

A company certainly may impose and require that their logo not be distributed  
within the trade in this manner. But what does that gain them? Then they  
must supply such clip art to the artist. In practice, many people authorized  
to let advertising or some other use do not have easy access to their  
company's style sheets, or simply don't think to provide them. When the  
advertising is created in-house this is not a problem since the art department  
always has access to the style sheets, but a great deal of advertising is  
created by contractors and specialty houses.

When that happens the artist is reduced to drawing them from memory or  
making a fuzzy copy from the yellow pages. Drawing from memory is usually  
unsatisfactory. The yellow pages are hardly much better. And I have often  
done both in my time. Inclusion of such logos in a library is usually  
considered "fair use" under the copyright law unless the copyright owner  
specifically objects to the publisher. Only the subsequent unauthorized  
reuse of the logo in a specific advertisement or other publication would  
constitute a violation of copyright and/or trademark. Further, there are  
other "fair use" situations that are also excepted, such as news and  
personal photography (Amtrak derails! ...accompanied by footage of an  
Amtrak emblazoned passenger car on its side... News at 11).

I will reiterate what Peter very rightly points out: anyone using a company's  
logo in a fraudulent manner is breaking the law.

Gary Greene            Santa Clara, CA.

---

**Re: Digital Logos (Peter J Denning, [Risks 16.41](#))**

"Ray T. Stevens" <74074.1746@compuserve.com>  
22 Sep 94 20:06:22 EDT

It may very well be that the DISTRIBUTION of these logos without the owner's

permission is legal [although USE may not be]. It would take a lawyer to figure it out (and most likely two lawyers to make a debate on the subject). In the printing industry we get books of clip art, and some of these books contain a large number of Logos. I can't believe that the people putting out the books really got permission from everyone. In fact, all of these books that contain trademarks contain a disclaimer that says in legal gibberish that you and darn well better have permission from the trademark holder before using them.

The real risk I see is to the user who may not realize what they need to do in order to be legal. This is another case where technology has brought a tool, which in the past required a specialist, directly to the users without bringing with it the knowledge of using it properly.

[This interpretation may indeed violate copyright law. However, we are drifting beyond the scope of RISKS... PGN]

---

## Call For Papers: 8th IEEE Computer Security Foundations Workshop 1994

*Li Gong <gong@csl.sri.com>*

*Thu, 22 Sep 94 15:45:53 -0700*

Call For Papers  
8th IEEE Computer Security Foundations Workshop  
June 13-15, 1995  
County Kerry, Ireland  
Sponsored by the IEEE Computer Society

This workshop series brings together researchers in computer science to examine foundational issues in computer security. We are interested both in papers that describe new results in the theories of computer security and in papers and panels that explore open questions and raise fundamental concerns about existing theories.

Possible topics include, but are not limited to:

access control authentication data and system integrity  
database security network security distributed systems security  
security protocols security models formal methods for security  
as well as foundational issues relating to other critical system  
properties and in emerging areas such as ubiquitous computing.

The proceedings are published by the IEEE Computer Society and will be available at the workshop. Selected papers will be invited for submission to the Journal of Computer Security.

Instructions for Participants: Workshop attendance will be by invitation only and limited to about 35 participants. Prospective participants should send 5 copies of a paper (limit 7500 words) or proposal for panel discussion to Li Gong at the address below. Please clearly identify the contact author and provide email addresses and telephone numbers (both voice and fax).

Important Dates: Author's submission: February 3, 1995

Notification of acceptance: March 14, 1995  
Camera-ready final papers: April 3, 1995

Workshop Location: The Computer Security Foundations Workshop is known for its peaceful rural setting, and in 1995 the workshop will be held at Dromquinna Manor, County Kerry, which is situated on the South West coast of Ireland. Built in 1850, and located in quiet picturesque countryside about 3 miles from Kenmare town, Dromquinna Manor has its own private grounds of woodland and lawns that sweep down to the sea. The South West coast of Ireland claims some of the most varied and spectacular scenery in the country, and the coastline, sculptured by the ice-age and influenced by the warm waters of the Gulf Stream, is steeped in ancient history and folklore. This mountainous area has an abundance of natural beauty and is enriched by sub-tropical flora produced by the unusually warm and temperate climate.

The nearest international airports are Shannon and Cork. There are direct flights from North America to Shannon and Dublin, and from major European cities (for example, London and Amsterdam) to Cork. Connections from many other cities can be best made by using London or Amsterdam or by availing of the scheduled services from Dublin to Cork. There are also car/passenger ferries from the United Kingdom and Europe to Cork, Dublin and Rosslare.

For further information contact:

General Chair	Program Chair	Publications Chair
Simon Foley	Li Gong	Joshua Guttman
Dept of Computer Science University College Cork Ireland	SRI Computer Science Lab 333 Ravenswood Avenue Menlo Park, CA 94025 U.S.A.	The MITRE Corp. 202 Burlington Road Bedford, MA 01730-1420 U.S.A.
+353 21-276871 x2929 s.foley@cs.ucc.ie	+1 415-859-3232 gong@csl.sri.com	+1 617-271-2654 guttman@mitre.org

More information at <http://www.csl.sri.com/ieee-csfw/csfw.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 16: Issue 43**

**Tues 27 September 1994**

## Contents

- [Pretty Bad Privacy in Top-Level Negotiations](#)  
[Charles Dunlop](#)
- [Re: Mexico election](#)  
[H?vard Hegna](#)
- [Coyote sues Acme Co.](#)  
[Luis Fernandes](#)
- [Reasoning 101, the FBI Telecom Bill, and EPIC](#)  
[Jerry Leichter](#)  
[Marc Rotenberg](#)
- [Please!, let's call it the "Government Wiretap Bill" !!!](#)  
[Jim Warren](#)
- [The high-tech university: 500 channels, all alike](#)  
[Phil Agre](#)
- [Pagers and power supplies](#)  
[Laszlo Nemeth](#)
- [Marketing of science](#)  
[Michael Jampel](#)
- [Power Disasters](#)  
[Matthew D. Healy](#)
- [Re: Power Outage in Russia?](#)  
[Arthur D. Flatau](#)
- [Questions re: security of computerized medical records](#)  
[Richard Goldstein](#)
- [Network Security Observations](#)  
[NSO](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Pretty Bad Privacy in Top-Level Negotiations

"Charles Dunlop" <[cdunlop@spruce.flint.umich.edu](mailto:cdunlop@spruce.flint.umich.edu)>  
Sun, 25 Sep 1994 18:43:58 -0400

\_Business Week\_ (October 3, 1994) has obtained a tape of two telephone calls made by an aide to Jimmy Carter on September 18 during negotiations over

Haiti. The calls were made over an unsecured radio link from Port- au-Prince to Carter's plane -- one to a National Security Council staff person, and the other to Carter himself. Shown transcripts of the calls during a CNN interview, Carter responded that he was "taken aback", and commented "Now I see what happened to Prince Charles".

[I guess that some public figures still haven't see the air of their waves.]

C.E.M. Dunlop, Philosophy Department, University of Michigan, Flint  
Flint, Michigan 48502-2186 (810) 762-3380 cdunlop@umich.edu

---

### Re: Mexico election (Sullivan, [RISKS-16.36](#))

*H?vard Hegna <Havard.Hegna@nr.no>*

*Mon, 26 Sep 1994 09:57:15 +0100*

John Sullivan quotes IFE (Federal Electoral Institute) officials who deny there were problems with the computer system but continues an investigation on an apparent effort to infiltrate a computer virus into the main computer system.

In Norwegian newspaper Aftenposten on August 26., the election is reported as "a great step forward for Mexican democracy" with a turnout of 75% of the 45 mill. electorate, as compared to the normal 50%.

In a report from Mexico on The Norwegian Broadcasting System (NRK) Radio Program 2 (P2) on Saturday August 27., Joar Hoel Larsen quotes a professor in political science at UNAM (?) Louis Javier Garrido who claims that the means for rigging an election are much more sophisticated now than ever before. With todays computers and networks one person in the right spot can easily manipulate a whole election, something which would require an army of election officials in the earlier primitive systems employed.

Larsen's view was that the Mexicans really wanted to make the election open and fair this time, and had control rules on election day that bordered on the paranoid and went a lot further than procedures that are considered quite acceptable in for instance Norway. So there were few irregularities reported at the voting stations. Instead, according to professor Garrido, the manipulation was done at the electorate registry level. 7-8 mill. voters from districts that were known to have a clear majority in opposition to the ruling PRI party, were removed from the electorate. Not everybody, but the necessary percentage from each such district.

The result was a normal turn-out (percentage-wise) and the normal majority in these districts, but their influence on the totals was reduced. Resulting in the PRI staying in power. Again according to Garrido, a serious political independent who is not a member of the loosing PRD, says Larsen.

I have seen reports of complaints on the Mexican election in various media, but very little mention of this accusation. Has it been reported elsewhere? Does it have any substance?

Does anybody know what kind of computerized system was used in Mexico this time, before, during and after the election? Any Direct Recording Equipment?

Hevard Hegna, Norwegian Computing Center, P.O. Box 114, Blindern, 0314 Oslo, Norway (+47) 22 85 25 00/ (+47) 22 85 26 21 Fax : (+47) 22 69 76 60

---

## **Coyote sues Acme Co.**

*Luis Fernandes <elf@eccles.ee.ryerson.ca>  
Sat, 24 Sep 1994 13:18:34 +0500*

What follows is an excerpt of an article that appeared in the 26 Feb 1990 issue of "The New Yorker" magazine.

Specifically, the article is about a suit brought against Acme Company, incorporated in Delaware, by Wile E. Coyote who lives in the Arizona Desert and is seeking, "compensation for personal injuries, loss of business income, and mental suffering caused as a direct result the actions and/or gross negligence of said company's... mail-order department..."

The article illustrates the RISKS of operating badly documented and labeled equipment; the RISKS of using improperly designed equipment, and the RISKS of using equipment for unintended purposes.

This is a quote from the opening statement of Mr. Coyote's attorney:

Mr. Coyote states that on December 13th he received of Defendant via parcel post one Acme Rocket Sled. The intention of Mr. Coyote was to use the Rocket Sled to aid him in pursuit of his prey. Upon receipt of the Rocket Sled Mr. Coyote removed it from its wooden shipping crate and, sighting his prey in the distance, activated the ignition. As Mr. Coyote gripped the handlebars, the Rocket Sled accelerated with such sudden and precipitate force as to stretch Mr. Coyote's fore-limbs to a length of fifty feet. Subsequently, the rest of Mr. Coyote's body shot forward with a violent jolt, causing severe strain to his back and neck and placing him unexpectedly astride the Rocket Sled. Disappearing over the horizon at such speed as to leave a diminishing jet trail along his path, the Rocket Sled soon brought Mr. Coyote abreast of his prey. At that moment the animal he was pursuing veered sharply to the right. Mr. Coyote vigorously attempted to follow this maneuver but was unable to do so, due to poorly designed steering and a faulty or nonexistent braking system. Shortly thereafter, the unchecked progress of the Rocket Sled brought it and Mr. Coyote into collision with the side of a mesa.

In another incident, Coyote purchased a pair of rocket skates which, his attorney claims, Acme sold without sufficient caveat and with "little or no provision for passenger safety", because the design attached very powerful jet-engines to "inadequate vehicles"; i.e. the roller-skates.

Other products, manufactured by Acme, that have caused Mr. Coyote great

anguish include: itching-powder, giant kites, Burmese tiger traps, anvils, and two-hundred-foot-long rubber bands.

RISKS readers are advised to be cautious with products purchased from the Acme Mail-Order Catalog and especially with explosives purchased from the Acme Mail-Order Explosives Catalog; the explosives tend to detonate prematurely very possibly due to the use of faulty primer-cord.

(If ever there was a candidate suitable for the role of RISKS mascot, Wile E. Coyote is that animal.)

---

## Reasoning 101, the FBI Telecom Bill, and EPIC

*Jerry Leichter <leichter@lrw.com>*

*Fri, 23 Sep 94 17:59:42 EDT*

Marc Rotenberg quotes a 1992 GSA report that the FBI's proposals for access requirements to the telephone system would have an adverse impact on national security. He says this speaking for the "100 Reasons ... project of the Electronic Privacy Information Center [EPIC]".

I haven't read the GSA report in question, but from context and the parts quoted by Rotenberg, it seems clear that the particular issue concerning GSA was one feature of the 1992 (1991?) version of the FBI proposal, which called for the telephone companies to link to a central, government-controlled office somewhere which would then have the ability to initiate taps anywhere without any further assistance from the telephone companies. The GSA was correct in pointing out that any breach of the security of this centrally controlled system could have serious implications. The GSA was also not alone in pointing this particular risk.

This year's version of the proposal explicitly states that tapping is to be done *\*by telephone company personnel\**, on telephone company premises (as is the case today). The central tapping facility is gone.

How shall we then classify Reason 55? A straw man attack? An appeal to emotion? (For many years, "national security" was the standard justification for almost anything the government wanted to do. Now EPIC has appropriated that battle cry.) Disingenuous? Dishonest?

At the least, if EPIC is going to quote the GSA's report, honesty requires that they quote enough context to show what the statement is based on. If their going to use an analysis of the 1992 bill, it's incumbent on *\*them\** to argue that analysis is applicable to the 1994 incarnation, which has undergone substantial changes - some of them presumably a direct result of the GSA's analysis.

In any case, proponents can as easily quote an FBI report to the effect that *\*not\** passing this bill would have an adverse effect on national security. Why should one prefer the statement of one three-letter government agency over another? Duelling appeals to authority do not rational debate make.

-- Jerry

---

## Re: Jerry Leichter's response

Marc Rotenberg <rotenberg@washofc.epic.org>

Mon, 26 Sep 1994 12:51:45 EST

There is nothing in the GSA memo that supports Jerry Leichter's interpretation. The memo did not even mention the problems associated with centralized monitoring. Although, it's good of Jerry to bring that up. <grin>

The memo is reprinted in full, along with accompanying materials, in Banisar and Rotenberg, *The Third CPSR Cryptography and Privacy Conference* (1993). The memo is also available at the CPSR ftp site. CPSR.ORG  
/cpsr/privacy/communications/wiretap/gsa\_wiretap\_memo.txt

The GSA memo contains at least *\*ten\** Reasons to oppose the wiretap plan (incompatibility, impact on federal communication networks, scope of proposed change, powers of Attorney General, national security, network security, standards, current capability, cost effectiveness, delay in development of new systems, international trade, associated costs, impact on new services).

We cited only one Reason -- national security.

A story appeared in *\*The New York Times\** when the memo was obtained (15 Jan 1993, "FBI's Proposal on Wiretaps Draws Criticism from GSA").

Quoting from the NYT article, "the GSA said the proposed legislation was unnecessary, could hurt the nation's competitiveness in the international trade arena, and posed a possible danger to national security."

Marc Rotenberg, EPIC

---

## please!, let's call it the "Government Wiretap Bill" !!!

Jim Warren <jwarren@autodesk.com>

Sun, 25 Sep 94 12:45:38 PDT

It is *\*much\** more accurate and much more provocative to call the "digital telephony" bill the "Government Wiretap Bill."

1. It helps their propaganda and harms our propaganda to call it the *"\*FBI\* Wiretap Bill."*
2. The FBI Wiretap Bill implies that only the FBI would use its access, whereas all the phrasing of the versions seems to include a catch-all like, "... and as otherwise authorized by law."
3. We need to emphasize that it's the *\*government\** that wants the snoop-n-peep power.

4. We need to point out that \*all\* levels of government can use it, "when authorized by law," of course.

---

### **The high-tech university: 500 channels, all alike**

*Phil Agre <pagre@weber.ucsd.edu>*

*Sun, 25 Sep 1994 20:04:33 -0700*

In a recent issue of Forbes, Thomas Sowell reports that he's looking forward to the day when market pressures require universities to distribute a large proportion of their lectures over video. The reference is:

Thomas Sowell, Letting in the light, Forbes, 12 September 1994, page 98.

He anticipates many advantages of this system. Among them, he says, is that professors who engage in "propaganda", "pretentious mush", "strident ideology", and "recruitment of disciples" will be caught on tape and exposed to public censure. Sowell is a conservative economist and these are all obviously code-words for the expression of political views with which conservatives disagree. This is to be expected.

But the danger that such proposals represent is independent of your political views. Imagine what this new world will be like. It will become unwise to engage in unscripted give-and-take with students, lest an ambiguous remark be placed in a foreign context by someone with video editing equipment and a political axe to grind. It will become unwise to express unpopular opinions in lectures, and even fundamentally conformist lectures will have to be structured as a series of soundbites, each of which will survive being edited into arbitrarily unfriendly contexts. University education, in other words, will be converted into television -- 500 channels, all alike, and all subject to the leveling force of external pressure.

These scenarios might seem paranoid, but one perfectly robust model for them can already be found in journalism. Substantial institutions have arisen for harassing journalists whose articles diverge from the political views of those who care to fund them. Mistakes are magnified, passages are taken out of context, and political evaluations are assembled and made available to people whose cooperation the journalist may require to gather stories. Of course, these activities are all perfectly legal and covered by the First Amendment. But they are regrettable nonetheless.

(Such practices could already be organized in universities simply through having monitors sit in on classes and forward notes to a central organization. This is indeed done on a small scale, but video recording would make it much easier.)

It will be argued (and indeed, Sowell does argue) that the warnings of college professors like me are just the self-serving obfuscations of interest groups with something to hide. But the consequences of such phenomena go far beyond the university. When work activities that were formerly conducted face-to-face start to be mediated on a large scale by digital video and other computerized telecommunications technologies, unless those communications are given vastly more statutory protection than seems at all likely, the door will

be opened to greatly intensified monitoring and regulation of those activities by anyone who has legal access to recordings of the signals. If this happens, we will realize how much slack we got from face-to-face interaction, and we will be forced to look to one another to find ways of getting it back.

Phil Agre, UCSD

---

## Pagers and power supplies

*Laszlo Nemeth <laszlo@eclipse.cs.colorado.edu>*

*Fri, 23 Sep 1994 21:01:59 -0600*

A rather humorous thing happened the other day. I was connecting up a scsi disk to a sparc 10 (nice small power supply) and had powered everything of. while leaning over the system to connect the various cables to the disk, my pager went off in vibrate mode.

I wear my pager clipped backwards in my front jeans pocket (so the nice clear face doesn't get scratched, it mutes the sound of the pager, and gives really good contact when vibrating) a very tender spot on most people.

when that pager went off I had a flashback to a time when I forgot how much power is in a sun 4/260 power supply and decided to test it with me as the path.

both times I have made it across the room before I knew what happened. From now on when a system is open, the pager is elsewhere.

laz

---

## Marketing of science

*Michael Jampel <jampel@cs.city.ac.uk>*

*Mon, 26 Sep 94 11:29 BST*

Phil Agre <pagre@weber.ucsd.edu> asked [[RISKS-16.41](#)] asked (re: uninterruptable power supplies causing power failures):

> Where do hubristic terms like "uninterruptable" come from?

They come from marketing people and sales people. Scientists and engineers often have contempt for these people, but unfortunately their mistakes and their hubris may lead to an anti-science back-lash. Therefore we can't just let them get on with it: it's not the sales people who will get the sack when a UPS proves to be interruptible; but the whole discipline of electrical engineering loses a little credibility. So next time an engineer says something like "We must not do X because it is very unsafe", it is possible that those who have been misled by advertisements will say "Yeah, yeah, what do you know." This is a risk (not of computers, but applying to any technical discipline).

Phil then added:

> I've got an "inherently safe nuclear reactor" to sell you

There is a difference between inherent safety and engineered safety. And one of the first nuclear reactors was inherently safe. It was in Sweden, called the Triga, and the opening ceremony (by Niels Bohr) consisted of removing all the cooling rods from the core. Within a minute, the reactor had stabilised, rather than starting to melt-down, due to the physical properties of the materials it was made from. (The damping effect went up exponentially with increasing temperature.) My guess is that the reason no reactors are like this is commercial, i.e. it didn't make as much power per dollar's worth of uranium, not technical. Another risk when scientists allow people they hold in contempt to do a job that doesn't interest them; the anti-nuclear power lobby has good reasons for its views, all due to mistakes made for commercial reasons. Possible end result: the whole world is condemned to lack of power when the oil runs out, because nuclear power will still be considered taboo.

Michael Jampel <jampel@cs.city.ac.uk>

---

## Power Disasters

Matthew D. Healy <healy@seviche.med.yale.edu>

24 Sep 1994 01:42:23 GMT

All the postings about various incidents in which main power and backup were both lost serve as examples of a point often missed by risk planners: the multiplicative probability rule only applies if the events are truly independent. A common mode failure can take out several "redundant" systems at once.

It's extremely difficult to design truly redundant systems.

The O'Hare incident also seems to illustrate another point. All I know about this incident is what was posted to RISKS; I gather they were doing some kind of test on the UPS.

Chernobyl was a disastrous failure triggered by a test of emergency generation capabilities! The problem was exacerbated by numerous problems in design and maintenance, but the trigger event was a misguided test of generating emergency power from the main turbines as they spun down and the diesel generators were started up.

A test is an inherently hazardous situation; various common-mode failures can be triggered by tests. Therefore one must be especially careful about scheduling and running tests!

Matthew D. Healy healy@seviche.med.yale.edu  
Postdoc, Yale School of Medicine

---

**Re: Power Outage in Russia? ([RISKS-16.42](#))**

Arthur D. Flatau <flatau@cli.com>

Mon, 26 Sep 94 11:20:28 CDT

Dave Barry (syndicated humorist) wrote an article a while back about another similar situation in Russia. The power to some military complex was shut off because the bill was not paid, the officer in charge ordered a tank be driven and parked next to the electric company building. The business end of the tank was pointed at the building and miraculously power was quickly restored.

The rest of the article was about the advantages of having a tank in resolving disputes with creditors and how one acquires the tank. The latter is done by sending in all the credit card applications one gets in the mail, acquiring enough credit and then charging the tank. When the credit card companies start demanding payments, it is easy to satisfy them because now you have a tank.

Art flatau@cli.com Computational Logic, Inc. Austin, Texas

---

### questions re: security of computerized medical records

Richard Goldstein <richgold@netcom.com>

Mon, 26 Sep 1994 07:56:04 -0700 (PDT)

I am a statistician and I sit on the Human Studies Committee (IRB) of a local HMO. I have been assigned as primary reviewer for our committee for a recently submitted protocol dealing with security issues on the HMO's computerized patient data base. (Note: this may not need committee approval under Federal rules, but it does under local rules.) I am requesting some help regarding issues I should be asking about and guidance on literature.

Brief explanation of project: the current computerized medical record has two sections (I am oversimplifying some issues here, without, I hope, being misleading): a coded section that can be searched via computer and a text section that currently cannot be automatically searched. The HMO has entered into an agreement with a 'local' university (about 90 miles away) to attempt to develop tools for exploiting clinical text data (e.g., access, search, extract, manipulate the text portion of the record).

The process includes providing the university with example records (size of sample not known), where the records have been 'sanitized'. "The sanitization process has three stages:

1. automated masking or identifiers such as addresses and telephone numbers in ... extract headers as created [at the HMO]
2. automated masking of medical record numbers
3. automated masking of each segment of each member's name everywhere these segments occur in the ... extract"

There are some known problems with this masking (e.g., regarding the occurrence of names in the record other than than of the particular patient). My problem is that I have no idea how much faith, trust, etc. to put into the "automated masking" process. Of particular help would be guidance on what

questions to ask about this process to help make decisions about whether it is sufficient (guidance on literature would also be appreciated).

I note also that the people on the project appear to be unaware of the possibility of identifying patients via combinations of coded information. As a statistician, I am aware of some of the large literature on this question, especially with respect to Census information. However, I am not familiar with recent literature on this question or with computer algorithms; further, I am not aware of any literature dealing specifically with this question for medical records (except that I do have a copy of the 9/93 publication from the Office of Technology Assessment entitled *Protecting Privacy in Computerized Medical Information*; however, this is not a technical publication).

Another question relates to what we should be asking about the security of the university computer; we have been told that the center "has implemented data access security by granting electronic access to [HMO] data only to researchers designated as members of the [HMO] project." However, we have been provided with NO details; again, what questions should we be asking and how do we interpret the responses.

I should mention that our committee very strongly opposes any movement of HMO data outside the HMO, but in rare circumstances we have agreed when we were satisfied with the security situation (usually a stand-alone computer in a room that could easily be locked).

Any help or advice would be greatly appreciated and should, preferably, be sent directly to me at "richgold@netcom.com". If desired, I could post a summary of the resulting responses to this group.

Rich Goldstein

---

## Network Security Observations

*Network Security Observations <NSO@delphi.com>*

*Tue, 27 Sep 1994 05:21:00 -0400 (EDT)*

November 1994 NETWORK SECURITY OBSERVATIONS will be out with its inaugural issue. NETWORK SECURITY OBSERVATIONS is expected to be the leading international journal on computer network security for the science, research and professional community. Every annual volume contains five issues, each offering ample space for vigorously reviewed academic and research papers of significant and lasting importance, and a wealth of other network security information, including security patches and other technical information supplied by manufacturers, related governmental documents (international), discussions about ethics and privacy aspects, the Clipper chip and other cryptologic issues, viruses, privacy enhanced mail, protocols, harmonization of computer security evaluation criteria, information security management, access management, transborder data flow, EDI security, risk analysis, trusted systems, mission critical applications, integrity issues, computer abuse and computer crime, etc. etc.

If and when appropriate reports of major international conferences, congresses

and seminars will be included, as well as information made available by governments, agencies, and international and supra national organizations. Network Security Observations is published in the English language, and distributed Worldwide. The publication does NOT feature commercial announcements. National and international organizers of dedicated conferences, etc. can offer calls for papers and invitations to participate. Relevant posting from other publishers announcing new relevant books, etc are welcomed as well.

NETWORK SECURITY OBSERVATIONS provides the in depth and detailed look that is essential for the network system operator, network system administrator, edp auditor, legal counsel, computer science researcher, network security manager, product developer, forensic data expert, legislator, public prosecutor, etc., including the wide range of specialists in the intelligence community, the investigative branches and the military, the financial services industry and the banking community, the public services, the telecom industry and the computer industry itself.

Subscription applications by email or fax before November 1, 1994 are entitled to a special rebated subscription rate. Special academic/educational discounts, and rebates for governmental personnel, and other special groups, are available upon request. Network Security Observations is a not-for-profit journal, and therefore we are sorry to reject requests for trial orders.

For further information please contact:

by email> NSO@delphi.com

Or by fax> +1 202 429 9574

Or alternatively you can write to:

Network Security Observations, Suite 400, 1825 I Street, NW  
Washington DC, 20006, United States



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 16: Issue 44**

**Thus 29 September 1994**

## Contents

- [Re: Neural Redlining == Plausible Deniability ?](#)  
[Jim Horning on Brian Randell](#)
- [Response to various comments on Internet Security](#)  
[Winn Schwartau](#)
- [Present Internet Security](#)  
[George Thornton](#)
- [Re: Mexico election](#)  
[Alex Lopez-Ortiz](#)
- [Re: Uninterruptables](#)  
[Phil Agre](#)  
[Martyn Thomas](#)
- [Safety issues with Screen Savers](#)  
[Rich Baker](#)
- [Re: Phil Agre on high-tech university](#)  
[Robert Ashcroft](#)
- [Re: Neural networks and testing](#)  
[Fred Cohen](#)
- [Re: Yet More daring tales of address disasters!](#)  
[Dan Fass](#)  
[Andrew Marc Greene](#)  
[Steve Summit](#)  
[Jan Mandel](#)  
[Jonathan I. Kamens](#)  
[Mike Crawford](#)  
[Chris Smith](#)  
[Paul Robinson](#)  
[Michael Jampel](#)
- [Privacy & American Business conference in DC next week](#)  
[Lance J. Hoffman](#)
- [Info on RISKS \(comp.risks\)](#)

---

**Re: Neural Redlining == Plausible Deniability ? ([RISKS-16.40](#))**

<[horning@src.dec.com](mailto:horning@src.dec.com)>

*Mon, 26 Sep 94 17:40:08 -0700*

Brian Randell's posts to early volumes of RISKS about the St. George's medical school scandal are quite pertinent here. They are well worth re-reading in their entirety from the RISKS archives ([RISKS-4.27](#) and 6.34). I give only the highlights here:

"Leading medical schools face an investigation into allegations that they are discriminating against women and black students. This follows the discovery by two consultants that their own school, St. George's in south London, has been using a computer selection programme which deliberately down grades applicants if they are female and non-white...

"The St. George's claim is particularly worrying because the school has a better record on discrimination than most other colleges. The computer selection programme was designed to mimic the decisions of the school's panel which screened applicants to see who merited an interview. It matched the panel's results so closely that the panel was scrapped and for several years all St. George's applicants have been screened by computer...

"St George's was caught, officials admit, only because the attitudes of its selectors in years gone by were enshrined in a computer program: that program deliberately downgraded non-Caucasians and women...

"Being non-Caucasian, and or a women, resulted in a lower grade on the interview scale: simply having a non-European name could take 15 points off an applicant's score. Sex had less effect: on average, being female took no more than three points off the score. That was enough, the Commission found in its investigation, to deprive 60 candidates a year of the interviews for which they should have qualified...

"In fact, since the program mimicked the previous human assessors, it is probable that discrimination occurred before the program was introduced, the report says...

"In November 1986, Dr Collier discovered, by accident, that the program was weighted. He wrote to the dean. Dr West asked Mr Evans to run a few cases through the program. When he saw the effect, he immediately stopped its use."

Jim H.

---

## **Response to various comments on Internet Security ([RISKS-16.42](#))**

*"Winn Schwartau" <p00506@psilink.com>*

*Thu, 29 Sep 94 11:53:25 -0500*

[MODERATOR'S NOTE: I have omitted several of the flames that attacked Winn for the perceived high hype of his press-conference note in [RISKS-16.42](#). I ran his message because I know enough about the underlying technology to have some significant hope that the system will do something useful. But excessive hype always tends to be offputting. PGN]

We understand a handful of RISKS readers wanted to know the sources of some fascinating data we recently published in a Press Conference announcement. Here goes.

The 85-97% figure came from Jim Settle, former Head of the Computer Crime Squad, FBI. These are the figures he cited on "Under Scrutiny," an FX channel (Fox network) TV show where he appeared with Robert Steele of Open Source Solutions and Chris Goggans, 'national resource hacker.' One government study he mentioned cites the higher figure of 97% of all computer intrusions go undetected. Settle also said that the experience of the FBI Computer Crime Squad is in excess of 85% computer intrusions go undetected.

The million plus computer breakins figure came from USA Research as reported by Information Week. The industrial espionage figure is from Parvus and Assoc. - an international Private Investigation company who specialize in high tech commercial espionage - and ASIS, American Society for Industrial Security representing the findings of a study into this area: (The figures are for 1985 through 1991.)

- \* Foreign sponsored information theft is up 400%
- \* US sponsored industrial espionage is up 260%

According to the Washington Post, as of April 1993, the industrial espionage case load of the FBI was up a whopping 500%!

The billions of dollars that espionage costs the US econotechnical infrastructure is well documented in Schwartau's book, "Information Warfare: Chaos on the Electronic Superhighway," available anywhere. Take a read.

We hope this settles any misunderstandings on the part of RISKS readers.

Kevin Sorensen, Secure Computing, Inc.  
Winn Schwartau, Interpact, Inc. P00506@Psilink.Com

[Winn's message actually said "Information Warefare", which is sort of a nice pun, but he meant to write "Information Warfare". PGN]

---

## Present Internet Security

*George Thornton <dgthornton@v-one.com>  
Wed, 28 Sep 1994 12:15:25 GMT*

I noticed [RISKS-16.42](#) contained the announcement for Internet security, and thus wish to append my own such announcement. Not to upstage such a fine organization but such solutions to internet security already exist, have been announced, are shipping, and will be discussed in full at the Federal Smartcard Users Group at The Smartcard Forum.

The "Present" of Internet is Secure!  
The Role of SmartCARDS in the Era of Network Security And NII  
A Shrink-Wrapped Solution Strategy

Ray Hanner, V-ONE Corporation, Rockville Md

Also Presenting  
Platform Issues of Smartcard Implementation  
Institutional Solution Strategy  
Avi Zahavi, ATT Smart Card Division, Highland Park, NJ

On Sept. 27-28, Tyson Ritz Carlton Hotel, 1700 Tysons Blvd., Mclean, Virginia  
703-506-4300

Voice 301-881-2297 Fax 301-881-5377 dgthornton@v-one.com

---

**Re: Mexico election (Sullivan, [RISKS-16.36](#))**

*Alex Lopez-Ortiz <alopez-o@neumann.UWaterloo.ca>*

*Tue, 27 Sep 1994 19:16:36 -0400*

>... according to professor Garrido, the manipulation was done at the  
>electorate registry level. 7-8 mill. voters from districts that were known  
>to have a clear majority in opposition to the ruling PRI party, were removed  
>from the electorate. ...

This technique is known as "shaving" the voter's list. It is one of many techniques allegedly used by the ruling party to rig the elections. How many voters were shaved is anybody's guess. Estimates have ranged from 2-4% to 25%.

On the eight million figure, the minister of the interior declared:

Luckily they [the PRD] came up with a ridiculous large figure for shaved voters. This places their claims in the realm of the absurd.

It should be said that the minister of the Interior, which is in charge of the election procedure, is a noted academic known for his political independence and does not belong to the ruling party.

>I have seen reports of complaints on the Mexican election in various media,  
>but very little mention of this accusation. Has it been reported elsewhere?

The Wall Street Journal and/or the Washington Post explained several known schemes for rigging the election, including shaving, the "taco" (a roll or premarked electoral ballots inserted by a voter), and the "carousel" (voters go around and around voting time and time again).

>Does it have any substance?

The eight million figure certainly not.

Were there some shaved voters? Yes.

How many? According to audits commissioned by the government and performed by independent national and international firms, about 2-4% of the voters had taken the steps to register but did not appear in the lists.

It is not known how many of those are due to administrative errors (such as entering and incorrect address and having the voter appear in an incorrect voting station) and how many are intentional.

>Does anybody know what kind of computerized system was used in Mexico this  
>time, before, during and after the election?

There are no systems used during the election. All the voting is a manual process done in see-through ballot boxes (to avoid pre-stuffing them with votes).

After the election, a series of Tandem systems were used. The government has refused to make details specific, according to "security considerations". From declarations by election officials, it seems that the central system is connected to computers in each state and that elections results were transferred electronically, and later verified manually.

Alex Lopez-Ortiz, Computer Science Dept, University of Waterloo, Waterloo, Ontario Canada <http://daisy.uwaterloo.ca/~alopez-o/home.html>

---

### Re: Uninterruptables ([RISKS-16.41](#))

*Phil Agre <pagre@weber.ucsd.edu>  
Tue, 27 Sep 1994 15:35:40 -0700*

My note about uninterruptable power supplies in [RISKS-16.41](#) brought quite a bit of interesting correspondence. Most of it asserted (with no more evidence than I presented in my own note) that phrases like "uninterruptable power systems" come from sales and marketing people. This might be, but it doesn't explain why technical people go along with them. They must accept that it's reasonable to call something "uninterruptable" if it prevents one particular failure mode, regardless of any others. This would be like calling a child's toy "unbreakable" if it cannot be broken by being chewed on, even though it shatters into long, sharp needles when used to pry something open. The point is not to discredit electrical engineering, which brings many benefits to society, but simply to encourage broader systems thinking and more rigorous truth in labeling.

The same thing goes for "inherently safe nuclear reactors". I'm sure that such reactors can pass coolant-loss tests, but that's only one of the many dangers from nuclear power. This probably isn't the place to argue the merits of nuclear power in general, but I do think that the analogy between these two cases of misleading terminology is strong. In each case, absolute statements are made based on the defeat of single failure modes that can be represented within a narrowly technical definition of the system's operation.

Phil Agre, UCSD

---

**uninterruptable thought patterns**

*Martyn Thomas <mct@praxis.co.uk>  
Wed, 28 Sep 1994 10:27:44 +0100 (BST)*

My least favourite tendentious phrase is "incredible accident" for the low probability incidents in the analysis of system hazards. I first met it in the nuclear industry, but it's more widespread than that.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.  
Tel: +44-225-444700. Email: mct@praxis.co.uk Fax: +44-225-465205

---

## **Safety issues with Screen Savers**

*Rich Baker <rbaker@rr25.modicon.com>  
Sat, 24 Sep 94 22:36:31 EDT*

I am doing some research on Safety issues concerned with Screen Savers. Do you know of any incidents that have been caused by Screen Savers masking out critical information on a screen or on the reactivation of a screen saver causing inadvertent actions in an application?

Richard Baker, Modicon, Inc., North Andover, MA 508-975-9789

---

## **Phil Agre on high-tech university**

*Robert Ashcroft <rna@sphinx.Stanford.EDU>  
Tue, 27 Sep 1994 22:22:46 -0700*

> ... Substantial institutions have arisen for  
>harassing journalists whose articles diverge from the political views of those  
>who care to fund them. ...

Anyone with even a passing acquaintance with universities realizes that this already happens internally at universities. Even at the Graduate School of Business at Stanford, there is a problem with at least the perception of a "party line" over which it is not safe to step (regularly bemoaned in the school newspaper, in case anyone cares to check).

At the most, video of university lecture just enlarges the group that decides, through whatever mechanism, what is the "party line". It's not clear that one group's decision is any better than another's.

In fact I have serious doubts about two parts of Agre's scenario:

- 1) That many lectures will in fact be found interesting (or lucrative) enough to bother broadcasting, outside of technical subjects like EE, which are not subject to these kinds of controversy. Face it, a heck of a lot of stuff that goes on at a university is just plain boring to the vast majority of folks.
- 2) In the event that any "radical" is caught in such a thing as the above, s/he is more likely to be delighted by the attention. Supposing the

professor has tenure (and few professors stick out their necks before achieving this status) s/he is perfectly safe from retribution, and is more likely to leverage their new-found notoriety, a la Rush Limbaugh. Imagine, everyone tuning into your lecture every week to hear your latest pronouncements. It's every professor's dream.

A new media star is born, the University makes a bundle selling off the lecture broadcasts to HBO, and everyone goes home happy.

RNA

---

### Re: Neural networks and testing (Re: [RISKS-16.42](#))

<Fred Cohen <fc@netaxs.com> [[ADDRESS REJECTING FOR ME. PGN]]>  
Mon, 26 Sep 1994 06:30:05 -0400

Peter Denning suggested that we could test away the uncertainty with neural networks, however, doing a complete test is infeasible for all but the simplest systems, and not doing a complete test leaves the possibility that an unlikely (i.e., low enough probability that it was not worth testing) chain of events will cause catastrophic results. Recent research has shown that even the best tested systems fail under the combination of only two unlikely events a lot of the time. In a random world, this is perhaps good enough, but in a world with malicious attackers, testing neural networks will simply not do.

---

### Re: Yet More daring tales of address disasters! ([Risks 16.42](#))

Dan Fass <fass@cs.sfu.ca>  
Mon, 26 Sep 1994 15:21:26 -0700

I doubt I'm the only person to point this out, but Charles Reichley's proposal does not deal with the problem you posed. If the acknowledgement is sent to both the old and new addresses, and if a bogus Change of Address form had been previously sent to the local Post Office, then the acknowledgement sent to the old address is forwarded to the imposter.

- Dan Fass

[Also noted in one form or another by  
Barry Jaspan <bjaspan@cam.ov.com>,  
Ping Huang <pshuang@MIT.EDU>, who notes that  
Fidelity Investments notifies both OLD and NEW addresses,  
and suggests phone verification as well (although call  
forwarding can also be spoofed),  
Jim Hiller <JHILLER@lancer.afit.af.mil>, who adds  
"As with any trusted distribution system, I submit that,  
once the reference monitor (the PO in this case) is hosed,  
it's all over."

I am probably overly permissive in letting the following bunch through, because the topic is marginal to begin with, but I am

feeling tolerant today. STOP NOW if you have already had enough. PGN]

---

### **Re: Yet More daring tales of address disasters!**

<Andrew\_Marc\_Greene@frankston.com>

Sun, 25 Sep 1994 10:57 -0400

[Regarding sending notification to OLD and NEW addresses:]

But this won't solve the problem unless the one sent to the old address says "DO NOT FORWARD" -- and even then the post office will probably simply return it to sender regardless of whether the change-of-address form was legit or not.

- Andrew

[Yes, human fallibility is also a problem. Evidently, my postperson does not read English very well, but has less trouble with numbers. I get some mail for several other blocks in my area for houses with the same street number, and they get mine. PGN]

---

### **Re: Yet More daring tales of address disasters! ([RISKS 16.42](#))**

Steve Summit <scs@eskimo.com>

Sat, 24 Sep 1994 14:10:11 -0700

I'm not sure how safe it is to assume that an acknowledgement mailed to the old address will be forwarded; I for one am seriously considering \*not\* notifying the Post Office the next time I move, since filling out one of their change-of-address forms automatically gets you lots of new junk mail. (Evidently the U.S. Postal Service refuses not to sell the recently-moved address lists, as they're a money-maker and the USPS is chronically strapped for cash.) [...]

Steve Summit scs@eskimo.com

---

### **Re: Address disasters**

Jan Mandel <jmandel@carbon.denver.colorado.edu>

24 Sep 1994 19:06:06 -0600

Assume for privacy sake one will want to move without leaving a forwarding address, and notify all that one does business with about the new address. In that case the practice to send the acknowledgement to the old address will backfire. And of course, try to tell that to the companies you do business with, when their computers are programmed that way.

Forwarding by US Mail does create serious privacy issues. I hear that the Post Office stopped/will stop giving the new address to anyone. That's good. But the PO will give your address to anyone who sends you a letter after one

year but before the record expires; the letter is sent back to sender with a big yellow sticker with your new address on it...

Jan Mandel, Center for Computational Math, University of Colorado at Denver  
jmandel@colorado.edu

---

## Authentication of changes of address (Re: Postal address disasters)

*"Jonathan I. Kamens" <jik@cam.ov.com>*

*Sun, 25 Sep 1994 10:55:50 -0400*

Six months or so ago, my father went to the post office to put a temporary hold on his mail because he was going on vacation, and the clerk he spoke to said something to the effect of, "Now, when you say on this form that you want your mail to start being delivered on date <x>, you really mean that you want it to start being forwarded to your new address, right?"

Puzzled, my father responded, "What new address?"

The clerk responded, "The address you sent us on your change-of-address card."

My father hadn't sent in a change-of-address card. Subsequent investigation (and a number of interviews with the postmaster at that post office) revealed that someone had sent a fraudulent change-of-address card in my parents' name to the post office, forwarding their mail to a non-existent address in California. The card was sent from another state. It seems unlikely that whoever sent it will ever be caught.

Fortunately, the deception was detected before they started forwarding the mail, because of the coincidence of the timing of my father's visit to the post office. If he hadn't gone in to put a hold on his mail, the post office would have happily started forwarding it with no questions asked.

Obviously, the problem here is that there was no authentication whatsoever of the change of address. Admittedly, the post office does send a change-of-address kit to anyone who files a card, but if the card asks for the forwarding to begin immediately, it will start happening quite a while before the kit arrives. And the kit will be forwarded to the new address, which doesn't do much good if it's a fake!

Even something simple like delivering a confirmation card to any address that requests a change of address, and requiring that it be filled out and returned before processing the change, would be a huge improvement over the current system. Who knows why the post office doesn't do this.

Jonathan Kamens | OpenVision Technologies, Inc. | jik@cam.ov.com

---

## Re: Yet More daring tales of address disasters!

*Mike Crawford <crawford@scipp.ucsc.edu>*

*Fri, 23 Sep 1994 19:52:22 -0700*

The California Legislature recently passed a bill forbidding prison inmates from changing their names without the permission of the prison warden. It seems that a "resident" of Pelican Bay state pen, reputedly the state's toughest prison, changed his name to that of the ex-husband of a woman who had accused him of molesting her daughter. The fellow succeeding in changing this woman's postal address to his prison address so he could read all her mail, and I believe he even obtained her credit record!

This went on despite her complaints until the San Francisco Chronicle ran a full page article detailing this fellow's activities.

Apparently the prison had tried to punish him further, but they could not stop him from sending mail. Now mail from California prisons is stamped with the name of the prison so that the recipient can get a clue to be suspicious.

Mike Crawford [crawford@scipp.ucsc.edu](mailto:crawford@scipp.ucsc.edu)

---

### **Mail Forwarding must have been purchased by addressee**

*Chris Smith <[cjsmith@io.org](mailto:cjsmith@io.org)>  
Sun, 25 Sep 1994 18:23:46 -0400 (EDT)*

Depending on such a feature can be a RISK, since Canada Post treats such a service as an additional-cost item. It is purchased ahead of time, and for a certain period of service. If the addressee is not aware that a change of address notification will be mailed to the old address, they may not bother purchasing the service.

Of course, during a recent move, the "guy in charge of putting the stickers on the P.O. boxes didn't trust his stand-in, so he didn't leave instructions to do it" -- and we had no mail forwarded for 10 days.

An additional RISK? Beware of internal processes that extract an address and *\*use\** it two months later! A recent, automatic credit-card replacement didn't get to us because (1) it depended on an address taken from the database 2 weeks before we moved, but not used until 6 weeks *\*after\** we moved, and (2) for security, it was sent via a courier -- who does not have access to the mail-forward info, even if you *\*have\** purchased the service.

Chris Smith <[cjsmith@io.org](mailto:cjsmith@io.org)>

---

### **Re: Yet More daring tales of address disasters!**

*Paul Robinson <[PAUL@tdr.com](mailto:PAUL@tdr.com)>  
Mon, 26 Sep 1994 04:34:34 -0500 (EST)*

[...] By sending the confirmation to the *\*old\** address, it warns the person who owns the stock that their address is being changed, *\*in the event the change is fraudulent\**. If that confirmation is sent with a signature required and a do not forward order on it, it provides excellent protection to the

original owner that the change of address is not fraudulent.

Realize that for most stock, ownership includes certain benefits including right to vote at the stockholders meeting, and something important to a lot of people, dividend checks.

Because of laws on the right of stockholders to submit candidates for the board of directors, just about anyone, and certainly anyone who owns even one share of stock in the company, has the right to obtain a list of every stockholder in the company including their name and address (in order to solicit them to support a new board of directors and to solicit them for proxies for their vote). This was common practice for doing a hostile or friendly takeover before Michael Milken got the idea of selling bonds and buying a company instead of simply getting the owners of a company to fire the board of directors via proxy fights.

Now imagine what happens if someone decides to get the list of stockholders and sends in fake change of address requests during the week just before the dividend checks are issued, for the top five largest individual stockholders. If the acknowledgement of change of address is sent to the new address, the stockholder would never know that someone had changed their address. Who pays for it if someone then forges the signature of the recipients and cashes thousands or tens of thousands of dollars in dividend checks?

---

## Re: address disasters

*Michael Jampel <jampel@cs.city.ac.uk>  
Mon, 26 Sep 94 11:34 BST*

Douglas Adams, author of Hitch-Hiker's Guide to the Galaxy, created a computer game called Bureaucracy, the aim of which was to get a company to acknowledge a change of address card. (They insisted you inform them of changes of address on an official form, which they were happy to send to the old address.) At one stage you had to get a green form in order to get a red form, but in order to get a red form you needed a yellow form. guess why you needed a green form in the first place?

Anyway, the game is good, in an infuriating way.

Michael Jampel <jampel@cs.city.ac.uk>

---

## Privacy & American Business conference in DC next week

*"Lance J. Hoffman" <hoffman@seas.gwu.edu>  
Wed, 28 Sep 1994 12:00:39 -0400 (EDT)*

"Managing the Privacy Revolution" Oct. 4-5, 1994 Features  
Top Privacy Experts in Landmark Washington Conference

Fifty leading privacy experts from the administration, federal and state government, the business community, public interest and advocacy groups,

corporate legal representatives, telecommunications, the academic and policy community, national industry associations, the media, and survey research will participate in "Managing the Privacy Revolution," the first annual business/privacy conference sponsored by Privacy & American Business, October 4-5, 1994 at Loews L'Enfant Plaza Hotel, Washington, D.C. (Program, speakers, and P&AB information attached)

The conference will also offer the first look at a new P&AB/Louis Harris survey on the Consumer, Interactive Services, and Privacy.

Geared to assist those who handle personal information about consumers, clients and employees, the conference is expected to attract those who manage information privacy issues and policy in consumer credit, telecommunications, banking credit cards, employment, life/health/ property insurance, health care, telemessaging, direct marketing and medical records.

The conference will lay out the sweeping political, legal, and technological changes affecting the way every U.S. business will handle personal customer and employee information in the future and will provide a forum for addressing the changes.

The \$595 registration fee for the two day conference includes all sessions, private time with speakers, interaction with fellow conferees, cocktail party and buffet reception, two banquet luncheons, two continental breakfasts, three refreshment breaks. Also a Washington Legislative Briefing Book, a Handbook of Company Privacy Codes, a specially prepared 35-page book of Highlights from 1994 Louis Harris Privacy Surveys and a six-month trial subscription to Privacy & American Business (or a six month renewal of an existing subscription). Special rates for nonprofit organizations, multiple registrations, and a \$100 Early Bird registration discount are available.

For further conference information, call P&AB, 201-996-1154 or fax 201-996-1883.



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 16: Issue 45**

**Monday 10 October 1994**

## Contents

- [Anonymity and the Stock Markets...](#)  
[Peter Wayner](#)
- [ICL loses 1.3m pounds poll-tax case](#)  
[Jonathan Bowen](#)
- [AOL sells its subscriber list](#)  
[David L. Gehrt](#)
- [Twins out of luck in Brazil](#)  
[Debora Weber-Wulff](#)
- [Confidential information passed on](#)  
[Nik Clayton](#)
- [Privacy Digests -- and Digital Telephony](#)  
[PGN](#)
- [CFP for CFP'95 \(Computers, Freedom, and Privacy\)](#)  
[Carey Heckman](#)
- [CALL for PAPERS: EUROCRYPT '95](#)  
[Jean-Jacques Quisquater](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Anonymity and the Stock Markets...

*Peter Wayner <pcw@access.digex.net>  
Fri, 7 Oct 1994 22:59:20 -0500*

People embroiled in the debate over anonymity on the networks might want to check out an article entitled "Reuter's Instinet is Biting Off Chunks of Nasdaq's Territory" in October 4th edition of the Wall Street Journal (p. C1).

The article doesn't deal directly with anonymity-- it just charts the success of Reuter's Instinet, a computer network that matches up buyers and sellers of large blocks of stock. The article mentions that many clients selling large blocks of stock turn to the Instinet because it is anonymous. It's main competitors are not. It reads, "Large investors, who wish to keep their long or short positions confidential, especially want to avoid tipping other investors off about their bets in the volatile, mostly small-capitalization

over-the-counter market."

Ideally, this feature allows the market to be more efficient and more fair. People who just happen to be selling, say, Apple Computer Company stock to say, Motorola, won't be able to use their casually acquired knowledge. (Just a hypothetical example.) Another chance for "insider" like trading is gone.

This anonymity, though, is almost certainly not absolute. The SEC would probably be able to unwind the trades if they needed to do so. But I'm just guessing about this.

---

## ICL loses 1.3m pounds poll-tax case

*<Jonathan.Bowen@comlab.oxford.ac.uk>*

*Mon, 10 Oct 94 09:58:46 BST*

Front page news in "Computing", 6 October 1994:

Headline: ICL loses 1.3m pounds poll tax case

In a landmark award, St Albans City Council has won a 1.3m pounds High Court judgement against ICL for supplying flawed poll tax software, precipitating a flood of similar claims against the supplier. Monday's judgement has industry-wide implications because the judge in the case, Mr Justice Scott Baker, ruled that a clause in ICL's standard contract limiting the supplier's liability if problems arose did not apply under the Unfair Contract Terms Act 1977.

Notes:

1. "Computing" is a UK computing industry weekly newspaper.
2. ICL is a Japanese owned UK based computer company.
3. 1.3m UK pounds is approximately \$2 US million.
4. The "poll tax" was the abortive uniform local tax on individuals introduced by the Conservative government under Mrs Thatcher, but now replaced due to public resistance.

Jonathan Bowen, Oxford University Computing Laboratory, Programming Research, Wolfson Building, Parks Road, Oxford OX1 3QD UK [Jonathan.Bowen@comlab.ox.ac.uk](mailto:Jonathan.Bowen@comlab.ox.ac.uk)

---

## AOL sells its subscriber list

*"David L. Gehrt - RIACS" <dlg@skydesign.arc.nasa.gov>*

*Wed, 05 Oct 1994 10:03:16 -0700*

On the front page of the buiness section of the San Jose Mercury today (5 Oct 1994) is an article describing one of the most egregious privacy violations I have heard of. America Online, described in the article as the fastest growing on-line service providers, has or appears to be ready to peddle subscriber information. The kind of information by AOL collected upon sign up is (IMHO) excessive. My wife signed up and I nearly told her to find another

service provider and if she had known about the possibility that the info would be sold I am sure that she would have not signed up.

According to the article the information which might be included in the sale of AOL subscriber info includes: "...name, gender, address, income, family, type of computer equipment, and payments to the company."

My hope is that other subscribers will rise up in anger and convince AOL that this invasion of their privacy will cost them more \$\$\$ in lost subscribers than they can hope to gain via the sale of the info.

David L. Gehrt

---

## Twins out of luck in Brazil

*Prof Weber-Wulff <weberwu@tfh-berlin.de>  
5 Oct 1994 15:42:41 GMT*

The German daily newspaper "Tagespiegel" notes this past weekend that for any set of twins (or triplets, etc.), in Brazil, only one may register to vote for the upcoming election. Seems the unique key for the voter registration form consists of the names of the parents and the birthdate. It was noted that the problem could not be corrected in time for the election, presumably there will a number of people contesting the election.

Debora Weber-Wulff, Technische Fachhochschule Berlin, FB Informatik,  
Luxemburger Str. 10, 13353 Berlin, Germany email: weberwu@tfh-berlin.de

---

## Confidential information passed on

*Nik Clayton <Nik.Clayton@brunel.ac.uk>  
Wed, 28 Sep 94 12:57:09 +0100*

"Watchdog", a consumer affairs television program shown on the BBC, Monday 26th September, reported on the experiences of a customer of Dixons (a computer and other electrical goods retailer). The customer had bought a PC from them, and had used it extensively, writing letters, doing business and accounts and so on. The PC started to malfunction, the symptoms being wrong characters generated by the keyboard. For example, "w" translated to an "f" and so on.

Dixons said that they couldn't fix it, but would charge UKP 250 for an upgrade to a new machine. The customer agreed to this, and told them, before he gave the computer back, that he had confidential information stored on it, and would they remove it for him. Dixons agreed to this. 6 months later, he received a phone call from a family who had purchased his old computer from Dixons, saying that they had found his data still on the computer.

RISKS: Obviously, the retention of the data is a large risk. But in addition, I think there are several others. Most obvious is the fact that the customer, while storing important information on the machine

had made no efforts to make it secure. The situation could have been much worse if the computer had been stolen, or if his children had access to the data to change it.

Other risks include believing what the retailer tells you. We weren't told any more technical information about the problem with the machine, but it looked very much as though either the keyboard was faulty, or, more likely, that one of the keyboard drivers had become corrupted. Certainly not something that should UKP 250 to fix.

Also, the second owners of the machine believed that what they were getting was brand new, with the caveat that it had been used a display machine. Obviously, it wasn't. But even if it had been a display machine, it should be a trivial matter to walk into one of the stores and put a virus on many of the machines available. This could cause havoc for first time buyers.

Nik

---

## Privacy Digests -- and Digital Telephony

*Peter G. Neumann <Neumann@csl.sri.com>*

*Mon, 10 Oct 94 09:00:10 EDT*

Periodically I remind you of TWO useful digests related to privacy, both of which are siphoning off some of the material that would otherwise appear in RISKS, but which should be read by those of you vitally interested in privacy problems. RISKS continues to carry general discussions in which risks to privacy are a concern. The most recent issues of PFD and CPD include extensive material on the newly passed Digital Telephony Bill that now awaits Presidential signature. Because of the extraordinary volume of that material, we do not attempt to cover the issues here. If you are seriously interested in the discussions on privacy, I recommend you try BOTH digests for a while (free trial subscriptions are terrific, but especially when the long-term subscriptions are also free AND, perhaps more important, you don't wind up on anyone ELSE's mailing list!).

\* The PRIVACY Forum Digest (PFD) is run by Lauren Weinstein. He manages it as a rather selectively moderated digest, somewhat akin to RISKS; it spans the full range of both technological and non-technological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line:

information privacy

as the BODY of a message to "privacy-request@vortex.com"; you will receive a response from an automated listserv system. To submit contributions, send to "privacy@vortex.com".

\* The Computer PRIVACY Digest (CPD) (formerly the Telecom Privacy digest) is run by Leonard P. Levine. It is gatewayed to the USENET newsgroup comp.society.privacy. It is a relatively open (i.e., less tightly moderated)

forum, and was established to provide a forum for discussion on the effect of technology on privacy. All too often technology is way ahead of the law and society as it presents us with new devices and applications. Technology can enhance and detract from privacy. Submissions should go to [comp-privacy@uwm.edu](mailto:comp-privacy@uwm.edu) and administrative requests to [comp-privacy-request@uwm.edu](mailto:comp-privacy-request@uwm.edu).

There is clearly much potential for overlap between the two digests, although contributions tend not to appear in both places. If you are very short of time and can scan only one, you might want to try the former. If you are interested in ongoing detailed discussions, try the latter. Otherwise, it may well be appropriate for you to read both, depending on the strength of your interests and time available.

PGN

---

## **CFP for CFP'95! (Computers, Freedom, and Privacy)**

*Carey Heckman <ceh@leland.Stanford.EDU>*

*Thu, 6 Oct 1994 06:12:05 -0700 (PDT)*

Call for Participation - CFP'95

The Fifth Conference on Computers, Freedom and Privacy  
Sponsored by the ACM SIGCOMM, SIGCAS, SIGSAC and Stanford Law School  
28 - 31 March 1995  
San Francisco Airport Marriott Hotel, Burlingame, California

### **INVITATION**

This is an invitation to submit session and topic proposals for inclusion in the program of the Fifth Conference on Computers, Freedom and Privacy. Proposals may be for individual talks, panel discussions, debates, or other presentations in appropriate formats. Proposed topics should be within the general scope of the conference, as outlined below.

### **SCOPE**

The advance of computer and telecommunications technologies holds great promise for individuals and society. From convenience for consumers and efficiency in commerce to improved public health and safety and increased participation in democratic institutions, these technologies can fundamentally transform our lives. New computer and telecommunications technologies are bringing new meanings to our freedoms to speak, associate, be left alone, learn, and exercise political power.

At the same time these technologies pose threats to the ideals of a just, free, and open society. Personal privacy is increasingly at risk from invasion by high-tech surveillance and eavesdropping. The myriad databases containing personal information maintained in the public and private sectors expose private life to constant scrutiny. Political, social, and economic fairness may hinge on ensuring equal access to these technologies, but how, at what cost, and who will pay?

Technological advances also enable new forms of illegal activity, posing

new problems for legal and law enforcement officials and challenging the very definitions of crime and civil liberties. But technologies used to combat these crimes can threaten the traditional barriers between the individual and the state.

Even such fundamental notions as speech, assembly and property are being transformed by these technologies, throwing into question the basic Constitutional protections that have guarded them. Similarly, information knows no borders; as the scope of economies becomes global and as networked communities transcend international boundaries, ways must be found to reconcile competing political, social, and economic interests in the digital domain.

The Fifth Conference on Computers, Freedom and Privacy will assemble experts, advocates and interested people from a broad spectrum of disciplines and backgrounds in a balanced public forum to explore and better understand how computer and telecommunications technologies are affecting freedom and privacy in society. Participants will include people from the fields of computer science, law, business, research, information, library science, health, public policy, government, law enforcement, public advocacy, and many others.

Topics covered in previous CFP conferences include:

- Personal Information and Privacy
- Access to Government Information
- Computers in the Workplace
- Electronic Speech, Press and Assembly
- Governance of Cyberspace
- Role of Libraries on the Information Superhighway
- Law Enforcement and Civil Liberties
- Privacy and Cryptography
- Free Speech and the Public Communications Network

We are also actively seeking proposals with respect to other possible topics on the general subject of computers, freedom and privacy. Some new topics we are considering include:

- Telecommuting: Liberation or Exploitation?
- Courtesy, and the Freedom to be Obnoxious
- Commercial Life on the Net
- How Does the Net Threaten Government Power?
- Universal Access to Network Services
- The Meaning of Freedom in the Computer Age
- Online Interaction and Communities
- Government-Mandated Databases

#### PROPOSAL SUBMISSION

All proposals should be accompanied by a position statement of at least one page, describing the proposed topic. Proposals for panel discussions, debates and other multi-person presentations should include a list of proposed participants and session chair. Proposals should be sent to:

CFP'95 Proposals  
Stanford Law and Technology Policy Center  
Stanford Law School  
Stanford, California 94305-8610

or by email to:

cfp95@forsythe.stanford.edu

with the word RProposalS in the subject line. Proposals should be submitted as soon as possible to allow thorough consideration for inclusion in the formal program. The deadline for submissions is 1 November 1994.

#### STUDENT PAPER COMPETITION

Full time students are invited to enter the student paper competition. Winners will receive a scholarship to attend the conference and present their papers. Papers should not exceed 2,500 words and should examine how computer and telecommunications technologies are affecting freedom and privacy in society. All papers should be submitted to Professor Gary T. Marx by 20 November 1994. Authors may submit their papers either by sending them as straight text via email to:

Gary.Marx@colorado.edu

or by sending six printed copies to:

Professor Gary T. Marx  
University of Colorado  
Campus Box 327  
Boulder, Colorado 80309-0327  
(303) 492-1697

Submitters should include the name of their institution, degree program, and a signed statement affirming that they are a full-time student at their institution and that the paper is an original, unpublished work of their own.

#### INFORMATION

For more information on the CFP'95 program and advance registration, as it becomes available, write to:

CFP'95 Information  
Stanford Law and Technology Policy Center  
Stanford Law School  
Stanford, California 94305-8610

or send email to:

cfp95@forsythe.stanford.edu

with the word "Information" in the subject line.

## THE ORGANIZERS

General Chair  
Carey Heckman  
Stanford Law School  
Stanford Law & Technology Policy Center  
Stanford, CA 94305-8610  
415-725-7788 (voice)  
415-725-1861 (fax)  
ceh@leland.stanford.edu

To discuss potential CFP'95 speakers, topics, and formats, and to receive additional CFP'95 information, subscribe to the CFP95 list. Send to [cfp95@lists.stanford.edu](mailto:cfp95@lists.stanford.edu) a plain text message consisting of subscribe cfp95.

Program Committee  
Sheri Alpert, Internal Revenue Service  
Judi Clark, ManyMedia  
Kaye Caldwell, Software Industry Coalition  
Esther Dyson, EDventure Holdings  
Mike Godwin, Electronic Frontier Foundation  
Peter Harter, National Public Telecommuting Network  
Lance J. Hoffman, George Washington University  
Ellen Kirsh, America OnLine  
Bruce R. Koball, Motion West  
Gary T. Marx, University of Colorado  
Mitch Ratcliffe, Digital Week  
Marc Rotenberg, Electronic Privacy Information Center  
Deborah Runkle, American Association for the Advancement of Science  
Barbara Simons, USACM  
Ross Stapleton-Gray, Georgetown University  
Glenn Tenney, Fantasia Systems  
Jeff Ubois, Author and Consultant  
J. Kent Walker, Jr., Department of Justice  
[Affiliations are listed for identification only.]

---

## CALL for PAPERS: EUROCRYPT '95

*Jean-Jacques Quisquater <jjq@dice.ucl.ac.be>*  
29 Sep 1994 14:47:11 GMT

EUROCRYPT '95

May 21 - 25, 1995, Saint-Malo, France

FINAL CALL FOR PAPERS

General information  
Eurocrypt '95 continues the tradition of European IACR conferences dedicated to the theory and applications of cryptologic techniques. Original papers are solicited on all aspects of cryptology.

### Topics of interest

The topics of interest include but are not limited to:

- . Applications
- . Authentication
- . Combinatorial aspects
- . Computational complexity aspects
- . Computer security aspects
- . Conventional cryptosystems
- . Cryptanalysis
- . Cryptographic hash functions
- . Digital signatures
- . Electronic money
- . Foundation and theory
- . Implementation aspects
- . Information theoretical aspects
- . Key distribution
- . Number theoretical aspects
- . Practical aspects
- . Protocols
- . Pseudo randomness
- . Public key
- . Secret sharing
- . Standards
- . Voting systems
- . Zero knowledge

### Instructions for authors

Send a cover letter, one title page and 18 copies of an extended abstract to be received by November 21, 1994, (or postmarked by November 10, 1994 and sent via airmail). The title page should contain the title, the name of the authors, their phone and fax numbers, their postal and e-mail address and the abstract. The extended abstract should start with the title and the abstract, but should be anonymous (Please, reserve the acknowledgments for the final version of the paper). This should be followed by a succinct statement appropriate for a non-specialist reader specifying the subject addressed, its background, the main achievements, and their significance to cryptology. Technical details directed to the specialist should then follow. A limit of 10 single-spaced pages of 12pt type (not counting the bibliography and clearly marked appendices) is placed on all submissions. Since referees are not required to read the appendices, the paper should be intelligible without them.

Abstracts that have been or will be submitted in parallel to other conferences or workshops that have proceedings are not eligible for submission to Eurocrypt. The authors must state compliance to this rule in their cover letter. A LaTeX style file and an example of a cover letter will be available.

### Conference proceedings

Eurocrypt '95 will be the first Eurocrypt conference where proceedings will be available at the meeting. The proceedings will be published in the Springer-Verlag's Lecture Notes in Computer Science. Clear instructions about the final copy will be sent to the authors. The final copies of the accepted papers will be due on March 6, 1995. Authors of accepted papers must guarantee that their paper will be presented at the conference.

A limited number of stipends are available to those unable to obtain funding to attend the conference. Students whose papers are accepted and who will present themselves are encouraged to apply if such an assistance is needed. Requests for stipends should be addressed to the general chairperson.

#### Program Committee

Chaired by Louis Guillou, the following persons are the Members of the Program Committee:

Mihir Bellare	Johannes Buchmann	Mike Burmester	Paul Camion
Donald W. Davies	Amos Fiat	Hideki Imai	Lars Knudsen
Ueli Maurer	Birgit Pfitzmann	Jean-Jacques Quisquater	Ronald Rivest
Jacques Stern	Douglas Stinson	Moti Yung	Gideon Yuval

#### Important information

Submission receipt deadline: November 21  
(or postmarked airmail: November 10)

Notification sent to authors: January 23

Final copies due: March 6

Send submissions to:

Louis Guillou, Program Chair  
CCETT (Eurocrypt '95)  
4, rue du Clos Courtel  
F-35512 Cesson-Se'vigne' Cedex  
FRANCE  
Tel: +33 99 12 42 47  
Fax: +33 99 84 56 00  
Email: iacr95@ccett.fr

For other information, contact:

Franc,oise Scarabin, General Chair  
CCETT (Eurocrypt '95)  
4, rue du Clos Courtel  
F-35512 Cesson-Se'vigne' Cedex  
FRANCE  
Tel: +33 99 12 41 98  
Fax: +33 99 12 40 98  
Email: iacr95@ccett.fr



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 16: Issue 46

Weds 19 October 1994

## Contents

- [Risks of putting out RISKS](#)
- [Software Bug Cripples Singapore Phone Lines](#)  
[Lee Lup Yuen](#)
- [Cellular Phone Scam](#)  
[PGN](#)
- [Barclays Bank Banks Big-Bang Bump-up \(a success story\)](#)  
[Brian Randell](#)
- [Data security in Iceland](#)  
[Haukur Hreinsson](#)
- [Memory Chip Theft](#)  
[R. Szczesniak](#)
- [Risks of not thinking about what you're stealing](#)  
[Mark Brader](#)
- [Calling Number ID debate](#)  
[Phil Agre](#)
- [Creating kidspaces on the net](#)  
[Prentiss Riddle](#)
- [And you thought one-letter passwords were RISKy ...](#)  
[Dan Astoorian](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Risks of putting out RISKS

"Peter G. Neumann" <[neumann@chiron.csl.sri.com](mailto:neumann@chiron.csl.sri.com)>  
Tue, 18 Oct 94 15:20:44 PDT

\* I have been travelling extensively for the past few weeks (National Computer Security Conference, AAAS/ABA Conference on Computers, Ethics and the Law, National Research Council crypto study, etc.) and have had neither much net access and nor much free time.

\* I returned to find my monitor fried as a result of the FOURTH recorded squirrelcide at SRI --- which brought down the entire institute last Wednesday (for something like eight hours) and created all sorts of internal

power surges, despite the isolation supposedly provided by our cogeneration plant hookup. [I presume this squirrel got turned into rodental floss.]

By the way, the RISKS book (Computer-Related Risks, ACM Press and Addison-Wesley) is finally available. I thank all of you whose contributions to RISKS are noted therein.

PGN

---

## Software Bug Cripples Singapore Phone Lines

*Lee Lup Yuen <lupyuen@singnet.com.sg>*

*Thu, 13 Oct 1994 21:11:36 +0800 (SST)*

>From The Straits Times, 13 Oct 94:

A bug in a newly-installed computer software knocked out two-thirds of Singapore's telephone lines late yesterday morning. Handphones, fax machines, pagers and credit cards were all hit by the disruption which began at 11.31am in the City Exchange. It took Singapore Telecom's engineers about five hours to get services back to normal again.

At a press conference last night, Brig-Gen Lee Hsien Yang, its deputy president and executive vice-president for local services, said the disruption hit 65 per cent of the lines. Subscribers on the remaining 35 per cent of the lines had trouble putting calls through.

The problem started when a software bug corrupted one of the two common channel signalling systems. These systems link the different exchanges. The problem soon spread to all but two of the 28 exchanges. Only the Ama Keng and Pasir Ris exchanges were not affected. When Telecom engineers shut down the affected channel, this caused the other to overload.

Big-Gen Lee said the new and the older systems run side by side and serve as mutual back-ups. If there were only one system, then the whole island's telecommunications network would have been crippled.

---

## Cellular Phone Scam

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

*Wed, 19 Oct 94 12:01:31 PDT*

Clinton L. Watson, 44, was arrested on 18 Oct 1994, along with his son and a family friend, and charged in San Jose, California, with three counts of wire fraud and grand theft, with a possible prison sentence of 30 to 45 years.

Watson allegedly altered and sold more than 1000 cellular phones with illegally acquired identifiers, whose use resulted in millions of dollars of phone calls being billed to unsuspecting persons. Legitimate cellular-phone identification numbers were allegedly captured using scanners, and entered into identity-reprogrammable clone phones that were fabricated from new programmable chips --- which permitted the original identity numbers to be

replaced, and the new purloined identifiers to be easily replaced at future times when they were disabled because of detected misuse. (The Secret Service noted that Watson is currently on probation from a 1988 conviction on 14 counts of wire and mail fraud in Missouri.) [Source: Article by Maria Alicia Gaura, San Francisco Chronicle, 19 Oct 1994, p. A11.]

---

## **Barclays Bank Banks Big-Bang Bump-up (a success story)**

*Brian Randell <Brian.Randell@newcastle.ac.uk>*

*Thu, 13 Oct 1994 15:50:56 +0100*

Attached below is the full text of the front page summary of a longer inside-page article in (UK) Computer Weekly for Oct 13. Nice to report on a risk that apparently paid off! :-)

Client-Server Gamble Pays Off for Barclays, by Tony Collins

Barclays Bank this week went live with the UK's largest client-server system in spite of internal documents warning of the "high-risks" of its Big Bang approach. Without any announcements to the public about the project, the bank stopped up to 10,000 end-users accessing the bank's main customer systems for the whole of Friday and Saturday morning. And while end-users reverted to manual procedures, the IT staff commandeered the bank's mainframes to build a new database holding 25 million customer accounts ready to go live on Monday morning. More than 1,200 IBM RS/6000 servers had already been installed in branches ready to link up with the new database.

Barclays refuses to disclose the cost of the project, but it is believed to have invested f10m in customer-based systems. Andersen Consulting, which has had an average of 50 consultants managing and helping to develop the new system, was warned by the bank that it would not be paid - and may never work for Barclays again - if the systems did not go live. But by noon on Monday about 800 of the 1,000 branches planned for that time had gone live. The remainder had local problems configuring their RS/6000 systems, running the Ingres database, to interface with the new IBM DB2 mainframe database. Later on Monday, nearly 1,100 branches had gone live, leaving only about 12 branches with residual hardware and configuration problems.

The pioneering project's success vindicates the "Big Bang" approach for major client-server systems, and may lead to other major users being more forthcoming with similarly large implementations. But Barclays briefing documents issued before Monday had warned of the risks of opting for a Big Bang rather than region-by-region implementation. "It is a massive undertaking but we have to use this [Big Bang] approach . . . since to create one master database we cannot have existing systems running concurrently," said one briefing document.

The new customer system, the biggest IT project in the bank's history, replaces three incompatible databases - which previously covered customer accounts, Barclaycard and financial products - with a single database. Bill Gordon, managing director of the banking division, said the new database replaces "current systems and practices that have hampered our ability to

serve the customer". The new system will allow bank staff to see customer transfer files and approve or reject a new account within 30 minutes and will use a computerised credit scoring to give an almost instant "Yes" or "No" on loan and overdraft requests. Customer records will no longer be "owned" by a particular branch or manager but by the bank as a whole.

Dept. of Computing Science, University of Newcastle, Newcastle upon Tyne,  
NE1 7RU, UK Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923

---

## Data security in Iceland

*Haukur Hreinsson <hauh@ismennt.is>*

*18 Oct 1994 19:23:48 -0000*

I laughed when I heard this on the news about a month ago:

There's this relatively well known writer in here in Iceland named Thrainn Bertelsson. He was working on a script for a movie that is supposed to be shot sometime soon. Then somebody goes ahead and breaks into his office, taking care not to forget the computer on the way out; nothing else was stolen. Now the writer realizes that, not only does someone have his script, but that someone has the \*only\* copy of it in the world. The man hadn't made a backup from day one!

It's sad, I guess, especially when you consider that the guy was desperate enough to immediately offer hard cash for the data and sent out a plea to the perpetrator. It looks like he was listening because he gave the computer back. ...after wiping the entire hard disk. And that's Government wipe, not overwrite once!

I haven't heard any more, I guess Thrainn is busy rewriting his little script now. I don't know if I should laugh or cry.

Haukur Hreinsson Hagamel 20 IS-107 REYKJAVIK Iceland hauh@ismennt.is

---

## Memory Chip Theft [Losing your memory is contagious?]

*R.Szczesniak <u9236635@sys.uea.ac.uk>*

*Sun, 16 Oct 94 13:20:21 BST*

In Manga Mania (Nov 94):

Thieves broke into a London finance firm recently and stole all of the memory chips from the firm's computers - over UK#5000's worth! That night, three other outfits also lost their memory to the same gang. The week before, another London company was hit, and replaced its chips only to be hit again three days later. Unlike banknotes, chips have no serial numbers and are almost impossible to identify.

---

## Risks of not thinking about what you're stealing

<msb@sq.com>

Jack Decker (ao944@yfn.yzu.edu) posted this to alt.dcom.telecom and comp.dcom.telecom.tech:

So tonight I get a call from my friend who sells beepers. He just opened up a store on Thursday, and let's just say that there were still a few holes in his security. Anyway, a couple of kids decided to each grab a beeper and make off with it.

Now, my friend's beepers are all pre-activated, which means that if you buy one, you walk away from the store with a working beeper that you can start using immediately. And these beepers were indeed activated.

So when my friend gets back to his office, he starts to wonder if there isn't some way to get his beepers back. And then he remembers... he has an 800 number that's provided by a company called Arch Telecom. And Arch captures the ANI (Automatic Number Identification) of the calling party on all 800 number calls. So he dials up the "missing" beepers and punches in his 800 number as the callback number.

And believe it or not, the thieves CALLED HIM BACK! Both of them! And of course when he got the calls, he informed the kids that he now had their home phone number and it just might be a good idea if they stopped by his store tomorrow and either returned the pagers or paid for them!

And THEN, he called the Arch Telecom customer service office (this was on a Sunday, mind you) and they looked up the ANI of the calls he'd just received. He called the numbers back and got the PARENTS on the phone, and had a little chat with them as well.

He told me that if by some odd chance the kids don't return his pagers first thing tomorrow, he'll take further action, but he really expects to see his pagers come back to him tomorrow.

I figure that anyone who steals a beeper is pretty stupid anyway, since they are pretty useless if you're not paying for the paging service (and you can bet that if my friend hadn't received those calls, those beepers would have been deactivated tomorrow!) but to steal a beeper and then start calling numbers that appear on it... well, I'll bet those boys learned a little lesson about the capabilities of modern telephone technology (then again, maybe they still haven't figured it out... thieves generally aren't all that bright to start with!).

I just thought it was funny that those kids would be dumb enough to call an unknown 800 number that appeared on a pager they had just stolen. I'm sure that there have been dumber thieves, but these two sound like they might have half a brain between them! :-)

If you, too, find this amusing, feel free to cross-post it to any appropriate newsgroup if you like (e.g. rec.humor.\* - I only posted this to the telecom groups) but please keep the whole thing including my .sig

file intact.

Jack Decker aa931@detroit.freenet.org =or= ao944@yfn.ysu.edu

There were several followups, including one by Stephan Piel (spiel@unix.cc.emory.edu) who told of a murder victim whose pager had also been stolen. The police called the pager, and sure enough...

And Dale Farmer (dalef@bu.edu) wrote about an acquaintance whose job involves lending out pagers for things like trade shows. These go missing often enough that he has developed a repertoire of messages to send when it happens. Dale quoted three:

"This pager has been deactivated, please return it to [address]"

"Stolen pager tracing activated"

"Pager tracing successful, located in [city]"

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

---

## Calling Number ID debate

*Phil Agre <pagre@weber.ucsd.edu>*

*Thu, 13 Oct 1994 14:13:13 -0700*

Calling-Number ID (abbreviated CNID [and sometimes misnamed Caller ID]) is a technology that enables your telephone to digitally send its phone number to the telephone of anybody you call. Controversy about privacy issues in CNID has swirled for years. The NYT has an article on the subject:

Matthew L. Wald, A privacy debate over Caller ID plan, *\*The New York Times\**, 13 October 1994.

The United States Federal Communications Commission recently proposed rules, due to go into effect in April, to create uniform CNID protocols across state lines. While the FCC plan does protect privacy in some ways, e.g., preventing a business that captures your phone number from selling it to others without your permission, it does not mandate per-line blocking, which is necessary if you never want to send out your phone number, or if you only want to send it out when you enter a special code.

The article states clearly that the real reason for CNID is commercial. Privacy advocates have been saying this for years, and for a long time they have gotten patronizing lectures about how CNID is for residential use in catching harassing phone callers. But CNID is a poor way to catch harassing phone callers. Moreover, that single application wouldn't nearly make CNID profitable. The point is that CNID is a good way to let companies collect marketing information and automate service interactions.

Which is fine. Hardly anybody opposes CNID outright. But in order for CNID to avoid inadvertently giving away the phone number of someone who is being stalked, or who otherwise needs to keep their number a secret, it needs a few

simple features:

- \* per-line blocking -- a simple, no-cost way to declare that this telephone should not send out its number when dialling
- \* per-line unblocking -- a simple, no-cost way to declare that this telephone now *should* send out its number when dialling
- \* per-call blocking -- a simple, no-cost way to declare that, regardless of whether this line is blocked, this particular call should not include the calling number
- \* per-call unblocking -- a simple, no-cost way to declare that, regardless of whether this line is blocked, this particular call *should* include the calling number

In order for people to get the benefit of these commands, some further rules are needed:

- \* All four of these commands should be entered with *different* codes.
- \* Most especially, the blocking and unblocking commands should not be implemented with toggle commands (for example, \*67 blocks the line and then another \*67 unblocks it -- or, wait!, did the first \*67 unblock the line so that the next \*67 blocked it?).
- \* All of these commands (or at least the per-call ones) should take effect instantly, without requiring a pause before dialling a number, so that phone numbers stored in modems can include the codes.
- \* All of the commands should be standardized everywhere.
- \* All of the commands should be clearly and concisely explained in some convenient place in the phone book. If at all possible, the commands should be listed on a simple cue card that can be attached to the telephone alongside the emergency numbers. (Of course, if a telephone had a real user interface then cue cards would not be necessary.)

Don't all of these rules sound like common sense? Of course they do. They allow everyone complete freedom of choice. If you like CNID then you can turn it on and forget about it. If you want to refuse calls that do not include caller numbers then you're free to do that. If you don't care to call anyone who requires a caller number then you're free to adopt that policy as well. If you never want to send out your number because you're being stalked or are running a shelter then you can do that. Free choice.

So why do proponents of CNID go to extraordinary lengths to defeat these simple, ordinary protections? Because they're afraid that large numbers of people would use per-line blocking, thus making the system less attractive to the businesses who want to capture lots of phone numbers. Like many schemes for using personal information, then, CNID is founded on trickery -- that is, on the gathering and use of information without free choice, full informed consent, and convenient, easily understood mechanisms for opting out.

You might ask, "doesn't per-call blocking alone provide the necessary choice?" No, it doesn't. Per-call blocking is like saying, "every single time you drive your car into a gas station, your car instantly becomes the property of the gas station unless you remember to say abracadabra before you start pumping your gas." In each case, the cards are stacked against your ability to maintain control over something of yours, whether your car or your information.

What can you do? Write a letter to the FCC, with a copy to your state attorney general and public utilities commission and to your local newspaper. Send them the list of CNID commands I provided above. Spell it out for them, and provide answers for the obvious pro-CNID arguments. Your state regulators might even agree with you already, in which case they need your support.

For more information, send a message that looks like this:

To: rre-request@weber.ucsd.edu  
Subject: archive send cnid

Or contact the organizations that are working on this issue:

- \* Computer Professionals for Social Responsibility, cpsr@cpsr.org
- \* Electronic Privacy Information Center, epic@epic.org
- \* Electronic Frontier Foundation, eff@eff.org

Or start something of your own. The best way to predict the future, after all, is to create it yourself.

Phil Agre, UCSD

---

## Creating kidspaces on the net

*Prentiss Riddle <riddle@is.rice.edu>  
Wed, 28 Sep 1994 12:38:13 -0500 (CDT)*

Pardon the lengthy cascade, but I believe it illustrates some of the RISKY thinking on this topic. This is from a thread in alt.internet.media-coverage and elsewhere:

Michael Dillon (mpdillon@halcyon.com) wrote:  
: Bruce Robertson <broberts@sam.neosoft.com> wrote:  
: > tappd@sam.neosoft.com writes:  
: > > I mentioned to the folks at Neosoft that they should package a  
: > > "parent-lock" account...just like their standard stuff, but the  
: > > account owner could set the acceptable newsgroups at the server  
: > > with a special password so that the client reader never saw  
: > > them. They expressed some minor interest  
: >  
: > There's no simple way for a service provider to do this. Nor anyone  
: > else, that I can see.  
:  
: I'm surprised that a Senior TECHNICAL Editor at such a magazine

: can't think of half a dozen ways to do this. Indeed it is  
: technically feasible to make a "safe space" on the Internet  
: for kids and in some ways it is almost a trivial thing to do.  
:  
: As for justification, do we hold school classes on the streets  
: in a red light district or in a bar? No, we create a "safe space"  
: for youngsters and hold classes there, in the school.  
:  
: The moderated newsgroup mechanism combined with controlled  
: feeds (somewhat like clari.\*) could be easily adapted  
: to create newsgroups in which only registered people or  
: registered sites could post. This would merely involve  
: a bit of work with shell scripts or PERL scripts.  
:  
: Securing the Web or Gopherspace would be a little more challenging  
: but a start would be a modified Gopher or WWW client that  
: can only access authorised sites or sites registered with  
: a central authority.

I think that this approach is naive, but not *\*entirely\** unfeasible.  
Some general points:

(1) There is no way to do this solely at the client side. Existing services on the Internet are not reliably marked as to their suitability for children. Only by creating centralized authorities on the *\*server\** side could one add the markers needed to limit children's access to objectionable materials. So in the context of what a service provider like Neosoft can do, Bruce Robertson was quite right.

(2) If the net establishes widely used protocols to allow central authorities to control what children can and can't see, then those same protocols could be used to control what adults can and can't see. We should be aware of this consequence before we adopt such technology.

(3) There are fundamental problems of scale in any such system which would necessarily turn a many-to-many interactive medium into a few-to-many broadcast medium, thus eroding the principal benefit of computer networks. You and I would be unlikely to have this conversation under such a scheme.

(4) The major attraction of distributed document retrieval systems like the World Wide Web and gopher is that they are *\*distributed\**. Many individuals and institutions working in parallel come up with a greater variety of useful resources than could ever be planned and executed by a single, centralized organization. This is fundamentally at odds with the concept of a central registry of "approved sites". Furthermore, a central approval authority would have to be not merely a registration service for sites which educators had deemed harmless, but would have to exercise *\*control\** (through a contract or other means) over the content at those sites. Otherwise, one would continually find that yesterday's kid-safe site had today been blemished by objectionable material.

(5) One fallacy common to proponents of isolated child-friendly

networks is that problems only occur when children can communicate freely with adults other than their teachers. In fact, children are very good at communicating objectionable material to other children. (I'm sure we can all think of examples from our own childhood.) What's more, I suspect that the average adolescent (male, at least) is far more likely to publish objectionable material than the average adult, which casts doubt on the advantages of isolated K-12 networks. Only by limiting the children's ability to publish information -- denying children access to E-mail, for instance -- could one be sure that an isolated educational network would be free of objectionable material.

(6) The existing Usenet moderation mechanism is notoriously easy to spoof. Any bright 12-year-old with access to the manuals could figure out how to forge an "Approved:" line. Any rating or registration mechanism would have to have complex authentication mechanisms built into it or face the likelihood of being foiled (probably by the kids themselves).

(7) Any system based on adding a backwards-compatible restriction mechanism to existing protocols runs the risk of being foiled by users surreptitiously gaining access to unrestricted versions of the same client software. Thus a kid-safe network would either have to guarantee that children couldn't download an unhobbled version of Mosaic, say, or it would have to isolate itself further by using purposely incompatible protocols.

For all of these reasons, I have my doubts about the usefulness of attempts to build an isolated "kidspace" on the net. If you can't deal with the risk that some children at some time will run into some objectionable material, keep them off the net and stick to CD-ROMs. (Or, the cynical might say: keep them locked in a closet and don't teach them to read.)

Prentiss Riddle Systems Programmer and RiceInfo Administrator, Rice University  
2002-A Guadalupe St. #285, Austin, TX 78705 / 512-323-0708 riddle@rice.edu

---

### **And you thought one-letter passwords were RISKy ...**

*Dan Astoorian <djast@utopia.druid.com>  
Tue, 4 Oct 1994 23:31:04 -0400*

Another anecdote illustrating the RISKS of ill-designed user interfaces....

Our office E-mail system is Microsoft Mail. A couple of weeks ago I was chatting with a co-worker, and asked her whether she had read a certain mail message that morning. She told me she hadn't, because she was having problems with her password in Mail.

She told me that in the middle of changing her password, the window just "disappeared," and that now her old password wasn't working anymore.

After thinking a bit about how the "change password" dialog works, I

figured out what had happened. The form has three fields:

Old Password: \*\*\*\*\*

New Password: \*\*\*\*\*

Re-Enter New Password: \*\*\*\*\*

along with the OK and Cancel buttons. The OK button was only active when the New Password and Re-Enter New Password fields matched.

What she had done, of course, was type her old password and press Enter, thinking this would move her to the New Password field (she should have pressed Tab); unfortunately, Enter meant "OK" for the change password dialog. Since "New Password" and "Re-Enter New Password" were both empty (and thus matched each other), pressing OK set her password to the null string without her realizing what had happened.

Perhaps it's reasonable for some systems to allow their password systems to be disabled by setting a null password, but being able to do it by accident is somewhat scary; it's almost farcical that my co-worker, having deleted her password, was now unable to log on (since she was presented with a password challenge, the *only* correct answer to which was "nothing", yet she had no reasonable way of knowing this).

Dan Astoorian, Mississauga, Ontario, Canada [djast@utopia.druid.com](mailto:djust@utopia.druid.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 16: Issue 47**

**Thursday 20 October 1994**

## Contents

- [Computer mess at Greyhound](#)  
[Phil Agre](#)
- [British Rail Journey Planner](#)  
[Marcus Reynolds](#) via [Clive D.W. Feather](#)
- [Spin control by computer](#)  
[Rob Hasker](#)
- [Tampering blamed for rebuffed candidacy in Peru](#)  
[PGN](#)
- [Re: Data Security in Iceland; Software Bug Cripples Singapore](#)  
[Jim Haynes](#)
- [Tarom Airbus: automatic mode switch escaped the commandant](#)  
[Daniel Salber](#)
- [Computer risk that nearly proved deadly](#)  
[Carl Maniscalco](#)
- [Software reuse](#)  
[Mark Gonzales](#)
- [Risk of seeming similar interfaces](#)  
[Monta Elkins](#)
- [Re: squirrelcide](#)  
[Douglas W. Jones](#)
- [Re: CNID](#)  
[Peter da Silva](#)  
[Scott E. Preece](#)  
[A. Padgett Peterson](#)
- [Washington DC ACM Professional Development Seminars](#)  
[John Sheckler](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Computer mess at Greyhound

*Phil Agre* <[pagre@weber.ucsd.edu](mailto:pagre@weber.ucsd.edu)>  
*Thu, 20 Oct 1994 11:55:19 -0700*

The 20 Oct 1994 Wall Street Journal contains an article about computerization

at Greyhound that you'll have to read to believe. The full reference is:

Robert Tomsho, How Greyhound Lines re-engineered itself right into a deep hole, Wall Street Journal, 20 October 1994, pages A1, A10.

After Greyhound came out of bankruptcy a few years ago, a new management team declared that they would revolutionize the company but cutting costs and creating a huge computerized reservations system to replace the existing collection of incompatible systems and things done by hand. They called it "re-engineering". Wall Street liked this idea and bid up the company's stock price. The managers, feeling obliged to keep the stock price up, promised that the system would work on schedule.

But of course it didn't, for reasons that won't surprise Risks readers. The main problem is that buses make many more stops than airplanes, meaning that a bus scheduling system is an order of magnitude harder to build than an airline scheduling system, which is already one of the most complex things anybody ever built. The system started slipping behind schedule, and the prototype had a terrible interface, crashed all the time, and hung up on people.

Meanwhile, Greyhound was falling apart. Employee turnover was very high, customer service was terrible, the computer was messing up everything it touched, and the company advertised a discount program even though it had no chance of handling the expected volume of business. Yet the stock price stayed high because stock analysts, who make dramatically more money than Greyhound's customers, don't ride buses and so didn't see the problems. This postponed the day of reckoning long enough to cause tremendous disruption for the customers -- and long enough for the top managers of the company to cash in a pile of options while the stock was still at its highest level.

"Looking back, Mr. [Thomas] Thompson [the vice president in charge of developing the system] says, "I should have quit or just said that I couldn't do it." Instead, most copies of his report [warning of difficulties with the system] were destroyed, and any mention of it was purged from many Greyhound agendas, calendars and computer files, many people say."

It's distressing that words like "re-engineering" can have such magical force for so many people that well-known pitfalls in system implementation can go undetected for so long -- except, of course, by the working people who have to use the systems or get around on the bus.

Phil Agre, UCSD

[But don't wait for Greyhound to put on the dog. PGN]

---

## British Rail Journey Planner

"Clive D.W. Feather" <clive@sco.com>  
Mon, 17 Oct 1994 12:03:41 +0100 (BST)

On Saturday morning, 15 Oct 1994, two trains collided head-on on a section of

single track south of London. The causes of the crash aren't yet known, but someone on the newsgroup uk.transport looked up one of the trains in question using British Rail's own software (sold to the public):

> Newsgroups: uk.transport  
> From: Marcus@mreyno.demon.co.uk (Marcus Reynolds)  
> Subject: BR Journey Planner (Uckfield - Oxted)  
> Date: Sun, 16 Oct 1994 09:12:21 +0000  
>  
> When asked for the times of trains between Uckfield & Oxted on a Saturday  
> morning, British Rail's own Journey Planner software offered:-  
>  
>           Arrival  Departure  
> Uckfield           8:00  
> Cowden            8:29   8:29   no change  
> Oxted             8:48  
> Journey time 0:48  
>  
>           Other Solutions  
>  
> INTERRUPT ODH, GENERAL PROTECTION FAULT   possible illegal address  
> error code = 0000  
>  
> [Etc., etc.]  
>  
>   Clearly this is a computer programme with second sight. [MR]

Clive D.W. Feather, Santa Cruz Operation, Croxley Centre, Hatters Lane,  
Watford, WD1 8YN, United Kingdom clive@sco.com +44 1923 813541 FAX-813811

---

## Spin control by computer

*Rob Hasker <hasker@hal.cs.uiuc.edu>  
Fri, 14 Oct 1994 13:19:38 -0500*

As to be expected, the governor's race in Illinois is pretty heated and involving a fair bit of mud-slinging. The latest story (reported in the Oct. 11 Champaign-Urbana News-Gazette) concerns the husband of one candidates, Dawn Clark Netsch; apparently he failed to pay property taxes for four years on a condominium in Chicago that they owned. Of interest to RISKS readers is that he blames the problem on a computer at the county tax office; he claims that he didn't pay because the county sent the tax bill to the wrong address. The condo is on Goethe street, and the story is that both E's in the street name were dropped in the county tax records, leaving 'Go th' and making it appear that the street was '60th.' According to Netsch's husband, this meant he never got the tax bill. Whether or not this is a valid excuse, I thought it was an interesting application of computers to spin control.

Rob Hasker hasker@cs.uiuc.edu

---

## Tampering blamed for rebuffed candidacy in Peru

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

Thu, 20 Oct 94 10:00:22 PDT

Susana Higuchi, deposed wife of Alberto Fujimori (president of Peru), had her presidential hopes quashed by Peru's electoral board because of a shortage of valid signatures. Higuchi claims to have submitted about 130,000 signatures, while the board claims only 11,851 were valid, short of the required 100,000. Higuchi claimed some 150,000 signatures were erased from her party's computers during a blackout that affected only the block in which her offices were located. She blamed her husband's cronies for high-tech fraud. [Source: San Francisco Chronicle, 20 Oct 1994]

The moral of this story is certainly familiar to RISKS readers.

I paraphrase an old song:

Backup your troubles in your old kit bag, and smile, smile, smile.

[And read the next item. PGN]

---

## Re: Data Security in Iceland; Software Bug Cripples Singapore

Jim Haynes <haynes@cats.ucsc.edu>

Thu, 20 Oct 1994 14:55:17 -0700

>From: hauh@ismennt.is (Haukur Hreinsson)

>Subject: Data security in Iceland

>[story of theft of a computer, containing the only copy of a writer's MS]

Some years ago I received a letter from the publisher of a small magazine that I subscribe to. Someone had broken into their office and stolen the computer, and (this was back in CP/M days) all the floppy disks that were nearby. So they had done a mailing from some old paper copy of a list of subscribers, and were asking us to tell them when our subscriptions expired, by looking at mailing labels on the last copies received.

Ever since then, wherever I go, I preach to people about making backups and keeping a copy of the backup in some safe place where it won't be easy to steal along with the computer. I wonder if there's a way to get this message out to the myriads of small business and organization people who aren't in a position to read the computer industry literature. If only we could get the story to be spread and repeated as well as the Craig Shergold plea and the gold star tattoo urban legend!

>From: Lee Lup Yuen <lupyuen@singnet.com.sg>

>Subject: Software Bug Cripples Singapore Phone Lines

I wonder if the writer of the software bug will be tried and sentenced to caning. A new concept in software quality assurance!

## **Tarom Airbus: automatic mode switch escaped the commandant's notice**

*Daniel Salber <daniel.salber@imag.fr>*

*Wed, 19 Oct 1994 23:59:21 +0100*

This is a shortened translation of an article published in Le Monde, date 16-17/10/94, p. 9.

Le Monde is considered by many as the major and most-respected French daily newspaper. It always has very documented and accurate reports.

Thanks to Francis Jambon for help with the translation of technical terms.

In-flight stall of an A310 Airbus

An automatic mode switch escaped the commandant's notice

The investigation commission shed more light this Friday on the incident that involved an A310 of the Tarom airline on the 24th of September over the Orly Paris airport. It appears that the aircraft which was in "landing approach" mode was too fast. This triggered a "mode" switch response from the aircraft. In other words, the aircraft started to go upwards to slow itself down.

The aircraft was flying at 364 kilometers per hour (226 mph or 202 knots), slightly over the speed limit of this configuration which is 360 kmph (224 mph or 200 knots). This triggered the automatic response. The pilot tried to counter its effect and thus started a process that provoked the stall of the aircraft. This new information lead the French civil aviation authority (DGAC) to decide to inform immediately the French airlines that use A310s and A300-600s equipped with the same protection mechanism. The DGAC asked the airlines to draw the attention of the crews on the required observation of established speed limits. Airlines should also make sure that the crews are perfectly-well informed of the logics of the protection system that automatically triggers in case of abnormal speed.

Daniel Salber, Grenoble, France, Daniel.Salber@imag.fr

---

## **Computer risk that nearly proved deadly**

*<HeavyWater@aol.com>*

*Tue, 11 Oct 94 17:17:50 EDT*

A woman with whom I am acquainted recently wound up in the intensive care unit of a local hospital due to a computer risk.

The woman, who has been in ill-health for some years and has been undergoing regular dialysis, accidentally pulled out her shunt (a semi-permanent connection point for the dialysis machine) while sleeping and had to undergo urgent but relatively minor surgery at the local hospital emergency room. During this procedure, the ER physician - who had been informed that the woman had a pacemaker implanted - used an electrocautery device to stop the bleeding. The surgery itself went well; however, the woman's condition deteriorated. After some days went by and doctors had told relatives that the

woman was not expected to survive, it was discovered that the electromagnetic field created by the electrocauterizer had apparently corrupted the software of her microprocessor-controlled pacemaker, causing it to fire in a pattern out of sync with her natural cardiac rhythm. The difference was slight enough to avoid immediate detection but serious enough to cause problems. A representative of the pacemaker's manufacturer was able to reprogram the unit (using data transmitted to the still implanted unit as audio tones via a transducer) and the woman is now recovering quite nicely.

I believe the risk here is pretty obvious.

Carl Maniscalco (heavywater@aol.com) San Diego, CA

---

## Software reuse

<markg@ichips.intel.com>

Wed, 19 Oct 94 14:39:18 PDT

There's an interesting letter in the October '94 IEEE Computer Magazine (page 5). I'll quote the first paragraph:

Marty Leisner of the League of Programming Freedom writes:

Capers Jones had a nice article in Computer on the economics of software re-use, but he should have changed "First, you cannot safely reuse garbage." to "First, you cannot economically reuse garbage." Many computer applications don't exhibit "safety" aspects (the worse that can happen is they do not work as advertised).

I think this is a risky attitude in the modern world. Almost any program that produces output that is used by humans can have a safety aspect - people can be physically or economically injured if the application gives the wrong answer. This means any program from a spreadsheet, to a C compiler, to a nuclear power plant control system can be safety critical for some or all of its users.

Published reusable software should be as carefully designed and verified as any other safety critical software, since its publishers will have no control over what systems it gets reused in.

Mark Gonzales markg@ichips.intel.com

---

## Risk of seeming similar interfaces

Monta Elkins <Monta@vt.edu>

Thu, 20 Oct 1994 13:16:39 -0400

We're a PC compatible office that may switch to Power Mac's (due to external economic incentives). While installing software on a new Power MAC my colleague needed the serial number on the disk in the drive. He reflexively reached up and pressed the button below the disk drive to eject the disk,

except on the Power Mac this is the POWER button. This crashed the installation (and generally confused the operating system).

For a company that actively seeks converts from the PC compatible market; they (Apple) should have caught this problem and moved the power switch AWAY from the disk drive.

This illustrated the risk of SEEMINGLY similar interfaces.

(maybe pressing the power off button should light a second button, labeled "Are You Sure?" :)

monta@vt.edu

Monta Elkins Career Services Virginia Polytechnic Institute and State Univ.

---

### Re: squirrelcide (PGN, [RISKS-16.46](#))

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

Thu, 20 Oct 94 09:57:37 CDT

A brand-new locally invented anti-squirrelcide device is currently under test by Iowa Illinois Gas and Electric in my neighborhood. Their initial reports are extremely favorable (transformers equipped with the device in a 6 month test run killed no squirrels, other transformers in the same area had their usual kill rate). Given that it costs the utility about \$100 a squirrel kill to replace blown fuzes etc, the device is showing up as a winner (it's trivial to install and inexpensive).

The device is a band which snaps around the insulator on the high voltage feed to the transformer (the favored site for squirrels to zap themselves) and gives them a warning tingle before they get a chance to do themselves in. Just a plastic band with stainless steel fingers, with all electric current needed to provide the tingle coming from leakage through the air and over the insulator surface. SRI and PG&E ought to look into something like it!

Doug Jones jones@cs.uiowa.edu

---

### Caller ID flamage... not again...

Peter da Silva <peter@nmti.com>

Thu, 20 Oct 1994 12:25:20 -0500

Another Anti-CNID fella misses the point:

> The article states clearly that the real reason for CNID is commercial.

Be that as it may, we have CNID now and it's proven a valuable weapon against telemarketers. Virtually all telemarketers call from their own business phone, transmitting the business address. It's great: here's three calls fifteen minutes apart from the Houston Symphony. No thanks. We can pick and choose who we want to listen to (Hi! Sure, I've got a bag of clothes for your charity) and who we want to do the receiver drop on

(companies with names like Allied Marketing are a good choice).

Best of all, I can call my wife! She's a little phone-shy, so she doesn't answer the phone much during the day... but with CNID she knows it's from work and I can talk to her.

> Privacy advocates have been saying this for years, and for a long time they  
> have gotten patronizing lectures about how CNID is for residential use in  
> catching harassing phone callers.

CNID is for all sorts of things, including things the companies pushing it have never thought of. I include telemarketers in the category of harassing phone callers and it catches them just fine.

> But CNID is a poor way to catch harassing phone callers.

Really? You think it's responsible to call the cops on some dumb kid with a little spare time? I call their parents and let them resolve the problem at home. Haven't used CNID for that yet, but Call-Return worked in one case... in the other the kids called when their parents were out :-< but next time they'll have to deal with daddy :->.

[stock id-blocking feature list]

Your enhancements are fine, and I have no problem whatsoever with them. I would still buy CNID with them in place. In fact I'm pretty sure they are... I've had a couple of calls like that... and I still bought the service. Certainly the local stores selling ID boxes are doing a brisk business.

I don't know who you think CNID proponents are, but it's nowhere near as simple as you make it out.

> What can you do?

Well for a start you can quit pushing it as a "pro-CNID" "anti-CNID" argument, because all that does is polarise people who *would* be on your side into taking an opposed position just to defend a capability they consider important. And you can quit acting like all the pro-CNID people are nasty telemarketers, too.

You can catch more flies with honey, and all that rot...

---

## Calling Number ID debate

*Scott E. Preece <preece@predator.urbana.mcd.mot.com>  
Thu, 20 Oct 1994 08:27:21 -0500*

Phil Agre suggests some simple rules for calling-number ID. I'd like to promote a simple adaptation that would retain essentially all of the subscriber benefit of CNID, even when blocked. Require the phone company to assign a second unique number (a blind identifier, not a directly dialable number) to each telephone and supply that number, instead of the regular phone

number, when the caller is blocking. This would allow the recipient to identify the caller without giving the recipient a callable number.

As an enhancement, the phone company could be allowed to offer to attempt calls through that number (call an 800 number then key the blind identifier), but the subscriber must be able to specify that (1) all such calls are to be rejected, (2) all calls from a particular number are to be rejected, or (3) all calls from a particular number are to be accepted.

I don't think this represents a serious technological hurdle; I think it answers the privacy concerns and provides a significantly more useful service than one that allows simple blocking.

scott preece motorola/mcg urbana design center 1101 e. university, urbana, IL 61801 217-384-8589 preece@urbana.mcd.mot.com fax: 217-384-8550

---

## Calling Number ID Debate

*A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>*

*Thu, 20 Oct 94 09:55:17 -0400*

First, readers should be aware of the CNID FAQ which I wrote some time ago - it is available at the Telecom archive or I can send a copy.

Second, I am strongly in favor of nationwide CNID as should be all system owners with dialup lines (of course I am also in favor of Clipper as soon as the gov - next month ? - drops key escrow so be forewarned 8\*).

Why, because with CNID, crackers/phreaks/war dialers will have to find another way - unless the number is known and on an approved list, the modem doesn't answer at all. True, not all people call in from known numbers but in the two years I have been testing, a very high percentage - over 80% - of the dialins are local and known. Of the other 20%, nationwide CNID will handle about 5% leaving 15% that will need a different number to dial and OTP devices.

Further, since starting to play with this two years ago (my FreeWare .ASP for Procomm + is still in the Telecom archives), I have found it possible to not only block unwanted calls but create a tailored menu/connection for employees calling from home that connects directly to their preferred platform (normal authentication is still required but it does not have to be multi-step).

Somehow in all of the noise, this market seems to have been missed entirely but with more and more telecommuters/service providers/dial-up accounts/etc. it is a natural protection and additional layer of security/logging that also happens to be invisible to conventional attack.

True, a caller does not have to give their number and the telcos will provide means to accomplish it but \*I reserve the right not to answer blocked calls\*. Using crude equipment (a Supra (plug) v.32b modem - the CNID was a \$20 option) this was possible two years ago. What I do not understand is why more people are not using it - a whole untapped market that seems to have been ignored.

Sure there are problems - my biggest one was the time to scan an "approved" list that kept growing using a 386-25/ST-225 combination - sometimes it would take five rings before the whole list could be scanned & the modem told to answer - but that's what engineers are for 8\*).

Padgett

ps please do not inquire about a product. Other than the original freeware .ASP, the rest has been a hobby: there is no GUI or pretty packaging, that's what vendors are for. The point is it \*can\* be done - after proving that, I tend to lose interest.

---

## Washington DC ACM Professional Development Seminars

*John Sheckler, ATSC, 301/805-3258 <ndqajds@atscv1.atsc.allied.com>  
20 Oct 1994 10:53 EST*

The Professional Development Committee of the Washington, D.C. Chapter of the Association for Computing Machinery (ACM) presents technical and management seminars for computer professionals and managers. This fall, the Committee will offer ten one-day professional development seminars during the week of November 14 - 18, on topics of current interest.

### Monday, November 14

- Mr. Allen S. Perper - Business Process  
Engineering/Reengineering
- Mr. Will Tracz - Domain-Specific Software  
Architectures -- Process,  
Products, and Infrastructure

### Tuesday, November 15

- Dr. Cy Svoboda - Information Engineering
- Mr. Mike Gorman - Managing the Development  
of Client/Server Applications

### Wednesday, November 16

- Mr. Ed Krol - The Whole Internet -- Archie,  
Veronica and the Gopher Explore  
the World Wide Web
- Mr. William Durell - Data Administration and  
Management

### Thursday, November 17

- Dr. Robert N.Charette - Profiting from Risk Management  
of Business Processes
- Mr. Watts S. Humphrey - Personal Process Improvement

### Friday, November 18

- Dr. Robert S. Arnold - Legacy System Migration
- Mr. Edward V. Berard - Testing Object-Oriented  
Software

Additionally, on Thursday, November 10, 1994, the Professional Development

Committee will host our 13th International Speaker, Philip Zimmermann, presenting a seminar entitled "Public Key Cryptography."

Thursday, November 10 - 13th International Speaker

Mr. Philip Zimmerman - Public Key Cryptography

The seminars will be held at the Center of Adult Education, University of Maryland, College Park, Maryland, at the intersection of University Boulevard (MD 193) and Adelphi Road. The seminars run from 9:00 a.m. (registration at 8:30 a.m.) until 5:00 p.m.

Attendance at each course will be limited to the capacity of the room being used (check with the ACM/PDC answering machine, (202) 462-1215, for availability). Detailed registration information and assistance can be obtained by calling Nora M. Taylor (301) 229-2588. Additional information about the Fall 1994 professional development seminars presented by the Washington, DC Chapter of the ACM can be requested via e-mail to [dcseminars@acm.org](mailto:dcseminars@acm.org) and is available also via anonymous ftp from [acm.org](http://acm.org) in: [chapter\\_forums/chapter\\_articles/prochap/DC\\_ACM\\_Fall\\_94\\_PDS\\_General.txt](ftp://acm.org/chapter_forums/chapter_articles/prochap/DC_ACM_Fall_94_PDS_General.txt). A description of each seminar is available also. [File names deleted, along with registration info.]



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 16: Issue 48**

**Friday 21 October 1994**

## Contents

- ["The Mother of All Utility Bills."](#)  
[F. Barry Mulligan](#)
- [Observed Electro-Magnetic Interference](#)  
[Henry Troup](#)
- [Re: Computer risk that nearly proved deadly](#)  
[Mark Thorson](#)  
[Gary Koerzendorfer](#)
- [Cellular Phone Fraud Operator Arrested](#)  
[Paul Robinson](#)  
[Chip Maguire](#)
- [Not enough bytes bites again](#)  
[Marc Auslander](#)
- [Inadvertent postal forwarding](#)  
[V. Michael Bove Jr.](#)
- [Computer model of Haiti](#)  
[Phil Agre](#)
- [Re: Risks of not thinking about what you're stealing](#)  
[Joel Finkle](#)
- [Re: Risk of similar interfaces](#)  
[Chris Norloff](#)  
[Erann Gat](#)  
[John Mainwaring](#)
- [Re: Software reuse](#)  
[David Honig](#)
- [Re: Greyhound](#)  
[Danny Burstein](#)
- [CNID and Don Norman -- CNID can be private](#)  
[Justin Wells](#)
- [Re: CNID](#)  
[Andrew Klossner](#)  
[Phil Agre](#)
- [Info on RISKS \(comp.risks\)](#)

---

**"The Mother of All Utility Bills."**

"F. Barry Mulligan" <MULLIGAN@ACM.ORG>

Fri, 21 Oct 1994 13:08:57 -0500 (CDT)

From The Atlanta Constitution, Tues 18 Oct 1994, p.1, by Christopher C. Warren

Imagine a single monthly statement listing all utility charges, including phone, cable, gas, electricity, water, garbage collection and sewerage charges. It could be the mother of all utility bills and would allow consumers to write only a single check for all their services. One Check, as the proposal is being touted, would ease consumer's household management by reducing utility bills to one monthly payment, said Maureen Bailey, vice president of public affairs with American Express, the company proposing the service.

The article goes on to describe the pilot test being proposed for the Atlanta metro area. The cost of the service would be shared by the utilities and the consumer.

Risks? A little late with one payment and you're instantly in arrears with every company in town. Billing disputes "still would be handled through the individual utility companies", but what if the utility says it didn't get a payment you sent to the service company? If your combined statement is mailed on the 15th and a utility transmits a new charge to the service bureau on the 16th, what happens to the payment grace period? If you've ever had to rob Peter to pay Paul, how do you deal with Peter & Paul, Amalgamated?

Perhaps the real question is 'Do I want to give a complete, itemized description of all monthly utility consumption to American Express?' (and pay for the privilege).

---

## Observed Electro-Magnetic Interference

"henry (h.w.) troup" <hwt@bnr.ca>

Fri, 21 Oct 1994 13:39:00 -0400

On Thursday 20 October 1994, I attended an Emergency Response seminar held in the auditorium of a high-tech institute. There were a number of fire and ambulance personnel there "in-service" with two-way radios. A radio transmission inside the auditorium triggered all kinds of equipment - the video projector turned on, the slide projector turned on, and some unidentified motor noise started up.

Nothing new, but an example of a widespread problem (still sometimes not accepted as real.)

Henry Troup - H.Troup@BNR.CA (Canada)

---

## Re: Computer risk that nearly proved deadly (Maniscalco, [RISKS-16.47](#))

Mark Thorson <eee@netcom.com>

Fri, 21 Oct 1994 10:31:02 -0700

The posting in [RISKS-16.47](#) about reprogramming pacemakers through audio tones seems a bit alarming to me. Does that mean someone could have a tape player (i.e. "boom box") with a tape of pacemaker programming signals which would be deadly to certain members of the public? Imagine some guy walking around with that on a crowded train or bus.

How about cutting into the SCA-encoded Muzak played in supermarkets? That's broadcast on the same frequencies used for ordinary FM radio. Often, wireless mikes are used at lectures and concerts. Care to find out how many Rolling Stones fans have pacemakers? The power level from the speakers at a concert hall ought to be much more than is needed for programming.

Anyone know the name of the company that made the malfunctioning pacemaker? It might be interesting to do a patent search on them.

Mark Thorson (was mmm@cup.portal.com, but now eee@netcom.com)

---

### **Re: cauterizer corrupts pacemaker**

*Gary Koerzendorfer <garyk@hpesds3.cup.hp.com>  
Fri, 21 Oct 94 16:20:49 PDT*

I was surprised that a pacemaker would be susceptible to this interference, that it didn't figure it out, and apparently had no fallback mode. I'm not sure what EMI field strength the electrocauterizer created; should a patient be advised to avoid proximity to arc-welders and to 50KW broadcasting facilities like the one next to a bridge in San Francisco Bay?

Secondly, a state-verification circuit (or even a "heartbeat"!) could have detected the malfunction, and regressed to a fallback fixed rate. Your own heart has a 30 beats/minute tertiary protective function - you're unable to engage in strenuous activity, but you remain alive until you can seek help.

An incapacitated patient would be unable to inform ER staff that they had a pacemaker - perhaps if I had one I'd wear a MedicAlert tag.

Gary Koerzendorfer, Hewlett-Packard Co., Systems Techn. Div., 19447 Pruneridge Ave. m/s 42L2, Cupertino Calif 95014 garyk@cup.hp.com (408) 447-4783

[For younger RISKS readers, TWO cases of deaths due to pacemakers being affected by interference are included in the RISKS archives. PGN]

---

### **Cellular Phone Fraud Operator Arrested (Summary and Comments)**

*Paul Robinson <PAUL@tdr.com>  
Thu, 20 Oct 1994 21:37:55 -0500 (EST)*

The following article summary is followed by some comments:

In a Front Page article appearing in the Wed 19 Oct 1994 {Washington (DC) Times} entitled "High-Tech sleuthing busts cellular phone fraud ring" reporter Doug Abrahms tells us that Clinton Watson and two other persons were arrested Monday for selling cellular phones with altered serial numbers, causing the charges to be sent to legitimate cellular users.

According to an Indictment in U.S. District Court in San Jose, when police raided Watson's house, they found 30 phones with counterfeit ID, 16 altered memory chips and 600 mobile phone numbers which could be used for fraudulent calls. Some of Mr. Watson's phones had as many as 12 different ID numbers, thus spreading usage patterns over a large area. Other phones were designed to allow the ID to be changed at will.

Police and cellular companies have turned to using more sophisticated means to find illegal cellular phones, including helicopters, voice prints and traffic analysis.

Mr. Watson is a Computer Programmer who designed his own software to program integrated circuits to include numbers read from scanners used on the cellular band. The phones so set up were referred to as "lifetime" phones since they never got a bill. They sold for \$1,200 to \$1,500 and have been found all over North America, according to Ron Nessen of the Cellular Telecommunications Industry Association (CTIA), which estimates that cellular fraud is a \$1 million a day problem, with people stealing cellular IDs by waiting near tunnels, airports and parking lots to snatch the ID code transmitted.

New York's NYNEX is introducing a PIN code on cellular calls. The Mayor and Police Commissioner of New York City have had the IDs for their cellular phones stolen six times this year. A division of TRW is developing a means to prevent calls unless the user's voice print matches the print on file.

#### Comments:

1. Cellular Companies have been notorious for evading security problems in their phones. Rather than spend the money to add encryption in their switch software, they got a law passed to make it illegal to listen to cellular frequencies and to build equipment that can monitor cellular bands.
2. Cellular phones transmit call information in the clear, so a thief can just use someone else's number and steal a few minutes of airtime from them; if you bleed 10,000 customers of ten extra minutes a month, almost none of them individually will recognize that their bill is ten minutes too high. Unless customers complain, the Cellular Company won't care.
3. A typical practice of an aerospace/military contracting company like TRW is to try an implement and expensive complicated system such as voice print matching instead of something simple and cheap like a device to implement either Kerberos validation, S/Key style one-time passwords, or MD-4/MD-5 arithmetic checksum of some stored value. Putting such methods in as an inexpensive box like a Radio Shack tone dialer might cost users \$20 and installing it in new phones might cost an extra \$2 or \$3. Persons having portable PCs could run a program to generate the code. Since everything is done without a secret being transferred, the software to do this can be public and nothing is compromised.
4. Does using a biometric validation system on a communications network

- scare anyone? I can think of a half-dozen reasons to dislike it, including:
- use of the system to track and locate dissidents and anyone the people who run the government don't like;
  - my sister wants me to call someone for her and find out something without them knowing it's her asking; I don't match her car phone profile;
  - I borrow her car to do an errand; I can't call her back to let her know what I found out for her;
  - Bugs in the software might not recognize the owner with a cold, after an accident that damages their throat, or after some forms of surgery;
  - Checking voice prints will require very heavy processing capability, quite likely slowing down call connection times;
  - I bug someone's car and simply play back the recording to unlock their phone.

I think that this is an attempt to "kill flies with nuclear weapons," e.g. excessive overkill. There are cheaper alternatives such as mathematical verification that will probably be quite effective without using a system that requires expensive and complicated subsystems such as voice print recognition.

---

### Re: (mobile-ip) Cellular Phone Fraud Operator Arrested

<maguire@it.kth.se>

Sat, 22 Oct 94 01:00:54 +0100

Actually - FBI/Cellular operators/... could just buy suitable equipment from a major electronics manufacturer in France - it reportedly even includes key-word spotting.

Certainly why I look forward to widely available portable crypto for mobile voice and data.

Chip

---

### Not enough bytes bites again

Marc Auslander <marc@watson.ibm.com>

Fri, 21 Oct 1994 13:41:16 -0400

---222---

NOTICE ADVISORY TO NAVSTAR USERS (NANU) 222-94266

SUBJ: TIME TRANSFER DATA ANOMALY

1. CONDITION: USERS OF GPS TIME TRANSFER INFORMATION ARE ADVISED THAT THE DATA IS SUSPECT AS OF DAY 266 (23 SEP 94) BEGINNING AT 1500 UTC AND CONTINUING UNTIL FURTHER NOTICE.
2. GPS NAVIGATION POSITIONAL DATA ACCURACY IS UNAFFECTED.
3. POC: CPT JAMES AT COMMERCIAL (719) 550-6378 OR DSN 560-6378.

---223---

NOTICE ADVISORY TO NAVSTAR USERS (NANU) 223-94266

SUBJ: USERSET TIME TRANSFER ERRORS

1. CONDITION: INVESTIGATION HAS REVEALED THERE IS NO CURRENT OR

PAST PROBLEM CONCERNING TIME TRANSFER INFORMATION. WE HAVE DETERMINED THAT SOME USERSETS MAY NOT ACCOUNT FOR ROLLOVER OF THE 8 BIT GPS UTC REFERENCE WEEK. IAW ICD GPS 200, PARAGRAPH 20.3.3.5.2.4, PAGE 18 OF SUBFRAME 4 INCLUDES THE PARAMETERS NEEDED TO RELATE GPS TIME TO UTC. THE USER MUST ACCOUNT FOR THE TRUNCATED NATURE OF THE UTC REFERENCE WEEK. THIS USERSET DISCREPANCY WILL OCCUR EVERY 255 WEEKS AND WILL LIKELY CLEAR AT END OF WEEK ROLLOVER.

2. POC: 1LT PETERSON AT COMMERCIAL (719) 550-6378 OR DSN 560-6378.

Marc Auslander <marc@watson.ibm.com> 914 784-6699 (Teline 863 Fax x6306)

---

## inadvertent postal forwarding

*V. Michael Bove Jr. <vmb@media.mit.edu>*

*Fri, 21 Oct 94 16:12:43 -0400*

The following concerns an acquaintance whom I'll call S, who works at the corporate headquarters of a large firm which I'll call FooCorp (the pseudonyms are used because none of what happened seems to be FooCorp's fault, but some of their clients might be a bit distressed to hear about it).

Having recently changed residences, S filed a mail-forwarding order in her name at her former post office. A few days later, mail addressed to the offices of a number of FooCorp employees started showing up at her new house, complete with yellow computer-generated forwarding stickers. How this happened is partial conjecture on S's and my part, as the postmaster in S's former town of residence wasn't terribly helpful in unraveling the mystery. The trigger seems to be the fact that as part of her employment S has a commercial credit card in the name of FooCorp, and the bills were mailed to "FooCorp, [S's old home address]." Somehow, some combination of postal employees and postal software decided therefore to generate a forwarding order such that mail addressed to FooCorp passing through the postal sorting facility nearest to S's former home should be forwarded to S's new address.

The outcome is that various important-looking pieces of FooCorp's mail were diverted to a rural mailbox in front of a horse barn in the middle of nowhere, and apparently no one in the Postal Service thought this at all odd.

The postmaster thinks the forwarding order has now been eradicated, and S has contacted her credit card issuer to cause the bills to be mailed in her name, not FooCorp's. However, the misdelivered mail hasn't totally stopped, since while the order was in effect, the Postal Service dutifully notified anyone whose envelope said "Address Correction Requested" that FooCorp had moved; there are now at least a few mailing databases out there which think that FooCorp is located at S's house.

The lesson, of course, is that procedures that try automatically to do the right thing without being asked sometimes need a reality check applied to the results.

---

## Computer model of Haiti

Phil Agre <pagre@weber.ucsd.edu>

Thu, 20 Oct 1994 18:15:37 -0700

In an article in The Nation, Allan Nairn asserts that the American military force occupying Haiti is more concerned about the popular movement that elected Jean-Bertrand Aristide than it is about the oligarchy that created the attaches. I don't know whether this assertion is fair, but Risks readers might be interested in one part of his evidence. The full citation is:

Allan Nairn, The eagle is landing, The Nation 259(10), 3 October 1994, pages 344-348.

Here's a quote:

... the Pentagon's Atlantic Command (ACOM) has commissioned Booz, Allen, Hamilton, a corporate consulting firm, to devise a computer model of Haitian society. A similar model was ordered for Iraq for Desert Storm. The model tries to predict "the effects of social, political and economic actions on various sectors of society". In an April 29 report Booz, Allen presented a "Power Relationship Matrix" which divides Haitian society into seven groups, including the "Lower Class Majority", and asks questions like "What would mobilize the masses to take action?"

The crux of the Booz, Allen/ACOM planning theory is thus: "Whether political power is a direct function of popular support or based on the allegiance of key groups and coercion of the remainder of the populace, cohesion of support is a critical question in assessing political power". They place greatest emphasis on the importance of "Organized Civil Society" -- popular and professional groups, unions and associations, development workers -- seeking to identify the points at which mass cohesion will crack. This, they say, is the key to any program for "control of the populace".

Their priority is to build an "organized information bank" and to run a systematic, ongoing "assessment of the relative strengths of opposition organizations", as well as of leading "political personalities". "The tracking of opposition organizations", they say, "should be limited to those which are known to have a basis of political action and some established capacity for taking political action".

As the Washington Office on Haiti has documented in detailed reports, A.I.D. [the US Agency for International Development] is already exploring this divide-and-conquer strategy in Haiti, seeking to cultivate and fund, as on embassy memo put it, "responsible elements within the popular movement" along with "moderate Duvalierist factions". (pages 347-348)

An exercise for the reader: if they implemented such a program for your home town, what would it look like?

Phil Agre, UCSD

---

**re: Risks of not thinking about what you're stealing**

Joel Finkle <jjfink@skcla.monsanto.com>

Fri, 21 Oct 1994 12:55:34 -0500

Tumbling a beeper's activation code is trivial. You can take your beeper to any beeper service company, ask to be switched to their line of service, and they'll recode and activate you, assuming (a) that you're using the same brands that they are and (b) you're \*not\* using the same service company they are (or they can't switch you). Presumably, a stolen beeper could be handled as if you owned it, then there's a high likelihood that you'd get it reactivated.

---

**Re: Risk of seeming similar interfaces (Elkins, [RISKS-16.47](#))**

<cnorloff@tecnnet1.jcte.jcs.mil>

Thu, 20 Oct 94 22:48:41 EDT

ARRRRGGGHH!! And the risk of idiots designing switches! It does not take a rocket scientist to figure out that a critical switch should be put in a hard-to-access location or should have a protective cover over it. This kind of stuff is taught in very basic human engineering classes.

There are certain errors designers are doomed to keep repeating, and switch design is one of them.

Chris Norloff cnorloff@tecnnet1.jcte.jcs.mil

---

**Re: Risk of seeming similar interfaces (Elkins, [RISKS-16.47](#))**

Erann Gat <gat@aig.jpl.nasa.gov>

Fri, 21 Oct 94 11:09:00 PDT

Monta Elkins writes:

>on the Power Mac this is the POWER button

Geez! Will Apple never learn? The original Apple II was notorious for having its reset button on the keyboard immediately adjacent to the return key, with predictable results. If any company should know to put power and reset buttons far away from everything else on the machine you'd think it would be Apple. Sigh.

Erann Gat gat@robotics.jpl.nasa.gov

---

**Re: Risk of seeming similar interfaces (Elkins, [RISKS-16.47](#))**

"john (j.g.) mainwaring" <crm312a@bnr.ca>

Fri, 21 Oct 1994 14:33:00 -0400

The late lamented Commodore company did the same with the Amiga 3000, which has a push power switch in almost the same location as the disk eject button of the A1000. I don't suppose that was the only reason for the company's demise. Still, fond as I have been of the A3000 since the day I got it, that design feature led me to wish an even worse fate on the company on numerous occasions during my first several months of ownership.

---

**Re: Software reuse (Gonzales, [RISKS-16.47](#))**

*David Honig <honig@buckaroo.ICS.UCI.EDU>*

*Fri, 21 Oct 1994 12:18:24 -0700*

>Published reusable software should be as carefully designed and verified as  
>any other safety critical software, since its publishers will have no control  
>over what systems it gets reused in.

I think this is wrong. Ensuring safety is the requirement of the human organization producing a potentially hazardous product. The \*organization\* must have adequate quality checks. One engineer's bad day, one alpha particle, or one bolt's failure, should not harm people.

One wouldn't disallow the reuse of used power supply designs, for instance. Instead, if you were putting them into an important machine, you would not only test their published performance, but perhaps \*add\* additional safety-relevant tests. And then you would design in several of them if the application justified it.

If you want to reuse some code (or other artifact) in a RISKy application, maybe you'll have to characterize it more than a less critical user. What else is new?

Computer professionals should learn that (organizations of) people are responsible; technical professionals are responsible for making technical observations and their implications known to others in the organization.

---

**Re: Greyhound ([RISKS-16.47](#))**

*danny burstein <dannyb@panix.com>*

*Thu, 20 Oct 1994 22:43:44 -0400 (EDT)*

While I haven't seen the original piece, I would expect that it glossed over what may very well be a major, if not -the- major, cause of of the problems -- namely, the horrendous management-labor problems at the company that led to a strike/lockout/mass firing (take your choice....) of the vast majority of bus operators. The bosses, though, as well as the finance MBA types, stayed in office. And, as the article mentioned, cheerfully exercised their stock options to make huge profits.

-dannyb@panix.com (or dburstein@mcimail.com)

---

## CNID and Don Norman -- CNID can be private

Justin Wells <rjwells@undergrad.math.uwaterloo.ca>

Fri, 21 Oct 1994 13:29:49 -0400

In Don Norman, in his book "Things That Make Us Smart", makes some interesting points about Call Number ID. He writes that the emphasis on NUMBERS stems from a mechanistic view of the phone system -- a human view of the phone system wouldn't depend so heavily on numbers (which we have trouble remembering).

He suggests that other information should be sent instead of a telephone number. Perhaps each telephone owner could set a string that accompanies their call instead of their phone number. It need not be more than a few characters -- maybe your first name, maybe the name of your company.

His point is that the average person wants to know WHO is calling, and only businesses, etc., really care about the phone number. This solution should retain the value of CNID (knowing whether you want to answer the phone), but eliminate the privacy risks (including the need for call blocking, etc.)

I found lots of excellent commentary on this and other sorts of RISKS in his book. I know he's posted here before, and I noticed he has a reference to RISKS in his book. I recommend it to everyone.

Justin

[Don also wrote a column for the April 1993 CACM Inside Risks, which has been adapted as a section in my COMPUTER-RELATED RISKS book. PGN]

---

## Re: CNID (Preece, [RISKS-16.47](#))

Andrew Klossner <andrew@frip.wv.tek.com>

Fri, 21 Oct 94 11:54:46 PDT

Require the phone company to assign a second unique number ... to each telephone... I don't think this represents a serious technological hurdle...

It does. Almost all area codes in North America are more than half populated. In order to double the number of phone numbers, most area codes would have to be split.

-- Andrew Klossner (andrew@frip.wv.tek.com)

---

## Re: CNID

Phil Agre <pagre@weber.ucsd.edu>

Thu, 20 Oct 1994 19:09:09 -0700

In his comment ([RISKS-16.47](#)) on my message about CNID, Peter da Silva

<peter@nmti.com> refers to me as an "Anti-CNID fella". But I am not opposed to CNID, only to bad implementations of it that make free choices about CNID difficult. At the same time, he is correct to criticize my generalizations about "CNID proponents". I didn't mean to refer to everyone who finds CNID useful, only the folks who wish to profit from bad implementations of CNID and can hire lobbyists for this purpose.

Phil Agre



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 16: Issue 49**

**Monday 24 October 1994**

## Contents

- ["Computer Related Risks" by Neumann](#)  
[Rob Slade](#)
- [Half a degree is better than none?](#)  
[Mark Brader](#)
- [Re: Barclays Bank Banks Big-Bang Bump-up](#)  
[Mark Brader](#)
- [Re: Not enough bytes bites again](#)  
[Dave Moore](#)
- [The FTC wades in](#)  
[Don Blumenthal via Joel K. Furr](#)
- [That Macintosh Power Switch](#)  
[Don Norman](#)
- [The Risks of Ignorant in Computer Science](#)  
[Yaron Y. Goland](#)
- [More on risky interfaces](#)  
[Mike Perry](#)  
[Gary Page](#)  
[Brad G. Parks](#)  
[Jean Renard Ward](#)  
[Kevin Purcell](#)  
[Kent Borg](#)  
[Mike Alexander](#)
- [Info on RISKS \(comp.risks\)](#)

---

## "Computer Related Risks" by Neumann

*"Rob Slade, Ed. DECrypt & ComNet, VARUG rep" <roberts@mukluk.decus.ca>  
Sun, 23 Oct 1994 20:01:52 EST*

BKCMRLRS.RVW 940906

"Computer-Related Risks", Neumann, 1994, 0-201-55805-X, U\$24.75

neumann@csl.sri.com

%A Peter G. Neumann

%C 1 Jacob Way, Reading, MA 01867-9984

%D 1994

%G 0-201-55805-X

%I Addison-Wesley Publishing Company

%O U\$24.75 (22.25 for ACM, order no. 706943)

%P 384

%T "Computer-Related Risks"

Heather Rignanesi, Marketing, x340, 73171.657@Compuserve.com

Barbara Warren, Marketing barbarw@aw.com

Tiffany Moore, Publicity tiffanym@aw.com

800-822-6339

617-944-3700

Fax: (617) 944-7273

Every technologist should, at some point in the educational process, be required to read this book. (The preceding proviso is, unfortunately, subject to the risk that said technologist may fail to grasp the book's underlying lessons.)

Peter G. Neumann is well known to the members of the Association for Computing Machinery (ACM), but to thousands more he is known as moderator of the RISKS-FORUM Digest electronic mailing list (or its Usenet mirror, comp.risks). (RISKS is notable for the quality and interest of its material, and is a recommended mailing list for all newcomers to the Internet, regardless of their areas of interest.) This work is not merely a compilation, but a distillation of the type of material discussed on RISKS. The occasional item is not strictly computer related (an ongoing RISKS discussion itself), but all demonstrate the variety of ways in which technology may constitute a hazard.

Written primarily in the format of a textbook for an academic environment, the material is not only readable but fascinating for a non-technical audience. The end notes, challenge questions and bibliography make it an excellent choice for any course dealing with security, safety or general systems development issues.

(We interrupt this review to note that PGN is able to write over two-and-a-half pages of the Preface before we find the first pun. By the end of Chapter two, he is in full flight. I refer you to "Tempest Puget, or The Sound and the Ferries" for full multi-model, cliché-referential punning entries.)

As well as system and software engineering students, this book should have a place on the desk of anyone involved in a technology development project. It *can* happen here.

copyright Robert M. Slade, 1994 BKCMRLRS.RVW 940906 604-984-4067  
DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733  
Author "Robert Slade's Guide to Computer Viruses" (Oct. '94) Springer-Verlag

[Thanks, Rob! PGN]

---

**Half a degree is better than none?**

Mark Brader <msb@sq.sq.com>

Sun, 4 Sep 1994 00:59:38 -0400

I recently obtained the new 5th edition of The Official Encyclopedia of Bridge, the major reference book published by the American Contract Bridge League. It happens that several different numbers that relate to bridge can occur in half-integers -- you can be in a 6.5-table duplicate game, hold 3.5 quick tricks, score 1.5 (in the American style) match points, and so on. Where I have used the two ASCII characters .5 in this posting, the book naturally uses the single character 1/2 instead.

Or rather, it tries to. Somehow, wherever the character 1/2 is supposed to occur, instead there is a degree sign!

Somehow I doubt that that'd ever have happened without computer typesetting. An obvious guess is that all drafts for proofing were done with a font having a different character set or encoding from the one used in final production.

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

---

### Re: Barclays Bank Banks Big-Bang Bump-up (Randell, [Risks-16.46](#))

Mark Brader <msb@sq.sq.com>

Thu Oct 20 15:28:01 EDT 1994

> Barclays refuses to disclose the cost of the project, but it is believed to  
> have invested fllOm in customer-based systems. ...

FLLOM to you too! I assume that's 110 million pounds sterling.  
Risks of using a scanner to submit to RISKS...

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

[Also noted by Amos Shapir <amos@nsof.co.il>, and  
by PGN, who did not get around to fixing it. Cute. PGN]

---

### Re: Not enough bytes bites again (Auslander, [RISKS-16.48](#))

Dave Moore <davem@garnet.spawar.navy.mil>

Mon, 24 Oct 1994 10:39:39 -0400 (EDT)

<>NOTICE ADVISORY TO NAVSTAR USERS (NANU) 222-94266

I just wanted to make clear to anyone interested that the described problem is not a defect in the GPS system, it is a failure by certain receiver manufactures to properly implement the specifications.

The referenced subsection refers to the handling of "Leap Seconds".  
<Note: Leap Seconds are unrelated to leap years.>

GPS maintains time as second count from a base value. Off the top of my head, I believe that the base time is midnight Jan 5/6 1980. GPS maintains a COARSE time field as a 10 bit week count from this base. There is also a sub field that warns of leap seconds in the near future or recent past. To save bits, the leap second warning only uses the least significant 8 bits of the 10 bit week field. The receiver is supposed to performed a clearly specified algorithm to account for this 4+ year subrange. Apparently some receiver manufactures did not properly implement this.

On a speculative note: The GPS satellite 10-bit week field should roll over sometime around August 1999. At that time the base time reference of Jan 1980 becomes August 1999. I wonder how many receivers will correctly handle that rollover? If any of you out there have access to a receiver you can play with; try initializing it with a date of Oct 1999 and see if it correctly initializes itself to 20 years (1024 weeks) in the future from current time, or drops back to current time implying a hard coded base of 1980 that may not work after August 1999. Note that this is speculation on my part; I don't know for sure that this interpretation is correct.

As always; your mileage may vary!

---

## The FTC wades in

Joel K. Furr <jfurr@acpub.duke.edu>  
24 Oct 1994 11:39:19 -0400

From: Don.Blumenthal@wpo.ftc.gov

FOR RELEASE: SEPTEMBER 14, 1994

FTC TARGETS ADVERTISING ON "INFORMATION SUPERHIGHWAY":  
Credit repair co. urged consumers to falsify data, FTC Charged

In its first case targeting advertising on the "information superhighway," the Federal Trade Commission has charged a Sacramento, California, man with making false claims in the course of promoting his credit-repair program on an on-line computer service. The FTC alleged that Brian Corzine, doing business as Chase Consulting, promoted his \$99 program on America Online. The program allegedly advises consumers to take illegal steps in order to repair their credit records, while representing that it is "100% legal." At the FTC's request, a federal district court has ordered a temporary halt to the alleged deceptive promotion, and frozen Corzine's assets to preserve any funds for consumer redress.

"As these computer networks continue to grow, we will not tolerate the use of deceptive practices here any more than we have tolerated them on other recently-emerged technologies for marketing products and services to consumers," said FTC Chairman Janet D. Steiger in announcing the case.

In its complaint detailing the charges in the case, the FTC alleged that Corzine (also known as Brian Chase) advertised his credit program on America

Online, instructing consumers to contact Chase Consulting through the computer service. Corzine allegedly enticed consumers to do so by using statements such as:

-- "FOR JUST \$99.00 WE WILL SHOW YOU HOW TO CREATE A BRAND NEW CREDIT FILE AT ALL 3 OF THE MAJOR CREDIT BUREAUS...100% LEGAL AND 200% GUARANTEED."

Consumers who contacted Chase Consulting by computer received a three-page description of the program instructing them to obtain a "taxpayer identification number" from one of a few specific Internal Revenue Service regional centers and then to use this number in place of their Social Security number on credit applications. The complete "file segregation" program included a booklet which further instructed consumers to obtain two new addresses: one for use on their driver's licenses and one for use on credit applications. Corzine allegedly represented that the program is legal. But consumers who falsify statements on certain loan and credit applications or falsify their Social Security number would violate one or more federal criminal statutes, the FTC said.

The FTC has asked the federal district court to issue a permanent injunction against Corzine prohibiting him from engaging in these kinds of practices in the future, and ordering him to pay consumer redress.

The FTC vote to file the complaint was 3-0, with Commissioner Dennis A. Yao not participating. It was filed under seal in U.S. District Court for the Eastern District of California, in Sacramento, on Sept. 12, 1994. The seal was lifted late yesterday.

NOTE: The Commission files a complaint when it has "reason to believe" that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. The complaint is not a finding or ruling that the defendant has actually violated the law. The case will be decided by the court.

Copies of the complaint and free FTC brochures for consumers titled "Credit Repair Scams," "A New Credit Identity: A New Credit Repair Scam," and "How to Dispute Credit Report Errors," which offer tips on avoiding these types of schemes and correcting your own credit record, are available from the FTC's Public Reference Branch, Room 130, 6th Street and Pennsylvania Avenue, N.W., Washington, D.C. 20580; 202-326-2222; TTY for the hearing impaired 202-326-2502.

###

MEDIA CONTACT: Bonnie Jansen, Office of Public Affairs  
202-326-2161  
bonnie.jansen@wpo.ftc.gov

STAFF CONTACT: Bureau of Consumer Protection  
David Medine, 202-326-3224  
david.medine@wpo.ftc.gov

Jeffrey S. Markowitz, 202-327-2460

jeffery.markowitz@wpo.ftc.gov

(FTC File No. 9423295)  
(Civil Action No. CIV-S-94-1446 (DFL))  
(chase)

---

## That Macintosh Power Switch

*Don Norman <dnorman@apple.com>  
Sun, 23 Oct 1994 10:39:00 -0700*

Suddenly RISKS has become concerned over the placement of the power switch on the on a model of the Mac. Sigh. The concern is justified, but the solution not quite so apparent.

Would RISK readers be reassured or appalled to discover that several months ago I thrust myself into the battle and now am in charge of solving the problem? Ah, a simple problem, one I thought would offer some relief from the more substantive issues I normally grapple with. All I had to do was find a consistent logical spot to put the power switch, and do it right, once and for all.

Wrong. Now several months later, after numerous meetings and roughly ten draft proposals, meeting with roughly 30 people from several divisions of the company, we are perhaps near a solution. Perhaps, but hardly a week ago a new problem arose that, as yet, does not have a solution.

Let me tell you, it isn't easy to do a consistent policy on power switches. The proposal, plus justification is 21 pages. First of all we have an incredible variety of machines, from those used as high power workstations, to servers (which need protected power switches), to office, home, and educational machines. And portables. Some machines are placed on the desk, often with the monitor on top. Some are placed on the floor. Some are rotated to stand on their side. Some would seem to require clearly marked, easily accessible switches. Some need switches out of reach.

On top of these problems, we don't even want people to use the power switch: it invariably leads to damage. We prefer them to use the shutdown menu which can do a neat, orderly quitting of applications and safe shutdown. Under normal conditions, it would be best not to have a power switch at all. But sometimes it is necessary to disconnect power. And I have even heard it claimed that our software sometimes crashes (really?), so that a soft, graceful shutdown isn't possible. In this case, some sort of shutdown switch is required, one that bypasses system software.

Some otherwise simple solutions are ruled out by cost considerations. In the low-end market, where cost dominates and the profit margins are negligible, even a very slight extra cost can disrupt product sales, so if we want a uniform policy for all machines, it has to be one acceptable to the most cost-conscious product.

Finally, we must satisfy international safety requirements, have a solution

that works across the world with a variety of languages and cultural expectations, and that can be used by people with a variety of disabilities. It has to be readily understood by first-time users, people who may never have used a Mac before, but not annoy our skilled, power users. Moreover, the problems are tightly coupled with the need to reboot occasionally, and programmers need a way of getting into the debug state. And as I said, the solution has to work for both the normal situation and the case where the system software is no longer responding. The power switch problem therefore also becomes the problem of providing capabilities to "reboot," to do an "emergency power down," and to get access to the "debug state." Not to mention labeling the power key.

You wouldn't believe how much time we spent on the problem of appropriately labeling the switch. The left-facing triangle on the keyboard switch is there because it doesn't mean anything. (Honest.) The earlier symbol (vertical line inside a circle) was not permitted because the European standards people wouldn't let us use it -- that symbol was reserved for hard power switches. The triangle has no meaning, so it didn't violate any standards. Mind you, the legal symbols are just as non-meaningful to most people. Few -- European or American -- are confident about the meaning of the vertical bar and circle (on and off, respectively), let alone bar inside of circle (a toggled on/off), or vertical bar inside broken circle (toggled soft-power), but the European standards committee is very strict. There are safety risks associated with thinking a shutdown switch removes all power from the machine when it doesn't. (Today, many electronic devices never have all power removed. The "power" button on the television remote does not do a hard shutdown, nor does the "shut down" menu choice on the Mac. After all, if they really shut down all power, the TV remote wouldn't be able to turn the power back on, nor would the Mac's keyboard turn on the machine. Your clock radio, for example, is not really off when you turn "off" the power. If it were off, how would the clock be powered?)

So, what seemed to be a very simple task, one that would remove all the confusions of our power switch locations, to say nothing of the infamous problem newly discovered by RISKS readers (but well known within Apple) where the keyboard can accidentally hit the power switch (nobody in RISKS commented on that -- you guys are slipping!) turned out to be incredibly complex. Yes, people turn off the power thinking they are pushing the diskette eject button. Macs don't have a diskette eject button -- we eject disks gracefully, under program control -- which is why the designers failed to note this problem prior to manufacture: it is users of non-Mac machines that have this problem. This is not justification, but I am continually amazed by the number of usage combinations that have to be tested -- it feels infinite -- so no matter how thorough the user testing, new situations arise after the product is shipped, situations that the bystander thinks so obvious that the designers must have been stupid not to have noticed (ah, that famous paper again: hindsight is not equal to foresight).

(By the way, you can't have a warning message come up when the power switch is hit for several reasons, the simplest being that if the software has crashed, you can't guarantee that the message would be displayed or the response attended to -- you need some way of forcing a shutdown when everything else has failed.)

(And while I am at it, don't suggest that our job would be simpler if we simply made software that never crashed. Or that we could use a watchdog timer to do automatic reboots. Yes, but ... .)

So what will we come up with? Can you live without a power switch on the CPU box, assuming all other cases have been dealt with? Assuming the system were protected against accidents. What if the switch were only in the rear? (Remember, we don't want people to use it under normal circumstances.)

Will my committee actually be able to find a common proposal that all the divisions of the company can accept? Who knows? Will the solution we are close to adopting solve all problems? Almost definitely not. Will it be an improvement over the current solution? Absolutely. Could we have done better? Maybe, but if we knew how, we would.

Whew: look how long this simple note has become, just to clarify the nature of the problem. Symptomatic.

(As for Calling Number Identification: once the power switch task is finished, it will be a relief to turn to something easy.)

Don Norman (severely chastened design critic and practitioner).  
User Experience Architect. Apple Computer. Cupertino, CA USA. [dnorman@apple.com](mailto:dnorman@apple.com)  
....

---

## The Risks of Ignorant in Computer Science

*Yaron Y. Goland <[ygoland@hollywood.cinenet.net](mailto:ygoland@hollywood.cinenet.net)>  
22 Oct 1994 11:34:24 -0700*

I am a senior at UCLA in Computer Science and Engineering and we have no such thing as 'human engineering classes', 'interface design classes', or 'software management' classes. We are taught lots of theory about computer science but absolutely nothing about how all this theory is supposed to translate into products that people can use. So the next time you want to smash your computer into pieces because its interface is a nightmare or the system has just crashed for the 7,000th time you can feel sure that the next generation of computer scientists, at least from UCLA, hasn't been taught a single thing about how to do better.

The risks should be obvious.

Yaron Y. Goland, School of Engineering and Applied Science, University of California, Los Angeles [ygoland@seas.ucla.edu](mailto:ygoland@seas.ucla.edu) [73160.327@compuserve.com](mailto:73160.327@compuserve.com)

---

## Re: Risk of similar interfaces

*<[Mike\\_Perry@dge.ceo.dg.com](mailto:Mike_Perry@dge.ceo.dg.com)>  
Mon, 24 Oct 94 10:18:48 edt*

The postings on the problems of similar looking buttons ([RISKS-16.47&48](#)) reminded me of a related RISK of failing to understand user perceptions.

Some years ago, an electronics/avionics/computer/etc company (best they remain anonymous) manufactured a military C3 system for use in trucks. Part of the equipment consisted of a small minicomputer which was installed under a desktop in the back of the truck. The mini had a button on the front labelled "BOOT". The squaddies operating the gear took this to mean the method of operating the button, rather than its function. Not surprisingly, the button and switch had a very short life. Education consistently failed to solve the problem, and in the end the switch had to be redesigned with a large, heavy duty, heavily sprung steel button that then could ONLY be operated by a kick.

Mike Perry [mike\\_perry@dge.ceo.dg.com](mailto:mike_perry@dge.ceo.dg.com)

---

### **Another problem with seemingly similar interfaces**

*ICTT)*

*Mon, 24 Oct 94 10:32:44 EST*

The recent article about the location of power buttons reminded me of an incident that occurred a few years ago.

The bank that I used switched over from one version of ATM software to another. In the old version you had to enter your PIN, then press a special key to get the ATM to accept it.

Somebody decided that this was a waste of effort, since all the PINs were the same length, so the machine could tell when you were done. Therefore, they removed the extra keystroke.

This might have been fine except for what they did with that key. It became a selection of what you wanted to do. Unfortunately, it became the Fast Withdrawal button, which takes a fixed amount of money out of checking, without any more chances to stop it.

Just imagine what this could do for people who were trying to put money into checking because the balance was too low.

Anyway, there were huge signs up around the ATM for months warning up this. Even so, I made the mistake myself once.

This shows the RISKS of even good-hearted changes to the user interface.

Gary Page International Centers for Telecommunications Technology  
[page@acd4.acd.com](mailto:page@acd4.acd.com)

---

### **RISKy interfaces**

*Brad G. Parks <[bparks@intcorp.com](mailto:bparks@intcorp.com)>*

*Mon, 24 Oct 94 15:29 CDT*

The power switch isn't the only button that can be dangerous to have near other familiar buttons. As a help-desk assistant at a small Minnesota college, [I noted] the most common mistake students and faculty would make on the Heath terminals wasn't the power switch. (The terminal could just be switched back on to pick up where they left off) Instead, people were often pressing "Hold Screen" -- a pretty handy button for lengthy and scrolling messages -- which was right next to the shift key.

Before notifying the lab assistants that their terminal "just froze up" they would try everything in their power to get the terminal to respond. This included pressing every function key and command sequence -- often with disastrous results and changes (which never appeared until "Hold Screen" was toggled again) to their document in their favorite terminal based word processor.

Many documents were lost and professors embarrassed by mistakenly pressing that one key.

Brad G. Parks (bparks@intcorp.com) [Software Engineer, O-Programmer]  
Introl Corporation (612)-631-7810 2675 Patton Rd. St.Paul, MN 55113

---

**Re: Risk of seeming similar interfaces (Elkins, [RISKS-16.47](#))**

*Jean Renard Ward <jrward@world.std.com>*

*Sat, 22 Oct 1994 19:46:16 -0400*

This discussion reminds me of a bit of folk-wisdom in the Software community in this area: All PC's made to run Microsoft's Windows and DOS products seem to be designed mechanical switches to open the floppy drive, and with the reset (or at least the power or "hard reset") button mounted \_\_conveniently\_\_ on the \_\_front\_\_ of the computer for easy access. Most machines made now to run Unix (Sun, HP, other workstations) and Apple's MAC operating system do \_\_not\_\_ have mechanical switches on the floppy drive, and do \_\_not\_\_ usually have the "emergency" reset switch on the front.

The folk wisdom is that you \_\_need\_\_ these emergency switches located for easy access when the software you are running is unreliable and crashes often.

Jean Renard Ward Boston, MA USA jrward@world.std.com

---

**Re: Risk of seeming similar interfaces (Elkins, [RISKS-16.47](#))**

*Kevin Purcell <xenolith@halcyon.com>*

*Fri, 21 Oct 1994 19:39:51 -0700*

The misplacement of the front-panel-mounted push-button power switch on a Power Mac 6100 or Centris/Quadra 610 shows the interesting effects of the interactions of manufacturing costs and human interface design.

It seems as if there were two goals:

1. Putting a power switch on the back panel of the computer hides the switch and makes the user rely on memory to operate the switch. So, moving it to a place where it is visible is a good idea.
2. Power supplies with a relay triggered by a momentary action switch (or a signal on the Apple Desktop Bus) are more expensive than power supplies that have a simple on/off latching switch.

Finally, the unwritten assumption that all Macintoshes have a powered eject of the floppy disk that automatically ejects the disk from the disk drive when you ask for the disk to be removed. No Mac user every pushes a button to eject their disk. This includes all the Macintosh hardware designers.

The goals (1) and (2) are combined to place a on/off latching switch on the front panel, despite the fact that the Machintosh system software has always used a shutdown command selected from a menu to do an orderly close down.

The original design problem was solved with the introduction of the Mac II. A switch on the keyboard turns the Mac on, but the Mac can only be shut down by the menu command.

A combination of these two concepts plus a blindness (from good design) leads to the poor design where a user can destroy all of his work in a second or so. In the best case, I've seen a user press the button, realize that they've just made a big mistake, and start to save their documents while keeping their finger on the button.

Kevin Purcell, Seattle dBug Mac Developers SIG Organiser kevinpu@atm.com  
xenolith@halcyon.com 206/649-6489 N7WIM + G8UDP

[Several garbles edited around by PGN.]

---

### **Re: Risk of seeming similar interfaces (Elkins, [RISKS-16.47](#))**

*Kent Borg <kentborg@borg.org>  
Sat, 22 Oct 1994 01:40:21 -0400*

Would you like to understand *\*why\** Apple put an eject-looking power switch on some of their machines?

Stupidity is too easy an answer. A more subtle explanation revolves around the fact that Macs don't *\*have\** disk eject switches. They eject floppies by software. How can a power switch look like something that doesn't exist? It can't. This button is not much of a risk...to *\*Mac\** users. It is the IBM-compatible folks who will be screaming bloody-murder.

Moral: Anticipate users from beyond your own little world. (Particularly if your marketing folks are trying to sell to them.)

-kb, the Kent who uses Macs.

Kent Borg kentborg@borg.org kentborg@aol.com +1 (617) 776-6899

---

**Re: Risk of seeming similar interfaces (Elkins, [RISKS-16.47](#))**

"Mike Alexander" <Mike.Alexander@umich.edu>

Sat, 22 Oct 94 23:21:48 -0300

>... Will Apple never learn? ...

I find this thread a bit odd. I've used many Macs, including both the PowerMac 7100 and 8100, and none of them newer than a Mac SE even has an accessible power switch. Assuming the original poster is talking about the reset button, on all of the machines I've used, it is a small button placed about as far away from the floppy disk drive as is reasonable. For example on the 8100 I'm using to send this, it is at the bottom right corner while the floppy and CD Rom drives are at the top. It would be very hard to confuse the reset button with an eject button. Perhaps the 6100 has this problem, I haven't used one of them, but if so it's the exception not the rule.

Mike Alexander, University of Michigan, ITD - Research Systems  
mta@umich.edu MAlexander@aol.com AppleLink: UMICH



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 16: Issue 50**

**Tuesday 25 October 1994**

## Contents

- [Another way for computer failure to delay trains](#)  
[Mark Brader](#)
- [Bank Robber Foiled by Security Screen](#)  
[Paul Gillingwater](#)
- [Re: Ignorance in Computer Science](#)  
[Roy Maxion](#)
- [Re: Don Norman and the Power switch](#)  
[William Hugh Murray](#)
- [Re: deadly risk](#)  
[Scot E. Wilcoxon](#)
- [Re: Cell Phone Fraud Countermeasures](#)  
[Bill Hensley](#)
- [Re: Badly designed interface in MS Mail](#)  
[Russell Stewart](#)
- [Re: Inadvertent postal forwarding](#)  
[Kent J Quirk](#)
- [Re: Data security in Iceland](#)  
[Curtis Jackson](#)
- [Mailing lists risk critical-mass spamming](#)  
[Benjamin A Ostrowsky?](#)
- [Sears takes digitized signature for CC transactions](#)  
[Steve Holzworth](#)
- [Re: CNID](#)  
[Lauren Weinstein](#)  
[Michael D. Sullivan](#)  
[Tim Duncan](#)  
[B.M. Cook](#)  
[J. Eric Townsend](#)  
[Michael Jampel](#)  
[Mark Stalzer](#)
- [Info on RISKS \(comp.risks\)](#)

---

**Another way for computer failure to delay trains**

Mark Brader <msb@sq.com>

Tue, 25 Oct 1994 18:15:21 -0400

Operational notices for the US passenger rail service Amtrak are now being posted to rec.railroad, and I spotted this item in one of them:

Termination of Train 352(19) at Detroit, MI

1045pm, ET train 352(19) diesel 359, CC 9649, 3 cars, arrived Detroit on time. Train was terminated due to no engineer was available to handle train to Toledo due to a Crew Management System failure. Regular man had called in at 245pm, ET, and advised was having automobile trouble and would not make train and marked off. Crew Management advised was having computer failure but engineer had marked off prior to the computer system outage. Investigation to be scheduled. Passengers were handled via alternate transportation to Toledo. Equipment was deadheaded to Toledo when relief engineer was called.

Delay: 352(19) term. passengers delayed 1'05"

Notations: MI = Michigan, ET = Eastern Time, 352(19) = train number 352 on the 19th of the month, engineer = driver, 1'05" = 1 hour 5 minutes.

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

[Presumably, the relief engineer was not a grateful deadhead. PGN]

---

## Bank Robber Foiled by Security Screen

Paul Gillingwater <paul@hp4at.eunet.co.at>

Wed, 26 Oct 1994 00:20:16 +0100

A New Zealand newspaper, "Waikato Times", for Sept. 2, 1994, reports a coroner's court finding that a bank robber in Sydney (Australia) died after being trapped for more than 15 minutes by a 250-kg steel security screen, which rose to the ceiling and trapped him by the throat.

The screen had been activated by staff in July 1991, whilst the robber was crawling across the counter. The robber, Steven Kovacs (age 37), died of asphyxiation.

The risk? When designing control systems for steel bullet-proof security screens that actuate in less than half a second, consider what happens if someone is in the way!

paul@actrix.co.at (Paul Gillingwater) :: Home Office in Vienna, Austria

[I suppose this would be more computer-related if it were triggered automagically, but it is still certainly RISKful. PGN]

---

**Re: Ignorance in Computer Science (Goland, [RISKS-16.49](#))**

Roy Maxion <maxion@K.GP.CS.CMU.EDU>

Tue, 25 Oct 94 19:11:44 EDT

> ... we have no such thing as 'human engineering classes', 'interface design  
> classes', or 'software management' classes. ...

I hope you will be pleased to note that here at Carnegie Mellon I am teaching just such a course. It's called Dependable System Design, and it's mission is to teach students how to design/implement/evaluate dependable systems so that we see fewer problems of the kind recently described in RISKS. Excerpts from the course description follow:

System dependability has been a major concern since the dawn of the electronic computer age. Dependability, taken in its broadest context, includes metrics such as reliability, availability, testability, maintainability, usability, mean time to failure, etc.

...

The goal of dependable system design is to ensure that the system continues to deliver its specified service to the client even in the face of error on the part of the user, the system or the environment.

...

User interfaces, while just as critical for dependability as reliable hardware and software, have received little attention from the dependability and fault-tolerance community. Because the philosophy of dependable system design crosses the boundaries of hardware, software and user interfaces, a major portion (but not all) of the course will focus on the most recently critical aspect of dependable systems: user interfaces and user-system communication.

...

Upon completion of this course, the student should be able to: acquire system requirements, develop system specifications embodied in one or more dependability metrics; critique an initial design; identify weak portions of a design; suggest a variety of alternatives to improve dependability; use contemporary techniques to evaluate, compare and contrast alternative designs, conduct system-evaluation experiments, and produce balanced, cost-effective system designs.

...

Topics include: Theory and practice of traditional dependability; robust benchmarks and fault injection; dependable user interfaces; experimental design; concepts of reliability and validity; system evaluation techniques; requirements acquisition; human error and reliability - causes, effects and mitigation; system monitoring, diagnosis and data analysis; task analysis.

Dependability Motto:

Anyone can build something that works when it works.  
But it's how it works when it doesn't work that counts.

Roy Maxion Computer Science Dept. Carnegie Mellon University

[And WHO'S counting? PGN]

## Don Norman and the Power switch

William Hugh Murray <0003158580@mcimail.com>

Tue, 25 Oct 94 15:21 EST

Don's tale of woe reminded me of my colleague who was assigned the task of standardizing keyboards across IBM.

And they wonder why we security people cannot decide on safe defaults.

William Hugh Murray, New Canaan, Connecticut

[DeFault is easy to assign. But don't

Pin the Tale on the Don Quixote.

BTW, Don Norman says he has NEVER had so many responses to any of his previous RISKS submissions as he had on the power-switch posting.

He must have pushed a lot of your buttons. PGN]

---

## Re: deadly risk

<fieldday!sewilco@kksys.com>

Sun, 23 Oct 94 17:38 CDT

>... electrocauterizer had apparently corrupted the software of her micro-processor-controlled pacemaker ... I believe the risk here is pretty obvious.

Yes, it is obvious that the woman might be in danger whenever she is near loud music. I hope they don't really use AUDIO tones.

A less deadly risk is assuming that experienced RISKS readers can only find one risk.

Scot E. Wilcoxon    sewilco@fieldday.mn.org    +1 612-936-0118

---

## Re: Cell Phone Fraud Countermeasures

TRW <trw-okc@qns.com>

Sun, 23 Oct 1994 00:48:49 -0500 (CDT)

A recent post described a TRW effort to use technical means of defeating cellphone fraud, and was described as voice print recognition. FYI, the actual method stores the electronic signature of the telephone instrument transmitter. A cloned phone will have a different transmitter signature and calls from that phone will be blocked. This system has been described in some detail in Communications Week, and several other trade journals (that's where \*I\* get my info :)

Bill Hensley, TRW Oklahoma City Engineering Office bhensley@oceo.trw.com  
bhensley@ocdis01.tinker.af.mil 405.732.3433 (v) 405.737.2043 (f)

---

**Re: Badly designed interface in MS Mail (Astoorian, [RISKS-16.46](#))**

*Russell Stewart <diamond@RT66.com>*

*24 Oct 1994 19:08:14 GMT*

>... Since "New Password" and "Re-Enter New Password" were both  
>empty (and thus matched each other), pressing OK set her password to the  
>null string without her realizing what had happened.

This is extraordinarily stupid on Microsoft's part.

I have only been programming for about 6 months now (and only with Visual Basic), but one of my fundamental rules is to NOT allow the user to leave a dialog box until he or she has supplied all required information (or, in the case of something ambiguous, like an empty password, at least ASK the person before moving on).

If anyone finds the programmer responsible for that mistake, he should be taken out and shot (and then dug up and shot again).

---

**Re: Inadvertent postal forwarding (Bove, [RISKS-16.48](#))**

*Kent J Quirk <kentq@world.std.com>*

*Sat, 22 Oct 1994 00:13:52 -0400*

In [RISKS-16.48](#), V. Michael Bove Jr. writes about a post-office forwarding problem. We had a similar problem once. My wife once ran a small business called Engineering Services Group. When we moved, she forwarded mail to our new address. One of the mailing lists she was on was at Hewlett-Packard (HP). HP got the change of address notice, and (apparently) maniacally changed *\*every\** occurrence of Engineering Services Group in their list to our new address. As you might imagine, several companies have an ESG as an internal group -- something like this:

H. Dilbert Gweep  
Graphic Doodler  
Engineering Services Group  
Habeas Corp.  
Anytown, OH, 00666

All 25 of these people suddenly stopped getting their 6-color HP spreads on 90-pound stock. All 25 copies suddenly started arriving in our mailbox with disconcerting regularity, each one with a different name.

The hard part was getting HP to turn the bloody thing off. The 800 numbers printed on the literature were useless. I finally found a person named on the masthead of some "magazine", and called her directly. After several cross-country phone calls, she eventually managed to reach someone who could (and did) make it stop.

The risks? Besides the danger of herniated homeowners and mail carriers,

there are 25 people out there who are no longer on a mailing list they might have actually wanted to be on. I doubt HP kept their old addresses lying around. Imagine if her company had been named "Engineering Department", or worse yet, "Craig Shergold".

Kent

(For the urban-legend-impaired, Craig Shergold is the now-grown English boy who no longer wishes to receive a world-record number of postcards.)

Kent Quirk 7 MacLeod Lane Acton, MA 01720 508-263-8344 kentq@world.std.com

---

### Re: Data security in Iceland (Haynes, [RISKS-16.47](#))

<cjackson@adobe.com>

Sun, 23 Oct 1994 00:38:33 GMT

}... If only we could get the story to be spread and repeated as well as the  
}Craig Shergold plea and the gold star tattoo urban legend!

If you could, it might make a difference to the small business people, but might not make a difference to an individual.

Back in the "good old days", hard drives were small enough that backup to floppies was feasible on a regular basis, and it was therefore cheap.

Today, I have a 1GB external disk on my Mac that I use for all my work, including lots of transitory data that I don't care about, and I backup the things I do care about to my internal 230MB drive. If my computer is stolen, I will certainly lose everything.

Am I naive? Stubborn? Stupid? Well, possibly. But my motivation in this case is cost. Unlike IBM-compatible PCs, sizeable removable media backup systems for Macintoshes are extremely costly. It is \*much\* cheaper to simply keep buying bigger and bigger hard drives, and use the older smaller one for backup and the newer larger (and faster) one for main use.

I am choosing not to "pay for full coverage insurance" for cost reasons; I am protected if my main hard disk dies an untimely death, but not if all of my computer equipment is stolen.

Consider it a RISK of one technology far outstripping another technology on which the first is dependent. Non-removable media cost per MB, speed, and even reliability have far out- paced that of removeable media.

Curtis Jackson cjackson@mv.us.adobe.com

---

### Mailing lists risk critical-mass spamming

<sylvar@alder.circa.ufl.edu>

*Sat, 22 Oct 1994 00:37:13 -0400*

At what point is it worth a lawyer's time to spam the net? A certain size of audience must be reached, and easily. Public mailing lists risk presenting an easy way to spam.

Many lists accept posts from non-subscribers. One need only know that the list exists and where to send contributions. It would be a simple task to poll ten thousand LISTSERVs for a list of lists. Having compiled such a listing, one could then send one's advertisement into several hundreds of thousands of mailboxes.

A more pointless exercise, and one which would cause even greater havoc, is to set up a LISTSERV list on one's own system which would link every list to every other list. It takes no imagination at all to see how quickly this would create a logjam.

---

### **Sears takes digitized signature for CC transactions**

*Steve Holzworth <sch@unx.sas.com>*

*Tue, 25 Oct 1994 07:55:55 -0400 (EDT)*

A few days ago, I was in the local Sears store (Cary, N.C.). I was purchasing a few items and decided to charge them against a Visa card. The clerk dutifully rang in the charges. While she was doing that, I noticed that a small digitizing tablet was attached to the register. I had a feeling I new what was coming next...

She pulled the receipt out of the register, slid it under a hold-down on the tablet, and instructed me to sign within the little plastic guide. I refused, stating that I would gladly sign the receipt, but not on the tablet. Apparently, I was the first to refuse :-). She had to look up a magic phone number, ominously entitled "Loss Prevention", to determine what to do. The person on the other end OK'd my signing without having my signature digitized.

Some might argue that my refusal was meaningless because Sears could always scan my signature from the receipt. Maybe so, but nothing says I have to make it easy for them. Small encroachments eventually lead to large losses.

Steve Holzworth SAS/Macintosh Development Team SAS Institute Cary, N.C.  
sch@unx.sas.com

---

### **CNID (numbers vs. names)**

*Lauren Weinstein <lauren@vortex.com>*

*Fri, 21 Oct 94 20:46 PDT*

The assertion has been made that perhaps calling number ID would be more acceptable if something other than numbers were sent. In fact, that is already part of the CNID spec (calling name delivery), though it is not implemented in all CNID systems. In most implementations I've seen \*both\* name and number are delivered--which rather kills the idea of delivering "who is calling" info rather than "where are they calling from" info.

There isn't much enthusiasm among the commercial end-users for name-only delivery. The reason is obvious--you can't collect phone numbers for return sales calls when you're just handed a name. While the telcos have touted CNID as being for individuals, the real focus has always been on commercial use as the real money maker.

At this point, the CNID controversy boils down to the seemingly simple question, "Since it is mandated that everyone must have per-call blocking available, why can't per-line blocking be made available?" Once again, I think the reason is obvious. Most people aren't on PBX systems that are easily programmed to dial the three digit blocking code on each call, nor will most people want to spend money for add-on gadgets to do this. So the hope of the telcos is that most people will forget or won't bother to use the per-call code most of the time. If per-line blocking were available (and surveys show most subscribers would want it--people want to know who's calling, but don't want other people to always know \*their\* number!) then CNID's commercial value would be significantly lowered.

--Lauren--

---

**Re: CNID (Preece, [RISKS-16.47](#), Klossner, [RISKS-16.48](#))**

*Michael D. Sullivan <mds@access.digex.net>*

*22 Oct 1994 02:44:36 -0400*

Andrew Klossner objects to the proposal to assign each phone a second unique number solely for CNID; This would be accessible only through an 800 number. Klossner claims this would be impractical because "Almost all area codes in North America are more than half populated. In order to double the number of phone numbers, most area codes would have to be split." This does not present a major obstacle, however. The pseudo-number would not have to be a valid phone number. [This was also pointed out in a subsequent message by Scott Preece himself. PGN] Such a number could fit within the existing CNID transmission system if it utilized the same number of digits as a valid US number (10 digits), but there are no valid 10-digit numbers beginning with 0 or 1 (20% of the numberspace), no valid 10-digit numbers with 0 or 1 as the fourth digit (20% of the numberspace, overlooking overlap with the foregoing), no valid 10-digit numbers with 11 as the second and third digits (reserved for 911, 411, and other service codes) (1% of the numberspace), no valid numbers with 11 as the fifth and sixth digits (same reason) (1% of the numberspace), no valid numbers with 00 as the fifth and sixth digits (to avoid confusion with 800, 900, etc.) (1%), no valid numbers with 200, 300, 400, or 600 as the leading digits, etc. Over 40% of the numberspace is reserved, and the remaining 60% is far from fully occupied -- only recently have a handful of area codes with 0 or 1 in the middle been assigned (20% of the numberspace remains relatively vacant), and likewise phone numbers with a 1 or 0 as the fifth digit (i.e., in the middle of the NXX "exchange" group) have been assigned only in major urban areas. It is very unlikely that anywhere near 50% of the numberspace is actually assigned -- keep in mind that there are 10 billion unique numbers available in a ten digit numberspace.

Clearly, then, it would be technically possible for the foreseeable future to assign each telephone number in the North American Numbering Plan a unique second number. This number would not be usable as a telephone number, but it would only work through an "800" number, which would decode it.

Moreover, there is no reason why such a non-dialable number should be uniquely assigned to each number. The telephone companies could use the non-dialable subset of 10-digit numbers as a pool of codes for one-time use in each area code. The real dialable number is actually transmitted between central offices, but is not transmitted to the end user. If the "privacy" bit is toggled on, the central office could store the real number and transmit a non-dialable number from a one-time pad, and it would only be mapped to the real number for a limited time, such as 48 hours, if keyed into the "800" number associated with the same telephone company and dialed from the number that was called (i.e., from the phone that received the non-dialable number). There is no reason for a permanent association between the non-dialable number and the real number; in fact, that would defeat the purpose of CNID and unpublished numbers. Calling the pseudonumber, through the 800 gateway, would be a one-time deal. There's no major technical obstacle to that.

Michael D. Sullivan | INTERNET E-MAIL TO: |also: avogadro@well.sf.ca.us |  
Washington, D.C. | mds@access.digex.net | 74160.1134@compuserve.com |

[Various astute messages from  
keener@upenn5.hep.upenn.edu (Paul T. Keener),  
"john (j.m.) clarke" <jclarke@bnr.ca>,  
George Swan <gswan@io.org>,  
and others tend to make similar observations, and are omitted. Please  
forgive me if I have oversimplified the points made by the omitted plethora  
of messages. I think you would all be overwhelmed if I included  
everything. PGN]

---

## Re: CNID and Don Norman -- CNID can be private (Wells, [RISKS-16.48](#))

*Tim Duncan <timd@edinburgh.ac.uk>  
Sun, 23 Oct 1994 13:18:42 +0000 (GMT)*

|> [Don Norman] suggests that other information should be sent instead of a  
|> telephone number. ...

This is currently being tested by British Telecom in Edinburgh. Subscribers have been given the option of submitting their own identifying string (16 characters) instead of the default which is their name as it appears in the phone book.

Tim Duncan, AI Applications Institute, Univ. of Edinburgh, 80 South Bridge,  
Edinburgh EH1 1HN, Scotland, UK Tel: +44 31 650 2747 Email: timd@ed.ac.uk

---

## Calling Number ID - in the UK

"B.M. Cook" <barry@cs.keele.ac.uk>

*Tue, 25 Oct 1994 09:26:24 +0000 (GMT)*

We're about to get calling number ID in the UK, too - from British Telecommunication (BT) at least. It is being promoted on the benefits to the subscriber, e.g. "This service has already been available in North America for some time, where it has had a major impact on malicious and fraudulent calls."

The fact that lines for which information has been previously withheld (ex-directory numbers) will send information is hard to spot in the literature!

The features listed in DIGEST 16.46 appear to have implemented, but not well publicised - I get the distinct feeling that the service will be of most benefit to companies who want to create lists of 'phone numbers!

We will be getting -

1. Per-line blocking - FOC, just call and ask for it.
2. Per-line unblocking - the default unless you change it.
3. Per-call blocking - dial 141 before the number you want.
4. Per-call unblocking - dial 1470 before the number you want.

1. and 2. need a phone call but it costs nothing.
3. is advertised in the literature.

BUT 4. took some discovering! I want to block outgoing ID by default and allow it only on certain calls (e.g. friends, certainly not businesses who will record it, sell the lists etc.) so per-line blocking with per-call unblocking is the answer.

This option is not mentioned in the literature, I phoned the further information freefone number to be told that what I wanted is not possible. Rather than give up here, as I guess most people would, I asked them to record my requirement so that if enough other people also wanted it they might think about providing it. They said they'd get someone to call me back which they did the next day. A very pleasant call from Edinburgh from someone who knew rather more about the system (it had been on trial in Scotland before being introduced elsewhere). No problem, he said, we already have what you require, just have the line blocked and put 1470 in front of calls you want to unblock - I'll put the line block on for you. The next day we had confirmation, by mail, that it had been done.

So, it looks as though we will be getting a decent service (it goes live on November 5th) - but only if you know what you want and work a little to get the information!

---

### **Bypassing CNID in an emergency**

*J. Eric Townsend <jet@abulafia.genmagic.com>  
24 Oct 1994 05:05:25 GMT*

I see a big RISK in "ignore all phone numbers I don't recognize". At least

once every 6 - 12 months, I get an emergency call at my house from a friend or family member. The call usually comes from a pay phone, but has originated at a business or a residential line as well.

By blocking "unknown numbers", I would have missed calls with the following content in the past year.

- "best friend severely injured in a vehicle accident, come immediately"

- "we broke down coming back from a late nite concert, it's 0230 and we're stuck in the middle of a really bad section of town with no transportation. can you come get us?"

- "my flight was canceled, so I caught one that arrives 3 hours earlier and at a different airport. come get me before I'm bored to death!"

And, most importantly to \*me\*:

- "Hi, I just got your resume from a friend of yours, and we'd like you to come in for an interview."

I ended up getting a great job from that one...

I don't see what is significantly gained by CNID that isn't gained by using an answering machine to screen calls. I do see what can be lost by ignoring calls from numbers one does not recognize, however.

J. Eric Townsend jet@genmagic.com USA 415.335.7463 aka jet@well.sf.ca.us  
work: jet@genmagic.com AT&T PersonalLink: A5803643645@attpls.net

---

## Caller Number Identification in the UK

*Michael Jampel <jampel@cs.city.ac.uk>  
Mon, 24 Oct 94 10:45 GMT*

British Telecom is starting a CNID (Caller Number Identification) in the UK. If you do nothing, your number will be sent out every time you make a call. But if you dial 1471 (I think -- anyway, some 4 digit code) before dialling the number you want to call, then your number will not be sent out.

Or you can ask for your number \_never\_ to be sent out. But in this case it is \_not\_ possible to dial, say, 1472 to have your number sent out occasionally.

So if you don't particularly want to tell life insurance companies your phone number, and if you don't trust yourself not to forget to dial 1741 double-bucky, you are put in the situation where you can never send out your number, which will usually not matter, until the day that it does matter.

I feel that BT are not serving the needs of their domestic customers here: CNID is great if someone you know is getting dirty phone calls, but otherwise its main function is to benefit commercial customers. But there is nothing we can do about it.

Michael Jampel

---

## Re: CNID and Don Norman -- CNID can be private

<stalzer@macaw.hrl.hac.com>

Mon, 24 Oct 1994 09:03:41 +0800

It would not take the database miners of the world long to build a cross reference between user selected call number ids and the real phone numbers. To keep off the list, you would have to never let a company associate your real phone number with your id. This would be hard to do if you use credit cards, mail order outfits, etc. Also, given the penchant for phone companies to charge a few bucks for every trivial service change, like changing an id, the cross reference would tend to remain up to date.

Although, I should add that if people conspire to choose the same id, like PRIVACY, we can give the marketers a real headache.

-- Mark



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 16: Issue 51**

**Friday 28 October 1994**

## Contents

- [Stolen account used to send hate mail at Texas A&M](#)  
[Bruce Sterling via Prentiss Riddle](#)
- [Orwell was off by 499 channels, and what to do about it](#)  
[Phil Agre](#)
- [GRE Computer-Based-Testing scores reconsidered](#)  
[Carlos I McEvilly](#)
- [America Online Offlines America](#)  
[PGN](#)
- [More on backspace problems](#)  
[John Vilkaitis](#)
- [CAPS-LOCK Considered Harmful](#)  
[Barton C. Massey](#)
- [Microsoft Natural Keyboard](#)  
[Don Alvarez](#)
- [Re: Mailing lists risk critical-mass spamming](#)  
[Paul Wallich](#)
- [Re: CNID and screening](#)  
[Robert Ellis Smith](#)
- [Drivers license as universal ID?](#)  
[John Sullivan](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Stolen account used to send hate mail at Texas A&M

*Prentiss Riddle* <[riddle@zilker.net](mailto:riddle@zilker.net)>  
27 Oct 1994 12:25:39 GMT

Bruce Sterling ([bruces@well.sf.ca.us](mailto:bruces@well.sf.ca.us)) cited the following in the [austin.eff](#) newsgroup:

: \*The Australian\* on Tuesday October 25, 1994:  
:  
: Hacker uses Internet e-mail account to send racist material  
:

: CHARLESTON, West Virginia: A college professor in Texas says someone broke  
: into his electronic mail account and fired off racist messages to about  
: 20,000 computer users in four States.  
:  
: The message brought death threats and other harsh responses from nearly 500  
: users who thought it came from Professor Grady Blount, a white professor of  
: environmental science at Texas A and M University.  
:  
: "My door is locked. We cancelled a class last night and one today will be  
: moved to another location," Professor Blount said. He also changed his  
: computer password.  
:  
: His password was used to send electronic mail messages to 20,000 Internet  
: users in Mississippi, Wisconsin, Colorado and Texas.  
:  
: The Internet computer network links colleges research facilities and  
: individuals worldwide.  
:  
: The racist message echoes a flier printed by a white supremacist group  
: called the National Alliance.  
:  
: It urges readers to send "minority parasites packing to fend for  
: themselves" and condemns community development funding as support for black  
: "breeding colonies".  
:  
: A Texas A and M spokesman, Mr Greg Orwig, said the e-mail address  
: apparently was picked at random by someone who tapped into the university's  
: computer system on Sunday.

-- Prentiss Riddle riddle@zilker.net Moderator of austin.eff

---

## **Orwell was off by 499 channels, and what to do about it**

*Phil Agre <pagre@weber.ucsd.edu>*

*Thu, 27 Oct 1994 12:48:17 -0700*

The NYT has an article about Bell Atlantic's video plans:

Edmund L. Andrews, A launching pad for a video revolution, New York Times,  
27 October 1994, pages C1, C6 [business section].

The point of the article is that BA wants to deliver video to customers, and  
is teaming up with Hollywood types to obtain the content. The main focus for  
Risks, though, is probably the privacy aspects of the scheme. A few quotes  
will probably give the idea:

"Company executives, convinced that they must distinguish themselves from  
today's established cable programmers [and so they plan to] offer more  
customized entertainment and shopping.

"Thus, the company has tied together a computer system that could, almost  
like Orwell's Big Brother, monitor the movies that a person orders and then

suggest others with the same actors or themes.

"Going a step further, the system would enable advertisers to send commercials directly to customers known to have bought particular kinds of merchandise. Thus, people who bought camping equipment from a video catalogue might start seeing commercials for outdoor clothing."

... "The scale of the new center ... makes clear how serious Bell Atlantic is about this venture."

If this sort of thing is really what people want, of course, then that's their perfect right. But advocates for other visions of technology can do plenty to ensure that people make informed choices. One is to inform people (in honest but vivid terms) that their program selections and purchases are being recorded, kept, and used for secondary purposes. Another is to keep on building things like the Internet and community networks, and redouble efforts to publicize them by telling clear, powerful stories about them. The point is to show that privacy-enhancing and *\*genuinely\** interactive technologies exist, and that they are useful, accessible, democratic, entertaining and convenient.

As my colleague Francois Bar emphasizes, this sort of end-user experimentation is crucial for defining the architectures of the future. Bell Atlantic and its brethren are creating top-down, privacy-invasive, 500-channel visions of the future -- even though they haven't worked very well in pilot tests in carefully selected communities -- because that's the business model they know. We can try to suppress the Risks associated with this model, but that's like shoveling the tide back into the ocean -- a lot of work. Another approach to pursue in parallel is to create alternatives that offer *\*both\** democratic values *\*and\** a lucrative business model for the people who can supply the necessary infrastructure.

This process starts with experimentation and continues with public relations. Here's a plan. If you're doing something terrific with networks, volunteer to demonstrate it in your local school. Have great stories ready to tell about it. Ask the kids to tell their parents. Then write a press release. Send it to all the newspapers and TV stations in your area -- especially the small ones. And make it available on the net as a model for others to follow.

Phil Agre, UCSD

---

## **GRE Computer-Based-Testing scores reconsidered**

*Carlos I McEvelly <cim@c3serve.c3.lanl.gov>*

*Tue, 25 Oct 1994 23:58:40 -0600*

A friend of mine who is from outside of the US, and who is now in the US for graduate school, took the computer-administered version of the GRE (Graduate Record Examination) General test last year.

The school where this individual was enrolled had a policy that allowed accepted students in some departments to begin graduate studies prior to having taken the GRE, so long as the GRE was then taken and passed with a

minimum aggregate score by the beginning of the second semester. The aggregate score was to be the total score in the verbal and quantitative testing categories -- the other category, analytical, was not considered.

With analytical out of the picture and with this person being a non-native speaker of English, the math (quantitative) section offered the best hope for scoring badly needed points.

With preparation, things would go fine. The Computer-Based-Testing option seemed perfect, because it was scheduled late in December which allowed some vacation days for pre-test cramming, and it also promised quick scoring, which would ensure that the results would arrive at the school before the start of the spring semester.

When the day of the test arrived, my friend felt well prepared and was especially confident for the math section.

For the five-section test, the software makes a random assignment of sections drawn from the three categories: verbal, quantitative, and analytical. Therefore some categories are repeated (with different questions, of course). With my friend's fortunes resting so heavily on the quantitative category, naturally the computer's random algorithm chose to assign not two, but THREE analytical sections -- the one category not regarded by the school. This left one verbal and one quantitative section. (It seems strange that the computer was not programmed to choose combinations of 2,2,1 and avoid those of 3,1,1 -- but there's more to this story.)

The Computer-Based-Testing administration of the GRE is also known as the "Computer Adaptive Test (CAT)," because it uses a new technique that presents different questions of varying difficulty based on this examinee's previous answers. Since my friend had done a good job boning up on math, the software, detecting a run of correct answers, began selecting more advanced questions. This was no problem, but it did mean that it took more time to answer each question. And the test had both a time limit, and a minimum number of questions that had to be answered.

Now you see where this story is going -- when my friend had ALREADY clicked the answer of the last required question, and was just about to click "Confirm" with the mouse, the time expired and the screen went blank. So instead of a good score for answering difficult questions, or a low score for leaving one question blank, my friend received a "No Score," or "NS." Added to a low verbal score, this was enough to ensure that there would be no more graduate studies for this student, at least not at the original school.

The rest of the story:

In September 1994 a carefully hedged letter arrived from the ETS (the Educational Testing Service, which administers the GRE). "...We have recently determined that it is possible that a small number of examinees who took the [CAT] received a NS (No Score) because they were unable to confirm an answer selection before time expired..."

The ETS offered to replace the NS with a newly calculated score based on the completed questions. The new aggregate score turned out to be 130 points HIGHER than the minimum that would have been required for the student to maintain graduate status at the school.

The offer of score adjustment is welcome, but seems to trivialize the (already incurred) very heavy costs to the student, who had to sacrifice a full semester of a graduate career while still being responsible for maintaining cost of living abroad--many visitors to the US on student visas are not allowed to work, so this was a great drain financially, in addition to being very stressful for the student.

Compared to some of the stories we read about x-ray machines and airplanes, this may not seem like much, but it is another reminder that as designers of information systems we need to remember that our work affects people's lives, and we should try to anticipate this in our designs.

Carlos McEvelly mcevelly@netcom.com, cim@lanl.gov

---

## America Online Offlines America

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

*Fri, 28 Oct 94 14:42:32 PDT*

AOL, now boasting 1.25M subscribers, up by a factor of more than three in the past year, apparently cannot boast about its E-mail performance. Yes, it is handling something like 15 million E-mail messages a month, about 7 times any of its competitors. But, No, it is not delivering 15 million E-mail messages a month. MANY MESSAGES sent to AOL are bounced back to the senders. Steve Outing, with 150 AOL subscribers on his discussion group, complained of getting a few hundred bounces a day. Message volume seems to be overburdening AOL's Internet gateway. AOL admits that a "bug" between 21 Sep and 5 Oct 1994 caused outgoing mail to "go awry" --- but that has been fixed. More recently, five-day delays have been reported for receipt of mail on AOL. [Source: An article by John Eckhouse in the San Francisco Chronicle, entitled "AOL Users Find E-mail Going Undelivered", 28 Oct 1994, p. D1.]

[From my vantage point of sending out RISKS, AOL FINALLY provides RISKS (comp.risks) as a newsgroup, although most of my direct subscribers have not caught on yet and are still getting private subscriptions. AOL apparently splits RISKS issues (normally just under 32K) into max-22K chunks, so perhaps one half of an issue gets through and the other half doesn't, which at least enables someone to realize that something is missing. A reminder to AOL subscribers: Your mailbox is limited to 550 messages, after which new incoming mail is simply rejected.

More-than-week-old messages just vanish. Presumably that means you should not use AOL if you are going to be away for more than a week, or if you get a lot of mail. I presume the newsgroup stuff ages just as rapidly. PGN]

---

## More on backspace problems

Javilk <javilk@netcom.com>

Wed, 26 Oct 1994 18:39:42 -0700 (PDT)

A follow-up to the backspace/delete problem I've been having with my cut-rate internet service provider, NETCOM.

PROBLEM: Dialing the standard local NETCOM number will occasionally give me one server which displays ^? when I hit backspace; and in a later session, \_without\_ reloading or restarting my telecom package, give me another server with a backspace key that properly ERASEs. I thank the avalanche(!) who provided me with suggestions on STTY and UNIX arcania. I apologize for resorting to form replies. Particular thanks for info on "The UNIX Hater's Handbook".

### OBSERVATIONS:

- 1.) Others e-mailed me with the \_same\_ NETCOM problem!
- 2.) the duration of the blink of the SD light on my modem clearly differentiates the Backspace key from the DEL key, and indicates I am always sending BACKSPACE.
- 3.) The only thing which changes between these sessions is:
  - a.) the telephone path,
  - b.) Equipment and software on THEIR end.
  - c.) The modem's compressions session???

### NETCOM's latest official response:

"Sir, with all due respect, other UNIX personnel do not have the ability to diagnose concerns about Netcom's system. They may have experience with differently configured Sparcs, but it's good to keep in mind that our configuration may not necessarily be what you are used to."

"You have repeatedly described a problem that is characteristic of terminal software problems. Our technical support staff has diagnosed this kind of problem innumerable times.... it is in our opinion clear [?] that any remaining problem is the fault of your terminal software. ... We have concluded to our satisfaction that this is not an error on our end." [With original a-gramatica.] They then repeatedly tell me to put STTY ^H in my .login, file, which they have already done WITHOUT my permission! It does NOT, and CAN NOT work as both my modem, and the command line clearly show they receive the ^? code, hex 7F, "DEL"; Not ^H, 08, "Backspace"."

### CONCLUSION:

Something on NETCOM's end occasionally decides (at log-in) to map both BACKSPACE and DEL together to the DEL code.

The ONLY way I can fix the problem, is by typing STTY ERASE, and then tapping the key which is, at the moment, producing the ^? code at their command level -- the backspace (^H) key; usually after I commit a blunder I can not backspace out of! I often hang up.

The RISK of not fixing intermittent problems is having to increase your marketing budget. Same for not understanding English.

John V. Vilkaitis, Senior Consultant, Software General Corp. 408-983-0518

[John asks whether anyone knows of a more competent internet server

for less money serving both Northern California and Connecticut. Unfortunately, each one has some partially overlapping set of problems. RISKS does not wish to get into a war among the Internet service providers, more or less all of whom have been dinged here at one time or another, and all of whom seem to be eagerly creating their images as fly-by-nighters. RISKS most equanimously hopes that a little public exposure will goad them into doing something reasonable. Our very best wishes to all of them for getting well soon. PGN]

---

## **CAPS-LOCK Considered Harmful**

*Barton C. Massey <bart@cs.uoregon.edu>*

*25 Oct 1994 22:49:40 -0700*

IMHO, the worst button-placement crime is one almost every computer manufacturer for the last 20 years has perpetrated: the CAPS-LOCK key on the keyboard.

Consider: this is a key which has a completely different interface than every other key on a standard keyboard (toggle instead of momentary contact), which performs a function almost completely obsoleted 15 years ago (by decent text-editing and word-processing software), and which is a factor in a number of fiendish user-interface traps.

As an example of the latter point, consider the most common solution around our shop to "I can't log into my account anymore", namely, "Did you bump the CAPS-LOCK key on?" Since the characters of the password are (IMHO quite rightly) not echoed, and since the password is (IMHO quite rightly) case-sensitive, there is no obvious indication given to the user of this error.

Another example, which has bitten me several times, is what happens under many versions of UNIX when I inadvertently type my login name (a single smooth motion) before realizing I have the CAPS-LOCK key on. The getty program (IMHO quite cleverly) decides that I must be on an uppercase-only terminal (when was the last time you used one of those babies?) and configures the TTY driver accordingly. The only ways I know of to cure this condition are (1) type a control-D at the login process to restart getty, or (2) get logged on (assuming that my current password contains no uppercase characters, or that I remember to backslash them) and type "stty -lcase" (I understand why the parameter is called "lcase" instead of "ucase", but I'm still amazed at the choice of name): suffice it to say that I consider neither method intuitive, or obvious to a novice.

Manufacturers, please: let's make this particular dinosaur extinct.

Bart Massey bart@cs.uoregon.edu

---

## Microsoft Natural Keyboard

*Don Alvarez <dla@cmb.rphys.cmu.edu>*

*Wed, 26 Oct 1994 16:38:53 -0400 (EDT)*

This is more of an anti-risk than a risk, but I thought a mention of the Microsoft Natural Keyboard might be appropriate. In case you haven't seen a picture of it, it's an ergonomic keyboard with the left and right hand key areas tilted in two planes for more natural hand positioning.

It was the best looking design I'd ever seen in a \$99 keyboard, so I bought one. At the risk of being incredibly subjective, I love it. This is one of the nicest keyboards I have ever used. (50th percentile hand dimensions make me a keyboard-designers dream)

*\*BUT\** it p\*\*\*es me off that it is still a secretary's keyboard. I understand that it has to be as close as possible to an 1890's QWERTY keyboard for backwards compatibility reasons, but:

The caps-lock key is where the control key *\*should\** be, requiring an impossible stretch of the left pinky every time a right-handed control character is required.

A similar stretch of the right pinky past the '/' key is required to get to the enter key. That stretch of the pinky was fine when you only hit the enter key every 60 characters or so, but it is (IMHO) unadvisable for programmers, spreadsheet users, etc., who are likely to need to hit the enter key every ten or fifteen characters.

Speaking from personal experience with a Dec keyboard I suffered considerable hand pains from those pinky-stretching motions until I rebound the control key on top of the physical caps-lock key and swapped the enter and '/' keys. The change in my hand problems was immediate and dramatic. [If anybody knows of a Dos/Windows way to do that rebinding please let me know (email to me, not risks... I'll summarize if people want). I've tried doing it with the DOS ANSI driver but the '/' and enter keys only seem to accept incompatible combinations of shift, control, alt, etc. modifiers]

Anyway, on the whole I'd say Microsoft did a real nice job on the hardware (installing the new keyboard driver software on my laptop was another story, but we all know hardware companies rarely write good software :-)

-Don

(Just my opinions, of course... your handage may vary)

---

## Re: Mailing lists risk critical-mass spamming (Sylvar)

*Paul Wallich <pw@sciam.com>*

*Wed, 26 Oct 1994 11:05:53 EDT*

Many lists accept posts from non-subscribers. One need only know that the list exists and where to send contributions. It would be a simple task to poll ten thousand LISTSERVs for a list of lists. Having compiled such a listing, one could then send one's advertisement into several hundreds of thousands of mailboxes.

It's been done. In mid-September I (and the readers of all the other publicly-known mailing lists beginning with A or B) got a pitch for a remote-backup service that started, "Dear Friend, since you read email..."

Paul Wallich

[It can happen to RISKS BITNET subscribers and USENET comp.risks readers, but not to the mainstream direct subscriptions. This was a problem only in the early days of RISKS, where my distribution macro on the Foonly made the live broadcast address accessible while it was being run. PGN]

---

## CNID and screening

*Robert Ellis Smith <0005101719@mcimail.com>*

*Wed, 26 Oct 94 12:56 EST*

A. Padgett Peterson wrote in RISKS that everybody should have Caller ID, to screen unwanted calls to a computer system or a personal telephone. There's a difference between Caller ID - which transmits and displays the number of the calling party, often without that person's full awareness - and programming one's telephone or modem to screen out unfamiliar incoming telephone numbers. Devices for screening out unfamiliar numbers are on the market and may be used without subscribing to Caller ID. These devices - or software that does the same thing - present no privacy problems that I can identify. It's the display of the number and the ability to capture it for later commercial exploitation that create the privacy problems. Robert Ellis Smith, Privacy Journal, Providence, RI 0005101719@mcimail.com.

---

## Drivers license as universal ID?

*<sullivan@geom.umn.edu>*

*Thu, 27 Oct 1994 15:05:53 -0500*

Minnesota is just introducing a new drivers license, with new security features, as well as a bar code and a magnetic strip (with full name, date of birth, and license number). The photo and signature are digitized, and presumably stored by the state as well as being printed on the card. I learned about the new licenses from an article in City Pages, a free weekly here in the Twin Cities.

The new licenses are produced (for \$1.29 apiece) by Deluxe (the check printers). About 4000 drivers had to go back to have their pictures retaken because they were transmitted at night from one computer to another over "incompatible phone lines" [whatever that means] and billions of bits went

"screaming into the ether". Deluxe blames a subcontractor.

Since the magstripe can hold about 256bytes, there have been discussions about what else might be stored there. Things like a list of cars and guns registered in your name, perhaps. Or, people receiving food stamps or welfare might use their license to obtain their benefits, either at a food-store cashier or from an ATM.

Don Gemberling, director of MN's Public Information Policy Analysis Division, evidently did raise the privacy issues during the planning process, noting that a "universal personal identifier ... has been consistently resisted in this country". Alice Gonzalo (assistant director of DVS, the state Driver and Vehicle Services Division) notes that DVS already sells driver's license information, sorted by different fields. (One could buy a list of Minnesotans over 6'3", for instance.)

There is already a national database of drivers with commercial licenses, called AAMVANET, and there are plans to expand this to all drivers. In Wisconsin, a driver's license can be suspended for failure to pay fines unrelated to driving (like library fines).

MN dept of Administration's Bob Schroeder says

In my opinion, the driver's license has nothing to do with driving. How many times have you pulled it out because an officer asked you for it? You pull it out much more because someone at a store or a check-cashing place wants to know who you are. It has less to do with driving and more to do with being a universal identifier, a way for you to be identified over the long term. Business really relies on the state to establish this sort of identifier for them.

-John Sullivan sullivan@geom.umn.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 16: Issue 52**

**Monday 31 October 1994**

## Contents

- [Telephone game glitch](#)  
[Julian Meadow](#)
- [The Sinking of the USS Gitarro](#)  
[Mike Crawford](#)
- [Re: FEC Voting "Standards"](#)  
[Rebecca Mercuri](#)
- [No Real Risks of Seemingly Similar Interfaces](#)  
[Roger Carasso](#)
- [There are risks and then there are risks](#)  
[Alan Wexelblat](#)
- [Re: Security screen \(Bank fences, power keys, etc.\)](#)  
[Frederick B. Cohen](#)
- [Re: More on backspace problems](#)  
[Esther Filderman](#)  
[Russell Stewart](#)
- [CAPS-LOCK](#)  
[Paul Barton-Davis](#)  
[P. Kevin Parker](#)  
[Rick Cook](#)  
[Phil Keys](#)  
[Doug Siebert](#)
- [Re: AOL](#)  
[Greg Lindahl](#)  
[Mike Crawford](#)
- [Re: Half a degree is better than none?](#)  
[Curtis Jackson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Telephone game glitch

*Julian Meadow* <[Julian\\_Meadow@qmailak.craycom.co.nz](mailto:Julian_Meadow@qmailak.craycom.co.nz)>  
*Mon, 31 Oct 1994 16:54:14 +0000 (GMT)*

Computer Lied When It Said All Callers Were Winners

New Zealand's \*Dominion\* newspaper, 29 Oct 1994,

The hundreds of people told they had won \$100 after a glitch in the telephone TV Trivia game last weekend will not get the money. The telephone game began awarding \$100 prizes to all callers during the weekend after a computer glitch caused by a power surge on Sunday evening. Callers said as soon as they pressed the number 1 on their telephones to start playing, a recorded message told them they had won.

But News Media (Auckland), which runs TV Trivia, yesterday said it would not pay the estimated 500 callers. The company said it was quite satisfied that all the callers who rang the 0900 number during the weekend were aware of the nature of the game. The company said the game involved participants using their skill and knowledge and if they were successful, they were rewarded. It was not covered by the Gaming and Lotteries Act 1977.

It was clear the 500 callers had not been asked any questions: they did not compete and so could not win. However, the company said it would reimburse the callers for the cost of their calls. The Consumers Institute said the legal issue was whether callers realised they were not playing the game properly. If they knew there was a glitch they would not have much of a case.

---

## The Sinking of the USS Gitarro

*Mike Crawford <crawford@scipp.ucsc.edu>*

*Sun, 30 Oct 1994 00:02:42 -0700*

I just read the section on defense in \*Computer-Related Risks\* and was reminded of the following incidents:

During 1967 and 1968 I lived on Mare Island Naval Shipyard, a submarine maintenance station just off the North end of San Francisco Bay, across a channel from Vallejo, California. Until recently most submarine repair (nuclear, conventional, attack and missile) for the Pacific fleet was done here; it has since been moved to Bremerton Washington; MINSY is being closed down.

Sometime during 1968, the USS Gitarro (sp?) was being repaired. The front sonar cover was taken off, and a hatch was left open so the repair crew could get out to work on it. The Gitarro was floating in the water, raised high to expose the sonar to the air.

A test engineer, who had nothing to do with the sonar people, wished to perform a test of some mechanism that required the submarine to be level. He went to the bridge (in the middle of the ship, far from the front) and let some water in the ballast tanks at one end of the ship, until the submarine was level, then closed off the tank... but he neglected to consider inertia. The submarine continued to settle for a bit after he closed the valve.

He did not take the obvious route of blowing some air back into the tank. Apparently he did not know how to raise the submarine, only lower it.

(Perhaps this was all that was given in his test plan; I don't know). Instead, he let water in the ballast tanks at the other end. Again he overshot, and again, and again... until he wiggled the open sonar hatch under the water.

Sea water came rushing in the front. Now, this would not be such a disaster under ordinary circumstances, as military ships are always compartmented so that whole sections of a ship can be flooded without sinking the ship. But this ship was in for repair, and temporary pipelines, hoses, and power cables had been run through the pressure hatches that were meant to close the compartments. Sailors tried to use fireaxes to cut through live power cables in order to close the hatches, but to no avail: the valiant Gitarro sank to the bottom of Mare Island Channel.

I don't know if anyone was killed or injured - I think not. Damage was mitigated somewhat by a quick thinking tugboat operator who saw the "sail" starting to roll over into the water. He rammed his tugboat up against the sail and kept pushing against it until a floating crane was brought in the next morning. Even so, damage came to \$30 million.

In another incident, the radioactive coolant water was being drained from a reactor. This submarine (not the Gitarro) was in drydock. The usual procedure is to cut a hole in the hull and run the water out a pipe into a cement mixer. The radioactive water is used to make cement and trucked to Hanford, Washington (about 800 miles) for "disposal".

The pipe from the reactor reached out to the hull, where it was connected via a flange to the pipe leading to the cement mixer. Only one time they forgot to bolt the flanges together; as the water was pumped out it showered upon a shipyard worker walking on the drydock below.

I understand that the shipyard worker not only survived but was still working at the shipyard during the '80s - but the clothes he was wearing at the time, and the patch of drydock he was standing on at the time are buried at Hanford. Also, this fellow exceeded his lifetime allowance for radiation exposure during this "hot shower", and is not allowed inside the nuclear yard.

In still another incident, the above mentioned cement mixer was stolen by the truck driver assigned to deliver the radioactive concrete to Hanford. He was caught - after he had used the mixer to pour a backyard patio at his house.

But wait, there's more! The Navy contracted with a private manufacturer to build a piece of equipment that would be installed in a room aboard a submarine. The Navy gave the manufacturer plans to this room. When the equipment was delivered, a hole was cut in the hull of the submarine, and the equipment was lowered in by a crane. Because submarines are very cramped there was not much room and the designers used up every bit of available space for their machine. When it was lowered into the submarine, it was found that this device did not fit! The Navy made all sorts of accusation's about the manufacturer's incompetence, but in the end it was found that the manufacturer did meet the specifications; the Navy's mechanical drawing had an error in which "1/2 inch" was written where "1/4 inch" was intended. (Note that one of the factors that limits the life of a submarine is the

number of times holes have been cut in its hull. After a while the hull is weakened so much that the submarine has to be scrapped.)

And finally, a note about the circumstances in which I lived at the base, and the importance of unambiguous language in giving commands. I lived there at the height of the Vietnam War, while my father was an instructor in the anti-aircraft missile school there. I spent the third and fourth years of my life living on a military base at the height of a war; I remember tanks rolling by and trucks and trains loaded with bombs. Being a small child I regarded this with the wonder and curiosity any childhood would have for his playground.

My parents sternly ordered me never to cross the street - but by walking some distance down my street and crossing an open meadow, I could freely enter the Marine Corps rifle practice range. Being three feet tall, my friends and I could easily walk unobserved in the culverts along the road. I remember watching the men firing their M16's, and one time I sat in a bunker below the targets - one could lower a paper target into the bunker to replace it or tally the score - watching bullet holes appear in the targets above.

The Marines did catch us, many times in fact, and always sternly warned us to stay away, but they never did tell my parents. I never felt I was doing anything wrong as I did not cross the street.

I did cross the street once, though... and the next street beyond, and snuck under the fence into the shipyard area itself, walking right past heavily armed sentries - remember all the riots were happening in Berkeley just 20 miles away, so I'm sure they were on the lookout for saboteurs. They just didn't think to look for intruders that didn't reach up to their knees! I remember quite clearly looking up into the cranes used to lift heavy equipment off of railroad cars, and all manner of heavy equipment that would have ground a four-year old boy into hamburger. [...]

Mike Crawford [crawford@scipp.ucsc.edu](mailto:crawford@scipp.ucsc.edu) [crawford@maxwell.ucsc.edu](mailto:crawford@maxwell.ucsc.edu)

---

## Re: FEC Voting "Standards" (Jones, [RISKS-16.52](#))

*Rebecca Mercuri <[mercuri@gradient.cis.upenn.edu](mailto:mercuri@gradient.cis.upenn.edu)>*

*Mon, 31 Oct 1994 16:54:28 +0500*

[CC of message to Doug Jones,]

I was forwarded your E-mail, which was posted in RISKS on-line. I wanted to comment on a few errors in your message.

First of all, the FEC Voting "Standards" do not "mandate" anything. These are not standards, they are merely suggested guidelines. The guidelines are just that because of "states rights." This is the right of states to have certain choices in a variety of matters. There is precedent for the federal government to mandate some things regarding voting. One of these is who can vote (as in women, blacks, people over the age of 18). But currently the federal government, although it oversees federal elections, does not MANDATE

any STANDARDS regarding voting machines. The FEC document you appear to have been reading is just guidelines. Some of the states have adopted these guidelines, and then they become a part of those states laws. But many states have not.

Secondly, you should know that these FEC guidelines were created with extensive assistance from voting machine vendors and other service providers. It was in no way a balanced group. What I and others have tried to point out in the years since the publication of these guidelines is that there are already good STANDARDS for assuring accuracy and integrity in computer-based systems. These standards are the "orange-book" system that the federal government uses for other federally-used computation systems. (Voting machines are exempt from the 1987 Computer Security Act and are not required to conform to these standards.) Within these standards is a system and organization for certifying secure systems at various levels. We would hope that eventually states (or the federal government) would enact laws that would bring voting machines into this system, and they could be examined for conformity. The FEC guidelines fall far short of the NIST standards, and we would like to see this changed.

I am not in any way suggesting that even the NIST standards would be sufficient to ensure accurate and secure electronic vote tabulation. I am just mentioning all of this here, because you are misled regarding the stringency of the FEC guidelines and of their application.

Rebecca Mercuri

---

## No Real Risks of Seemingly Similar Interfaces

*e.e. <carasso@inference.com>*

*Sat, 29 Oct 94 19:38:32 PDT*

RISKS should be a forum for real risks, not pet peeves, not minor inconveniences, not for harmless mistakes. I am amazed by the amount of whining in this forum.

If you hit you Mac's power switch trying to eject your floppy, you obviously just got your Mac, there's little of value on it, and it's unlikely that anything damaging will *\*really\** happen. There is very little real risk. You are whining about a SELF-FIXING-PROBLEM. You won't do it again. And if you do, it's called natural selection. Stupidity is its own reward.

If you accidentally push a wrong ATM button and get out \$40 when you didn't mean to, there is NO RISK. Just take the little envelope, deposit the \$40 back in, and I'm sure you won't do it again. And if you do, it's called natural selection. Stupidity is its own reward.

If these were nuclear warheads, municipal power stations, or something important, fine. Write about it. But for Heaven's Sake, leave your whining at the Gate.

roger

---

## **There are risks and then there are risks (ETS) (McEvilly, [RISKS-16.51](#))**

*"Girls & Boys" <wex@media.mit.edu>  
Sun, 30 Oct 94 14:52:04 -0500*

Carlos McEvilly tells of his friend who was denied a semester at school because of an interface problem with the computer-administered GREs.

While I sympathize with his friend's plight, it seems that blaming the test administrators (ETS) seems too easy and too simple-minded. As with other cases, we should bear in mind that there is a system and a whole process in place, with several opportunities for human intervention.

For example, the problem would never have been seen had the friend not chosen to take the computerized version in order to give himself more study time. The risks of failure to plan in advance seem to apply here.

The college's use of the GRE score as a binary decision-making factor is itself fraught with risks. First off, ETS itself advises against this -- the risk of using a product in a way it was not intended to be used. Second, my friends who are college professors all tell me that the best predictor of how good a student someone will be is not a standardized test, but rather the person's past performance as a student.

The college already had one semester's worth of evidence for this student's abilities, but they ignored it -- the risk of not considering all the evidence as well as the risk of ignoring the opinions of qualified experts.

I could go on, but let me just state my main point: We've all gotten to the stage where when we hear a so-called explanation like "Pilot error" or "computer error" we know to dig deeper. We know that there are processes involved, that there are opportunities for people to intervene, and that focussing solely on one event/incident/problem tends to obscure other possible causes. But we continue to apply this kind of shallow analysis to other situations.

In this case, while I can see the error in the ETS software as being a contributory factor, I can hardly give it primary, let alone sole importance.

Alan Wexelblat, Reality Hacker, Author, and Cyberspace Bard MIT Media Lab,  
Intelligent Agents Group wex@media.mit.edu 617-253-9833 Pager: 617-945-1842

---

## **Re: Security screen (Bank fences, power keys, etc.)**

*"Dr. Frederick B. Cohen" <fc@netaxs.com>  
Sat, 29 Oct 1994 08:29:18 -0400 (EDT)*

It seems to me that one of the risks of robbing a bank is getting killed by the guards, the security system, or the people you are taking money from. I am not convinced that we should try to make robbing banks safe.

Re: On-Off Switch on Macs ...

I don't really understand this issue at all. It seems to me the solution is not a better on-off switch, but a better operating system. My Unix box doesn't seem to need an on-off switch, but every DOS, Windows, and MAC system I have ever seen can't get along without one.

Re: Pacemaker failure ...

I appreciate that if my pacemaker fails, I will die, but I don't understand why that justifies not using a pacemaker. Without it, someone who needs it will die with  $P=1$ . With it, they have  $P=.001$  or whatever. We seem to overlook the issues of cost and probability in the risks forum when it comes to accidental risks, and frankly, this is a big mistake.

Re: CMU course on dependable system design ...

The description sounds interesting, but it also sounds like it ignores a great deal. I think that one of the problems with universities is what we expect of them. It has taken me many years of full time effort to gain the knowledge I have in the fields I explore. In a university, you get 9 hours per week (if you work hard) for 15 weeks on any particular subject. 135 hours on dependability is admirable, but that's about the same as 2-3 weeks of experience (depends on how many hours you work per week) in the field. Still, as a leading complainer about the lack of attention to information protection in our educational system, I should support the CMU initiative. The only problem I have with the course description is that it seemed to ignore the malicious aspects of risks in favor of accidental ones. Of course, we certainly have a lot of accidents to worry about.

Re: The risks of reading risks

Somehow, the news reader on this system, (tin) seems to believe that it is the only program users should ever run. It takes about 15 minutes to examine every news group that has ever existed, and after offering me a wide selection of new ones I have not previously asked not to get, finally allows me to read the risks forum. Of course, this process cannot be interrupted by the normal Unix interrupt character, and there don't seem to be options to have it simply read the risks forum and leave me alone. Perhaps this should be a class project at CMU's new class on dependability. While they are at it, they should look at the Elm email system, which insists that I answer the same questions every time I read mail, even though I always give the same answers. No, there is no way to default them - or at least I haven't found one.

---

**Re: More on backspace problems**

*Esther Filderman <moose+@CMU.EDU>  
Fri, 28 Oct 1994 19:57:02 -0400 (EDT)*

In [RISKS-16.51](#) John Vilkaitis describes trying to get Netcom to understand

that his system is showing intermittent problems connecting to Netcom, and that it is -not- failures of his "terminal software". At the end, he concludes,

> The RISK of not fixing intermittent problems is having to increase your  
> marketing budget. Same for not understanding English.

Understandable, but I suggest that the more frightening RISK is the following:

> They then repeatedly tell me to put STTY ^H in my .login file,  
which they have already done WITHOUT my permission!

I will run the risk (no pun intended) of offending my fellow systems administrators by saying that we all have heard horror tales of "well-meaning" systems and/or support folks screwing up users by editing their files without their permission, or without their understanding of the changes. They're generally making more work for themselves.

Esther Filderman moose+@cmu.edu  
System Mangler Library Automation Carnegie Mellon University

---

### **NETCOM Backspace Problem ["terminal software"] (javilk,[RISKS-16.51](#))**

*Russell Stewart <diamond@RT66.com>*

*Mon, 31 Oct 1994 14:17:49 -0500*

> Our technical support staff has diagnosed this kind of problem  
> innumerable times.... it is in our opinion clear [?] that any  
> remaining problem is the fault of your terminal software.

"It can only be attributable to human error." -HAL 9000

Russell Stewart Albuquerque, New Mexico diamond@rt66.com

---

### **CAPS-LOCK considered harmful**

*Paul Barton-Davis <pauld@cs.washington.edu>*

*Fri, 28 Oct 1994 17:07:20 -0700*

bart@cs.uoregon.edu (Barton C. Massey) writes of various problems with CAPS-LOCK. There's another, even more infuriating problem that CAPS-LOCK has a risk of creating, and already has on certain keyboards.

Under the X Window System, it is possible to remap the keyboard in any way you choose. This includes getting rid of CAPS-LOCK altogether, or so you might hope. I do this routinely to deal with some of the problems Barton mentioned, by mapping it be just another control key.

This works fine at work, on a DEC keyboard. When I get home, however, there's a problem. The keyboard on my NCD X terminal considers the "lock" attribute of this key to be a hardware feature, and thus regardless of what

I map it to under X, it always behaves like a CAPS-LOCK in terms of latching and unlatching. Since I map the key to be a control key, you may be able to imagine my frustration when I accidentally press the key and find that my emacs-editing-supported shell goes haywire as I try to type alphabetic characters. It sometimes take me quite a while to realize why nothing I type works.

One day, I'll figure out a better way to remap it. In the meantime, even if we're stuck with CAPS-LOCK, please hardware types: don't make the latching feature a function of the keyboard electronics, but leave it software controlled, where if its broken, some of us can fix it.

-- paul barton-davis UW CS Laboratory

---

### Follow up to CAPS-Lock and MS Natural Keyboard (Massey, Alvarez)

*P. Kevin Parker <kparker@chaph.usc.edu>  
28 Oct 1994 17:17:44 -0700*

Interesting that these two posts should appear one after the other:  
> CAPS-LOCK Considered Harmful (Barton C. Massey) <bart@cs.uoregon.edu>  
> Microsoft Natural Keyboard (Don Alvarez) <dla@cubr.phys.cmu.edu>

The RISK of the CAPS-Lock is eradicated--in Windows only--by this keyboard. Using the software provided by Microsoft, a user can disable CAPS-Lock entirely.

P. Kevin Parker kparker@scf.usc.edu kparker@eis.calstate.edu

---

### CAPS-LOCK Key Harmful?

*<rcook@BIX.com>  
Sat, 29 Oct 1994 02:29:53 -0400 (EDT)*

While I can sympathize with the contributor who dislikes the CAPS-LOCK key (my own keyboard has it placed cleverly just to the left of the space bar -- sure-fire sabotage), I'd like to point out that there is a growing group of people for whom it is vital. Those are the people who don't have the physical ability to press two keys at once.

For that reason I think CAPS-LOCK is a Good Thing and should remain standard on keyboards.

--Rick Cook rcook@bix.com

[There are other cases as well, for example, in programming languages that REQUIRE UPPER CASE, as noted by Brian T. Schellenberger, bts@unx.sas.com, who also notes the problems caused by the absence of a CAPS-LOCK indicator. PGN]

## **RE: CAPS-LOCK Considered Harmful**

*Phil Keys <100213.1013@compuserve.com>*

*29 Oct 94 05:55:03 EDT*

On 10/25, Bart Massey posted an article on the risks associated with the use of the CAPS-LOCK key on a keyboard & challenged manufacturers to come up with a better method. Whether it's better or not can be debated, but in Japan, AT compatible machines running bilingual (Japanese/English) DOS (called DOS/V) have adopted a convention where, to toggle the CAPS-LOCK key, you have to press both the Shift key & the DOS/V key at the same time. Personally, I don't like this since it forces you to remove your hand from the keyboard to toggle CAPS-LOCK, but, it does make it less likely that you will toggle CAPS-LOCK by mistake, thus reducing this risk.

Just thought I'd let you know that at least somebody, somewhere has been thinking about this issue too.

Phil Keys [and appropriately named for this discussion, too! PGN]

---

## **Re: CAPS-LOCK Considered Harmful (Massey, [RISKS-16.51](#))**

*Doug Siebert <dsiebert@icaen.uiowa.edu>*

*30 Oct 1994 21:53:34 GMT*

NeXT did this right in at least the revision of the keyboard I have on my color slab. The command key held down while hitting the shift key toggles caps lock on/off (and toggles the LED that is in both shift keys) That way the control key can be in the IMHO correct place, left of the 'A' key.

Doug Siebert dsiebert@isca.uiowa.edu

---

## **Re: AOL ([RISKS-16.51](#))**

*Greg Lindahl <gl8f@fermi.clas.virginia.edu>*

*Sat, 29 Oct 1994 16:01:55 -0400*

> I presume the newsgroup stuff ages just as rapidly [as E-mail]. PGN

Actually no -- it seems to stay for months, so you'll see AOL users restarting month-old flamewars by responding to something that's expired everywhere else.

[Ah, that suggests virtual time travel and multiple virtual realities.  
Deja vu all over again. PGN]

---

## **Re: America Online Offlines America**

*Mike Crawford <crawford@scipp.ucsc.edu>*

*Sat, 29 Oct 1994 23:08:14 -0700*

An official from AOL was quoted in the San Francisco Chronicle Business section today, 29 Oct 1994, denying that AOL was losing mail. This fellow (might have been the president, I'm not sure) went on to invite the Internet Community to "flood" AOL with mail.

Now, it's one thing to shoot your own self in the foot, but inviting the net to spam AOL.com in the national press is likely to have the added effect of overloading all the routers from here to there.

I'd like to suggest that the folks at aol ought to think twice before saying such things.

Mike Crawford [crawford@scipp.ucsc.edu](mailto:crawford@scipp.ucsc.edu) [crawford@maxwell.ucsc.edu](mailto:crawford@maxwell.ucsc.edu)

---

**Re: AOL Offlines America ([RISKS-16.51](#))**

<[RichWells@aol.com](mailto:RichWells@aol.com)>

Sun, 30 Oct 1994 12:57:12 -0500

It appears to be the Macintosh AOL software that has the 22K limitation on messages which prevents seeing an entire issue of Risks at one time. Even so, the entire issue can be read; you just cannot keep more than about 22K of it around at one time. This has the unfortunate consequence that you have to stay on-line for the time it takes to read it, rather than saving it to a file and reading it later off-line. The Windows AOL software does allow one to read the entire issue at one time, and to save it to a file for later reading.

[Stuff on deletion deleted. Also, clarification that comp.risks came up at the same time as other newsgroups on AOL.]

AOL's newsgroup access is indeed limited (note that I had to edit the subject heading to abbreviate America Online!), but it's not quite as bad as your postscript made it sound. [TNX. PGN]

---

**Re: Half a degree is better than none? (Brader, [RISKS-16.49](#))**

<[cjackson@adobe.com](mailto:cjackson@adobe.com)>

Sat, 29 Oct 1994 02:08:01 GMT

}Or rather, it tries to. Somehow, wherever the character 1/2 is  
}supposed to occur, instead there is a degree sign!

As Mark Brader, the poster of the above, can intimately attest from the work of both of us in certain international standards committees, this is a primary area of concern when one is defining standards for font use and especially font/glyph substitution. Our classic example in our ISO committee was of the American who sends in a bid on a bit of business in the UK, only to have his electronically-transmitted bid (these are the fast-moving '90s, after all) printed out with the '\$' replaced by the UK pound symbol. Quite a

hefty automatic bid increase, that one. Curtis Jackson  
cjackson@mv.us.adobe.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 16: Issue 53**

**Sunday 6 November 1994**

## Contents

- [UK boy cracks S.Korean system](#)  
[Mich Kabay](#)
- [CMU blocks access to nasty newsgroups](#)  
[Mich Kabay](#)
- [Roll-Over Date Frozen?](#)  
[Ed Ravin](#)
- [Followup on Sears captures signatures](#)  
[Steve Holzworth](#)
- [Minnesota driver license](#)  
[Daniel Frankowski](#)
- [Re: CAPS-LOCK Considered Harmful](#)  
[Jim Griffith](#)
- [RFD: sci.engr.safety](#)  
[Sethu R Rathinam](#)
- [2nd Conf. on Mathematics of Dependable Systems](#)  
[Victoria Stavridou](#)
- [Info on RISKS \(comp.risks\)](#)

---

### UK boy cracks S.Korean system

"*Mich Kabay [NCSA Sys\_Op]*" <75300.3232@compuserve.com>  
06 Nov 94 15:46:40 EST

>From the Reuter newswire (94.11.04) via CompuServe's Executive News Service:

RTw 11/04 0417 S. Korea says slim chance hacker got nuclear data

By David Brunnstrom

SEOUL, Nov 4 (Reuter) - The South Korean atomic energy institute said on Friday there was a slim possibility a teenage British computer hacker stole secret nuclear data from its computer system.

The Korea Atomic Energy Research Institute (KAERI) said it was investigating possible damage to its system after a report in the Washington Times newspaper on Thursday [94.11.03] which said the hacker managed to access it recently.

The article goes on to make the following key points:

- o "James Christy, director of computer crime investigation at the U.S. Air Force's office of special investigations," speaking "at a conference on global organised crime convened by Washington's Center for Strategic and International Studies," said that "Data Stream" was a 16 year old in Britain.
- o The youth cracked a system at the Rome Air Development Center at Griffith Air Force Base in Rome, New York state.
- o He copied files from the "South Korean Atomic Research Institute (sic)" to the disks on the Rome system. [SKARI?]
- o The youth "curled up into a foetal position and cried when" the British police arrested him.
- o KAERI officials said that technical information "such as that on reactor systems and fuel rod design" was "stored separately from other data and protected by multiple passwords."
- o "Chung Joon-keuk, director of public information at the institute,....said .... it was still not clear whether the institute referred to in the Times was in fact KAERI and it was possible the article should have referred to the Korea Aerospace Research Institute (KARI)."

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn

---

### **CMU blocks access to nasty newsgroups**

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
06 Nov 94 15:46:49 EST*

>From the United Press Intl newswire via CompuServe's Executive News Service:

UPn 11/04 1054 College blocks computer sex access

PITTSBURGH, Nov. 4 (UPI) -- Carnegie Mellon University of Pittsburgh said Friday it will block access on its campus computer system to sexually explicit material available on the worldwide computer network called the Internet.

Carnegie Mellon officials said they are acting out of concern that the university could be subject to prosecution under Pennsylvania's pornography and

obscenity laws.

The article goes to to explain that University spokespersons admit they will be "be accused of stifling free expression" but feel that the risks are too high, especially since children can easily access these materials. The decision was said to have been difficult and painful for the administrators, who strongly support the tradition of academic freedom. The decision was criticized by a student spokesperson, who compared it to banning books.

[Comments by MK:

The anonymity of the Internet will continue to cause difficult problems related to access by children. Right now, the response of well-meaning administrators and others is to put blanket restrictions on everyone so as to prevent unsupervised use of the Internet by minors.

Imagine a world where no one had developed the concept of an ignition key for automobiles. We can imagine well-meaning highway administrators concerned with access to the high-speed transportation infrastructure exclaiming, "Gosh, but with these highways and cars, children could travel to (gasp) brothels and pigsties! They could see things that their parents would never want them involved in." And so the highway administrators would shut down roads in an attempt to prevent access to bad places by children.

In both the real world and this imaginary world, these difficulties are caused by the lack of identification and authentication in accessing the highways. In the real world, we have ignition keys for automobiles and severe penalties for stealing automobiles or driving without a permit. We have no accepted standards for access to networks.

Parents who are concerned about access to a network by their children could take the responsibility of locking their computers or their modems. However, that's a pretty crude approach too--all or nothing. And what about the children's independence and growth?

There are already devices available for controlling access to television; parents program the times, channels and duration of viewing permitted for their children, who punch in a PIN to gain personally-tailored access to the TV. Maybe as Internet access grows, there will arise sufficient interest and demand for menu systems for access to the Internet. Parents could select the sections of the Internet which they wish to allow for their children; children and parents could explore the Internet together and add or remove destinations and newsgroups as they see fit.

Right now, CompuServe has access to Internet newsgroups. The administration has settled on a middle ground in restricting access to the Internet by limiting the listings of newsgroups. In fact, however, if someone already knows the name of a newsgroup, they are free to subscribe even if it isn't listed.

I think that we have to move beyond a crude TOTAL ACCESS / NO ACCESS dichotomy in regulating access to the Internet. We need finer granularity in our restrictions so that we don't infringe on the rights of adults.

A final note. In a recent thread on the NCSA FORUM on CompuServe, there was a discussion about whether there were mechanisms for restricting BBS and Internet access by children. I answered, "Yes--one is PARENTAL RESPONSIBILITY."]

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn (Carlisle PA)

---

## Roll-Over Date Frozen?

*Ed Ravin <elr@wp.prodigy.com>*

*Tue, 1 Nov 1994 13:15:13 -0500*

Another one for the "date-dependent" bugs collection:

Last month, all five hundred or so Fujitsu model SRS-1050 ISDN display phones here at Prodigy suddenly stopped their clocks at 11:59 PM September 30. [Typoed 31 fixed. PGN] The problem seems to be that the built-in clock on the phone freezes when trying to roll over into the first day of a two-digit month. Resetting the clock/calendar to the current date and time fixes the problem until the next month rolls around. While the clock is in its "stuck" state, the "message waiting" light will never go on, no matter how many voice mail messages are waiting for you (you still get the "stutter" dial tone, though).

These phones were newly installed in December of last year -- their EPROMS are dated November 1993. Apparently this bug crept in around then and has been installed in all Fujitsu phones of that model since. I'm told the manufacturer will need to replace tens of thousands of EPROMs in the field for their various business customers who have deployed these phones. The new EPROMs will be tested by an outside company before being delivered to the customers. Until then, we need to manually reset our phones on November 1 and December 1.

Previous RISKS reports of date bugs were usually overflows of 16 or 8 bit quantities -- is this a new record in lower limits?

Ed Ravin, Prodigy Services Company 445 Hamilton Avenue  
White Plains, NY 10601 +1 914 448 4737 elr@wp.prodigy.com

---

## followup on Sears captures signatures

*Steve Holzworth <sch@unx.sas.com>*

*Mon, 31 Oct 1994 18:44:44 -0500 (EST)*

Since my original post concerning Sears now digitizing signatures when you sign a credit card slip, bunches of people :- ) have sent me Email, either asking for elaboration on the risks involved, or adding anecdotes of their own. I'll attempt to describe the potential risks as I see them.

Summary of previous post:

Sears in my area has recently started asking for people to sign their credit card receipts while the receipts are on what is obviously a small digitizing pad. Sears doesn't make it obvious that this is the function of the device.

You can refuse to sign on the tablet. They'll probably have to call someone first to OK it.

Potential Risks of digitized signatures:

Capturing the act of signing gives the store more information than simply scanning a copy of a signed receipt would. In addition to the basic image of the signature, the tablet can also effectively record stroke information (direction of strokes, and possibly, pressure of strokes). This is important, because given stroke information, it is almost trivial to write a program to fake a signature with a pen plotter. Simply use the stroke points as control points for spline curves. Said control points can then be perturbed slightly to yield what appears to be the same signature STYLE, without being a direct copy of an existing signature.

Of course, Sears wouldn't do anything so stupid. However, once the data is available, a disgruntled or entrepreneurial employee could sell the data to other parties. Let's see. Bill Gates goes to Sears and buys a screwdriver on his credit card. How much is his signature potentially worth on the market? Or, (for the really paranoid :-), some government agency, say, DEA, known to be overzealous at times, decides to "apply" your signature to some incriminating evidence...

I don't believe Sears (and others mentioned) can perform dynamic signature verification on the fly. They can't possibly have that horsepower at the terminal (at present). Even simple credit card number verification takes 30 seconds or more. Imagine the complexities of looking up one of N million signatures, correlating it to the new sample, then issuing a go/no-go response in a reasonable time frame. The closest approximation to this so far is the Apple Newton handwriting recognition. It looks in a small (10k words) dictionary, has to be trained to your writing style over time, and still screws up often enough to cause some headaches. How tolerant is your customer base to having their charges denied when they KNOW they wrote a valid signature?

More importantly, what REASON can Sears have for wanting this information?

I proposed that they can't do anything useful with it yet, so why should we let them have it? Further, to the best of my knowledge, no credit card provider requires card owners to supply digitized signature information when initiating a transaction. My understanding is that, per the card issuer agreement with the merchant, the merchant CANNOT require ANY other identifying information, assuming they get an approval code from the card issuer. Keep in mind, you don't even SIGN a receipt for a mail-order purchase... Why should we let Sears et al digitize our signatures?

One limited use of a digitized signature could be to display a specimen of your signature on POS terminal so the clerk can compare with your receipt. Of course, that is supposedly what the signature on the back of the card

is for (among other things)...

One responder mentioned that if the customer was signing paper on top of a tablet, it was unlikely that much information could be captured beyond stylus pressure. This is incorrect. I developed high-end CAD software for civil engineering and land planning for many years. All of the digitizers we used were capable of capturing positional information through quite a number of layers of vellum, mylar, and/or paper. This was necessary because much of engineering work involves tracing existing maps or drawings.

Several responders stated that they had run into similar digitizers at Sears, Service Merchandise, and others. A few stated that my example of refusing to sign had encouraged them enough to "just say no" :- ) next time.

I'm not trying to be paranoid, but I attempt to see all of the angles when confronted with a situation as described above. I operate under the rule that unless you can give me an extremely good reason why I should give you some class of information about me, you don't get it. Numerous posts to RISKS have documented how quickly and easily information about someone is disseminated, and how difficult it is to correct misinformation, once it gets spread. I attempt to minimize acquisition of the information as a preemptive measure.

Steve Holzworth SAS Institute x6872 SAS/Macintosh Development Team  
Cary, N.C. sch@unx.sas.com

---

## Minnesota driver license

*Daniel Frankowski <dfrankow@winternet.com>  
Fri, 4 Nov 1994 15:55:56 -0600 (CST)*

\*City Pages\*, a great free news weekly here in the Twin Cities (Minnesota USA), recently had an article [1] chock full of privacy issues and implications of the new Minnesota driver license (not "driver's" but "driver" on our license). I approached the article with deep suspicions about a new card, and came away only slightly less suspicious.

The old license has been the same for 25 years. It has a picture, a license number and some personal information (address, height, weight, signature, birthdate, etc.).

.. [O]fficials were tired of the ease with which the old card could be forged and altered. In early 1990, local police officials uncovered a forgery ring in the Twin Cities that used fake Minnesota licenses to open bank accounts and pass close to \$1 million worth of bad checks.

To make it harder to forge, the new card is printed in several fonts and the location of your (digitized and stored) picture depends on your age. For the information age, there is a barcode with your driver license number, and a magnetic stripe that can contain three lines of about 80 characters each, currently slated to contain a person's full name, date of birth, and driver license number.

The article raises a plethora of issues, some of which follow. I have hastily tried to put them into categories, which unfortunately overlap.

#### INFORMATION HANDLING RISKS

- The state government assumes that the public should trust government agencies with these technologies. This resulted in a lack of public discussion or input because the government did not publicize the new card proposal. The article gave an example I had not heard why we should not trust government: upon dishonorable discharge from the US military, it assigned a code which potential employers and others could get. 257 meant "unfitness, homosexual acts," 261 was "psychiatric or psychoneurotic disorder," 287 was "unclean habits including venereal disease," and 289 "unsuitability, alcoholism."

- Currently, the Driver Vehicle Services (DVS) department makes all their information public except social security number and medical information. That is, registration and title info, driving records, and the personal information from your license. The state sells it ("provides it for a fee"), and currently has 600 online accounts (presumably customers buying the information). They can sort by age, area, or size of person, for example.

- The card is a universal identifier, a notion often reviled in RISKS.

- The article mentions a national database of 7 million commercial drivers (only truckers?) called (and operated by) AAMVANET which went online January 1989. It contains each person's name, date of birth, social security number, and physical descriptors. "It was mandated by the federal government because truckers were getting licensed in multiple states to avoid suspensions." Barry Goleman is the president of AAMVANET, Inc., a subsidiary of the American Association of Motor Vehicle Administrators. "Goleman says that in the future, the system will include all drivers-- currently a total of 160 million, nationwide."

- The license may be linked to issues unrelated to driving. In Wisconsin, your license may be suspended for failing to pay public fines. The article's example is a late book fine at the public library.

#### RISKS OF SUDDENLY SWITCHING TECHNOLOGIES

- The company producing them (Deluxe Check Corporation, big in Minnesota) promised quicker turnaround for new licenses, but their digitizing cameras overheated, and their incompatible transmission protocols lost about 4000 new pictures which have to be retaken.

#### RISKS OF MAGNETIC STRIPES

Goleman (see above) said "upward of" 22 states have magnetic stripe-reading technology for driver licenses already.

- You, the card holder, cannot easily read the magnetic stripe to ensure that there are no mistakes because a special machine is required.
- Businesses could modify credit card readers to read the license stripe "ostensibly to verify ID" and build databases of shopping habits and personal information.
- Minnesota businesses are trying to get extra information put on the magnetic stripe.
- A state group proposed distributing AFDC (welfare) money. The article hypothesized the card could be used (say) to track your location.

Comments:

At first, I was impressed with the fact that all information in the barcode and magnetic stripe would also be visible on the card. In other words, no hidden information. However, other points listed above drained away my relief.

I noted a fatalism about the article: it catalogued frightening consequences without proposing solutions or interviewing privacy experts. This seems typical of even good journalism these days.

So are there simple guiding principles about the use of information for a driver license?

Would it be a good idea to pass a law requiring cash machines to be able to display (for free) any information on a magnetic stripe given the appropriate PIN #?

How else can we solve the problems above?

1. Card Blanche, Jennifer Vogel, City Pages, Vol 16, No 725, October 26, 1994, pages 15-20.

Dan Frankowski dfrankow@winternet.com

---

## Re: CAPS-LOCK Considered Harmful (Massey, [RISks-16.51](#))

*Jim Griffith <griffith@netcom.com>*

*Mon, 31 Oct 1994 16:05:19 -0800*

>IMHO, the worst button-placement crime is one almost every  
>computer manufacturer for the last 20 years has perpetrated:  
>the CAPS-LOCK key on the keyboard.

This "risk" is made worse by the fact that different interfaces cause users to hack their way back to familiarity. We're currently having that problem at work, because our three-member UNIX team was imported intact from a

SPARCstation shop to an HP-UX shop. SPARC keyboards have the caps lock in the "standard" position, while HP's stick the caps lock in the CTRL position and the CTRL key beneath the shift key (standard PC configuration). And each of us have addressed this in different ways. One user has learned the new keyboard, one user has simply switched the internal mapping for CTRL and CAPS using xmodmap (without relabelling the keys), and the third switched the mapping while also moving the ESC and a couple of other keys.

The end result is that we can't use each other's machines without sacrificing as much as 25% efficiency (UNIX and vi being as CTRL-driven as they are). We have yet to see a case where this caused an unrecoverable disaster, but it's surely just a matter of time.

Jim Griffith griffith@netcom.com

[RISKS received a ton of responses on this subject. Sorry we can't use them all -- our readership would probably get totally fed up with me. PGN]

---

### **RFD: sci.engr.safety**

*Sethu R Rathinam <rathinam@ins.infonet.net>  
3 Nov 1994 15:32:41 -0500*

#### REQUEST FOR DISCUSSION (RFD) SCI.ENGR.SAFETY

Name : sci.engr.safety  
Status : unmoderated  
Distribution : World  
Summary : Safety of Engineered Systems  
Proposed by : rathinam@ins.infonet.net (Sethu R Rathinam)

#### Proposed Charter:

This newsgroup is being proposed as an open forum to discuss safety issues of systems built by humans. All aspects of safety relating to the risk of (or actual) loss of human life, loss of non-human life and/or property fall within this charter. Safety issues and concerns relating to all phases in a product's life cycle as well as discussions of Regulatory Issues and System Safety Processes and Software issues relating to safety fall within this charter as well.

Since various Engineering disciplines are involved, it is recommended the subject line be a clear reflection of the subject matter. Factual posts and informed discussion is encouraged and speculation should be kept to a minimum.

#### Rationale:

There is presently no group with a primary focus on safety, though various newsgroups discuss safety issues within the (relatively narrow) scope of that group. A more focussed group for safety will help people from one discipline have more visibility to safety issues and practices of other

disciplines.

Other:

Newsgroup line "All aspects of Safety of Engineered Systems"

Cross Postings:

[This RFD is cross posted to many others. Please excuse duplication.]

Voting process

This is the Request For Discussion. There will be a 30 day discussion period (discussion will happen in news.groups - followup is set correctly, so if you follow-up to this message, your posting will appear in news.groups). This RFD may be modified incorporating suggestions, if required, during this period. If there is no serious disagreement, a Call For Votes (CFV) will be issued by a third party. The CFV will last between 21 and 31 days (as announced by the third party vote taker). Please follow the instructions of the vote taker when we get to that point in time. For the group vote to pass, there should be 100 more YES (create) votes than NO (don't create) votes AND at least two thirds of the valid votes are in favor of creation of the group.

Sethu R Rathinam

rathinam@ins.infonet.net

---

## Mathematics of Dependable Systems

*Victoria Stavridou <victoria@csl.sri.com>*

*Mon, 31 Oct 1994 21:32:54 -0800*

THE INSTITUTE OF MATHEMATICS AND ITS APPLICATIONS  
2ND CONFERENCE ON THE MATHEMATICS OF DEPENDABLE SYSTEMS (MDS 95)  
4-6 September 1995 University of York, England

### ANNOUNCEMENT AND CALL FOR PAPERS

The construction of dependable systems, by which we mean systems providing high levels of reliability, availability, safety and/or security, is a problem of considerable concern to both providers and users of information processing systems of all types. Historically, different aspects of system dependability (e.g. reliability and security) have been studied quite independently, albeit that many of the goals are similar. For example, the notion of certifying functionality assurance levels applies equally to reliable systems and secure systems. In addition, users will often require some combination of security and fail-safe operation.

The purpose of MDS 95 is to consider the mathematical aspects of the provision of dependable systems, one goal being a comparison and possible unification of mathematical techniques for providing safe, reliable and secure systems. A number of different mathematical approaches have been taken to the overall problem, including probabilistic/statistical reasoning, formal models of safe, secure and reliable systems and logics of

authentication and access control/privilege delegation. Papers on all these areas are solicited, the unifying theme being the application of mathematical techniques to the overall dependability problem. Hence papers will be particularly welcome which cross-fertilise the application domains. The conference will consider dependability for both hardware and software systems.

**PROGRAMME & PROCEEDINGS** The conference will consist of three days of presentations by contributing authors. The programme will also include invited lectures by prominent researchers and practitioners in dependable systems theory and practice. Time will be made available for discussions. A digest of papers will be available to participants during the meeting and the proceedings will be published after the conference.

**INVITED SPEAKERS** Monsieur P Chapront (GEC Alsthom, France), Professor J Knight (University of Virginia, USA) and Professor D L Parnas (McMaster University, Canada).

**SUBMISSIONS** Five copies of complete papers (in English) should be sent to Mrs Pamela Bye, Conference Officer, The Institute of Mathematics and its Applications, 16 Nelson Street, Southend-on-Sea, Essex, SS1 1EF, England (Tel. +44 702 354020, Fax +44 702 354111, Email [imacrh@v-e.anglia.ac.uk](mailto:imacrh@v-e.anglia.ac.uk)) by 31st March 1995. Authors will be notified of the outcome of their submission by 26th May 1995. Revised manuscripts will be due by 14th July 1995. Papers must not exceed 6,000 words in length (with full-page figures counted as 300 words). Each paper should include a short abstract and a list of keywords for subject classification. All papers will be refereed and the final choice will be made by the programme committee on the grounds of relevance, significance, originality, correctness and clarity. Submitted papers must not be published or be under consideration for publication elsewhere in the same or similar form.

**PROGRAMME COMMITTEE** Programme Chair : V Stavridou (Royal Holloway, University of London), D Gollmann (Royal Holloway, University of London), M Ingleby (British Rail Research), J Jacob (University of York), N Jefferies (Vodafone Ltd), B Littlewood (City University), R Shaw (Lloyd's Register), B Wichmann (National Physical Laboratory).

**LOCATION** The conference will be held at the University of York, a modern campus built around a lake with excellent facilities. The campus is two kilometers from the centre of the medieval walled city of York, and 60 kilometers from the North Yorkshire coast. The city is also well placed for the Pennines and Yorkshire Wolds. York is very well connected by rail to London, Edinburgh and Manchester and the nearest airports are Manchester and Leeds/Bradford.



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 16: Issue 54**

**Monday 7 November 1994**

## Contents

- [\[NOTE: "September 31" typo\]](#)  
[30](#)
- [Fall time change and the usual computer system havoc](#)  
[L. Scott Emmons](#)
- [Ottawa Library fines people using unreliable automatic calling system](#)  
[Michael Slavitch](#)
- [Tele-Phoney](#)  
[John Vilkaitis](#)
- [Risks of assumption](#)  
[Tom Swiss](#)
- [Re: CMU blocks access to nasty newsgroups](#)  
[Bob Frankston](#)  
[Arthur Hicks](#)  
[Jim Huggins](#)  
[Harry Rockefeller](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Fall time change and the usual computer system havoc

*L. Scott Emmons <scotte@center.uscs.com>*  
*02 Nov 1994 20:51:57 GMT*

With the recent change back from daylight savings time, we can always expect the usual havoc caused by lousy operating systems that aren't smart enough to know how to switch time automatically. Of course, this issue has been discussed here before, so what happens at this location here may or may not be of particularly exciting news.

Anyway, there is a card-key system that locks up a certain development facility between 5pm and 8am. The system is run by one of the aforementioned lousy operating systems that is not smart enough to change the time automatically. So, for a few days each fall the facility is unlocked and locked early, and for a few days each spring the opposite occurs; until somebody bothers to report it to the right person who has control over the

system. I'm not sure which is worse -- the security risk of having an unlocked facility, or the annoyance factor in being unable to get into the building without the right key-card.

Fortunately, most of the systems I have to deal with are Unix boxes, which do set the time correctly. I wonder why other operating systems are so far behind?

L. Scott Emmons, U.S. Computer Services/CableData R&D Center (916) 939-6088  
scotte@center.uscs.com

---

### **Ottawa Library fines people using unreliable automatic calling system**

*"Michael Slavitch, Consultant, (613) 781-9824" <slavitch@on.bell.ca>  
Mon, 7 Nov 94 15:45:50 -0500*

About two months ago I reserved a book at my local library. The library has gone electronic in its reservation system. You reserve a book, and when your turn to receive it comes due a computer dials your home phone number. If an answer occurs, it assumes you heard the message; if you do not pick up the book in three days, you are fined \$2.00.

Basically, this is what happened to me. Their computer called my number and the phone went off hook, starting the meter running. For some reason my answering machine did not pick up the message (I have an answering machine and a fax modem hanging off the same line, but the fax modem is outgoing only).

The RISK here is obvious, and I consider it nontrivial. The librarian insisted that the "system" is "reliable" and "almost always" works. Well, my knowledge of datacomm says that if it does not always work it is not reliable, and that they are fining people based on an assumption that the message was received.

What's scary was the attitude of the librarian. Because she was told by someone that the system works, she insisted that I had received the call. I asked her for proof of that and she said that "the system said you got the call, it must be true". My attempt to describe the essence of data communications and reliable communication fell on deaf ears, and she refused to give me the name of her superior because "the system works and nobody should complain about it."

Well, I am. I know that it is only two bucks, but the implications that arise from misuse or overly trusting such a system are worrisome. What if the government started issuing parking tickets or summonses in this manner, or banks warning you of surcharges on financial transactions? What if my wife answered the phone and the book was "how to handle infidelity in you marriage" :) (it wasn't).

So how do you handle two things:

[One] An unreliable delivery system being assumed to be reliable.

[Two] People placing trust in such a system.

Michael Slavitch, Software Design & Analysis Consultant, assigned to:  
Bell SYGMA, Suite 250, 150 Elgin St., Ottawa, Ontario K2P 2C4, (613) 781-9824

---

## Tele-Phoney

Javilk <javilk@netcom.com>

Mon, 7 Nov 1994 01:48:00 -0800 (PST)

### Troubles with Tele-Phoney Systems

Getting a wrong-number call in the middle of the night from another human can be irritating. We may hope that future telephone numbers incorporate a check digit to reduce these errors, but I doubt they will.

But let us first look at our "Telephone Neighborhood". Do you have any idea who or what exists in the 62 or so valid telephone numbers only a slip of the digit away from yours? (Area codes brings it up to about 80, but they are less often dialed. Another problem.) Apparently I have several interesting entities in my telephone neighborhood. And with most calls being dialed by embedded microprocessors and computers these days...

What prompts this observation? Funny you should ask that...

On Friday, after the close of business for the weekend, (as in, when else?!) I began receiving a strange series of persistent wrong number calls from one gentleman in my area code. As I answered, I would hear the "musique de telephon" of another ten-digit number being dialed. Although apologetic, the caller insisted he was trying to reach several very different numbers in two adjacent area codes. Soon others joined him in reaching out and touching me with a number of different touchy toney loony tunes, complaining that I was not the party of their choice; then retrying the process with more diligence, and sometimes more stridence. But no matter the area code or number they dialed, they all rang my phone.

Some investigation on my part revealed they all originated from the same place, an apartment complex in a nearby city with a new PBX (Private Branch Exchange,) telephone system. To save the dwellers money, (or to line their coffers some more,) management had contracted with a private (discount) telephone and cable company called "Western Telephone and Television" (WTT) for a PBX with a feature called "least cost call routing." The physical PBX is a 6 x 4 x 2.5-foot box containing twin 680x0 processors for redundancy, each with its own hard drive, and each running a proprietary operating system called CORTELCO. The box can handle up to 500 telephone lines, although only approximately 300 lines were hooked up at that particular site.

Under normal circumstances, this PBX is programmed to quietly intercept the dialed number, dial a five-digit access code (a 10-xxx number) on one of several outgoing lines, and when the access number goes off hook (answers), echo the number that the customer dialed; whereupon the long distance service provider takes over. However at this particular location, a five-digit access code was not available, and so a full seven-digit access code had to be used. In other words, the system simply forwarded all calls to another ordinary-looking phone number. Unfortunately, the technician inadvertently entered `_my_` phone number while correcting a previously(!)

erroneous number.

Hence, all long distance calls placed from that apartment complex rang through to my number starting at 6pm Friday evening.

This prompts some interesting observations:

1. No caller ID is transmitted with the call,
2. There is no handshaking between PBX and the service provider.
3. Audio is immediately enabled upon completion of number dialed.

Speculations:

1. All accounting probably resides in the PBX
2. Most billing info and programming is done via modem.
3. Anyone with the seven digit access code...

...has unlimited free telephone service.

Kind of makes you wonder what the fraud rate is in this industry, and how much is added to the average telephone bill to offset it. (No, I did not ask what number the computers were trying to call or I'd be their prime suspect!)

Of course, once awakened, Murphy did not stop there. WTT's emergency pager number had been \_Disconnected\_. Nor could Pacific Bell Information find any local phone number for WTT. When I finally got the correct number from the apartment manager and called WTT, their automated attendant / voice mail system kept telling me to dial 0 for their operator (receptionist), then complained this and other automatically suggested extension numbers, were not valid. Whereupon the default error message, of course, again instructed me to dial 0 for the operator. (This kind of looping appears rather common in corporate automated attendant systems.) Eventually some error count was exceeded and at least \_this\_ computer had the sense to hang up.

The RISK of not checking your telephony systems for message loops, old numbers, etc. is looking like a corporation of idiots. Not to mention a telephone company not having a publicly listed telephone number! [I think we now might understand WHY! PGN]

(My favorite ploy in the case of such loops and lockouts, is to look for a Smith or Jones in their audio telephone directory, and inform him that his company is losing thousands of dollars in sales because the telephone system will not let callers speak to a human being; then ask he pass my number on to an appropriate party. Few ever bother. They must think it's not their job to help their company be profitable.)

Finally, The local Bell Systems affiliate repair service (good old 611) told me that the RISK of harassing innocent telephone subscribers, as they agreed WTT's automated equipment was clearly doing, was having telephone service to their equipment, and thus the entire apartment complex, disconnected. (Probably by Monday...)

But of course, Murphy being who he is, Repair could do nothing right now. And in retrospect, they really could not do much. Repair directed me to several different Pacific Bell departments, each with its own 800 number, but all of which had an identical automated voice issuing identical instructions. The RISK of using identical messages (computer voice screens?) is having customers think they are reaching the SAME number. For all I know, I may have been! Eventually, the chain of "if you have... then call 1-800-..." messages, which are heard after one finds one's situation is not on the menu, reached a recorded message informing me to call the local police to handle the situation.

Is the RISK of having electronic equipment becoming deranged, with no obvious "OFF" switch, having it SHOT by law enforcement officials? Something equipment designers really ought to think about!

After numerous complaint calls to the apartment manager, WTT, and

Pacific Bell by apartment residents, Pacific Bell, the apartment manager, and myself, a WTT technician entered another set of access codes into the system. The calls ceased shortly before noon, Saturday. I received a long and very apologetic call from the technician. We ended up discussing the operational details of the PBX. The technician also checked the voice-mail looping problem and reports they will have to completely reconfigure their company office's automated attendant system to avoid the "dial operator" loop problem.

#### The RISKS of Busy Telephone Neighborhoods

The people at the Misdialing Gardens Apartments were more polite than those involved when Coca Cola published my number as their in-warranty emergency repair number three years back. Now I say that I can fix almost anything (and often do), but those people insisted I fix their Coca Cola machines Right\_NOW\_For\_FREE since soda was usually spewing forth onto the carpet, etc. Complaints to Coca Cola Corp.'s headquarters met with Persistent Insistence that my number was Indeed The\_Correct\_Number for their in-warranty repair service. They kept looking it up in their corporate directory and their computers, and telling me it "The computer says that IS\_ The Correct Number, so stop bothering us!" (I couldn't seem to get a VP's secretary to understand the true nature of the problem. And of course, she would NOT pass me on up the line because I\_ was \_Obviously\_Wrong\_.) After a few go-arounds like that with Coca Cola's Headquarters, I just gave up and chanced my number to an unlisted number without a forwarding reference. It only cost me several hundred dollars to change stationary and notify all my clients...

... Some of whom had recently changed their fax numbers... And since I usually set up a computer to send these overnight... Well, I guess I just had all those "favors" returned this past week end!

#### The ADVANTAGE of Call Return

I still get calls at all hours, but not as often; the present phoney phone callers all hang up when they hear a human answer, making one think of burglars trying to see who is home, or the odd former acquaintance, ex-spouse, or ex-employee who might have traded a few marbles for some lead pellets. When I ordered call return to investigate this problem, the Pacific Bell representative told me to call these phoney callers back and say "I am working with" (not for) "the telephone company to determine why people call this number." The responses revealed that my current number in the slipped digit neighborhood of a touch-tone-based Automatic Bank Information system. If I politely return those phoney phone calls, I can keep the number of calls down to two or three a month as opposed to the original three or four a week. (Not to mention retain my peace of mind!) I guess people do learn.

Don't call me, I won't call you! Please!

Several individuals have commented that someone less ethical might have set up one of those \$95.99 voice mail cards to ask for the caller's account and PIN numbers, then apologize for the rest of the computers being unavailable. In effect, a telephonic analog of a terminal with a phony login screen. Which reminds me of...

## The RISK of Borrowing Time Sharing Programs

Back in college, some twenty two years back (seems like yesterday!), I had been assigned the task of catching a student who was using a phony log in-screen to steal account numbers on CPS, the time-sharing system which ran on UConn Research Computer Center's IBM 360. CPS (Conversational Programming System) was an interactive PL/1-like variant of BASIC. In one evening, I was able to cobble together parts of a utility program I was writing to create a 1,400-line PL/1 program which performed a brute force search over the CPS saved program hierarchy for the word "login". (Not so easy since CPS used its own file format, saving programs and data in tokenized form; but my utility already scanned comments for expiration dates.)

It turned out that the offending programs were saving themselves with the captured login data stored in arrays. As in interactive BASIC, the miscreant could query these arrays without executing the programs themselves. I "de-initialized" the arrays and subtly damaged the programs. An "On Error" statement was used to activate a few new lines near the end of the program to message the main operations console whenever the programs were either run OR the now invalid array elements were queried.

Several nights later, I arrived just in time to join two other staff members as they ran across campus to catch an unexpected second miscreant. She later managed to convince the powers that be that she was not The Real Miscreant; but had "merely borrowed a program to see how it worked." I always wondered about that. Did you really do it, Ellen? Or was it really the other fellow?

The RISK of stealing time-sharing programs is stealing Booby Traps.

-JVV-

---

## Risks of assumption (Carasso, [RISKS-16.52](#))

*Tom Swiss <tms@tis.com>*

*Tue, 1 Nov 94 15:18:19 EST*

First, I'd like to disagree with Mr. Carasso's belief that user confusion due to a lack of standards in control layout is "stupidity". It's very easy for users to develop an automatic patterns for some frequently performed operation, and then repeat that pattern in a circumstance where it is not appropriate. For instance, I've developed a habit of hitting Control-X Control-C y to exit emacs and confirm it's "Save file foo? (y or n)" prompt. Then I went to use an editor that, upon exit, prompted something like "File foo not saved - really quit? (y/n)" My fingers were running the emacs pattern and hit "y", thinking that that meant to perform the save, when in fact it meant to exit without saving. I can very easily imagine a long time PC user whose fingers get ahead of his brain, confuse the floppy eject with the power switch, and shut the machine off.

I'd also like to question his assumption that if you made such a mistake, you "obviously just got your Mac, there's little of value on it, and it's unlikely that anything damaging will \*really\* happen." It seems to

me that to properly assess the risks of such a situation, one should always assume a worst-case scenario.

So what kind of "what-ifs" can we add to this situation?

In the worst case, safety critical equipment might be controlled by that Mac. (Yes, we know that there should be a protective cover over that switch in such a case, but I'll bet you a nickel there's a system out there right now that could hurt someone if such down at the wrong time and is without such a cover.) That's a obvious risk.

Less obvious is the possibility of losing very important data. To take an example from my own experience, I was forced to do my first extensive Macintosh work (aside from some light word processing at an old job) for a robotics class Programs were compiled on the Mac and downloaded to the controller board. We saved our work on floppies so we could move the work between any one of several Macs.

Much of the work (at least for my team) turned out to be trial-and-error setting of various constants. It might take a dozen compile-download-test cycles to find a good value for one such constant. I can just imagine the horror, the wailing, and the gnashing of teeth had one of us gone to swap floppies to save some bit of work and, operating on auto-pilot (as is known to happen when you're working at some ungodly hour to meet a deadline) hit the power switch and sent that work to the bit bucket.

-Tom Swiss / tms@tis.com

---

## Re: CMU blocks access to nasty newsgroups

<Bob\_Frankston@frankston.com>

Mon, 7 Nov 1994 10:23 -0400

A few months ago I responded to a similar issue on another mailing list. As a parent, I can appreciate the problems with adding to the burden of parental responsibility in presenting one more threat we must shield our children against.

The real question is how to prepare children for a world in which censorship is not viable -- how to make them better participants in a world rich in information and sleaze. Which is which is often a matter of personal opinion. Ultimately they will have to make the judgment of how to handle it.

I realize that there are lots of issues here and that the mere presence of objectionable materials does open organizations up to harassment suits. But, ultimately, this country has made a bet that open access to information is the better option. Other countries have more or less censorship on various issues and are no longer across a wide ocean.

This does mean that one (as a parent, educator, whatever) needs to try to teach that not all information available is valid or representative of the

real world.

But some information can be real and disturbing. At one point while I was in elementary school, I had a great fear of news -- especially international news. Considering that it was in the 50s and duck and cover was a part of the curriculum and one standard topic was how big an H-bomb it would take to reach our school if it landed (precisely?) at Columbus Circle in New York, this was not totally irrational.

But is it better to grow up in a world unprepared, without an immune system?

---

## RE: CMU blocks access to nasty newsgroups

*Arthur Hicks <ahicksii@netcom.com>  
Mon, 7 Nov 1994 09:13:11 -0800 (PST)*

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com> wrote of attempts to resolve the problem of access by children to possibly unsuitable sexual material in certain USENET newsgroups. I would like to respond, as a seemingly responsible parent, with some examples of real parental controls, and real parental concerns about this issue. In our case the family MODEM is hardwired to a separate local-only phone line, somewhat reducing the scope of possible teenage computer activities, but Internet is another matter. I have applied suitable access limitations to my son's AOL sub-account, and my kids are never allowed any visual access to my passwords. My kids have also freely discussed these issues with me, and can be expected to understand them to the degree that they are willing to understand them. To that extent I don't worry about my kids and their activities. I am concerned however, with the very real problem of adult human "predators" who seek out congregating kids, whether it be outside the neighborhood convenience store or on the Net. It is a mistake to think that "good", intelligent kids can necessarily resist or even be aware of the attempts of an experienced adult "predator" to do them harm. This is why I remain concerned about the issue of suitable Net access for kids. The article by Mich Kabay appears to trivialize the real concerns of parents who are trying to be responsible about giving their kids access to contemporary tools, but also wish to avoid unreasonable risks to the well-being of their children. Art Hicks

---

## CMU and Newsgroups (Kabay, [RISKS-16.53](#))

*Jim Huggins <huggins@eecs.umich.edu>  
Mon, 7 Nov 1994 15:21:20 -0500*

Mitch Kabay comments at length about CMU's decision to block access to alt.sex.\* et. al. on its computer systems. Mitch's comments focus mostly upon access, calling for finer grains of access to the Internet rather than total vs. no access.

While Mitch raises good points, they really don't address CMU's dilemma. The following is an excerpt from the official on-campus

announcement of the change:

Pennsylvania laws prohibits us from carrying bulletin boards that are known to be used for the distribution of sexually explicit or obscene material. It is against the law for anybody to knowingly distribute sexually explicit materials to people under the age of 18, or obscene materials to people of any age. [...]

[T]he only criterion that will be used when considering the withdrawal of a bulletin board is that either the intended purpose for which it was established or its primary use (majority of the posts) makes it illegal for Computing Services to provide access to the bulletin board.

(N.B. Usenet groups at CMU are usually called bulletin boards.)

This isn't really an issue of whether minors can get access -- the vast majority of students at CMU are over 18, anyways. The problem is that obscene material cannot be distributed in PA, regardless of the age of the recipient. And so CMU needs to find a way to obey the law.

In some ways, this is already the finer-grain access that Kabay suggests. CMU isn't going to monitor every newsgroup for obscene materials; it simply will eliminate those newsgroups where such material is the most prominent.

Of course, whether or not local definitions of obscenity make sense anymore in a global infobahn is another question entirely, and one in which I'm still undecided.

Jim Huggins (huggins@umich.edu)

---

### **Re: CMU blocks access to nasty newsgroups (Kabay, [RISKS-16.53](#))**

*Harry Rockefeller <harryr@ssd.fsi.com>*

*Mon, 7 Nov 94 13:41:33 -0600*

Mich seems to discuss only one of three problems here. He notes that there is material suitable for adults but not for children. He correctly notes that it is the parent's responsibility to build a suitable barrier.

The other two issues of "censorship" he did not discuss are: 1) Highly offensive material not suitable for anyone, and 2) Any material offensive to a payer.

In category 1) may be child pornography, or bestiality pornography. The material (at a state or more local level IMO) may be simply ruled illegal.

In category 2) Realizing that CMU receives tax funds we should ask if

any of these tax funds pay for Internet? If yes, then a case may be made to eliminate several newsgroups because they are offensive to some segment of the taxpaying public.

Harry Rockefeller FlightSafety International, Simulation Systems Division  
Broken Arrow, OK 74012 [harryr@ssd.fsi.com](mailto:harryr@ssd.fsi.com) (918) 251-0500



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 16: Issue 55**

**Weds 9 November 1994**

## Contents

- [EMI and construction cranes](#)  
[Steve Summit](#)
- [Postscript FAX Security Hole](#)  
[Mike Crawford](#)
- [Hardware-borne Trojan Horse programs](#)  
[Chris Tate](#)
- [Risks of posting warnings with the wrong time or date](#)  
[George Swan](#)
- [Existential risks of computer systems](#)  
[Ian Horswill](#)
- [E-Signatures](#)  
[Benjamin Wright](#)
- [Re: Suitable for whom?](#)  
[Jon Green](#)
- [PBX at Large? \[Re: Tele-Phoney\]](#)  
[Stephen Bogner](#)
- [Re: Parental Responsibility](#)  
[Mich Kabay](#)
- [Re: Ottawa Library fines people ...](#)  
[Erik Jacobsen](#)  
[Daniel P. B. Smith](#)
- [Info on RISKS \(comp.risks\)](#)

---

## EMI and construction cranes

*Steve Summit* <[scs@eskimo.com](mailto:scs@eskimo.com)>

*Tue, 8 Nov 1994 12:31:17 -0800*

An article in Friday's *\*Seattle Times\** (Nov. 5, 1994) reports that "Microwave interference has stalled crane operations on the \$74 million Seattle Center Coliseum renovation project." Broadcast towers on nearby Queen Anne hill and consumer microwave ovens on the same hill are suspected, but "I don't know if we'll ever be able to pin that down," said Jack Donovan, construction manager for PCL Construction Services Inc."

Continuing from the article:

...when the crane operator tried the [crane's] electronic controls, they didn't respond correctly and haven't worked since, Donovan said. He didn't think the problem would delay the project... "Obviously, it's an inconvenience, but to this point we've been able to use alternate means to work around it," he said.

The crane operators are testing filters or shields around the controls to ward off microwaves. Electronic specialists were called in to work on the problem yesterday.

Steve Summit [scs@eskimo.com](mailto:scs@eskimo.com)

---

## Postscript FAX Security Hole

*Mike Crawford <[crawford@scipp.ucsc.edu](mailto:crawford@scipp.ucsc.edu)>*

*Tue, 8 Nov 1994 21:55:12 -0800*

I recently bought an Apple LaserWriter Select 360. While I wanted a laser printer anyway, I chose that particular model because it can accept a Postscript FAX card. I want to make a FAX/Email gateway that can send high quality faxes - one can mail a postscript file to the gateway, and a high quality fax will be transmitted. If one has the good fortune to be addressing another PS fax, the postscript is transmitted instead of the fax codes, for extra high quality.

But there's a big problem: PS is a programming language. This would allow people to program my laser printer via e-mail! People could do such things as change the printer password remotely. If one used a printer with an attached hard disk, one could mail in a command to erase the disk. Oops.

Would anyone know whether this has been considered under the postscript FAX standard? It seems to me it would be a problem for just regular PS faxes - one would just hack it over the phone line from another PS fax machine.

Can you imagine someone putting letter bombs in public domain clip art? Eek!

One could disable certain commands, and do save/restores, of course, but it is possible for postscript to be quite obtuse, and every printer has a number of undocumented postscript operators that would be hard to guard against in any general way.

Mike Crawford [crawford@scipp.ucsc.edu](mailto:crawford@scipp.ucsc.edu) [crawford@maxwell.ucsc.edu](mailto:crawford@maxwell.ucsc.edu)

---

## Hardware-borne Trojan Horse programs

*Chris Tate <[FIXER@FAXCSL.DCRT.NIH.GOV](mailto:FIXER@FAXCSL.DCRT.NIH.GOV)>*

*Tue, 8 Nov 1994 12:34:36 -0500 (EST)*

I had an unpleasant experience this past weekend, and I imagine some other readers of RISKS will find it interesting.

I recently purchased an Apple Macintosh computer at a "computer superstore," as separate components - the Apple CPU, and Apple monitor, and a third-party keyboard billed as coming from a company called Sicon.

This past weekend, while trying to get some text-editing work done, I had to leave the computer alone for a while. Upon returning, I found to my horror that the text "welcome datacomp" had been \*inserted into the text I was editing\*. I was certain that I hadn't typed it, and my wife verified that she hadn't, either. A quick survey showed that the "clipboard" (the repository for information being manipulated via cut/paste operations) wasn't the source of the offending text.

As usual, the initial reaction was to suspect a virus. Disinfectant, a leading anti-viral application for Macintoshes, gave the system a clean bill of health; furthermore, its descriptions of the known viruses (as of Disinfectant version 3.5, the latest release) did not mention any symptoms similar to my experiences.

I restarted the system in a fully minimal configuration, launched an editor, and waited. Sure enough, after a (rather long) wait, the text "welcome datacomp" once again appeared, all at once, on its own.

As a next step, I contacted John Norstad, the author of Disinfectant, and one of the international response team for dealing with new Macintosh virus sightings. Very promptly I received a response, which I shall quote here in its entirety (it's brief):

> Yes, we have heard of this. It's a practical joke in the ROM code in some  
> third-party keyboards. The only solution is to get your bad keyboard  
> replaced.

I was furious. Apparently there are hardware products on the market which have embedded "Trojan Horses," programs which affect the operation of the system without the user's consent (or knowledge!).

I have returned the keyboard to the store where I purchased it, and I plan to contact Sicon about the problem. The potential for abuses in computer systems here is apparent, especially when the system involves "intelligent" peripherals - such as many popular types of disk drive, Apple Desktop Bus devices (such as the offending keyboard), and so forth.

John Norstad informs me that he has little knowledge of the extent of this particular problem, other than the fact that he has received quite a bit of mail from people who have been bitten. What is almost as disturbing as having fallen prey to this particular joke is the lack of information about it - I can't find any mention of such a problem in any of the USENET Mac newsgroups' "Frequently Asked Questions" compilations, although those FAQs \*do\* mention viruses and how to deal with them. It definitely seems to me that people ought to be made more aware that this sort of thing is happening.

Christopher Tate fixer@faxcsl.dcr.t.nih.gov eWorld: cTate

---

## Risks of posting warnings with the wrong time or date

George Swan <gswan@io.org>

Tue, 8 Nov 1994 19:22:50 -0500

In the fall of 1990 a bomb threat was phoned in to the Waterloo (Ontario, Canada) Regional Police. The threat said that a number of bombs had been placed in various buildings on the University of Waterloo campus.

There was a recent discussion of this threat in alt.folklore.college. I posted a followup to this discussion. I thought I would post a shorter version for risks readers.

The entire campus was evacuated. It took several hours, as the University had no central public address system. The threat turned out to be a hoax. The news was circulated around the campus via a "phone-tree" and word of mouth.

I knew a few more details about this incident because the day before the bomb scare I had a long discussion with a young hot-head, who had said something stupid, and I had reported him to the campus police.

The young hot-head had been a devoted reader of the newsgroup "alt.sex.bondage". He was furious with the Dean of Computing because he had banned this newsgroup from all the campus computers. During the course of our discussion he said, "If I had a copy of 'The Anarchist Cookbook' I'd use it to bomb Johnny Wong's office!" (Dr. Wong was the Dean of Computing. 'The Anarchist Cookbook' is a how-to book on sabotage techniques, including how to build bombs.)

I reported his threat to the campus police. During my discussions with the campus police I learned that their big lead concerned the rash of news articles that had been posted to the newsgroup "uw.general" the afternoon of the bomb scare.

The campus police had arranged for someone to print out the news articles that concerned the bomb scare. One of the posts seemed to have been posted prior to the reception of the phone call that initiated the scare.

The risk?

I am sure that none of the people posting messages warning others of the scare gave a moment's thought as to whether their system's clock bore the correct time. I am sure they would be quite surprised to learn that they had become suspects. (Fortunately wiser heads within the University's Department of Computing Services were consulted first.)

There are some other risks I would like to comment on. When the bombs didn't go off as scheduled, the campus police were asked to check the campus. By the time I had my interview with them, the campus police had had a number of resignations. It seems to me that to do a proper job of checking the campus would require a regiment of combat engineers.

In my opinion, a phone-tree is not sufficient to meet this threat. The threat gave about four hours notice, and it took close to three hours to clear the campus. What if it had been a real bomb with only two hours notice? What if it had been a spill of toxic waste?

A recent risks digest said that CMU had recently announced bans of various newsgroups. Let's hope that none of CMU's administrators receive any threats.

---

## Existential risks of computer systems

*Ian Horswill <ian@ai.mit.edu>*

*Tue, 8 Nov 1994 18:12:42 -0500*

The hotel I was in last weekend had a nifty video-based message system. They had the standard spectra-vision pay-per-view interactive video hardware in the rooms so they set it up so you could review your bill, check out, and collect your messages using your TV and remote control as a terminal. Pretty nifty.

So one night, I get back to my room and press the "check messages" button. After a longish pause, my TV greets me with the message:

"We're sorry, but the hotel records indicate that this room does not exist. Please contact the front desk if this is not the case."

At first, this caused a sort of Sartrean crisis within me, but then I relaxed. According to the hotel phone directory, the front desk didn't exist either, so I was obviously in good company.

P.S. It would seem that someone inadvertently checked me out.

[Or else the database was inaccessible; your hypothesis suggests that someone checked out the front desk as well. PGN]

---

## E-Signatures

*Benjamin Wright -- Attorney ^ Counselor - Dallas <bwrigh01@reach.com>*

*Sat, 5 Nov 94 23:28:24 EST*

[This is an elaboration of an earlier RISKS item, which also appeared in a revised form in the October 1994 Communications of the ACM. PLEASE contact Ben if you want the entire article. PGN]

### ALTERNATIVES FOR SIGNING ELECTRONIC DOCUMENTS

By Benjamin Wright

Hospitals, banks, insurance companies and other organizations are looking to replace paper with electronic documents, but they need a way to "sign" those documents for legal and control purposes. This article considers the

practical features of two alternative signing methods: smart-card based public-key cryptography and PenOp, a pen computer technology that captures handwritten autographs. The article argues that PenOp holds certain advantages in that it does not require the signer to

- \* retain a token or smart card;
- \* remember a password;
- \* register with a bureaucratic certification authority; or
- \* depart from the custom of signing with an autograph.

PenOp also does not require the receiver of a signature to use technology that is compatible with that used by other people.

---

### **Suitable for whom? (Rockefeller, [RISKS-16.54](#))**

*Jon Green <jonsg@hyphen.com>*

*Tue, 8 Nov 1994 06:04:01 -0500 (EST)*

> The other two issues of "censorship" he did not discuss are: 1) Highly  
> offensive material not suitable for anyone, and 2) Any material  
> offensive to a payer. [...]

The concept of (1) frightens me. There is no material unsuitable for anyone, however repulsive a majority might consider it. By definition, someone wants it, otherwise it wouldn't exist. Who decides what's unsuitable? How often do open-minded individuals make the choice? It's usually made by a self-elected "moral majority" type, or a committee afraid of possible legal action initiated by the same.

The Internet is, and always has been, self-policing. If someone posts material considered by the vast majority to be utterly offensive, mass action ensures that the poster is effectively put out of business. That, not a "policy decision" made by someone we didn't choose to represent us, is the best way of dealing with socially unacceptable net use.

Once we permit certain limits upon our expression, we tacitly accept that further limits can be placed. I'd rather be free to express my opinions. I don't defend child abuse (or indeed animal abuse), but these are emotional arguments used to manipulate us into accepting the first of many serial limitations on our freedom to contribute to, and to enjoy, the Net.

Jon S Green

---

### **PBX at Large? (Re: Tele-Phoney, Vilkaitis, [RISKS-16.54](#))**

*Stephen Bogner <sbogner@dres.dnd.ca>*

*Tue, 8 Nov 1994 14:46:35 GMT*

A couple of years ago I checked into a hotel in Mississauga (near Toronto) that had just had its PBX stolen. As I struggled through a week in a strange city without a telephone, I could not for the life of me understand

why someone would steal a PBX, but I guess now I know....

Stephen Bogner (DRES/DTD/MES/Vehicle Concepts Group) sbogner@dres.dnd.ca  
(403) 544-4786 DRE Suffield; Box 4000; Medicine Hat, Alberta; Canada T1A 8K6

---

## Parental Responsibility

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
08 Nov 94 21:53:18 EST

Dan Weinreb <dlw@odi.com> wrote:

Exactly what does "parental responsibility" mean to you?  
That the parent should keep the child off CompuServe entirely? That the parent should sit behind the child during every moment that the child uses CompuServe, to supervise what he or she does? That any good parent would have a child so obedient that if the child is told "Do not look at this newsgroup and that newsgroup", the parent can be confident that the child will simply obey?  
Please enlighten us.

What an odd list of possibilities to propose for "Parental Responsibility."  
What about

"That parents should spend time with their children discussing their (both parents'; and children's) interests and activities and exchanging views in a mutually respectful atmosphere?"

or

"That parents have a right and an obligation to express their love for their children in many ways, one of which is the clear discussion of their values?"

Certainly the words "Parental Responsibility" do not by definition imply support for authoritarian personality traits nor do they suggest the exercise of simple-minded credulity as useful parenting skills.

As part of the National Computer Ethics Responsibility Campaign, Dr Peter Tippett has prepared the following document which addresses these questions. None of the suggestions, in my opinion, suggests that families become training grounds for a police state <g>.

===== %<>=====

Computer Ethics Campaign Information and Article

TEN QUESTIONS PARENTS SHOULD ASK THEIR CHILDREN

Peter S. Tippett, Ph.D., M.D.  
Symantec's Peter Norton Group  
Board Member, Computer Ethics Institute

1. Do you legitimately own all of the software, games, and programs you have or use?

Software Piracy, Clarifying Questions:

Are any of your programs or software bootlegged or pirated copies?

Where are the manuals, boxes, license agreements for the programs you have or use?

Where did you get that game? (program?, floppy?, software?)

When programs first start running on your computer, whose name comes on the screen as the "owner" or "licensed-to."

2. Where did the contents of your report / project / homework come from -- does any of it belong to someone else?

Did you write/create/author what you're passing off as your own work?

Where did you get the text and images you're using?

If you copied text and images from another source, did you have permission?

If you didn't need permission from the "owners" of the information you're using, did you credit them for the material?

3. Do you ever use other people's computer, disk-space or processing capability, or look at or copy their files or information, without their knowledge or permission?

4. Do you have any prank programs, computer viruses, worms, trojan horse programs, bombs, or other malicious software?

Malicious Software: Clarifying Questions:

Do you use bulletin boards or systems that contain these things, or have friends or acquaintances who do?

Do you write or create any software like this or deal with people who do?

Malicious Software: Explanation of the Problem

5. Do you have any computer graphics files, clips, movies, animations or drawings that you would be embarrassed about?

Do you have them legitimately (Piracy)

Are they things you would be comfortable showing me? Showing your grandmother?

Do you have any pictures, video clips, sound clips, articles, text, or other software or files which contain pornography, violence, dangerous instructions other distasteful material?

Do you access or view any of these kinds of things when using the net?

6. Do you have any newsletters, plans, guidelines, or "how-to" documents or files that you would not be comfortable showing to your mother?

Making Bombs, breaking into systems, stealing telephone access, stealing computer access, stealing passwords, pornographic or violent text, guides, descriptions, .....

Do you create, contribute to or receive anything like this?

7. Do you ever connect your computer to a telephone, use a modem, or otherwise use a network?

Clarifying Questions:

Do you use E-Mail (electronic mail)?

Do you use Bulletin Boards (BBS) (electronic bulletin board systems)?  
Is your computer ever connected to other computers?  
Do you use a Modem?

Explanation:

There is nothing either unethical or illegal about using networks or connecting computers to telephones. But, you should be aware that when computers are somehow part of a computer network, then they are not just used for "computing," but also for "communication" in a very broad sense of the word. Since "communication," by definition, always includes someone else, and since ethics, or lack of it, relates mainly to our interactions with others, the networking of computers, by any means, leads to many, many more potential ethical dilemmas for a computer user, than non-network computing.

The Questions above this one are all possible with both networked or non-networked computers. Whereas the questions below this mostly make sense for people who use networked computers. But, even for those issues related to the questions above, being connected to a network makes it easier to stray into trouble.

8. Who do you associate with when you use the Net?

BBS, Internet, CompuServe, Delphi, Fidonet, America On-line...

E-Mail, Discussion Groups, Gangs, Influence

Just as you would like to steer your children (and friends) away from bad influences in their daily lives, so should you attempt to discern the character of their cyber-friends

9. Do you ever use an assumed name, a handle, or an alias instead of your real name?

Do supply a false information about yourself when using a bulletin board, a news group, a message group, or forum, any part of the net, or when using e-mail or when otherwise communicating?

Do you use your real age & sex when communicating with your computer?

Do you use any false information like addresses, or phone numbers or use someone else's credit card number when using your computer?

Do you ever send messages or e-mail in such a way that the recipient cannot tell that you sent it?

Have you ever modified data, text, messages, or other computer information so that it looks like someone other than you created it or made the changes?

What are you trying to hide by not using your real name?

Are you trying to pretend you are something or someone you are not?

10. Do use telephone, video, cable-TV, computer network, bulletin board, or other network services without paying for them?

===== %<>=====

The National Computer Security Association (NCSA) and the Computer Ethics Institute are co-sponsors of the National Computer Ethics and Responsibilities Campaign (NCERC). Information about the NCERC can be

obtained in a dedicated display area, GO CETHICS, on the CompuServe Information Service.

In addition to the display area, NCSA has established a section within the NCSA InfoSecurity Forum (GO NCSAFORUM) for discussion of issues and concerns relating to ethics and privacy. Your involvement is encouraged!

The NCERC Guide to Computer Ethics has been developed to support the campaign. All files within the guide are available as individual files within Library 2 of the NCSA InfoSecurity Forum. In addition, the guide (including 16 informative articles) is available as a paper document. If you are interested in receiving more information about purchasing this document, and providing support for the campaign, send your request via EMail to:

74774.1326@compuserve.com

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn (Carlisle, PA)

---

### **Re: Ottawa Library fines people using unreliable ... calling system**

*Erik Jacobsen <ej@dec5102.aarhues.dk>*

*Tue, 8 Nov 94 13:29:49 WET*

Michael Slavitch ([RISKS-16.54](#))

>About two months ago I reserved a book at my local library. The library has  
>gone electronic in its reservation system. You reserve a book, and when  
>your turn to receive it comes due a computer dials your home phone number.  
>If an answer occurs, it assumes you heard the message; if you do not  
>pick up the book in three days, you are fined \$2.00.

There is also the possibility that a child picks up the phone, and before daddy or mommy gets to the phone, the information about the reserved book has been told to the child.

If the librarian does not accept a technical explanation (answer machine/faxmodem), this scenario should convince them that there is a problem.

Erik Jacobsen, ej@aarhues.dk

---

### **Risks of misjudging reliability of delivery systems (Slavitch, .16-54)**

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

*Wed, 9 Nov 1994 19:55:26 +0001 (EST)*

Michael Slavitch asks:

>So how do you handle two things:

> [One] An unreliable delivery system being assumed to be reliable.

> [Two] People placing trust in such a system.

I don't know. I have certainly been aware of small problems, ranging from nuisances to misunderstandings to hurt feelings, arising from the following assumptions many people make about the telephone system:

a) Each "ring signal" you hear is synchronized with the actual sounding of the bell (or electronic warbler) at the dialed instrument. Corollary: if you have heard four "rings," the party you are calling has heard four rings. Second corollary: if you have heard twenty rings, it cannot possibly be the case that the telephone you're calling did not ring at all; either nobody was there or they heard the bell and decided not to answer.

b) A cyclic buzz is a "busy signal" and means the instrument you dialed is off-hook, i.e. there's a strong presumption that somebody is there.

Telephone books once described these signals and their meanings. The ones I use today do not. I am sure this because the signals, which once were reliable and informative "error messages," no longer are.

When there is no connection, the telephone system does not reliably signal the reason for the failure. Overloaded system may deliver rings ("no answer") rather than busy signals for off-hook phones. They may deliver busy signals for phones that are actually on-hook (and, no, it is NOT always a distinguishable "fast busy.") I'm not aware of serious problems resulting from this, but one could construct scenarios in which the risks were significant.

Daniel P. B. Smith [dpbsmith@world.std.com](mailto:dpbsmith@world.std.com)

[Actually the synchronization is not precise. You may have noticed calling someone and having them answer without your hearing a ring. A slight delay is common on LONG-distance calls. 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 16: Issue 56**

**Monday 14 November 1994**

## Contents

- [Catalogin'](#)  
[Henry Cate](#)
- [Worker cleared of deleted planning files](#)  
[Vinc Duran](#)
- ["Netsafe makes the Internet safe for K-12 schools"](#)  
[Forman](#)
- [Alberta vote-by-phone fiasco](#)  
[Mich Kabay](#)
- [Rob Slade's review of Robert Slade's book](#)  
[Rob Slade](#)
- [Re: EMI and construction cranes](#)  
[Michael P. Hartley](#)  
[Arthur Byrnes](#)
- [Re: Ottawa Library fines people ...](#)  
[Peter Kaiser](#)  
[Sean Donelan](#)
- [Re: Postscript FAX Security Hole](#)  
[Andrew Klossner](#)  
[Brooks Benson](#)  
[Ross Oliver](#)  
[Kevin S. McCurley](#)  
[Ed Taft](#)  
[Barry Margolin](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Catalogin'

Henry Cate <[cate3@netcom.com](mailto:cate3@netcom.com)>  
{[Whenever]}

``It's not clear whether Morris Feline Stuart is a Democat, a Fat Cat or a Republicat -- or even a fan of Ross Purr-O -- but Morris is now a registered voter in Cuyahoga County." Normalee Stuart of Shaker Heights, Ohio, says that she registered her cat to prove there are few, if any, safeguards

against voter fraud in the county. She got the idea when a neighbor had told her of receiving a voter registration card addressed to a woman who had been dead for 12 years. Ohio law does not require people -- or cats -- to identify themselves when registering to vote. In fact, state law doesn't require identification from people when voting and allows mail-in registration. [Excerpted from a UPI item in the (Cleveland) \*Plain Dealer\*, as noted (without date) by Henry Cat(e). Soon cats and dogs will be able to vote by E-mail. On the Internet, no one knows whether it's reigning cats or dogs. Normalee, anyway. PGN]

---

## Worker cleared of deleted planning files

Vinc Duran <vincd@ile.com>

Thu, 10 Nov 1994 18:38:35 -0700 (MST)

Worker cleared of deleting planning files

By James Burrus, Camera Staff Writer

Boulder Daily Camera Thursday, November 10, 1994

A former Boulder County Planning Department employee was cleared Tuesday of charges that she deleted an unknown number of files from county computers. Charges against Vina Windes were dropped for "insufficient evidence" and because "information indicates no crime may have been committed," according to a motion filed Tuesday by the county's district attorney. Windes, 53, has worked as a secretary in the current planning division of the county Planning Department for five years.

Graham Billingsley, Boulder County land use director, said charges were dropped after his department and Windes worked out a deal Monday in which "she would tell us what she did so we can put together the missing information. So far she hasn't done that so we don't know" what happened.

But Windes said the files were never erased to begin with. "They just didn't know where anything was" in the computer system, Windes said. "All I did was leave. No one else did what I did, so they didn't know where to find anything on the computer when I was gone." Windes gave two weeks' notice of her resignation on Sept. 8 and started a new secretarial job Oct. 3. She was taken away from her new job in handcuffs Oct. 7 by Boulder County sheriff's officers and charged with computer crime, a felony, and abuse of public records.

"The whole thing got blown out of proportion because of a lack of communication," Billingsley said.

"Lack of communication?" Windes said. "There was no communication. All they had to do was call me and ask. Instead, they sent a sheriff's investigator to arrest me."

Vinc Duran vincd@ile.com or vduran@nyx10.cs.du.edu

---

## "Netsafe makes the Internet safe for K-12 schools"

<forman@cs.washington.edu>

Wed, 9 Nov 1994 18:30:35 -0800

Imagine how often your network could go down with this new service:

"Netsafe(tm) makes the Internet safe for K-12 schools.

Netsafe keeps information away from minds that are not ready for it."

Netsafe consists of a black box that monitors school traffic to the Internet and when an attempt to access a host with undesirable information is made (you select what categories to censor, they maintain the list of hosts), it shuts down all Internet access for 15 minutes and sends an email or beeper message to the local administration. Netsafe costs \$20,000 the first year, \$10,000 in successive years! They manage Netsafe over the Internet itself.

Excerpts from product announcement by Russell Nelson, nelson@crynwr.com

---

## Alberta vote-by-phone fiasco

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>

14 Nov 94 15:37:33 EST

The Canadian newspaper, *The Globe and Mail*, reports today (94.11.14) on a disastrous attempt to tally votes by phone:

Alberta phone voting crashes: Liberal fiasco casts doubt on future of high-tech balloting in Canada.

By Scott Feschuk, Alberta Bureau.

Calgary -- Alberta Liberal officials will be trying this morning to determine how the party's weekend leadership convention degenerated into what they concede was an outright debacle.

Edmonton MLA [Member of the Legislative Assembly] Grant Mitchell, 43, was selected to head the opposition party, but his second-ballot victory was all but overlooked as the telephone voting system crashed, and many members were unable to vote or their votes were not recorded.

The author continues with the following key points of interest to RISKS and NCSA FORUM readers:

- o Rural Albertans "found it all but impossible" to vote by phone during most of the first ballot.
- o The Maritime Telegraph and Telephone Co. claimed that "the system could handle more than 500 calls a minute" but the system crashed when a mere 11,000 people tried to vote in the 5.5 hours allotted.

- o The voting was stopped for 40 minutes in the middle of the process.
- o Distribution of the personal identification numbers (PIN) required to vote was incomplete, prompting complaints from disenfranchised voters.
- o Some users were informed by the computer system that their PIN had already been used to vote.
- o Some users reported that it took them over an hour to complete one vote.
- o Many users were informed that their vote had not been counted even though later analysis suggested it had.
- o The sequence of touch-tone buttons required to vote on the second ballot was different from the sequence used during the first ballot, resulting in confusion by an "unknown number of participants" whose votes were therefore lost.
- o Liberal Party officials are now "reluctant to pay Maritime tel's C\$100,000 fee [~U\$72,000]."
- o There were discrepancies in the numbers of people counted in the votes; at one point, the chief electoral officer reported "that more than 12,500 people had voted in the first ballot...." but he later reported just over 11,000 votes. However, "...[a]bout 19,000 people paid C\$10 to participate." Calgary MLA Frank Bruseker commented, "You really have to wonder what happened to those other 8,000 people.... Did they not vote, or did their votes get lost, or did they try to vote and just get too frustrated?"
- o The problematic balloting has discredited the Liberals' claim to be an efficient alternative to the current government.
- o Bad feeling has worsened between the rivals for the leadership as a result of claims of unfairness due to the technological breakdown.
- o Maritime Tel's system will next "be used again this weekend in Saskatchewan, where provincial Conservatives will select a new leader."

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn (HQ: Carlisle, PA)

---

<"Rob Slade, VARUG, SecSIG, BCVAXLUG, ComSIG and EdSIG">  
Fri, 11 Nov 1994 17:55:07 EST

Subject: Rob Slade's review of Robert Slade's (no relation :-) book

[Rob Slade is one of our most prolific reviewers.  
Here we give him a change to review Robert Slade's book. PGN]

BKCV.P.RVW

Please note that the following is a completely fair and unbiased review. I strive at all times to be even-handed in my reviewing. My vested interest in this work in no way can be said to influence my judgement. I mean, to say that just because I spent \*THREE SOLID YEARS\* writing it means I might have a biased opinion about it is a prejudiced opinion on your part, isn't it? :-)

%A Robert M. Slade  
%C 175 Fifth Avenue, New York, NY 10010  
%D 1994  
%G 0-387-94311-0 or 3-540-94311-0 in Europe  
%I Springer-Verlag  
%O U\$29.95 800-SPRINGER, fax 201-348-4505  
%O in Europe email ertel@springer.de, UK viv@svl.co.uk  
%O (and the title was \*NOT MY IDEA!\*)  
%P 480  
%T "Robert Slade's Guide to Computer Viruses"

This is the most FANTASTIC virus book EVER WRITTEN! This is the most FANTASTIC virus book that EVER WILL BE WRITTEN!! The day this book was released the ENTIRE VIRUS WRITING COMMUNITY committed suicide from depression over the fact that no one would EVER BE HURT BY A VIRUS AGAIN!

Book stores are advised to have LARGE STOCKS of the book on hand, prominently displayed, and probably to hire extra staff for the crush of buyers. Grown men have been known to pull their own liver out when told that they could not buy the book! (And that was before it was PUBLISHED!)

When we sent the books to reviewers, they typically danced in the streets for joy for several days. However, we reprint here some of the less effusive comments:

"Mr. Slade's lists are more interesting than the NYC phone book."  
- Dr. Fred Cohen

"Obviously some johnny-come-lately upstart."  
- Harold Joseph Highland

"Is this guy some kind of comedian?"  
- William Murray

"i think its cute and i like the title but i have a few questions ..."  
- sara gordon

"Wonderful! It certainly cured \*my\* insomnia!"  
- Dorothy Denning

"A mantlepice!"  
- Terry Jones

"I only have a hundred new samples that came in this week, and then I'll read it. Promise."

- Fridrik Skulason

"Should have had more sample code."

- Ralph Burger

""

- John McAfee (forwarded by Aryeh Goretsky)

"Vroooooom, vroooooom!"

- Padgett Peterson

"Too long."

- Ross Greenberg

"Still doesn't reliably detect MtE."

- Vesselin Bontchev

"[A bruised read]"

- PGN

"Should be powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards -- and even then I have my doubts."

- Eugene H. Spafford

"Where's my baseball bat?"

- Edwin Cleton

"Is this legal?"

- Paul Ferguson

"I don't think this is funny."

- Brad Templeton

"We're the federal government. We don't \*do\* that."

- James Earl Jones

"Let me diagram that on a Turing machine for you ..."

- Yaron Goland

"A great virus book. No, I meant a great \*anti\*virus book. No, I meant a great \*virus\* book. No ..."

- John Buchanan

"Cool."

- Ray Kaplan

"My title was better than his."

- Cliff Stoll

"I elisted this book, and I have the password. Therefore I am now the author."

- Gene Paris

"We probably shouldn't be publicising stuff like this."

- J. B. Condat

Cecil B. DeMille, Alfred Hitchcock, John Ford, John Houston and Federico Fellini are working on a co-production of the movie version. Casting is not yet complete, but rumours indicate that Tom Hanks will play frisk, Arnold Schwarzenegger will portray Padgett Peterson, and Mark Ludwig will be Stoned. The part of Vesselin Bontchev will be played by a Cray YMP.

DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733

---

<"Michael P. Hartley, \"Dreading the Info SuperTrafficJam\">  
Thu, 10 Nov 1994 14:01:07 -0500 (CDT)

Subject: Re: EMI and construction cranes (Summit, [RISKS-16.55](#))

While not directly related to computer RISKS, I feel a comment on how the FCC allocates frequencies is apropos here. Back in '91, the parts of the 72Mhz range that formerly were allocated in 40kHz wide ranges for R/C planes were re-allocated. Now, the R/C frequencies are 10Khz wide, 20Khz apart with various other devices allocated the frequencies between. These include pagers and some crane operations, among others. The old, pre-1991 transmitters are still legal to use until sometime around 1998.

An older or poorly tuned R/C transmitter can cause short-ranged problems, like spurious pager signals or disruption of crane operations. R/C Tx are very low powered. Their effective range may be as far as 3 miles.

The real RISKS are obvious to the public. In the R/C community, cranes are notorious for using very 'messy' and over-powered transmitters. A crane, pager tower, or other source of EMI could cause R/C fliers to lose control. A 10Kg object, hurtling through the air at over 200 KPH and spinning a razor- sharp 15" prop at 18000 RPM can cause a lot of damage or loss of life.

Michael P. Hartley loadstone@ins.infonet.net

---

### **Microwave oven RFI? (Summit, [RISKS-16.55](#))**

ATS)

Mon, 14 Nov 94 12:37:48 EST

"Broadcast towers ... and consumer microwave ovens ... are suspected, (of causing interference to the radio controls of a crane.)"

Not knowing the Seattle area, but assuming that the "Nearby hill" is probably several thousand feet away, and maybe several miles away, the quoted person's (Donovan) comment shows a very poor understanding of the technology he is working with.

It is outrageous that the blame can be placed on a microwave oven. Maybe, if the oven were inside the crane, there would be enough leakage to cause

interference, but it is not likely even then. Even a broken oven that would work with the door open, and pointed toward the crane, wouldn't interfere with the crane if it was more than several hundred feet away. We know of course that the "Broadcast Towers" themselves wouldn't affect the crane, but the transmitters using those towers could. The interesting thing is that in most cases of isolated RFI (interference affecting only a particular person or machine), the "Cause" is not the source of the interfering signal, but the receiver being affected. Poorly designed receivers are a major cause of headaches to legally operating radio transmitters.

Arthur J. Byrnes (Licensed Radio user Amateur, and Commercial.)

---

### **Re: Ottawa Library fines people ...**

*Peter Kaiser <kaiser@heron.enet.dec.com>*

*Thu, 10 Nov 94 08:20:27 MET*

Daniel Smith writes:

> a) Each "ring signal" you hear is synchronized with the actual sounding of  
> the bell...

No, it isn't. Our phone has a switch that turns the bell on and off. As we eventually discovered, a hard bump can switch off the bell; and in a household with children and animals, the phone is inevitably bumped hard enough.

Furthermore, it's unplugged at times.

It's obviously risky to assume that because one hears a ring signal, a phone is actually ringing.

\_\_\_Pete kaiser@acm.org +33 92.95.62.97

---

### **Re: Ottawa Library fines people ...**

*Sean Donelan <SEAN@SDG.DRA.COM>*

*Thu, 10 Nov 1994 2:56:08 -0600 (CST)*

The goals of automated telephone notification are to reduce the postage costs and to notify people more quickly. For example, alerting you to overdue books faster so the fines don't get as large.

DRA sells a few of different phone notification systems to libraries. Ottawa Public Library is one of our customers, but I don't know their exact setup. However, here is the basic (the specifics may vary depending on hardware platform) notification method.

- 1) Dial phone
- 2) Monitor call progress signals (if we're lucky the library has a telephone line that returns answer supervision)

- 3) When telephone line "answered"
  - speak notification message twice,
  - otherwise
  - after a number of failed attempts
  - send a mailed notice
  - otherwise
  - rescheduled call and exit
- 4) Wait up to 10 seconds for DTMF (touch-tone) key
  - if DTMF digit "0" pressed
  - go back to step 3
  - if other DTMF key pressed
  - record it in notice response (e.g. "Press 1 to confirm")
  - otherwise
  - record no response (rotary dial, answering machine?)

Its not a foolproof system. DTMF talk-off, wrong phone numbers, children answering the phone can cause the notice to be marked "SENT" (note: I don't use the word "received.") But it usually gets the job done under a variety of adverse conditions on low-bid hardware. (Hint, hint, pass that next tax increase for the library, and maybe they'll be able to afford a more sophisticated system.)

>Well, I am. I know that it is only two bucks, but the implications that  
>arise from misuse or overly trusting such a system are worrisome. What if  
>the government started issuing parking tickets or summonses in this manner,  
>or banks warning you of surcharges on financial transactions? What if my  
>wife answered the phone and the book was "how to handle infidelity in you  
>marriage" :) (it wasn't).

Some libraries use postcards to notify people when a copy of "How to handle infidelity in your marriage" is available. Parking tickets are presumed valid even if someone rips it off your windshield before you see it. There are all sorts of risks in all sorts of notification systems. Nevertheless we accept many risks as normal.

Libraries rarely send notices via certified return receipt requested mail. The problem of "lost" notifications is something libraries have dealt with for a long time. The dog ate it. The post office lost it. The kids hid the overdue notice before the parent gets home. Different libraries have different policies for handling reports of not receiving a notice. Generally proof of receipt is not a requirement.

What should be considered a reasonable attempt at notification?

Sean Donelan, Data Research Associates, Inc, St. Louis, MO  
Domain: sean@dra.com, Voice: (Work) +1 314-432-1100

---

**Re: Postscript FAX Security Hole (Crawford, [RISKS-16.55](#))**

*Andrew Klossner <[andrew@frip.wv.tek.com](mailto:andrew@frip.wv.tek.com)>*

*Mon, 14 Nov 94 07:08:27 PST*

A quick description of security for PostScript FAX (as implemented in various laser printers) follows:

If the ReceivePostScript FAX parameter is false, the printer will reject any attempt to inject PostScript through the modem. In this case, it will accept only the FAX format.

If the PostScriptPassword FAX parameter is not the empty string, then the transmitting printer must supply a password. Receiver challenge and encryption are used.

The default values of these parameters are true and the empty string, respectively, so a factory-new printer will accept PostScript without requiring a password. In this case, any attempt to change system or device parameters (such as passwords) from within an incoming FAX job will fail unless the (separate) system password is supplied. Also, attempts to generate outbound FAXes will fail. If no system password has been set (as in a factory new printer), then such attempts fail.

I can't find anything in the documentation which gives disk files better protection from a FAX job than from a local job.

The reference for all this is "PostScript Language Reference Manual Supplement for Version 2014" by Adobe Systems Incorporated. This is available, as a PostScript file (naturally), from ftp.adobe.com as "pub/adobe/DeveloperSupport/TechNotes/PS.Supp.2014.ps". "2014" here refers to the major revision number of the PostScript interpreter, as reported by the printer on the page that it prints at power-up. Similar files are available for versions 2011, 2012, and 2013.

-- Andrew Klossner (andrew@frip.wv.tek.com)

---

## Re: Postscript FAX Security Hole

*Brooks Benson <brooks\_benson@il.us.swissbank.com>  
Thu, 10 Nov 94 08:58:48 -0600*

A similar situation may exist with NEXTSTEP's Mail application. NEXTSTEP uses Display PostScript as it's imaging model. When one selects for display a piece of email that contains an encapsulated PostScript file attachment, the PostScript is sent to the window server and executed.

This feature has led several clever hackers to create NeXTmail PostScript "viri". I have seen several of these, all pranks, none malicious. One causes a number of spiders to scurry across the desktop, which must be squashed with a mouse click before allowing you to regain control of your desktop. Another causes all the window objects to drop off the bottom of the desktop one at a time, yet another shakes the entire desktop, giving the impression of an earthquake.

Although I have personally not seen any destructive email viri, I can't say

that none exist. I'll ask roughly the same question as the original poster. Was the possibility of malicious use of the PostScript language considered when determining standards for intelligent PostScript devices??

Brooks Benson Swiss Bank Corporation International Finance Division  
brooks\_benson@il.us.swissbank.com

---

## Re: Postscript FAX Security Hole

Ross Oliver <ross@ncd.com>

Thu, 10 Nov 1994 14:30:51 -0800

In [RISKS-16.55](#), Mike Crawford write about the risks of remote configuration of intelligent devices such as his Postscript printer.

One possible solution to this risk is to require a switch to be thrown, button pushed, jumper changed, or some other physical manipulation of the actual device before any critical configuration information can be changed. A physical "lock-out" would provide security when needed, yet still allow the benefits of remote configuration if desired.

The company I work for manufactures X terminals, and we have incorporated this type of feature into our terminals. When a special type of keyboard, called a "secure keyboard" is attached to the terminal, the critical portion of the terminal's configuration data (stored in non-volatile memory) can be locked against further changes. The secure keyboard is then removed and replaced with a standard keyboard.

Ross Oliver ross@ncd.com

---

## Re: Postscript FAX Security Hole

Kevin S. McCurley <mccurley@cs.sandia.gov>

Thu, 10 Nov 94 21:14:57 MST

In [RISKS-16.55](#), Mike Crawford pointed out that accepting postscript to a fax machine is really accepting a program to be executed. Postscript is a programming language with operators for renamefile, deletefile, createfile, and some others that are risky in some situations. Moreover, operators can be created from other operators, so it is not even sufficient to scan the postscript stream for the offending sequences before executing them because they can be built from other strings at runtime.

Many web viewers such as netscape and mosaic can be configured to invoke external viewers such as ghostscript that are in reality postscript language interpreters. It is therefore possible for someone to click on a URL inside a web viewer, and in so doing have changes made to their local file system that are not apparent to the user, because it caused a postscript file to be brought back and executed. The default mode (safer) for the recent version of ghostscript does not execute these operators, but the risk still exists for other configurations. Postscript is probably also not the worst

offender for this - what if your local web viewer on a UNIX machine processes Bourne shell scripts locally by feeding them to /bin/sh, or your DOS viewer executes .bat files by feeding them to command.com? Click here to reformat your disk ...

It is clearly possible to write internet software that is dangerous to operate, but the risk can easily be eliminated through proper configuration and coding. Many of us drive automobiles to work every day, recognizing that they possess the capability to inflict serious injury and death if used improperly or if they experience a catastrophic failure. Will the government someday legislate seatbelts for web viewers and fax machines because of the risks to uninformed or careless users?

Kevin McCurley Sandia National Laboratories

---

## Re: Postscript FAX Security Hole

*Ed Taft <taft@mv.us.adobe.com>*

*Fri, 11 Nov 94 10:25:10 PST*

> Would anyone know whether this has been considered under the postscript FAX  
> standard? It seems to me it would be a problem for just regular PS faxes -  
> one would just hack it over the phone line from another PS fax machine.

Indeed, this issue was considered at length in the design of PostScript fax. There are several passwords that control access to both PostScript fax specifically and to system administrator functions generally (such as erasing the disk).

The defaults are set up to be relatively permissive. This decision is based on the reality that many PostScript fax printers will be installed and operated by unsophisticated users having no system administrator support and who expect the product to work right out of the box. However, the defaults are such that system administrator functions can't be executed by a fax job.

This, of course, solves only part of the problem. There is no protection against a fax job that executes something like:

```
1000000 {showpage} repeat
```

More comprehensive facilities for authentication, access control, resource accounting, etc., await implementation in future versions of PostScript fax products.

Ed Taft taft@adobe.com

---

## Re: Postscript FAX Security Hole

*<barmar@near.net>*

*Fri, 11 Nov 94 17:34:38 EST*

Don't you run the same risk when you print any PS file that you download from the net or receive as email and then send to your printer? Do you examine every PS file for security holes before you print it? PS FAX just gets rid of the middleman.

As for changing the printer password, wouldn't they have to know the old password in order to get into the mode that allows it to be changed? [...]

What's needed is probably a general concept of trust levels associated with PS document sources. Dangerous commands would only be permitted for documents that came from a trusted source. When printing PS files, the user could indicate the trust level (high trust if they generated the file themselves from an application, low trust if they got it from the net). For automated processing like PS FAX, it could simply default to low trust, or perhaps permit passwords to be included (either in the PS code, or perhaps in the FAX wrapper).

In effect, a PS FAX machine needs to be like a computer with a dialin modem: you need to be able to define accounts and give them access privileges.

Barry Margolin BBN Internet Services Corp. [barmar@near.net](mailto:barmar@near.net)



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 16: Issue 57**

**Tuesday 22 November 1994**

## Contents

- [Cell-phone ergonomics side-effect](#)  
[Robert Stanley](#)
- [Pentium FDIV bug](#)  
[Bill Broadley](#)
- [All's Well that Orwells?](#)  
[Peter Wayner](#)
- [Spell Checker Goes Beserk; Editorial Maimed](#)  
[Robert Bane](#)
- [Security is not privacy](#)  
[Phil Agre](#)
- [Authorities Still Investigating Software Theft](#)  
[Edupage 15 Nov 1994](#)
- [Beware the Calendars](#)  
[Pertti Malo](#)
- [Re: Parental Responsibility](#)  
[Daniel P. Johnson](#)
- [Clarifying answers to TEN QUESTIONS PARENTS SHOULD ASK THEIR CHILDREN](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Cell-phone ergonomics side-effect

*Robert Stanley <[rstanley@sybase.com](mailto:rstanley@sybase.com)>*

*Wed, 16 Nov 94 16:52:30 EST*

Yesterday evening I returned home from work and, as usual, checked the answering machine on my normal voice telephone. Much to my surprise, I heard a somewhat muffled background conversation that I soon identified as that afternoon's conference in the office. This filled the tape to the end, and had caused several later calls to be rejected.

[aside #1: I hate these damn micro-cassette systems that only allow ten or fifteen minutes of message time, but they have become ubiquitous!]

Two aspects of this message puzzled me: how had it found its way to my answering machine, and why was it so muffled? The office has just completed installing a high-tech AT&T digital phone system with all sorts of fancy features, but I know that the trunk-to-trunk transfer features have all been disabled for security reasons. It is therefore not possible for our conference call link to another office to have been forwarded to my home phone. The only possible way for my phone to have been included in the conference would have been for it to have initiated the call (and then worked its way through a set of control codes.)

[aside #2: my former answering machine, which used real C-90 cassettes, did have the unfortunate habit of occasionally calling back the last number to have dialed it! Another story, and one which can wait for a rainier day to tell.]

[aside #3: the idea of disabling trunk-to-trunk switching to prevent improper (read: malicious cracker) usage really demonstrates the lack of thought that goes into much of what today passes for the design process. Hey, just compile it and debug it, that way you'll be \*doing\* something...]

Investigation at the office yielded disbelief followed by stunned surprise. No one had forwarded the phone, and my home phone number was not programmed onto any button in the system. However, we all rush to the documentation to check into just how the remote monitor feature works, and try to recall whether any visible telltales had been lit to indicate monitoring.

Finally, light dawns. A colleague's tiny Nokia cell-phone in his shirt breast pocket. He had called me at home earlier, and the phone has a last number redial button. The phone, non-folding, slipped into his shirt pocket with the controls outermost, had somehow had that button tripped, and had happily held the line open to my answering machine. The muffled broadcast was entirely attributable to the small microphone and the cotton pocket between it and our conference table.

However, it is an extraordinarily sobering experience to hear a sensitive work discussion issuing hours later from the speaker of your home voice messaging system.

A number of risks here, but the predominant one seems to be the conflict between added function and reduced footprint of portable cell-phones leading to the creation of unergonomic control systems. This is exacerbated by the novel situations to which the diminished footprint can give rise. This is surely the first generation of cell-phones that are sufficiently small (a) to be droppable into a toilet, and (b) actually flushed out of reach...

Robert Stanley - robert.stanley@sybase.com

---

## **Pentium FDIV bug**

*Bill Broadley <broadley@turing.ucdavis.edu>  
Mon, 21 Nov 1994 15:20:58 -0800 (PST)*

As this below tiny program from Thomas Koenig demonstrates the pentium sometimes only returns single precision when dividing floating point doubles.

```
#include <stdio.h>
int main()
{ double x,y,z;
  x = 4195835.0; y = 3145727.0;
  z = x - (x / y) * y;
  printf("%f\n",z);
  return 0;
}
```

It will return 256 if you have the fdiv bug, and zero if you don't.

I've written 3 similar programs:

- 1 like the above, but more resistant to compiler optimization
- 1 that searches randomly for the bug (no special seeds)
- 1 that searches linearly for the bug.

I'll leave it to the reader to interpret the risks of a cpu that silently returns 1/2 the precision that you expect.

BTW in my test it happens about about 1 in 10<sup>9</sup> divisions or about once every 21 minutes with a sequential search. I.e. if your running flat out divisions and multiplies (to check the divs).

It can be MUCH higher, up to once a second, with biased random numbers.

I'll make havebug.c rndsearchbug.c and linsearchbug.c available for anonymous ftp at math.ucdavis.edu

For further references read comp.sys.intel under the fdiv bug thread.

Bill Broadley, UCD Math Sys-Admin [Broadley@math.ucdavis.edu](mailto:Broadley@math.ucdavis.edu)  
<http://ucdmath.ucdavis.edu/~broadley>

## All's Well that Orwells?

*Peter Wayner <pcw@access.digex.net>  
 Tue, 15 Nov 1994 09:12:21 -0500*

I got a recent net leaflet that proclaimed that the US Geological Survey would cease printing their National Water Conditions Report in January 1995 to save money. The information would only be available on-line. This will supposedly save them plenty of liquid capital.

Normally, I would be happy when they go with the flow of technology. But the lack of a printed record seems like an invitation for adding Orwellian changes to the report in the future. What if you want to go into the past and use the report as a basis for some legal procedure? For instance, you might want to sue someone about cyanide levels in the water down stream from the gold mine. Suddenly two different versions of the report end up before

the judge. One gives the stream a clear bill of health while the other cites the danger. Which one will the judge and jury believe? How do we know that the archive in Washington is secure? No need to shred documents or stuff them in your underwear when a strong magnet will do the job.

Anyone who wants to jump into the deep end of paperless publishing should use both digital signatures and digital time stamps to ensure accountability.

---

## Spell Checker Goes Beserk; Editorial Maimed

*Robert Bane <bane@gst.gsfc.nasa.gov>  
Wed, 16 Nov 1994 14:32:07 -0500*

The following sentence was taken from Richard Cohen's column on page A19 of the November 15, 1994 Washington Post:

"GOP national chairman Haley Barbour instantly announced that New York City was no longer in the running for the Republican National Convention, and, more ominous, Sen. Alfonse D'Amato, the state's leading Republican and Pataki's Disk Operating System (DOS), said he would not seek revenge on Giuliani."

The only explanation I can come up with (other than Sen. D'Amato really being a copy of DOS) is that Cohen typed 'doss' instead of 'boss', and the spelling checker not only corrected it to DOS, but spelled the acronym out since it's the first appearance of it in a non-computer-related news story.

Bob Bane, Global Science & Technology, Inc., 6411 Ivy Lane, Suite 610,  
Greenbelt MD 20770 bane@gst.gsfc.nasa.gov, 301-474-9696

[I think David Letterman's phonetic spellchecker came up with  
Pootaki Sauce ... on Ghouliani. PGN]

---

## security is not privacy

*Phil Agre <pagre@weber.ucsd.edu>  
Tue, 15 Nov 1994 12:04:08 -0800*

\*The New York Times\* has an article about an attempt by tobacco company lawyers to subpoena reporters' travel and telephone records in an indirect attempt to identify their sources for stories asserting that the companies deliberately added nicotine to their cigarettes.

William Glaberson, A libel suit raises questions about the ability of journalists to protect sources in the electronic age, \*The New York Times\*, 14 November 1994, page C10.

Many readers of RISKS probably remember other attempted strategic uses of the discovery process by tobacco companies, including at least one attempt to subpoena raw survey data from smoking researchers and an attempt to obtain an electronic mailing list of anti-smoking activists. (Actually, the

article doesn't explicitly say that the companies want the subpoenas issued as part of the discovery phase of the trial, just that they want them and the major press organizations are trying to stop them.)

In any event, this case is an excellent example of why data security, while obviously important, does not guarantee privacy. I am sure that those travel and telephone records are as secure as they need to be, but that may not provide enough protection against the legal strategies of tobacco companies. Maybe this point is obvious to Risks readers, but it is certainly not obvious to many others, including many of the politicians who make laws about such things. So remember to let these folks know:

Security is not privacy.

The only guarantee of privacy is anonymity. Fortunately, technologies such as digital cash to implement anonymity are on their way. Insist that they be used in any new system that gets developed near you. And spread the word, because once privacy-invasive systems get standardized and installed they're hard to regulate and even harder to change.

Phil Agre, UCSD

---

## **AUTHORITIES STILL INVESTIGATING SOFTWARE THEFT (Edupage 15 Nov 1994)**

*Edupage <info@ivory.educom.edu>*

*Tue, 15 Nov 1994 19:46:58 -0500*

A surge of outside computers connecting to the National High Magnetic Field Laboratory's public information computer was the first sign something was amiss, with many of the suspect connections coming from a computer in the Center for Educational Technology, two miles away at Florida State University. "Hackers were using it so much it wasn't responsive to legitimate users," says the director of the magnet lab's computer center. The computers have now been cleaned of pirated software and electronic burglary tools, but even as the crackers were scurrying to cover their tracks, all related data was copied onto a back-up tape and turned over to the Computer Emergency Response Team for further investigation. "I think it's time to slap these little buggers upside the head," says the CEO of DeScribe, one of the companies whose software was posted. (Miami Herald 11/14/94 1A)

Edupage, a summary of news items on information technology, is provided three times each week as a service by Educom -- a Washington, D.C.-based consortium of leading colleges and universities seeking to transform education through the use of information technology. To subscribe to Edupage: send a message to: listproc@educom.edu and in the BODY of the message type: subscribe edupage Mick Jagger (assuming that your name is Mick Jagger; if it isn't, substitute your own name) ... To cancel subscription to Edupage: send a message to: listproc@educom.edu and in the BODY of the message type: unsubscribe edupage. [Edupage is also available in Portuguese and Spanish; to subscribe, send mail to edunews@nc-rj.rnp.br.]

---

## Beware the Calendars (Ravin, [RISKS-16.53](#))

*Pertti Malo <pertti@tmxbris.mhs.oz.au>*

*Sun, 13 Nov 94 00:51:29 AES*

In Australia, my wife brought home a calendar from the uni. There was an error in it. Magnetic calendars you get from schools, politicians, plumbers and others sometimes have errors as well.

In Finland, as a way to reduce RISKS caused by incorrect calendars the publishing of Finnish-language calendars has long been a monopoly that the government gives to one printer for a number of years. As a result some other printers, institutions, shops, and tradespeople now publish their unofficial calendars in other languages, mostly in English.

Pertti Malo <pertti@tmxbris.mhs.oz.au>

---

## Re: Parental Responsibility

*Dr. Daniel P. Johnson <drdan@src.honeywell.com>*

*Thu, 10 Nov 94 09:34:44 CST*

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com> wrote:

>What about

- > "That parents should spend time with their children discussing
- > their (both parents'; and children's) interests and activities
- > and exchanging views in a mutually respectful atmosphere?"

It is important to include the children's age in these discussions. For teenagers the view above is indeed a proper statement of parental responsibility. But that is not true for younger children, nor is it even true for many younger teenagers who are not maturing at the same schedule as some of their peers. They may know the values but not be able to judge the situation. I shudder to think of my third-grader son trying to deal with the e-mail response he would get if he posted to alt.barney.dinosaur.die.die.die for example. It's hard enough for him to cope with the taunts of a smug middle-schooler.

When a parent takes a child to see 'Jurassic Park' because the child wants to and the child has nightmares for the next several weeks, that was the parent's mistake, not the child's. The parental responsibility to say 'no' for the child does not go away after a discussion about scary movies. The child cannot yet judge what 'too scary' means. My most shameful moments as a parent have come when I have made the wrong choice. My most wonderful moments have come when I have made the right choice.

My son could thrive in a 'safe' on-line environment, asking children of France what their weather is, or looking up the Space Shuttle schedule, or monitoring the bombardment of Jupiter. But he can't act as his own censor or ignore ill-judged email responses, he doesn't have the judgment and the on-line services are not a controlled situation.

The proper analogy is the shopping mall versus the school. My son isn't old enough to go to the mall without a parent. He can go to an elementary school without a parent. He's not even close to being able to cope with the environment of life in a high-school.

Similarly, he isn't old enough to go on the infobahn by himself. Perhaps someone will develop a 'schoolnet' that he can navigate by himself. Until then, I will have to be at his shoulder.

Daniel P. Johnson, Honeywell Technology Center, 3660 Technology Drive,  
Minneapolis, MN 55418 drdan@src.honeywell.com 612-951-7427

---

## Clarifying answers to TEN QUESTIONS PARENTS SHOULD ASK THEIR CHILDREN

<[A well-known but suitably anonymized contributor]>

Tue, 15 Nov 1994 12:12:15 (xST)

Where are the manuals, boxes, license agreements for the programs you have or use?

They don't have manuals or boxes. Should I not use them?

Where did you get that game? (program?, floppy?, software?)

Usually over the net - how do I tell if it's legitimate?

When programs first start running on your computer, whose name comes on the screen as the "owner" or "licensed-to."

Very few have this feature.

Did you write/create/author what you're passing off as your own work?

I resent the use of 'passing off'. Almost all modern works are collaborative in nature - the selection of citations is not a trivial issue. Where did you get these questions? Are you passing off some of it as your work when in fact others first came up with some of these ideas? Where are your citations?

Where did you get the text and images you're using?

Many of them come from on-line sources. Does that make them legitimate or illegitimate?

If you copied text and images from another source, did you have permission?

Rarely - in most cases, fair use allows you to use them without getting formal permission. Kind of like these questions of yours.

If you didn't need permission from the "owners" of the information you're using, did you credit them for the material?

Only if I republish it. I have lots of on-line information without citations attached to it. But I see the author of this questionnaire thinks it's legitimate to do this without citation. I guess I should stop giving as much credit where due as I do.

3. Do you ever use other people's computer, disk-space or processing

capability, or look at or copy their files or information, without their knowledge or permission?

I almost never get permission to look at each file I view.

I go under the assumption that I may view anything that allows read access by me without going outside of the normal methods in use to read files. If it is interesting, I copy it for future reference. I hope they do not know any details about my use. After all, I want to retain my privacy and they should not be watching what I do.

4. Do you have any prank programs, computer viruses, worms, trojan horse programs, bombs, or other malicious software?

Several thousand of them. What's wrong with that? Don't you have some too?

Do you use bulletin boards or systems that contain these things, or have friends or acquaintances who do?

Certainly. The Internet has lots of these things, and I use it. The telephone system is used for abusive phone calls and I use it too. I don't really know what my friends do when they use computers. They have privacy rights too, and we rarely talk about what information service we use.

Do you write or create any software like this or deal with people who do?

All the time. I deal with Microsoft, Lotus, and many other companies that have widely distributed this sort of thing. I also know and deal with individuals who have done this, and I do it all the time. Is there something wrong with that?

Are they things you would be comfortable showing me? Showing your grandmother?

I would not show either you or my grandmother my files, but it has nothing to do with embarrassment. It is called privacy.

Do you have any pictures, video clips, sound clips, articles, text, or other software or files which contain pornography, violence, dangerous instructions other distasteful material?

Lots of them. Is this wrong for some reason?

Do you access or view any of these kinds of things when using the net?

All the time. In fact, if you know of any, I would be happy if you would forward information on them to me.

6. Do you have any newsletters, plans, guidelines, or "how-to" documents or files that you would not be comfortable showing to your mother?

Same answer as above. I value my privacy.

Making Bombs, breaking into systems, stealing telephone access, stealing computer access, stealing passwords, pornographic or violent text, guides, descriptions, ..... Do you create, contribute to or receive anything like this?

All the time. In fact, the Risks Forum is one of my best sources for this information. Should you stop making it

available to me?

7. Do you ever connect your computer to a telephone, use a modem, or otherwise use a network?

All the time.

8. Who do you associate with when you use the Net?

Lots of different people. How do I know who they really are anyway? If you claimed to be John Smith at the West Hannover Institute, how could I tell this was true, and why would I bother?

... so should you attempt to discern the character of their cyber-friends

How? We have congress-people that seem to lie all the time, and yet the majority of voters vote for them and they have a lot of power, are on TV all the time, and are supposed to be highly respected. Does this mean that lying is good or bad? Judge not - lest you shall be judged! Who shall cast the first stone? Do you attempt to discern the character of everyone on the net you communicate with? How about the thousands who read your postings to Risks? The nature of the net is that it provides anonymity and open forums for discussion. Why would I want to stifle free speech by asking character questions. The statements people make should stand on their own regardless of who states them. That is the best feature of the nets. A high school kid can shine and a Ph.D. can look like an idiot - based on what they say, not who they are.

9. Do you ever use an assumed name, a handle, or an alias instead of your real name?

Sure. I have asked this posting to be made anonymously in order to allow it to be judged based on its content rather than it's source. It's kind of like the referee process is supposed to be on professional papers. Maybe we would all be better off if all postings were anonymous (with a return address that permits response without identity).

Do supply a false information about yourself when using a bulletin board, a news group, a message group, or forum, any part of the net, or when using e-mail or when otherwise communicating?

At times. Especially when bbs systems ask extensive questions about who I am, my SSN, credit information, or other information that I don't think they have a right to have. I have also lied when connecting to hacker BBS systems because I don't think they have a right to know who I am when they all use handles instead of names anyway. I have also used telnet (25) into SMTP sites to forge e-mail as if I were Captain Kirk from the enterprise in order to have fun when communicating with friends. Is there something wrong with having fun in this way, or is the Internet only for serious work and not for having fun or playing around. If so, why are there thousands of fun and games forums in the Internet?

Do you use your real age & sex when communicating with your computer?

I rarely use either. Nobody has ever asked my sex (my name is probably a giveaway on that one) or my age. Besides, I think that discrimination based on age and sex are wrong, are against the law, and that forging a sex or age in order to have equal access is fair, reasonable, and appropriate in the network environment.

Do you use any false information like addresses, or phone numbers or use someone else's credit card number when using your computer?

Yes, yes, and no respectively. Theft (by deception) is very different than not telling someone where you live or what your phone number is. These are privacy issues, and privacy is a very important thing to have. Privacy through deception is not wrong. Even becoming someone's friend by lying to them about having something in common is not particularly wrong. Certainly giving a salesperson a polite wrong number and address is a reasonable privacy precaution against getting on mailing lists. It is probably even good to lie if you think someone is stalking you over the net. I think we have a right to lie, perhaps even a social responsibility to do so under certain circumstances.

Do you ever send messages or e-mail in such a way that the recipient cannot tell that you sent it?

In what sense? I have certainly sent e-mail that never got through - the intended recipient didn't know I sent it. I have sent e-mail from group accounts where the individual was not identified, but the group was. This is quite common in customer support. I have also forged e-mail addresses so that I could remain anonymous. Is that supposed to be wrong? Why? If I sent you a seasons greeting card from a false identity would you be upset and try to find me and have me arrested? There is a difference between malice and fun.

Have you ever modified data, text, messages, or other computer information so that it looks like someone other than you created it or made the changes?

Certainly. I had to make a change to the TeX sources once to get them to compile right, and I used the TeX user ID to do so in order to allow the compilation to work right. This is often called for in systems administration.

What are you trying to hide by not using your real name?

My identity. It's called privacy and anonymity. It's one of the basic principles of a free society - that's why we have anonymous voting - to protect anonymity and be certain that I can think and do what I feel are right without someone like you being able to seek retribution. I believe that a free society requires privacy and anonymity. Otherwise, someone like you who perhaps thinks that these ideas are too radical might try to black ball me. Anonymity in pre-war Germany could have saved millions of lives. Many in the US are trying to eliminate anonymity by such practices as federal ID cards, and I think that

is very dangerous.

Are you trying to pretend you are something or someone you are not?

I have a right to be whatever I want to be. If I claim to be an expert in business consulting, you use my services, and I do a good job, what does it matter that I don't even have a high school diploma. If you hire an MBA and they do a bad job, does that make it OK? There is nothing wrong with pretending, as long as you don't lie in order to take advantage of someone else. Theft by deception requires theft. If I knock on your door and claim to be a Jehova's witness when I am not, why should that offend you more than if I were a real one?

10. Do use telephone, video, cable-TV, computer network, bulletin board, or other network services without paying for them?

All the time. When I am at a friend's house and I make a phone call, I don't pay for it. I don't pay for Internet access, it is given to me. I use Freenets and other bulletin boards without paying for them too. I have even used friend's accounts to access the network on occasions when I didn't have any local access. I also used free compu-serv, America-Online, and Delphi services when they had free offers. The vast majority of people using the Internet until only a few years ago did not pay for their usage either. Their company, the federal government, or someone else paid for their usage.

The bottom line: Are these things also true for my children? Yes, I think they are. I hope that they learn how to do the same things I have learned how to do in order to protect themselves from the tyranny of the majority - or is it the vocal minority? I hope they keep things private from me when appropriate, and if they look at some dirty pictures once in a while, it won't greatly offend me.

Please consider that most issues of right and wrong are matters of degree and circumstance. Given more choice and less control, I think more people will make better decisions. Illegalize dirty pictures, and you will have a much larger audience. That's why so many motion pictures add nudity or violence if they don't get an R rating with the first cut. After all, an R picture on average sells a lot more tickets than a PG picture.



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 16: Issue 58**

**Friday 26 November 1994**

## Contents

- [Hacker learns intelligence secrets](#)  
[Mathew Lodge](#)
- [Automated Weather Reports for Pilots](#)  
[Tom Keenan](#)
- [Extended Phone Failure in Iowa City](#)  
[Douglas W. Jones](#)
- [Enormous water bills - gigo strikes again](#)  
[James M. Politte](#)
- [Computer-generated bridge-tournament hands](#)  
[G. Gates/M. Brader/PGN](#)
- [The PC as a RISC \(how could I resist 8\\*\)](#)  
[A. Padgett Peterson](#)
- [Problem with 911 service in Philadelphia](#)  
[Paul Robinson](#)
- [Department store security cameras linked to computer](#)  
[David Hembrow](#)
- [Children on the Infobahn](#)  
[Bradley K. Sherman](#)
- [Re: Pentium FDIV bug](#)  
[Mike Carlton](#)
- [Re: Cell-phone ergonomics side-effect](#)  
[Bill Innanen](#)  
[Paul Robinson](#)
- [Re: Anon. on "TEN Q's"](#)  
[Mark Seecof PSD x77605](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Hacker learns intelligence secrets

*Mathew Lodge* <[lodge@ferndown.ate.slb.com](mailto:lodge@ferndown.ate.slb.com)>

*Thu, 24 Nov 94 09:09:38 GMT*

The London "Independent" newspaper of 24-Nov-94 leads with a story that a "hacker" gained access to a sensitive database of telecommunications

information at British Telecommunications (BT), the UK's largest (and ex-state owned) carrier. The story was also carried by all the major television and radio news programmes.

Tim Kelsey, author of the Independent story, reveals that details such as telephone numbers and addresses for secret installations of the Ministry of Defence, MI5 (the British intelligence agency responsible for the UK) and MI6 (like MI5, but handles non-UK affairs).

"Thousands of pages of highly confidential BT records were sent across the Internet to a young Scottish journalist, Steve Fleming, in July". Mr Fleming received the information after making a news posting asking for information on BT and hacking. The informant remained anonymous -- details of how this was achieved are not given.

The hacker also gave details to Mr Fleming about how he too could access the information. He applied through an employment agency for a short-term contract at BT as a database designer, clearly stating on his CV that he was a freelance journalist. He got the job, and was able to gain access to the information because passwords were just left lying around the office.

BT is still going through a major staff restructuring programme, and as a result has a large number of temporary (contract) staff. These staff need passwords to the system to legitimately carry out their jobs, but because of the constant flow of people, the passwords are often written down.

Mr Fleming learned, among other things,

- \* The location of MI6's training centre ("spy school"), located in a non-descript building next to a pub in south London
- \* Information about the bunker in Wiltshire where the Government would go in the event of nuclear war
- \* Details of telephone installations at Buckingham Palace and 10 Downing Street [the Prime Minister's home], including personal lines to John and Norma Major.

The system itself, the "Customer Services System", was designed and implemented by an American company, Cincinnati Bell. It is supposed to have internal mechanisms to prevent hacking (!)

So, what are the risks (briefly!)

- 1) Allowing temporary staff passwords that allow almost any data to be retrieved. It sounds as if the security levels of the database were either non-existent, or compromised.
- 2) Keeping sensitive information in the same database as non-sensitive information.
- 3) The age-old chestnut of the uses of passwords.

A BT spokesman, speaking on the "Today" programme on BBC Radio 4 confirmed that a "top level" investigation had been launched, but refused to confirm or deny that the hack had taken place.

Mathew Lodge, Software Engineer, Schlumberger Technologies, Ferndown,

Dorset, UK, BH21 7PP lodge@ferndown.ate.slb.com (+44) (0)202 893535 x404

[The \*Independent\* items are in their entirety (28K) in  
[RISKS-16.58BT](#), courtesy of Brian Randell. PGN]

---

## Automated Weather Reports for Pilots

"Tom Keenan" <keenan@acs.ucalgary.ca>  
Fri, 25 Nov 94 0:31:28 MST

According to a piece on the CBC Alberta News on Nov 24:

Pilots are complaining about the inaccurate weather forecasts being provided by new automated weather briefing equipment installed at an Edmonton airport (and soon to be operational at the Calgary airport.) The system apparently cannot keep up with changing weather conditions and, in one specific case, a Canadian Airlines plane landed in snow although the forecast did not mention any snow. The airline has complained, and union members are arguing for a return to human delivery of weather info to pilots.

Dr. Tom Keenan, I.S.P., Dean, Faculty of Continuing Education, Univ. Calgary  
2500 University Dr. NW Calgary, AB T2N 1N4 CANADA (403) 220-5429

---

## Extended Phone Failure in Iowa City

Douglas W. Jones, 201H MLH, 3193350740 <jones@pyrite.cs.uiowa.edu>  
23 Nov 1994 04:08:25 GMT

On Saturday, Nov 19, Iowa City's telephone system, run by US West, shut down at about 3:30 PM, local time, and service was not restored until between 7:30 and 9:30 PM (service was brought up a bit at a time). As phone outages go, this was fairly severe! The population of the effected community is over 60,000.

The Iowa City Press Citizen, on Tuesday, Nov 22, reported that the cause of the failure has finally been determined. In July, a new telephone switching system was installed, and in the past week, the old system was removed from the building. As part of the removal process, the paper reports that an electrical grounding cable was inadvertently removed, leaving the new switch improperly grounded.

Apparently some customers noticed intermittent problems with their phone service earlier in the day, and US West had technicians working on the problem before the failure, but they were unable to diagnose the problem until some time after the failure had occurred.

Once the failure was diagnosed, the paper's description makes it sound as if the missing cable must have been easy to replace, but the 2 hour delay between the fix and the complete restoration of service is disturbing. They

had to cold-start the ESS system or systems involved (can you put over 20,000 phones on one system?), but this can't account for 2 hours, can it? My alternate hypothesis is that the improper grounding connection blew large numbers of fuses in alternate ground paths that weren't supposed to carry current, leading to a very time consuming job putting things right.

Lessons: First, this failure seems to be a perfect example of the fact that grounding problems are notoriously difficult to diagnose. Second, I suspect that nobody involved in the design of modern ESS systems would have guessed that it would take 2 hours to restore service after the fault was repaired. People who do such analysis or design other fault tolerant systems may need to look at this failure as an example. I'm eager to see more technical detail than the newspaper provided!

Doug Jones jones@cs.uiowa.edu

---

### **Enormous water bills - gigo strikes again.**

*"James M. Politte" <oprime@netcom.com>  
Wed, 23 Nov 1994 09:47:02 -0800 (PST)*

In the quiet western-Missouri town of Warrensburg, a small house with two occupants recently received a water bill amounting to \$4,704.88.

The water meter had been replaced with a new one, and being new, it read "000000". The previous reading from the last month, was "017060". The computer assumes that numbers on a water meter only go up, of course. So it was perfectly logical for the computer to assume that "000000" was caused by the meter rolling-over after reaching "999999".

Subtracting 017060 from 1000000 yields 982940 - and I was in fact billed for using 982940 cubic feet of water. (That's a column of water with a base the size of my house and 495 feet tall.)

The water company was quick to correct this problem upon hearing about it - but imagine if I had enrolled in the automatic payment program which subtracts bills directly from my bank account...

J.Politte - oprime@netcom.com

[A previous case due to the same cause, resulting in a water bill of \$22,000, appeared in [RISKS-12.16](#), Software Engineering Notes, vol 16, no 4, October 1991, and page 191 of my RISKS book. PGN]

---

### **Computer-generated bridge-tournament hands**

*"Peter G. Neumann" <neumann@csl.sri.com>  
Wed, 23 Nov 94 16:48:10 PST*

Mark Brader (msb@sq.com) forwarded a note from ggates@Starbase.NeoSoft.COM (Georgiana Gates) from rec.games.bridge. Georgiana played in the recent Minneapolis Women's board-a-match Nationals bridge tournament, and she and others noted that the computer-generated hands were IDENTICAL to those from

the first half of the semifinals of the Women's Knockout in San Diego (in which they had also played).

This is not the first time for such an occurrence. [RISKS-7.62](#), 7 Oct 1988 included an item from a New York Times column by Alan Truscott, contributed by Paul Abrahams, which I entitled "Bridge over troubled pseudo-random generation".

I presume that the initialization values for the pseudorandom generator were duplicates. It certainly gives a new meaning to the term "duplicate bridge".

---

### **The PC as a RISC (how could I resist 8)\***

*A. Padgett Peterson, Information Security <padgett@tccslr.dnet.mmc.com>  
Thu, 24 Nov 94 08:43:43 -0500*

Just in time for the holiday season comes a new feature for the PC - self-executing and playing Christmas Cards you can send to people with only E-Mail reception.

Did you know that it is possible to write a complex program on the PC using only ASCII printing characters ? XOR, AND, branching JMPs, PUSH, POP, SUB, INC, and DEC all exist within the range of 40h-7Eh. True, not all register and memory combinations can be used but enough.

After seeing an example done, I set out to make a few tests of my own and have determined that is possible to write a program using only ASCII characters that can decode and transfer execution to a "normal" .COM file that has been ASCII-encoded something like UUENCODE.

Of course with UUENCODE the problem is that first you needed to have the UUDECODE program. With an ASCII-executable program, the medium is the message.

This is just what the world needs: self-extracting and executing E-Mail.

Padgett

---

### **Problem with 911 service in Philadelphia**

*Paul Robinson <PAUL@tdr.com>  
Fri, 25 Nov 1994 15:20:24 -0500 (EST)*

CNN Reported that more than a dozen calls went into the Philadelphia 911 center to report a riot and fighting. Reports from callers ranged from civil to frantic as they called to report a serious incident occurring, while the 911 dispatch operators ranged from uninterested to downright rude.

A sample of one of the calls reported was something like this:

Caller: We need the police at 7100 Ridgeway, there's a group of

people in a fight...

Dispatch: (Bored) Is that all?

Caller: (Incredulous) IS THAT ALL? There's a caravan of cars  
coming down here to participate in a damn riot, that's all!

Another caller returned a call reporting a fight verging on a riot in their area. The 911 Dispatcher replied that she didn't know where they were.

It's that response that I wonder about; aren't most large city 911 systems equipped with name and ID for calls that come in? Smaller Cities, I can understand may simply use 911 as a substitute for dialing their emergency number and may not have name/phone lookup capability.

What got people upset was that, despite over a dozen 911 calls, police still took 40 minutes to show up, at which point they called the coroner to handle one dead 14-year-old, killed by some other teenagers armed with nothing stronger than baseball bats. (So much for the claims that gun control would make the streets safer.)

You can have all the high technology in the world and all the latest equipment, but if you either don't have the people on hand, or the people you have don't care, the technology can make things worse.

Paul Robinson - Paul@TDR.COM

---

## Department store security cameras linked to computer

*David Hembrow <davidh@harlequin.co.uk>*

*Tue, 22 Nov 1994 12:55:30 +0000*

Electronic Snap (UK "PC Week" magazine, 22 November 1994)

Not-so saintly shoppers in Marks and Spencer's will soon find themselves matched up in an electronic version of Snap! if they dare try beating the latest security move. The company will use ceiling mounted video cameras fitted to computers to compare pictures of known shoplifters in a trial in one of its stores. Watch out, Beadle's about, and the police aren't far away.

[Obvious risk of false positives ( which shoplifter do I look like? ), false data being in the computer in the first place etc.]

Jeremy Beadle is a much hated/loved TV presenter in the UK who presents a show a little like Candid Camera. Snap! is a card game played (predominantly) by children. The objective is to match two identical playing cards.

David Hembrow, Harlequin Ltd

---

## Children on the Infobahn

Bradley K. Sherman <bks@s27w007.pswfs.gov>

Tue, 22 Nov 94 22:38:04 PST

I'm the father of a 9-year-old girl and a 4-year-old boy. I live in a major metropolitan area --Oakland, California. As far as I'm concerned they can read anything they want. They're not going to find anything on the USENET that comes close to the real horror that exists on the streets of our cities. I'm just happy that they have the desire and ability to read (well, this is stretching it for the four-year-old).

I wonder what newsgroups the kids in Sarajevo are reading?

Bradley K. Sherman, Dendrome Project, Institute of Forest Genetics, PO Box 245  
Berkeley, CA 94701 bks@s27w007.pswfs.gov 510-559-6437

---

## Re: Pentium FDIV bug

Mike Carlton <carlton@ISI.EDU>

Wed, 23 Nov 1994 01:34:11 -0800

It would be nice to know just how bad the bug is. Intel certainly isn't being very helpful. I ran a set of experiments this last weekend and found 819 divide cases with less than single-precision accuracy on the pentium. I found 66 cases with just 14 bits accuracy (as in the first 4195835/3145727 example). BTW, that example was originally posted to comp.sys.intel by Tim Coe of Vitesse Semiconductor.

More info on my experiments is at: <ftp://www.isi.edu/pub/carlton/pentium>

For another simple example (the smallest my searching found), try the following in a spreadsheet or calculator program running on a pentium:

5505001/294911 = 18.66600093 on a buggy pentium  
= 18.66665197 the correct answer

The original reports of the bug mentioned double precision cases which returned 29 or so bits of accuracy, instead of the expected 52. At that point I wasn't very concerned by the bug (we had just taken delivery of a pentium workstation and I convinced the machine's user that it wasn't necessary to ask for a replacement processor). I've since changed my mind.

People have correctly pointed out that there are bugs in the OS, the compiler, your application program, etc. How many programs really need need more than 29 bits accuracy?

But Tim Coe's post showed that the error could get much worse than that. Tim also pointed out that the bug can occur in both single and double precision divides. Drawing upon his information, I was able to come up with a small set of divisors likely to cause the bug and write a search program that takes just 30 minutes to find the 800 cases.

The risk? How about the way Intel marketing has handled this

situation? They have not (yet) publicly described the extent of the bug. I've heard numbers like a 1 in  $10^{10}$  chance of hitting it and my back-of-the-envelope calculations tend to agree with this. It could be higher though, we have no way of knowing yet.

However, Intel hasn't described the magnitude of the errors. Could it be less than 14-bit accuracy? My experiments lead me to believe that it won't get any worse, but until Intel comes forward with a description of the cause of the bug we won't know. Until then, can people really rely on pentium calculations for critical work? If you can't trust any result there is no point in using the pentium.

What I really don't understand is why Intel didn't set up a PC doing random testing with one of the first pentiums off the fab line. Doing so would have exposed this bug in short order. It looks like that failure may turn out to be quite expensive.

--mike carlton@isi.edu USC/Information Sciences Institute (310) 822-1511

---

## Re: Cell-phone ergonomics side-effect (Stanley, [RISKS-16.57](#))

Bill Innanen <wgi@aplcomm.jhuapl.edu>

Sat, 26 Nov 1994 12:09:02 -0500

Robert Stanley (rstanley@sybase.com) wrote in [RISKS-16.57](#) about a mishap with a Nokia pocket sized cellular telephone. In this instance the one touch re-dial feature of the phone was inadvertently activated while in the owner's pocket, resulting in a supposedly private meeting being recorded on an answering machine.

As a (very satisfied) owner of a Nokia cell phone I would add a couple more RISKS. Namely, failure to become acquainted with the features of one's high tech widgets, and/or the failure to use same.

On my model 2120 Nokia there are two features either one of which would have prevented this mishap. As Mr. Stanley notes, the Nokia does not have a flip cover to protect the buttons from inadvertent presses. I personally think this lack is a Good Idea. The fewer moving breakable parts the better. However there is definitely a need to protect the keyboard. Nokia handles this electronically rather than mechanically. On my phone the "Keyguard" function is activated by the key sequence <Menu>\*. This this puts a notice on the screen that the keyboard is protected until the same key sequence is entered again. One can still answer the phone with the Keyguard active, however. I habitually keep the Keyguard active since I also carry my phone in my pocket. (Pants pocket in my case -- my shirt pocket is occupied by my "nerd protector" full of pens and pencils.)

The other Nokia feature that could have averted this problem is that the "one touch re-dial" can be turned off via the configuration menu. Personally I find it convenient and use it, relying on the Keyguard to protect me from unwanted redials.

Bill Innanen wgi@aplcomm.jhuapl.edu

---

**Re: Cell-phone ergonomics (Stanley, [RISKS-16.57](#))**

Paul Robinson <PAUL@tdr.com>

Wed, 23 Nov 1994 15:35:54 -0500 (EST)

> ... it is an extraordinarily sobering experience to hear  
> a sensitive work discussion issuing hours later from the  
> speaker of your home voice messaging system.

Question: is this real or are you just repeating the plot of Michael Crichton's {Disclosure}? :)

In {Disclosure}, the main character claims his boss - who is female - sexually harassed him by placing him in a compromising situation and trying to force him to have sex with her (he is married). He is able to show that she forced herself on him because he was testing a shirt-pocket sized cellular phone, had called a friend on it, and had not hit the "END" key, and his friend ended up with a recording of this "sensitive work discussion" on HIS answering machine...

Life imitates fiction.

Paul Robinson - Paul@TDR.COM

[Also noted by  
padgett@tccslr.dnet.mmc.com (A. Padgett Peterson),  
wolit@library.att.com (Jan I. Wolitzky),  
minow@apple.com (Martin Minow).]

---

**Re: Anon. on "TEN Q's" ([RISKS-16.57](#))**

Mark Seecof PSD x77605 <marks@bierce.latimes.com>

Wed, 23 Nov 1994 17:43:33 -0800

I agree with anonymized but urge: when giving "polite false" telephone numbers to salespeople, give NULL numbers, dammit, not random ones. I don't want calls from your sales contacts. (I find the TOD number (locally 853-1212) works well.)

Mark Seecof <marks@latimes.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 16: Issue 59**

**Weds 30 November 1994**

## Contents

- [The IRS knows "everything about you that we need to know"](#)  
[John Sullivan](#)
- [RISKS of electronic ticketing on buses](#)  
[Rhys Weatherley](#)
- [Why You Need a UPS For Your Bread Machine](#)  
[Curtis Jackson](#)
- [Listserv Loops](#)  
[Richard Klau](#)
- [NYNEX touts Credit Card authorization over Cell Phones](#)  
[Paul Green](#)
- [Re: Iowa phone switch](#)  
[Matthew Charles Wetmore](#)
- [Re: Reasonably Large Water Bill](#)  
[L. P. Levine](#)
- [Risks on TV: Eye-to-Eye-to-RFI](#)  
[Jan I. Wolitzky](#)
- [British Telecom "hacker" article was a hack!](#)  
[Sidney Markowitz](#)
- [The risks of media hack reports](#)  
[Rob Slade](#)
- [Re: Pentium FDIV bug](#)  
[Wilson P. Snyder II](#)  
[Peter da Silva](#)  
[Ron Heiby](#)  
[Dale R. Call](#)  
[Andy Grove via Richard Wirt](#)
- [Info on RISKS \(comp.risks\)](#)

---

### The IRS knows "everything about you that we need to know"

[<sullivan@geom.umn.edu>](mailto:sullivan@geom.umn.edu)

Wed, 30 Nov 1994 13:02:17 -0600

I read this paragraph from Wired in EDUPAGE ([listproc@educom.edu](mailto:listproc@educom.edu))

and found the implications disturbing:

#### IRS PLANS GOLDEN EAGLE TAX RETURN

The project manager for the Internal Revenue Service's Document Processing System described the "Golden Eagle" return, in which the government would automatically gather all a person's tax info and then compute the tax. "If I knew what you've made during the year, if I know what your withholding is, if I know what your spending pattern is, I should be able to generate for you a tax return. I am an excellent advocate of return-free filing. We know everything about you that we need to know. Your employer tells us everything about you that we need to know. Your activity records on your credit cards tell us everything about you that we need to know. Through interface with Social Security, with the DMV, with your banking institutions, we really have a lot of information ... We could literally file a return for you. This is the future we'd like to go to." (Wired, Dec.'94, p.174)

-John Sullivan [sullivan@geom.umn.edu](mailto:sullivan@geom.umn.edu)

[For info on receiving EDUPAGE, see [RISKS-16.58](#). PGN]

---

### **RISKS of electronic ticketing on buses**

*Mr Rhys Weatherley <[rhys@fit.qut.edu.au](mailto:rhys@fit.qut.edu.au)>  
Mon, 28 Nov 1994 09:46:06 +1000 (EST)*

The Brisbane City Council's bus service here in Australia is in the process of introducing an electronic ticketing system on all buses.

The old system used a bunch of "ticket pads" of different denominations: the driver would rip off a ticket from the right pad (you'd hope! :-), punch a hole in it, collect your money, and then give you the ticket.

The new system replaces the pads with a console which has a number of buttons for the denominations together with a printer to print the tickets. There are also two green boxes just inside the door in which commuters can insert the new magnetically encoded weekly and monthly bus tickets to have them checked.

I have yet to get my first magnetic monthly bus ticket so I can see how easy it would be to reprogram it, but I'm fairly confident that with the right equipment it is doable. For purely educational purposes of course. :-)  
RISK #1. I'm also interested in seeing if there is any identifying information on the cards permitting tracking of a person's movements. RISK #2.

The other day a schoolkid was waiting at my bus stop, and due to various stuff-ups in the scheduling, he was forced to catch my bus rather than the normal school bus. During peak hour my bus is a full fare bus, but of course the kid only had money for a half fare on him. In such cases, some drivers are complete mongrels and won't allow the kid on, but most will grumble a bit and then let the kid on for a half fare.

The driver stared at his console for a few seconds and then said (paraphrased) "There is no way to override this thing. Looks like you get a free ride today" and let the kid on for nothing. The console had automatically detected peak hour and disabled the half fare ticket buttons.

RISK #3 is fairly familiar: while enforcing "the rules" can be a good idea, sometimes it is necessary to override them for reasons of human kindness.

RISK #4 is that if an override button was provided, the console might log the fact and the driver might get in trouble (and then again, it might not: I don't know anything about the internals of the consoles yet). At least with the free ticket, no trace is left for the bus inspectors to whinge about. :-)

More information on the magnetic tickets as it comes to light ...

Rhys Weatherley, Queensland University of Technology, Australia.

---

## Why You Need a UPS For Your Bread Machine

*<cjackson@adobe.com>*

*Wed, 30 Nov 1994 00:27:33 GMT*

In order to more closely stick to a self-imposed lowfat diet, I finally broke down and bought a bread machine -- easy quick bread with no added fat. I was so pleased with the machine that I bought my breadophilic mother one and lugged it across the country to her house last week.

They were short on counter space in the kitchen, so they put the machine on a side-table and plugged it into an outlet that was activated by a wall switch that also controlled a light in the room. (I think you can guess what is coming next, and, yes, I did warn them. They said it was only a temporary placement and they'd remember.)

Sure enough, in the middle of the bread machine's 4-hour cycle, my stepfather turned off the light in the room (and thus removed power from the bread machine). I noticed this some indeterminate time later.

Problem #1: The bread machine has no NVRAM. So I had no idea whether it had been through only its first rise, or through a first rise, punchdown ("gas squeeze out"; this was a Japanese machine), and second rise.

Problem #2: The machine has a dough setting that will allow you to make dough, but not bake the dough. But there is no setting that says, "I already have dough, I just want you to bake it."

Problem #3: Neither my stepfather nor I had ever baked a loaf of bread by hand. Not once in our lives. And bread is quite a bit more sensitive to time and temperature than most other simple food items.

Luckily, I had also purchased a bread machine cookbook for my mother that suggested that one make a loaf of bread by hand first to get a feel for the

process, then proceed to using the machine. I used the book's baking time/temperature settings and ended up with an edible loaf of finished product. But, had we not had that book....

Curtis Jackson cjackson@mv.us.adobe.com

---

## Listserv Loops

*Richard Klau <kclairich@uofrlaw.urich.edu>*

*28 Nov 1994 21:30:27 GMT*

Along with Erik Heels (The Legal List), I own a list for law students discussion law & technology (StudentLawTech). We have just weathered a particularly disturbing incident, and would like some feedback on what has been done in the past with issues like these.

The facts, as near as we can tell, are these: a user set his e-mail system to refuse mail from the list. The system generated a refuse message for the sender to notify the sender that the message had not been read.

Since the list was the sender, this refusal notification was sent to the list. Because the e-mail system did not stamp the message with a "mailer-daemon" or some other appropriate flag, the list did not filter it out. The refusal notification was sent to the list.

Because the original user was not set to nomail (opting, instead, to do this at his level, rather than at the list level), he received the refusal notification. This notification in turn produced a notification of its own. The loop was started, and multiplied exponentially.

The system was not fully corrected until Saturday night, a full three days after the loops had begun. While we can't be sure, we think the total number of these looped messages prior to the fix on Saturday was near 1000 messages to each subscriber.

Needless to say, many have unsubscribed from the list. In addition, countless law students are now faced with the annoyance of having to delete mass quantities of mail. Most worrisome, of course, are those that pay for incoming e-mail.

So -- has this happened before? If so, what systems were involved? How was the situation remedied? What were the consequences?

Any advice is very welcomed. Replies by e-mail are preferred, but I will monitor this list.

Thanks for your help!

Rick Klau, Co-owner, StudentLawTech@Listserv.Law.Cornell.edu

---

## **NYNEX touts Credit Card authorization over Cell Phones**

<Paul\_Green@vos.stratus.com>

Tue, 29 Nov 94 17:43 EST

>From the September/October 1994 (Vol 9, #5) issue of "Accessibility", a newsletter that came with my most recent statement for my cell phones. Reproduced without permission. The flyer generally contains the typical marketing hype about ways to use your cell phone "more productively" (i.e., run up a bigger bill). The following anecdote is quoted in its entirety.

AIRTIME - Your Cellular Success Stories

Greg Maida  
Herkimer, NY

"We are in the craft business, and we use our NYNEX Mobile cellular phone to transmit credit card charges. This has saved us a lot of grief, because we are able to get credit card approvals within about 30 seconds. The cellular phone gives us the convenience of a phone at any locations and enables us to offer more purchasing options to customers."

\*\*\*

What can I say? Why worry about sending your credit card over the Internet, when this vendor will send it out over radio waves for you!

Just to add a little irony to this whole discussion, in the very same newsletter, on the facing page, appears the following "tip":

"Remember to lock your cellular phone! You will reduce the risk of incurring fraudulent calls if your phone is stolen. Don't consider this precaution an inconvenience. Lock your phone whenever you park your car with a parking attendant. If your phone can be removed, we recommend carrying it with you when you leave the car unattended."

The only word that springs to mind here is chutzpah!

PG

[accessability  
Marcia Williams Cromer, Editor  
NYNEX Mobile Communications  
2000 Corporate Drive  
Orangeburg, NY 10962  
(c) 1994 - All Rights Reserved]

---

## **Re: Iowa phone switch ([RISKS-16.58](#))**

Matthew Charles Wetmore <mwetmore@polyslo.csc.calpoly.edu>

Mon, 28 Nov 94 17:33:46 -0800

Phone systems do not exist in a vacuum, nor is restarting them as simple

as flipping a switch.

In this case, there'd be diagnostics to make sure that nothing actually \*was\* burned out. Then reloading the phone database and configuration information. The information might include special features with each phone for caller ID, forwarding numbers, voicemail options, et cetra. Next comes routing information from the various neighborhood multiplexors to the central office. Last, but not least, you have to convince any other computer system you are connected with (long distance carriers, billing computers, ...) that your system is alive and well again.

>Lessons: First, this failure seems to be a perfect example of the fact that  
>grounding problems are notoriously difficult to diagnose. Second, I suspect  
>that nobody involved in the design of modern ESS systems would have guessed  
>that it would take 2 hours to restore service after the fault was repaired.

"You get what you pay for," may be the case here. A "small" town with one system has all or nothing failures. New York, on the other hand, can shunt calls over to other offices while one is restoring.

Multiple redundancy is the most common "solution" to make a system fault tolerant.

These are only the technological factors... A human factors:

A new system having been recently installed: how many trained technicians did they have on hand, well versed in the new system lore? There's a fair chance a technician from the system manufacturer had to race out, and this accounted for a bulk of that time.

Matthew C. Wetmore -- ACM, c/o CSc Dept., California Polytechnic State Univ,  
San Luis Obispo, CA 93407 -- USA      mwetmore@galaxy.CSc.CalPoly.EDU

---

## Re: Reasonably Large Water Bill (Politte, [RISKS-16.56](#))

*"Prof. L. P. Levine" <levine@blatz.cs.uwm.edu>  
Sun, 27 Nov 1994 09:09:46 -0600 (CST)*

Some years ago I received a water bill from the Village of Shorewood in Wisconsin that was about 30 times too large. In my case also the problem was due to a failed repeater that mounted on the outside of my house and was delivered an electrical pulse each time 100 cubic feet of water was registered by the actual meter in the basement.

The system had been installed over ten years ago and had (apparently) been missing pulses from the very first. No one had noted the slight decrease in billing until the system finally had a hard failure and reported no water use during a quarter-year. When the new repeater was installed it was manually set to agree with the water meter in the basement (Wisconsin folks are smarter than they are in Missouri) and therefore included all of the "ticks" missed over a ten year period. They all appeared on the next bill.

Since we had, in fact, used the water that was billed there was no question we should pay. What was in doubt was just how much. Water

rates had increased substantially during the period because of the inclusion of sewer costs within the water bill during recent years. Negotiation with the village over the question "how much water was used when" settled the issue.

What's the risk? New machinery will soon enable more and more utility billing to be done automatically. Many of these systems will depend on repeaters for their data collection with the true numbers still available on more conventional meters located on site. My hundred dollar water bill will seem small compared to the complexity of just which owner/renter used the missing electricity after failed meter systems are fixed and their meters updated.

Prof. Leonard P. Levine, Computer Science, University of Wisconsin-Milwaukee  
Box 784, Milwaukee, WI 53201 levine@cs.uwm.edu 1-414-229-5170

---

### Risks on TV: Eye-to-Eye-to-RFI

<wolit@library.mt.att.com>  
Mon, 28 Nov 94 10:50:50 EST

This week's "Eye-to-Eye with Connie Chung" is scheduled to include a segment on radio-frequency interference risks. I was interviewed by one of her crews, demonstrating an automatic cardiac defibrillator being messed up by a public-safety band walkie-talkie. Other examples reportedly include an electric wheelchair being spoofed by a cellular phone, aircraft instruments confused by PCs, etc. I haven't seen any of the tape yet, so I don't really know whether I want to be announcing this, but it's likely to be of interest to participants of this forum. Thursday night, 1 Dec 1994, CBS, 10pm EST.

Jan I. Wolitzky, AT&T Bell Laboratories, 600 Mountain Avenue, Room 3D-590  
Murray Hill, NJ 07974-2070 USA 1 908 582-2998 wolit@library.att.com

---

### British Telecom "hacker" article was a hack!

Sidney Markowitz <sidney@taurus.apple.com>  
Tue, 29 Nov 1994 19:36:24 -0800

[Thanks to sidney@apple.com (Sidney Markowitz) for letting me see copyrighted Newsbytes material, which I have starkly abstracted. PGN]

Steve Fleming, the reporter noted in [RISKS-16.58](#) as responsible for the article on the "hacking" of BT's Customer Service System (CSS), has admitted that he himself was the unknown Internet hacker. "Instead of gaining unauthorized access to the BT computers, he actually worked for a lengthy period of time (three months, according to Newsbytes sources) and was required to access the CSS computer system as part of his job. "I didn't realize how sensitive the information was, but I was horrified how easy it was to get into the system," he is quoted as saying in the London Observer newspaper." Fleming may be prosecuted.

---

## The risks of media hack reports (BT and the Queen)

*"Rob Slade, Social Convener to the Net" <roberts@mukluk.decus.ca>*

*Sun, 27 Nov 1994 03:30:22 EST*

in re: Mathew Lodge's posting in 16.58:

I was wondering if this was going to make it into RISKS. I saw a TV report on the story (a re-use of an NBC story of the BBC story, apparently). There was the mention of the Internet, there was the use of the word "hacker", but there was, technically, no security system "breaking". Social engineering, definitely. Stupidity, beyond question. Loss of confidentiality, loss of privacy, yes, and again, yes. But no hacking, cracking or phreaking. Indeed, since the original informant is still unidentified, the word "hacker", even in its most debased usage, is extremely suspect.

The risks as I see it, is that once again the public is being led to believe that evil and powerful "hackers" can invade even the most highly protected inner sanctum of one of the worlds best secured telecom systems. In reality the "keepers of the keys" have simply left the doors wide open.

DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733

---

## Re: Pentium FDIV bug [random testing]

*Wilson P. Snyder II (DTN 225-5592 HLO2-3/C8) <snyder@ricks.enet.dec.com>*

*Mon, 28 Nov 94 17:38:23 EST*

Can't speak for Intel, but at Digital, our Alpha AXP processors are tested using psudo-random techniques which do exactly that. Random testing often finds interesting problems that would never be found by just writing specific tests. (The genetic algorithm folks can give lots of data on why this is so.) To implement the random method though, you have to code a entire simulation of the results that the CPU will produce.

Unfortunately, as readers of this group will appreciate, occasionally the template that describes the correct response, or limiting the range to test will be itself in error. (Comparing a transistor model to a bad software model is a good example of the first kind of error.) Even if all is set up perfectly, I've seen cases where it took several weeks to expose a bug.

---

## What are the odds Intel would pick this phrasing at random?

*Peter da Silva <peter@nmti.com>*

*Mon, 28 Nov 1994 09:43:03 -0600*

The problem I have with Intel's handling of this is the use of the word "chance", as if there was a random factor involved, that a calculation

will work right one time and fail the next so you can just run it again and get the right result. Of course no such thing is true, but that's the impression Intel's (deliberately?) spreading.

Also, people hear about a "1 in 10<sup>10</sup>" chance and think it refers to some statistical probability that their system will have a problem, rather than a measure of the proportion of inputs that will (consistently) produce an invalid response. For programs that require double precision calculations and involve arbitrary input the "chance" of that program hitting the bug approaches unity.

Nope... Pentium Bingo isn't a game of chance at all.

---

### **Re: Pentium FDIV bug**

*Ron Heiby <heiby@falkor.chi.il.us>  
Mon, 28 Nov 1994 21:52:12 GMT*

The chairman of the Computer Science Department at Hope College (when I was attending, and probably still), Herbert Dershem, told one of my early CS classes that, "any idiot can write a very fast sort routine, if it doesn't have to put the elements into the correct order." (That may not be an exact quote, but pretty close.)

It looks like intel has figured out that they can write a very fast floating point unit, if it doesn't have to produce the correct results!

Ron

---

### **Re: Pentium FDIV bug**

*Dale R. Call <dalec@ibeam.jf.intel.com>  
Wed, 30 Nov 1994 10:52:33 -0800*

For more information on the Pentium FDIV bug, and Intel's response, take a look at our corporate presence server ([www.intel.com](http://www.intel.com)):

<http://www.intel.com/about-intel/press/andy-msg.html>

This message was also posted on various net newsgroups.

Dale R. Call, Intel Architecture Labs

---

### **My Perspective on Pentium - AGS**

*<[several anonymous sources]>  
27 Nov 1994 19:31:21 GMT*

Andy Grove has asked me to post the following for him. Since it is the

weekend and we are out of the office, I am posting from my home system.

Richard Wirt  
Director SW Technology  
Intel Corp

This is Andy Grove, president of Intel. I'd like to comment a bit on the conversations that have been taking place here.

First of all, I am truly sorry for the anxiety created among you by our floating point issue. I read thru some of the postings and it's clear that many of you have done a lot of work around it and that some of you are very angry at us.

Let me give you my perspective on what has happened here.

The Pentium processor was introduced into the market in May of '93 after the most extensive testing program we at Intel have ever embarked on. Because this chip is three times as complex as the 486, and because it includes a number of improved floating point algorithms, we geared up to do an array of tests, validation, and verification that far exceeded anything we had ever done. So did many of our OEM customers. We held the introduction of the chip several months in order to give them more time to check out the chip and their systems. We worked extensively with many software companies to this end as well.

We were very pleased with the result. We ramped the processor faster than any other in our history and encountered no significant problems in the user community. Not that the chip was perfect; no chip ever is. From time to time, we gathered up what problems we found and put into production a new "stepping" -- a new set of masks that incorporated whatever we corrected. Stepping N was better than stepping N minus 1, which was better than stepping N minus 2. After almost 25 years in the microprocessor business, I have come to the conclusion that no microprocessor is ever perfect; they just come closer to perfection with each stepping. In the life of a typical microprocessor, we go thru half a dozen or more such steppings.

Then, in the summer of '94, in the process of further testing (which continued thru all this time and continues today), we came upon the floating point error. We were puzzled as to why neither we nor anyone else had encountered this earlier. We started a separate project, including mathematicians and scientists who work for us in areas other than the Pentium processor group to examine the nature of the problem and its impact.

This group concluded after months of work that (1) an error is only likely to occur at a frequency of the order of once in nine billion random floating point divides, and that (2) this many divides in all the programs they evaluated (which included many scientific programs) would require elapsed times of use that would be longer than the mean time to failure of the physical computer subsystems. In other words, the error rate a user might see due to the floating point problem would be swamped by other known computer failure mechanisms. This explained why nobody -- not us, not our OEM customers, not the software vendors we worked with and not the many

individual users -- had run into it.

As some of you may recall, we had encountered thornier problems with early versions of the 386 and 486, so we breathed a sigh of relief that with the Pentium processor we had found what turned out to be a problem of far lesser magnitude. We then incorporated the fix into the next stepping of both the 60 and 66 and the 75/90/100 MHz Pentium processor along with whatever else we were correcting in that next stepping.

Then, last month Professor Nicely posted his observations about this problem and the hubbub started. Interestingly, I understand from press reports that Prof. Nicely was attempting to show that Pentium-based computers can do the jobs of big time supercomputers in numbers analyses. Many of you who posted comments are evidently also involved in pretty heavy duty mathematical work.

That gets us to the present time and what we do about all this.

We would like to find all users of the Pentium processor who are engaged in work involving heavy duty scientific/floating point calculations and resolve their problem in the most appropriate fashion including, if necessary, by replacing their chips with new ones. We don't know how to set precise rules on this so we decided to do it thru individual discussions between each of you and a technically trained Intel person. We set up 800# lines for that purpose. It is going to take us time to work thru the calls we are getting, but we will work thru them. I would like to ask for your patience here.

Meanwhile, please don't be concerned that the passing of time will deprive you of the opportunity to get your problem resolved -- we will stand behind these chips for the life of your computer.

Sorry to be so long-winded -- and again please accept my apologies for the situation. We appreciate your interest in the Pentium processor, and we remain dedicated to bringing it as close to perfection as possible.

I will monitor your communications in the future -- forgive me if I can't answer each of you individually.

Andy Grove



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 16: Issue 60**

**Monday 5 December 1994**

## Contents

- [Excel linked spreadsheet bug](#)  
[Michael D. Crawford](#)
- [Random Testing of Floating Point: Doesn't Everyone?](#)  
[Robert Ayers](#)
- [3 hits and you're out? \(SSN use\)](#)  
[Geoffrey S Knauth](#)
- [The Economist and E-cash](#)  
[Mark Stalzer](#)
- [RISKS of Going to the Movies](#)  
[Keith Schengili-Roberts](#)
- [Providing Good Defaults \(and risks of not doing so\)](#)  
[Ry Jones](#)
- [The PC as a RISC](#)  
[Michael Slavitch](#)
- [HERE Rides Eye To Eye](#)  
[Winn Schwartau](#)
- [Interesting product claim](#)  
[Mike Kenney](#)
- [Criminals 1, Consumers 0](#)  
[Peter J. Denning](#)
- [Re: Duplicate bridge-tournament hands](#)  
[Asya Kamsky](#)
- [Re: Listserv Loops](#)  
[Steve Summit](#)  
[Peter da Silva](#)  
[Joe A. Dellinger](#)
- ["Tekroids" episode of Tekwar and the perception of viri](#)  
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Excel linked spreadsheet bug

*Michael D. Crawford* <[crawford@scruznet.com](mailto:crawford@scruznet.com)>  
*Sun, 4 Dec 1994 02:58:46 -0800*

There is a bug in Microsoft Excel for the Macintosh in which results from linked spreadsheets are incorrectly recalculated.

A friend of mine who owns a business overdrew his company checking account by \$4,000 as a result.

Interestingly, he had a "fail-safe" system, in which his accountant recommended which bills to pay based on the total account balances. The accountant recommend he pay a bill for about \$2,000, then inadvertently credited this to the balance sheet rather than debiting it. My friend checked the accountants work using a linked spreadsheet. The calculation showed that he had \$4,000 more then was really available. The unlikely coincidence of making a manual mistake that matched a software error convinced my friend that it was safe to write the check.

My friend can easily duplicate the bug. Apparently the bug is being discussed on Compuserve these days, with the word being that it only happens on really complicated spreadsheets. My friends spreadsheets, though, are quite simple - one spreadsheet to tally the checking balance, one to tally the credit card account balance, and a third to total the two accounts.

Michael D. Crawford [crawford@scruznet.com](mailto:crawford@scruznet.com) [crawford@maxwell.ucsc.edu](mailto:crawford@maxwell.ucsc.edu)

---

## Random Testing of Floating Point: Doesn't Everyone?

*Robert Ayers <[ayers@mv.us.adobe.com](mailto:ayers@mv.us.adobe.com)>*

*Sat, 3 Dec 94 13:41:33 PST*

In [RISKS-16.59](#) Wilson P. Snyder notes "at Digital, our Alpha AXP processors are tested using psudo-random techniques ... Random testing often finds interesting problems that would never be found by just writing specific tests."

Hasn't everybody done this forever?

Back in the '60s (yes that's "sixties") I watched IBM upgrade a 7090 to a 7094. The third \*day\* of the post-upgrade verification was a test of the new floating point arithmetic (a 7094 upgrade added double precision) using randomly generated data and a fixed-point simulation of the FP for comparison.

I asked the IBM CE whether that twenty-four hours of floating-point testing was really necessary. He replied "Yup. I've seen the test run OK for sixteen hours and then find a failure."

Bob

[By the way, I have suppressed a huge influx of Intel `humor' that has been submitted to RISKS. I have seen so many copies of so many different items on so many redistributions that it seems unnecessary to include them here, or to note that I have seen at least 63.999975 distinct jokes thus far. PGN]

---

### 3 hits and you're out? (SSN use)

Geoffrey S Knauth <gsk@world.std.com>  
Mon, 5 Dec 1994 16:29:30 GMT

Last week, a friend was writing software to make credit checks as part of a large project involving government loans to individuals. He returned home and told his wife we'd been using my social security number to test the interface, with my permission. His wife works at a bank, and she told him he'd better not do three checks on me, or I wouldn't get any more credit. I was surprised to hear that a credit check carries with it this sort of penalty. Can anyone from the credit industry confirm this?

My friend was recently given a "test" SSN to use, so I shouldn't have to worry more.

Geoffrey S. Knauth <gsk@marble.com> <http://www.marble.com/people/gsk.html>  
Marble Associates, Inc., (617) 487-0050 CRASH-B Sprints, Cambridge Boat Club

---

### The Economist and E-cash

Mark Stalzer <stalzer@macaw.hrl.hac.com>  
Tue, 29 Nov 1994 12:27:36 +0800

The 26 Nov 1994 issue of The Economist has a story on electronic money (p.21--23). It covers some of the current attempts to create "virtual banks" on the internet so that consumers can buy from electronic stores without sending credit card numbers in the clear. This is fairly mundane stuff to risks readers, but the story moves on to the evolution of digital cash. Some of the possibilities are interesting, such as private issuers of E-cash (that will probably be more stable than most governments!) to a world-wide currency (no exchanges rates and middle-people). Recommended reading if you're curious about some of the broader issues of electronic money.

Mark Stalzer, mas@acm.org

[E-cashibus unum. PGN]

---

### RISKS of Going to the Movies

Keith Schengili-Roberts <kschengi@interlog.com>  
Sun, 4 Dec 94 22:53 WET

Recently, my wife and I decided to go to see a movie at one of the cinemas in downtown Toronto. It was a rainy day, and there was a long line-up to see the film. I noticed that just inside the foyer of the theatre were a couple of automatic ticket dispensing machines. Nobody was at the machines,

save for a couple of kids who were playing with them.

I had used the automatic ticket vending machines before, and they operate in a similar fashion to automatic teller machines. Instead of cash, you get film tickets. You can also buy things like popcorn and cola in the form of tickets that you take to the concession stand. It was my wife's treat, so she shooed away one of the boys who was playing with one of the machines, and proceeded to swipe her credit card in the card-reader.

Tickets began to pour from the machine. General Admission, Senior's and Children's tickets along with coupons for purchasing a small mountain of popcorn and a river of cola issued from the machine, like a one-armed ticket-dispensing bandit gone mad. In the end my wife was charged for approximately \$375.00 of goods. The kids who had been playing with the machine before were nowhere to be seen, and the movie was about to begin.

What had happened was this: the kids who had been playing with this machine had made just about every conceivable selection on its touch-screen before my wife got to it. Part of the reason why it must have been fun for them to play with is because you do not have to prove your purchasing power with a credit/bank card beforehand. You can make as many on-screen selections as you like, and it will merrily rack up the total charges.

While there is a screen that asks if you want to purchase all of the items you have selected, to someone inexperienced with these types of machines, it appeared to be a "start" screen. A further risk was revealed when my wife used her Credit Card with the machine. It has its PIN number built-in, (convenient by highly RISK-y) so the moment she swiped the card past the reader, it confirmed the order immediately.

In the end the staff at the theatre were very helpful, and at the end of the movie my wife handed over her receipt from the machine, and expected to have the charges on her credit card reversed. Instead she was paid back in cash directly from the box-office takings by the theatre manager. When I asked why, it turned out that there was no procedure between the bank that installed the automatic ticket dispensing machines and the theatre-chain to deal with this type of situation. The manager said that they'd definitely "have to look into it". Luckily a bank was nearby and payment to my wife's account was made before any interest charges could accumulate.

When we went back to the same theatre again recently for another movie, I noticed a couple of changes. A ticket-agent stood guard to make sure that nobody played around with the machines who didn't intend to purchase anything, and there was a large sheet of instructions placed beside each machine. I paid for the tickets this time, and used a bank card that does not have a built-in PIN number. Everything went smoothly this time: we got the tickets we requested, and managed to zip past the rest of line and got good seats in the theatre.

The movie was good too!

Keith Schengili-Roberts, Writer/Reviewer, The Computer Paper - Toronto Office  
Canada's largest computer magazine, free, on-line at: <http://www.wimsey.com/tcp>

---

## Providing Good Defaults (and risks of not doing so)

Ry Jones <rjones%rjones@rjones.oz.net>

Sat, 26 Nov 1994 22:58:27 -0800 (PST)

One of the frequently referenced style guides for programming (the Indian Hill guide, I think) talks about the value of good defaults. The current Slackware Linux distribution does not do so in one important area, and I was able to 'explore' a system due to this flaw in the installation:

Slackware does not force a root password on install.

The system in question was hooked up to the internet for casual use by someone I have known for a long time. Apparently, the two way nature of a PPP link didn't cross the minds of the three people involved in getting the system on the net, and they never set any passwords.

I was able to get in as root and make clear to the machine's owner that he had no security.

I called him afterwards and we set things up much tighter, but it's disturbing to me that neither the OS install nor the network software install forces you to set any password.

To be sure, this is freeware, and is to be used by an experienced user community, but it was all too easy for them to escape onto the net without any warnings. I have noticed many linux systems on the net that still have the default users (gonzo et al) still installed.

Good defaults, I think, would solve this.

---

## The PC as a RISC (how could I resist 8)\*

"Michael Slavitch, Consultant, (613) 781-9824" <slavitch@on.bell.ca>

Mon, 28 Nov 94 09:44:03 -0500

A. Padgett Peterson writes:

> This is just what the world needs: self-extracting and executing E-Mail.

This was the case with several commercial (non-smtp) mail packages such as Novell's MHS. Several years ago I was developing software for the Novell platform (I still do when people throw money at me to do it :). I was having problems with one of my programs. I uuencoded the file and sent it to a buddy@novell.com, along with source, and for some reason :) the early-version MHS mail system immediately began to self extract the file.

Unfortunately, I had given the UUENCODED .NLM (Netware Server Executable) file a hard path (thinking that the smart engineer would see it and know where I had installed it, and yet being smart enough not to put it in a critical system).

Unfortunately, it had been expanded on a system by a dumb computer :) where the NW developer also had \*root\* like privs, so the file would expand and be placed anywhere in the network file server system. Luckily the program never loaded (although if it had been given a name of a program that was loaded periodically like as we had known it would have ceased to exist) and I found out about it through a \*confirmation message\* sent to me by the mailer.

Now think about this and remember the internet worm (this was \*years\* later). I told my buddy about this by email and within a couple of weeks there was a patch update to MHS. I got a lot of phone calls from Novell developers trying to figure out what I had done.

Basically, I could send a new password files to \*supervisor\* (NW's \*root\*) and then after that set file privileges by email to my hearts content. Scary.

Let me just say that MHS doesn't do that anymore. And yes, I've tried to break it (with permission) without success since. But I'm a medium-smart hacker. Some real devils out there could probably figure out a way to mess greatly with such systems, especially now that MIME and WWW are becoming more commonplace (what about Web-bombs using creaky web forms? It has been done by a relatively good hacker buddy of mine in a couple of minutes).

I am distrustful of the security of any system that allows a person to place a file without explicit authorization, as well as authentication (web forms, FTP, and self-extracting mail). Digital sigs will keep unauthorized people from doing dangerous things, but it won't keep authorized people from doing things that cause stupid computers to do stupid things.

Michael

---

## HERF Rides Eye To Eye

*"Winn Schwartau" <p00506@psilink.com>*

*Thu, 01 Dec 94 22:55:19 -0500*

Connie Chung's "Eye to Eye" (ABC, 12/1/94) provided an excellent primer on accidental electronic interference. (My book is a pretty good source, too. Can't resist the 'plug.')

They brought into living room TV color clarity more hard examples of EMI:

- \* Children's life support systems failing by cell-phone induced EMI.
- \* Defibrillators malfunctioning.
- \* Wheelchairs spinning in circles from portable radio interference.
- \* Airplane (727) avionics and guidance systems (both primary and secondary) going haywire from passenger radio.

The focus was on \_accidental\_ EMI events, which were low power events at that. Radio emissions and cell phones and such are not power intensive devices (a few hundred milliwatts) but still can cause dramatic systemic failures.

Obviously (for those who know my work) when intentional EMI is "turned up" to higher power levels, the interference is increased as well. Thus, as I discussed in "Information Warfare," when a bad guy has the capability to generate electromagnetic fields of a greater strength, control the frequency and focus or aim them upon targets, we can similarly expect to see man-made EMI events of greater intensity in greater numbers.

Bringing down financial econo-technical infrastructures (among other targets) through electromagnetic denial of service attacks is on its way, if it's not here already. I am currently investigating a number of fascinating 'incidents.' (Please let me know if you think you might have been 'hit' by either HERF Gun or EMP/T Bomb assaults.)

A while back [\[RISKS-16.26\]](#) I also posted in RISKS how airplane avionics interference is caused by on board digital devices and how such vulnerabilities could be exploited by suicidal maniacs or those of the terrorist flavor. I also recall a number of readers "doubting nay-sayers" pooh-poohing such hogwash.

Take a watch of Connie. HERF is again being vindicated.

Winn Schwartau, Executive Director, Interpact, Inc.

---

## Interesting product claim

*Mike Kenney <mike@wavelet.apl.washington.edu>  
Thu, 1 Dec 1994 10:11:42 -0800 (PST)*

I ran across the following product description in the Shareware Express catalog that my wife receives:

```
``COMPUTERIZE YOUR EMPLOYEE TIMECLOCK. Save time and money. Convert
your PC into an employee timeclock and bring timekeeping and payroll
tasks into the 20th century! TIMECLOCK logs your employees "in" and
"out" and calculates their hours automatically at the end of each
pay period. Unlike manual systems, it never makes a mistake ... "
```

```
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

Talk about your bold statements.

But what if you run it on a Pentium? :-)

While I'm on the subject of the Pentium I would just like to toss in my \$0.02. I don't have a problem with the fact that the chip had a bug ... it's certainly not the first and it sure won't be the last. I \*do\* have a problem with the way Intel has handled the situation and I'm speaking as someone who manages 3 Pentium systems. Since I'm at a university research lab, I had no problem getting replacements but others are not so lucky.

As CPUs get more and more complex, the chance of bugs slipping through will probably go up. I just hope whichever company it happens to next handles

the problem better than Intel.

Mike Kenney, UW Applied Physics Lab [mikek@apl.washington.edu](mailto:mikek@apl.washington.edu)

---

## **Criminals 1, Consumers 0**

*Peter J. Denning <[pjd@cne.gmu.edu](mailto:pjd@cne.gmu.edu)>*

*Thu, 1 Dec 94 09:23:59 EST*

Cellular One of the Baltimore-Washington area just distributed a notice to all customers that they have cut off roaming in the New York City area. They say that fraud has become too serious a problem. It is now not possible to have your calls forwarded to you in NYC. If you wish to make an outcoming call in NYC, an operator will take a credit card number and immediately bill that at rates considerably higher than the normal roaming rates (which are in turn considerably higher than the regular cellular rates).

The fraud is that thieves have been stealing electronic id numbers by scanning the cellular frequencies and picking them out; they then program those numbers in new (cheap) phones and sell them on the streets. By the time one finds out that someone else has cloned one's phone, hundreds or thousands of dollars of calls will have been logged.

[This problem is of course very widespread. It's more like CRIMINALS \$1B, CELLULAR ZERO. Some countermeasures are of course possible, but are impeded by lack of standards, lack of exportability, lack of incentives by vendors, lack of customer interest in paying more, etc. PGN]

---

## **Re: Duplicate bridge-tournament hands ([RISKS-16.58](#))**

*Asya Kamsky <[kamsky@sales.tgv.com](mailto:kamsky@sales.tgv.com)>*

*Wed, 30 Nov 94 14:41:09 PST*

That is not what happened at all. The bridge hands are dealt out by this machine, and it is set to deal out the same sets of hands until someone resets it, or puts in a new set of hands.

The machine wasn't used between the two tournaments, so it dealt out the last set of hands that was fed into it.

Usually when hands are duplicated like this, it's the same set of hands being used by humans, not the same set being generated by a machine.

As usual -- pilot error.

Asya

---

**Re: Listserv Loops (Klau, [RISKS 16.59](#))**

Steve Summit <[scs@eskimo.com](mailto:scs@eskimo.com)>

Thu, 1 Dec 1994 12:37:39 -0800

Mailer loops have probably been around since the dawn of e-mail. They're often astonishing, but they shouldn't be: any time mail can be generated by an automaton (e.g. error messages, "vacation" programs), or a single message can spawn multiple messages (e.g. "mail exploders" such as listserv), you have a system with gain. Undamped positive feedback can yield spectacular results, but again, this shouldn't be too surprising.

Anyone writing mail software, even of a rudimentary nature, which has even a hint of a possibility of inducing any gain, needs to be acutely aware of these problems, and to take every step possible to reduce the opportunities for positive feedback and to detect and damp it when (not if) it occurs. Without taking such precautions, disastrous mail loops are a certainty; with them, they are merely likely. (In other words, even mail systems which were supposedly designed to prevent loops are fairly regularly surprised when real-world installations discover new ways to connect some pieces together into feedback loops which manage to bypass any safeguards.)

I believe there was an article discussing this sort of thing in CACM in 1989 or 1990; unfortunately, I no longer have the reference.

Steve Summit [scs@eskimo.com](mailto:scs@eskimo.com)

---

**Mailing list problems...**

Peter da Silva <[peter@nmti.com](mailto:peter@nmti.com)>

Thu, 1 Dec 1994 13:51:49 -0600

OK. There's a number of things a list can do to prevent this sort of problem. You are probably doing at least some of these:

1. Stamp outgoing list mail as being "junk". I believe that this is in the "precedence" header. Many systems toss "junk" mail when it's refused.
2. Set outgoing mail to have an "Errors-To:" address.
3. Drop incoming mail that is marked as being "junk".

If you were doing all of these things, then the fault is due to the bouncing software. It should really support all three (mark its mail as junk, drop junk mail instead of bouncing it, and respond to an errors-to address), but for it to support NONE of the three is serious brokenness.

> So -- has this happened before?

Lots of times. A lot of people keep a human in the loop to prevent this sort of error cascade. The only other thing you can do is to be totally anal

retentive about how you treat headers. The three items I listed above are just a start.

[There were numerous similar responses on this topic, including from catfood@rosebud.strinc.com (Mark W. Schumann), who added that ``A subscriber site that does not honor the "Errors-to:" header is broken and should be turned in to the RFC822 Police."

{WOULD THAT THERE WERE SUCH!}

zerkle@cs.ucdavis.edu (Dan Zerkle),

flatau@cli.com (Arthur D. Flatau),

John Gardiner Myers <jgm+@CMU.EDU>,

stead@seismo.CSS.GOV (Richard Stead),

Peter M. Weiss <PMW1@PSUVM.PSU.EDU>,

crawford@scruznet.com (Michael D. Crawford),

thompson@se01.wg2.waii.com (James Thompson).

Thanks to all of you. Would that all mail servers were compliant!

The bad ones are driving me nuts. PGN]

---

## Re: Listserv Loops

*Joe A. Dellinger <jdellinger@amoco.com>*

*Fri, 2 Dec 94 18:50:57 CST*

The "vacation" command will cause the same problem, albeit it only sends one "I'm not here" notice to the entire list before ceasing auto-responding. As far as I know, there is no automatic way for the list processor to detect such auto-replies, and they will occur whenever anyone remains subscribed to a list while on "vacation".

In 1989, in the Geophysics department at Stanford, a similar incident involving the Bay Area Chinese Student's mailing list caused all our departmental computers to crash. In that case someone had simply forwarded all their mail to the list processor shortly before going on vacation. The reply addresses kept getting longer with each round-trip iteration, until they overflowed the fixed-length field in the Berkeley mail programs allocated for that string, causing the mail daemon to keep running doing nothing forever. After an hour or so there would be dozens of superuser-priority mail daemons all attempting to run simultaneously and the machine would crash. (Our machines crashed first because in our department we had the highest density of subscribers to that list.)

The moral of the story: anything which replicates itself has the built-in potential of becoming a cancer / virus.

Note the designers of "mail" recognized the problem and designed in prevention against infinite mail loops, by the brute force expedient of killing messages more than a certain number of hops old.

---

## "Tekroids" episode of Tekwar and the perception of viri

"Rob Slade, Social Convener to the Net" <roberts@mukluk.decus.ca>  
Sat, 03 Dec 1994 19:23:53 EST

TVTEKWAR.RVW 941201

Bill Shatner has been reading "Snow Crash" (cf BKSNCRSH.RVW)!

In tonight's episode of Tekwar, we find that police detectives, and the hero's ex-wife, have been felled by a nasty virus. A *\*computer\** virus. Call the Weekly World News.

Shatner is *\*much\** more ambitious than Stephenson. The "Snow Crash" virus, in graphical representation, looked pretty much as you'd expect--snow! The Tekwar virus looks like a young lady. (When she starts to open her blouse, you get just a hint of circuitry and bright light. Hubba, hubba!)

Oh, come now, Rob. Don't be a spoil sport. They can make programs that look like text, can't they? So why can't they make programs that look like pictures? Well, it is true that I have copies of the BOO programs, which are utilities for converting binary files into a format that was only printable characters. I understand that there is an MS-DOS program, called COMt, which turns COM files into *\*executable\** forms, using only printable characters. (Padgett Peterson was so taken with the idea that he wrote his Christmas card program using only printable characters.) The "text" programs, however, don't exactly look like a letter from Mom--they look like strings of garbage. Paradoxically, graphics images (realistic graphics, that is) give you even *\*less\** leeway, since the human eye is *\*very\** good at picking up anomalies.

The Tekwar virus is recovered from an imperfectly erased copy of the graphic. Under extrapolative recreation, the virus is virulent enough that just looking at it will fry your computer. (Try *\*that\** with your average copy of Stoned. "Lossy" compression wins again!) (By the way, in *\*that\** picture, the young lady has her shirt *\*on\**.)

If you look at the virus, it renders you unconscious. Fair enough: flashing lights can stimulate epileptic seizures. However, thereafter the virus slowly causes *\*physical\** degradation of your nervous system. Oh, please. What's the nerve equivalent of JMP?

Stay tuned *\*next\** week, when Bill Shatner uses the I-word. (Pay close attention when he announces the virus is loose.)

copyright Robert M. Slade, 1994 TVTEKWAR.RVW 941201

DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733



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 16: Issue 61**

**Tuesday 6 December 1994**

## Contents

- [Lots of Turkeys](#)  
[Debora Weber-Wulff](#)
  - [Fun with your phone company](#)  
[Russell Stewart](#)
  - [Pentium + Spell-Checkers](#)  
[Paul Fuqua](#)
  - [Pentium FDIV bug](#)  
[A. Padgett Peterson](#)
  - [Re: Interesting product claim](#)  
[Mathew Lodge](#)
  - [Virus alert virus alert](#)  
[Yehuda Berlinger](#)
  - [Re: Mailing list problems... \(Errors-To\)](#)  
[David Barr](#)
  - [Mailing-list deadman switch](#)  
[Steve Losen](#)
  - ["Applied Cryptography" by Schneier](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## Lots of Turkeys

*Debora Weber-Wulff* <[weberwu@tfh-berlin.de](mailto:weberwu@tfh-berlin.de)>  
6 Dec 1994 12:01:44 GMT

The "Stars and Stripes" (a "small-town" newspaper in English for the military communities in Europe, to which I am also allowed to subscribe in order to read the comics every day...) reports that the payments for the civilian employees in Germany this month were credited to the accounts of the employees twice. Seems that the payroll tape is usually run on the 24th of a month. Someone bright noticed that the 24th is turkey day, and ran the tape on the 23rd. Some other bright person also ran the tape on the 25th since the 24th was a holiday.... Suddenly they noticed that there were about 3.5 million dollars missing (good thing they have a bookkeeping system!).

The "turkeys" spent most of Saturday fussing with the system and rolling back the second set of transactions. It is reported that the civilians are hoping for another such windfall at Christmas...

Debora Weber-Wulff, Technische Fachhochschule Berlin, FB Informatik, 13353 Berlin, Germany weberwu@tfh-berlin.de <<http://sun24.tfh-berlin.de:8000/dww/>>

[Beware of Tur[n]key systems. They can gobble up lots of money. PGN]

---

### Fun with your phone company [foreshortened by PGN]

*Russell Stewart <diamond@RT66.com>*

*Tue, 06 Dec 1994 14:43:08 -0500*

[Russell submitted a longish item on how his phone company cleared a check of his for \$150, but did not credit his account. To make a long story short, he had changed his address and phone number from his parents' home, and the \$150 was credited to his OLD phone number, which was the number that appeared on his check. His father did not notice the credit on the home account. Apparently his phone company ignores the number on the bill! GROAN. PGN]

In other words, that little portion of the bill that you tear off and put in the envelope with your payment is completely useless, because they only check the phone number ON THE CHECK ITSELF. I don't know how many phone companies use this type of a system, but let this serve as a warning to anyone who has recently changed address...

Russell Stewart Albuquerque, New Mexico diamond@rt66.com

---

### Pentium + Spell-Checkers

*Paul Fuqua <pf@islington-terrace.hc.ti.com>*

*Tue, 6 Dec 94 11:40:37 CST*

On December 5, the {Dallas Morning News}, not the most technically-aware newspaper in the world, ran an article from the {San Jose Mercury News} about the recent Pentium FDIV situation.

Unfortunately, they ran it through a spell-checker first. The company names "Intel" and "Megatest" became "Until" and "Megadeath," which actually puts an interesting slant on the story.

I've only ever seen one writer's byline on computer-related articles in the DMN, so the root problem may be that no one else at the paper knows enough to catch this obvious (to us) error.

Paul Fuqua Texas Instruments, Dallas, Texas pf@hc.ti.com

[Until Megadeath Do It Part. PGN]

---

## Pentium FDIV bug

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>

Thu, 1 Dec 94 08:01:42 -0500

Interlocutor: Why did they call it "Pentium"?

Mr. Bones : Because when they added 100 to 486,  
the answer was 585.994257

---

## Re: Interesting product claim (more Pentium stuff)

Mathew Lodge <lodge@ferndown.ate.slb.com>

Tue, 06 Dec 94 12:59:28 000

Mike Kenney <mike@wavelet.apl.washington.edu> wrote

> As CPUs get more and more complex, the chance of bugs slipping through will  
> probably go up. I just hope whichever company it happens to next handles  
> the problem better than Intel.

When Inmos designed the T8 series of Transputers, they used formal methods to prove that the algorithms used in the on-chip FPU were correct. I am frankly amazed that a huge company like Intel relies solely on testing the hell out of a new chip -- which, of course, \*proves\* nothing. If a small British company like Inmos can prove an IEEE math FPU correct, why can't Intel?

Perhaps this recent debacle will convince at least some people that formal methods can be cheaper than mistakes.

Mathew Lodge, Software Engineer, Schlumberger Technologies, Ferndown, Dorset, UK, BH21 7PP lodge@ferndown.ate.slb.com (+44) (0)202 893535 x404

[We have not had any discussions on the appropriateness of formal methods in any systems, let alone critical systems, in a long time. Time to open up the Testing vs Formal Methods wars again? PGN]

---

## Virus alert virus alert

Yehuda Berlinger <yehuda@jerusalem1.datasrv.co.il>

Tue, 6 Dec 1994 10:14:47 +0200

I have been inundated with virus alerts. Somehow, this virus alert has been propagating out of control. It must be a virus in the virus alert. (Note: I don't mean to belittle the alert, but there must be some way of controlling its propagation. I have received it 4 times now from different sources.)

>I have just received this message and been asked to take it seriously:  
>There is a virus on America Online being sent by E-Mail. If you get  
>anything called "Good Times", DON'T read it or download it. It is a  
>virus that will erase your hard drive. Forward this to all your  
>friends.

>It may help them alot.

[I suppose you are lucky you only got 4 copies.

But it appears to be a complete hoax, as suspected by Rob Furr <rfurr@jazz.ncrn.net>, who was amused at the close timing of the AOL message and Michael Slavitch's item in [RISKS-16.60](#), and who added

There are idiots in the world who think it's awfully funny to cry "Wolf" as soon as someone else notices that it's theoretically possible that wolves exist. Rob F.

PGN]

---

## Re: Mailing list problems...

David Barr <barr@pop.psu.edu>

Mon, 5 Dec 1994 22:10:38 -0500

> ``A subscriber site that does not honor the "Errors-to:"

Except that "Errors-To" was introduced by sendmail, and is not in any RFC, 822 or otherwise. The 822 Police will arrest YOU for false arrest. :-)  
(The Risk in assuming the most popular implementation of a protocol is The Way Things Are. See also Return-Receipt-To:)

The correct way is to set the envelope FROM to the bounce address. On those systems which don't have envelope addresses, it's up to them on how to preserve the bounce address in-band -- which is where much of the problems with mailing loops get started.

It's surprising the number of people (and therefore the number of misconfigured mailers and gateways) which don't understand the mail specs. However, it's understandable given that 822 and 821 are 12 years old and are probably one of the most cryptic and vague out there, especially considering how critical they are to the Net. They really need to be updated and clarified.

Something like "Precedence: junk" is bad, because there's never any feedback to the system. Addresses which fail simply get tossed, and they never get removed from the list. The list grows linearly, and you waste more and more resources trying to deliver mail to addresses that go nowhere anyway.

--Dave

[Also noted by brian@nothing.ucsd.edu (Brian Kantor), who said, "If you can find errors-to in RFC822, you've got better coffee than we do."]

---

## Mailing-list deadman switch

Steve Losen <scl@sasha.acc.virginia.edu>

Tue, 06 Dec 94 11:03:26 -0500

I am a unix system administrator at the University of Virginia and we regularly run across "abandoned" mailboxes that are growing rapidly with messages from busy mailing lists. This is particularly troublesome over the summer break and winter holidays. I have noticed that some mailing lists have what I call a "deadman switch" feature, whereby the listserver periodically sends all subscribers a message requesting that they confirm their subscription by replying. Anyone who fails to reply gets unsubscribed. When a user is unsubscribed in this fashion, the listserver sends a final message with instructions for getting back on the list. I think that some of these lists are smart enough to not send requests for confirmation to members who have posted to the list recently. I think that this is an excellent feature because many folks who subscribe to lists never figure out how to get off them or never bother. Some folks get a new account and never bother to deal with mail still coming to the old one.

I encourage anyone who runs a high volume mailing list to consider using a deadman switch to ensure that mail is going to mailboxes that are actually being read.

It would also help if mailing list administrators would regularly send out a brief message with information on how to unsubscribe.

Steve Losen scl@virginia.edu phone: 804-982-4711  
University of Virginia ITC Unix Support

---

## "Applied Cryptography" by Schneier

"Rob Slade, Social Convener to the Net" <roberts@mukluk.decus.ca>  
Tue, 06 Dec 1994 15:04:46 EST

BKAPCRYP.RVW 941012

"Applied Cryptography", Schneier, 1994, 0-471-59756-2, U\$44.95  
schneier@chinet.com

%A Bruce Schneier

%C 22 Worchester Road, Rexdale, Ontario M9W 9Z9

%C 605 Third Avenue, New York, NY 10158-0012

%D 1994

%G 0-471-59756-2

%I John Wiley & Sons, Inc.

%O U\$44.95 800-263-1590 fax: 800-565-6802 800-CALL-WILEY

%O jdemarra@jwiley.com aponnamm@jwiley.com

%P 618

%T "Applied Cryptography"

For anyone who wants to study cryptography, you can save yourself a lot of time and effort by getting Schneier's book. From the simple Caesar cipher to RSA and beyond, there is nothing the book doesn't at least touch on. Protocols, techniques, algorithms, and even source code are included. A "Real World" section looks both at specific implementations and at the politics of

encryption.

Schneier notes that his work is *\*not\** a mathematical text. It is difficult to say how much of a shortcoming this is for any given reader, but a safe bet is "not much". For those who do need more rigorous treatments of specific topics, the bibliography lists almost a thousand references, all of which are described and cited within the book text at some point.

He also states that the encyclopedic nature of the book detracts from its readability. Not so. The work is both encyclopedic *\*and\** readable. Schneier has done marvelously well with what is normally a dead and dry topic. His examples are ludicrously absurd--and therefore lucid and memorable. (He even uses Monty Python's immortal phrase, "My hovercraft is full of eels" in one illustration.)

As course text, research basis or just a (serious) hobbyist's reference, this work is highly recommended.

copyright Robert M. Slade, 1994 BKAPCRYP.RVW 941012

DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733



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 16: Issue 62

Weds 7 December 1994

## Contents

- [Baby-proof keyboard handling needed](#)  
[Amos Shapir](#)
- [Network file race condition](#)  
[Andrew Koenig](#)
- [Power failure causes airline check-in chaos](#)  
[Fernando Pereira](#)
- [Pepsi promotion misfires - computer error](#)  
[John Dalbey](#)
- [Formal verification of the AAMP5 Microprocessor](#)  
[John Rushby](#)
- [Re: Formal methods and the Pentium FDIV](#)  
[Mark Stalzer](#)
- [Re: Formal verification of INMOS T800](#)  
[Patrick Campbell-Preston](#)  
[Mathew Lodge](#)
- [Re: Formal methods ...](#)  
[Steve Kilbane](#)  
[Mark Lomas](#)
- [Re: Slade's review of Schneier's "Applied Cryptography"](#)  
[Richard Schroepfel](#)
- [Self-extracting emacs elisp code](#)  
[David Blob](#)
- [Virus time](#)  
[Dwight Silverman](#)  
[Zygo Blaxell](#)  
[Reuven Lerner](#)
- [Program Announcement - ISOC 1995 Symp. Netw. & Distr. Sys. Security](#)  
[David M. Balenson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Baby-proof keyboard handling needed

*Amos Shapir <[amos@nsof.co.il](mailto:amos@nsof.co.il)>*

*Wed, 7 Dec 94 14:09:56 IST*

We were having the whole family for a Hannukah party last week. Grandpa sat at a chair next to the PC (which was up and running Windows), holding six-month-old May in his arms. Being a digital kid, she quickly reached for the keyboard. By the time we noticed and managed to turn off the computer, half the system files were gone (which is what we discovered the next day, when the system started to behave strangely).

Trying to figure out what had happened, it seems little May could only reach the bottom line of the keyboard -- but that's where the ALT, ENTER, DELETE and the arrow keys are! In Windows 3.1, ALT puts the cursor into the command menu, ENTER activates the menu item it's on; in some menu, DEL deletes the marked files...

Amos Shapir nSOF Parallel Software, Ltd. Givat-Hashlosa 49905, Israel  
amos@nsof.co.il Tel: +972 3 9388551 Fax: +972 3 9388552

---

## Network file race condition

*<ark@research.att.com>*

*Wed, 7 Dec 94 10:58:06 EST*

A story with entertainment value, albeit no clear moral:

A couple of nights ago I was working away at my workstation when the world (figuratively) collapsed: suddenly all my network connections had gone haywire. A little investigation revealed that `/etc/hosts`, the file that lists names and IP addresses for the rest of the universe, had become corrupted: it had huge quantities of null characters in it and very little useful data. How had that happened?

After some poking around and much thought, I came to the following conclusion. I've recently been setting up some machines for a few of my colleagues. The most straightforward way of getting those machines into a sensible initial state, I thought, would be to restore the dump tapes from my own machine onto theirs. After all, I keep my machine in pretty decent shape.

Of course there was no need to restore my home directory on each machine. Instead, I told each of the other machines that my home directory was really a link to the mounted file system that contained my home directory on my 'home' machine. All pretty routine so far, but that turned out to be cause number 1.

Cause number 2 was that when I cloned my machine, what I cloned included `/usr/spool`, the directory with all the spool files. That directory includes files that tell cron, a program that starts background jobs at particular times, what jobs to start. That meant that the 'midnight' job that normally ran on my home machine now ran automatically on each of several machines. Because my home directory was mounted on each of these machines, that job did its thing simultaneously several times in the same directory.

Cause number 3 was that my midnight job, among other things, extracts a complete new /etc/hosts file from one of our other servers and installs it. It checks that what it got is sane, to defend against /etc/hosts becoming empty when the server is down, but of course it doesn't defend against having several instances running at the same time. So what must have happened is that two of those instances finally hit the same file at the same time, causing parts of it to overlay other parts and general chaos to ensue.

Andrew Koenig ark@research.att.com

---

## Power failure causes airline check-in chaos

*Fernando Pereira <pereira@research.att.com>*

*Tue, 6 Dec 1994 23:21:53 -0500*

This Monday, 5 December 1994, I was traveling with a colleague from Denver Stapleton to Newark on United flight 302, supposed to leave at 6:06 PM. When we got to the airport at 3:30 (in plenty of time to beat threatened snow), the baggage check-in agents were not actually checking-in passengers but simply tagging bags by hand, because a power failure had brought down the check-in database servers. After the bags were checked in, we were directed to another agent that looked up the gate for flight 302 on a printout. Actual passenger seat assignment and check-in was to be done manually at the gate. Since we were early, we waited at the gate until 5 PM, not wanting to bug the overworked gate agents until near our scheduled departure. But when we talked to the gate agent soon after 5 PM, she told us that she had no information about flight 302; some other flight was due to leave that gate too close to 6:06 PM to allow time for flight 302, and she had no way of finding out where 302 was supposed to be. She finally told us to call the central 800 number for United reservations to check the gate info! My colleague is a United Premier member. He called the Premier help desk, who gave him another gate number for a supposedly on-time departure. He communicated that information to the original gate agent, who proceeded to announce it over the PA for other 302 passengers without further confirmation from any other authority.

We went to the new gate, where we found neither plane nor gate agents. We asked the agent at the next gate for help. He knew nothing about 302, and expected some other flight to use the empty gate. His paper notes indicated the original gate for 302. But he eventually called around, and found out yet another supposed gate for the flight.

Third time lucky. That turned out to be the correct gate, although its electronic flight info display was showing a different flight. All the departures monitors in the terminal were also showing outdated and scrambled information without any indication of its incorrectness. Enterprising gate agents were taping paper signs with correct flight numbers over the bogus electronic signs.

But the problems were not over. The plane for flight 302 arrived, we boarded, and were supposed to leave just 20 or so minutes late. Except that

the flight crew was delayed in an incoming flight, and that information, normally handled by the downed computer system, was not made available to the ground staff for assignment of an alternate crew. We ended leaving around 1 1/2 hour late.

This all happened in a relatively light traffic non-holiday Monday, in pretty good weather (the snow didn't materialize). I can't imagine what the chaos would have been like around a major holiday. It was clear from all our interactions with all the gate agents that they were not operating according to a well-designed, well-drilled manual backup procedure. They behaved professionally for the most part in a difficult situation, but much of what they were doing seemed decided on the spot, from personal initiative, and without good phone access to an authoritative manual database of flights and gates, even though that information was obviously still available to the air-traffic and airport systems, given that flights were still landing and taking off.

Fernando Pereira, 2D-447, AT&T Bell Laboratories, 600 Mountain Ave, PO Box 636 Murray Hill, NJ 07974-0636 [pereira@research.att.com](mailto:pereira@research.att.com)

---

### **Pepsi promotion misfires - computer error**

*John Dalbey <[jdalbey@galaxy.csc.calpoly.edu](mailto:jdalbey@galaxy.csc.calpoly.edu)>  
Wed, 7 Dec 1994 11:05:27 -0800 (PST)*

Time magazine (Aug 9) reports a computer error in a Pepsi promotional lottery in the Philippines. The computer generated 800,000 winning numbers instead of 18. Obviously, Pepsi didn't pay the \$32 billion in prize money their mistake would have cost them.

Pepsi has paid nearly \$10 million in "appeasement" efforts (\$20 "goodwill" prize), but this apparently didn't satisfy disgruntled "winners." Over 22,000 people, each of whom believed they had won the \$40,000 prize, have filed about 5,000 criminal and 700 civil suits. The Philippine Senate Trade Committee faults the company for "gross negligence" and "misleading or deceptive advertising."

If anyone knows any technical details about the nature of this "computer error," I would like to hear about them.

John Dalbey, Computer Science Dept, Cal Poly, SLO, CA [jdalbey@calpoly.edu](mailto:jdalbey@calpoly.edu)

---

### **Formal verification of the AAMP5 Microprocessor**

*John Rushby <[RUSHBY@csl.sri.com](mailto:RUSHBY@csl.sri.com)>  
Wed 7 Dec 94 11:41:18-PST*

With messages in RISKS about formal verification (not) being applied to commercial processors, this might be a good time to mention the work that's going on across the hallway from PGN:

"Formal Verification of the AAMP5 Microprocessor:  
A Case Study in the Industrial Use of Formal Methods"

by Steven P. Miller (Collins Commercial Avionics) and Mandayam Srivas (SRI)

To be presented at WIFT '95: Workshop on Industrial-Strength Formal  
Specification Techniques, April 5-8, 1995, Boca Raton, Florida USA.

Available over the web through <http://www.csl.sri.com/aamp5.html>  
or by ftp from ftp.csl.sri.com/pub/reports/postscript/aamp5.ps.gz

The AAMP5 doesn't have floating point, but it is a real processor with  
a pipeline, microcode, and 500,000 transistors (it's a derivative of  
the AAMP2, of which there are 30 on board each 747-400).

John

---

### Re: Formal methods and the Pentium FDIV (Lodge, [RISKS-16.61](#))

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

*Wed, 7 Dec 1994 09:22:40 +0800*

The NY Times (or was it LA?) a few days ago reported that the double  
precision fddiv problem in the Pentium is due to a table that was incorrectly  
copied from the 486 -- not an algorithmic bug. Many formal approaches would  
not have caught this kind of error since it would have been natural to  
assume that the table was correct (I mean, after all, it was generated by  
computer!) Also, one of the floating point bugs in a previous x86 processor  
(I think it was the atan bug in the 486) was due to electrical difficulties  
-- the algorithm was correct, but the electrons had different ideas in a  
certain case. This is a class of errors that only testing or circuit  
simulation with accurate device models can catch.

Mark Stalzer, mas@acm.org

[Also noted by "Jeffrey P. Bradford" <jbradfor@ecn.purdue.edu>, who added,  
"We all know computers make mistakes, either HW or SW, and any results  
from computers need to be compared against common sense." PGN]

---

### Re: Formal verification of INMOS T800 (Lodge, [RISKS-16.61](#))

*Patrick Campbell-Preston <PATRICKCP@shapel.ug.eds.com>*

*Wed, 07 Dec 1994 13:33:12 -0300 (BST)*

When the T800 came out, my then employers (FEGS Ltd) were working on a  
research project in collaboration with INMOS and several other partners.

At one point INMOS told us they had had to halt production of T8's after  
a bug had been found in the floating-point microcode, resulting in the  
wrong result being given for some IEEE-defined special case (I think  
it was zero divided by zero giving the wrong flavour of NaN). I think

the bug was found by the formal verification process, of which they were certainly very proud.

One more point is worth mentioning: the T800 is a very simple chip architecture compared to something like the Pentium, and I would guess formal verification of the latter would be a much larger task.

Patrick

---

**Re: Formal verification of INMOS T800 (re Patrick Campbell-Preston)**

*Mathew Lodge <lodge@ferndown.ate.slb.com>*

*Wed, 7 Dec 94 17:53:40 GMT*

Perhaps this is a case of less RISK for RISCs! (sorry, couldn't resist)

Inmos formally proved only the FPU: they didn't do it for the whole processor. Does the Pentium implement so many more floating point operations that proof is intractable?

Mathew Lodge, Software Engineer, Schlumberger Technologies, Ferndown, Dorset, UK, BH21 7PP lodge@ferndown.ate.slb.com (+44) (0)202 893535 x404

---

**Re: Formal methods ... (Lodge, [RISKS-16.61](#))**

*Steve\_Kilbane <steve@cegeleproj.co.uk>*

*Wed, 7 Dec 1994 08:56:00 +0000*

Proving that the algorithms used are correct is one thing, but getting a correct implementation of those algorithms in silicon is another, and that's where the testing comes in.

Steve\_Kilbane@cegeleproj.co.uk

---

**Re: Formal methods ... (Lodge, [RISKS-16.61](#))**

*<Mark.Lomas@cl.cam.ac.uk>*

*Wed, 7 Dec 1994 18:08:02 GMT*

Some staff from Inmos gave a talk here some time ago on their procedure for verifying a floating-point implementation. Their experience was slightly more interesting than Mathew suggested.

Apparently, in addition to their formal model they had a "known correct" implementation built by a competitor. All tests were verified against this reference implementation.

At one point during testing they found that their implementation disagreed with the reference implementation and spent quite some time trying to diagnose

the fault. It turned out that their implementation had been correct first time, but that they had discovered a bug in a competitor's product.

No prizes for guessing who built the reference implementation

Mark

---

## Rob Slade's review of Schneier's book "Applied Cryptography"

*"Richard Schroepel" <rsc@cs.arizona.edu>  
Wed, 7 Dec 1994 13:27:37 MST*

Rob Slade's review of Schneier's book "Applied Cryptography" should have mentioned that the book contains a substantial number of typos, and that Schneier offers an errata sheet (schneier@chinet.com). This will be especially important if you try to use the programs in the appendix. I like the book.

Rich Schroepel rcs@cs.arizona.edu

---

## Self-extracting emacs elisp code

*David Blob <blob@syl.dl.nec.com>  
Wed, 7 Dec 1994 11:57:50 -0600*

With all this talk about self extracting mail "viruses", a friend showed me that in emacs (which I use to read mail, along with vm) has the ability to self-extract elisp code. This feature seems to be turned on by default, and it not only applies to mail read with emacs, but rather every file visited (when the feature is on, of course).

The way it works is by having a line which reads "Local Variables:" followed by the lisp variables you would like to set...well, it may seem petty, but you can execute programs, make connections and much more through cleverly written elisp code contained within.

It's simple to turn off, at any rate...

```
(setq enable-local-variables f) ;; turns off feature (in emacs 19)
(setq enable-local-variables 1) ;; makes it ask first (in emacs 19)
(setq inhibit-local-variables t) ;; turns off feature (in emacs 18)
```

Anyhow, I think the risks here speak for themselves...

---

## Virus time

*Dwight Silverman <Dwight.Silverman@chron.com>  
Tue, 6 Dec 1994 21:05:18 -0600 (CST)*

Shareware has a bad rap as a carrier of computer viruses. But one of the commercial software industry's dirtier little secrets is that viruses often get transmitted via shrink-wrapped boxes in stores.

Or, sometimes, viruses just get sent to computer writers.

A California company called Bit Jugglers called me today to say a title they'd sent me, Kids World, was infected with a virus. This only happened to the copies sent to the press -- those folks who write about computer software in magazines or newspapers. The virus did not make it into copies shipped to stores.

Bit Jugglers urged me to destroy my copy of Kids World. And if I'd installed the software (I have not), they would have sent me the latest version of McAfee's Scan, a virus detection program. A new, clean copy is on its way to my desk.

The moral of the story is obvious. Trust NO floppy -- you don't know where it's been. Scan everything.

Dwight Silverman

The Houston Chronicle, Computer columnist [dwight.silverman@chron.com](mailto:dwight.silverman@chron.com)  
713-220-6873 Fax: 713-220-7273 Audiotext: 713-468-7866 ext. 1001

---

### **Virus \_IS\_ virus alert (Berlinger, [RISKS-16.61](#))**

*Zygo Blaxell <[zblaxell@miranda.uwaterloo.ca](mailto:zblaxell@miranda.uwaterloo.ca)>  
Wed, 7 Dec 1994 03:41:04 -0500*

> I have received it 4 times now from different sources.)

Obviously, the alert itself is the virus. Watch:

<>I have just received this message and been asked to take it seriously:

This gets the virus scheduled on the CPU (note that it occurs at the beginning of execution).

<>There is a virus on America Online being sent by E-Mail. If you get

This is the target architecture and operating system: AOL users. Note that it also works on similar architectures with different operating systems.

<>anything called "Good Times", DON'T read it or download it. It is a  
<>virus that will erase your hard drive.

This is something that looks like a useful message to fool the user while the virus does its work.

<>Forward this to all your friends.

<>It may help them alot.

...and this is the propagation code. ;-)

Zygo Blaxell, Math student at the University of Waterloo.  
System/network admin for the Computer Science Club and miranda.

---

## Good Times

*Reuven Lerner <reuven@hpwadck.wal.hp.com>*

*Wed, 7 Dec 1994 09:51:05 -0500*

I'm sure that I am not the only RISKS reader who has been bombarded by warnings regarding the supposed "Good Times" virus. Just about all of the warnings I received were forwarded from two or three previous people, said that the virus was distributed from America On-Line, and claimed that if you were to download or read the message (which had a subject of "Good Times"), your hard disk could be reformatted.

Each copy of the warning then suggested that people forward the warning to as many other users and mailing lists as possible, because of the severity of the problem.

I've seen at least one announcement from CIAC (at least, I *\*think\** it was from CIAC) telling people that there is indeed no virus, that most mail readers won't automatically execute programs sent via e-mail, and that people generally shouldn't worry.

There seem to be several risks associated with this incident:

- (1) People don't understand what e-mail can and cannot do. Most of the people forwarding the warnings didn't understand the difference between viewing a mail message and turning the contents of that message into an executable program, let alone the fact that different platforms work differently and thus would require separate viruses.
- (2) Rumors spread quickly. I was amazed to see just how fast this rumor spread; within a 24-hour period, I saw a dozen or so copies of the warning on five or six different mailing lists. People wanted to help their fellow users (a good thing), but passed the warning on without verifying the rumor's validity (a bad thing). You could probably make a good argument that the warning itself was a virus!
- (3) Explanations spread slowly. More than two days after I first saw the virus warning, people continued to forward copies of it to various mailing lists -- even after I and others told list members that the virus announcement was probably a hoax. It will probably be another few days before the CIAC warning (along with assurances from computer experts) reaches all of the people who are no longer sure whether it is safe to read their e-mail.

(4) Bugs do exist. The fact is that there probably are holes in mail readers that will do nasty things to people's files and accounts. But now that people have been told not to worry, they'll take future warnings less seriously. Without a universally known and trusted authority on these issues -- and let's face it, most users would probably trust their friends more than CIAC or CERT -- this may turn into the computer equivalent of the children's story, "The Boy Who Cried Wolf."

Reuven

---

## Program Announcement - ISOC 1995 Symp. Netw. & Distr. Sys. Security

"David M. Balenson" <balenson@tis.com>

Wed, 07 Dec 1994 13:57:48 -0500

David M. Balenson, Program Co-Chair, ISOC '95 SNDSS  
Trusted Information Systems, 3060 Washington Rd., Glenwood, MD 21738 USA  
balenson@tis.com; tel 301.854.6889; fax 301.854.5363

THE INTERNET SOCIETY SYMPOSIUM ON  
NETWORK AND DISTRIBUTED SYSTEM SECURITY  
16-17 FEBRUARY 1995  
CATAMARAN HOTEL - SAN DIEGO, CALIFORNIA

The symposium will bring together people who are building software and/or hardware to provide network and distributed system security services. The symposium is intended for those interested in the more practical aspects of network and distributed system security, focusing on actual system design and implementation, rather than in theory. We hope to foster the exchange of technical information that will encourage and enable the Internet community to apply, deploy and advance the state of the available security technology.

P R E L I M I N A R Y P R O G R A M  
[meals, breaks, registration info removed by PGN]

WEDNESDAY, FEBRUARY 15

6:00 P.M. - 8:00 P.M.  
REGISTRATION AND RECEPTION

THURSDAY, FEBRUARY 16

7:30 A.M.  
CONTINENTAL BREAKFAST

8:30 A.M.  
OPENING REMARKS

9:00 A.M.  
SESSION 1: DIVERSE APPROACHES TO SECURITY AT THE NETWORK LAYER

Chair: Stephen T. Kent (Bolt, Beranek and Newman, USA)

Multicast-Specific Security Threats and Counter-Measures, Tony Ballardie and Jon Crowcroft (University College London, United Kingdom).

Design of a Key Agile Cryptographic System for OC-12c Rate ATM, Daniel Stevenson, Nathan Hillery, Greg Byrd, and Dan Winkelstein (Microelectronics Center of North Carolina - MCNC, USA).

IpAccess: An Internet Service Access System for Firewall Installations, Steffen Stempel (University of Karlsruhe, Germany).

11:00 A.M.

SESSION 2: PANEL: SECURITY ARCHITECTURE FOR THE INTERNET INFRASTRUCTURE

Chair: Robert W. Shirey (The MITRE Corporation, USA)

Security for the Internet Protocol (IP) and IP Next Generation, Paul A. Lambert (Motorola, USA).

Security for the Internet Domain Name System, James M. Galvin (Trusted Information Systems, USA).

Security of Routing Protocols in the Internet, Gary Scott Malkin (Xylogics, USA).

Security Approaches to Routing in the Internet, Sandra L. Murphy (Trusted Information Systems, USA).

2:00 P.M.

SESSION 3: OFF-LINE OBJECT DISTRIBUTION SECURITY

Chair: Jeffrey I. Schiller (Massachusetts Institute of Technology, USA)

Trusted Distribution of Software Over the Internet, Aviel D. Rubin (Bellcore, USA).

Location-Independent Information Object Security, John Lowry (Bolt Beranek and Newman, USA).

3:30 P.M.

SESSION 4: INTERNET PAYMENTS

Chair: Ravi Ganesan (Bell Atlantic, USA)

Electronic Cash on the Internet, Stefan Brands (Centrum voor Wiskunde en informatica - CWI, The Netherlands).

PANEL: Internet Payment Mechanisms - Requirements and Architecture

Chair: Ravi Ganesan (Bell Atlantic, USA)

Panelists: B. Clifford Neuman (Information Sciences Institute, USA), David Crocker (Brandenburg Consulting, USA), and others TBD

7:00 P.M. DINNER BANQUET

FRIDAY, FEBRUARY 17

8:30 A.M.

SESSION 5: SECURITY MONITORING TOOLS - PRACTICE AND EXPERIENCE

Chair: Michael St. Johns (Advanced Research Projects Agency, USA)

NERD: Network Event Recording Device: An Automated System for Network Anomaly Detection and Notification, David G. Simmons and Ronald Wilkins (Los Alamos National Laboratory, USA).

An Overview of SNIF: A Tool for Surveying Network Information Flow, Jim Alves-Foss (University of Idaho, USA).

Distributed Audit Trail Analysis, Abdelaziz Mounji, Baudouin Le Charlier, Denis Zampunieris and Naji Habra (Facultes Universitaires de Namur - FUNDP, Belgium).

10:30 A.M.

SESSION 6: AUTHENTICATION AND AUTHORIZATION

Chair: B. Clifford Neuman (Information Sciences Institute, USA)

SESAME V2 Public Key and Authorisation Extensions to Kerberos, Piers McMahon (ICL, United Kingdom).

Yaksha: Augmenting Kerberos with Public Key Cryptography, Ravi Ganesan (Bell Atlantic, USA).

GSS-API Security for ONC RPC, Barry Jaspan (OpenVision Technologies, USA).

1:30 P.M.

SESSION 7: MECHANISMS OF IDENTITY - THE CERTIFICATE INFRASTRUCTURE

Chair: Hilarie Orman (University of Arizona, USA)

A Certificate Management System: Structure, Functions and Protocols, Nada Kapidzic and Alan Davidson (Stockholm University & Royal Institute of Technology, Sweden).

PEMToolkit: Building a Top-Down Certification Hierarchy for PEM from the Bottom Up, Alireza Bahreman (Bellcore, USA).

A New Approach to the X.509 Framework: Allowing a Global Authentication Infrastructure Without a Global Trust Model, Suzan Mendes (TS-E3X - Research and Development Center, France) and Christian Huitema (INRIA, France).

3:30 P.M.

SESSION 8: PANEL: SECURITY ISSUES FOR MOSAIC AND THE WORLD WIDE WEB

Chair: Fred Avolio (Trusted Information Systems, USA)

Panelists: Peter J. Churchyard (Trusted Information Systems, USA), Allan M. Schiffman (Enterprise Integration Technologies, USA), and Bill Cheswick (AT&T Bell Laboratories, USA)

GENERAL CHAIR

James T. Ellis, CERT Coordination Center, Carnegie Mellon University

PROGRAM CO-CHAIRS

David M. Balenson, Trusted Information Systems

Robert W. Shirey, The MITRE Corporation

FOR MORE INFORMATION, contact Gloria Carrier by phone at (703)-883-4508 or via email to [gcarrier@mitre.org](mailto:gcarrier@mitre.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 16: Issue 63**

**Friday 9 December 1994**

## Contents

- ["High-Tech Can Hinder Policy Work"](#)  
[PGN](#)
- [Laptop proscription](#)  
[Bob Morris](#)
- [Our police and media in action \[RF interference\]](#)  
[Lynn Gold](#)
- [Digital cash on the web -- comments?](#)  
[Justin Wells](#)
- [New printer font: Sloppy Handwriting 14pt](#)  
[Norman H. Cohen](#)
- [Multicast backbone blunder \[risks of hidden transmission\]](#)  
[Alan Clegg](#)
- [A Question for the Community regarding National Crypto Policy](#)  
[Herb Lin](#)
- [Problems with compiler optimisation \(Pentium related\)](#)  
[Martin Poole](#)
- [Risk of \\_not\\_ using floating point.....](#)  
[David Lesher](#)
- [Re: Formal methods and the Pentium FDIV](#)  
[Tim Bradshaw](#)
- [It's all my fault, really \[re: Good Times\]](#)  
[Martin Minow](#)
- [Good Times is a \\*meta\\*virus](#)  
[Joe Chew](#)
- [Good Times is a Meme](#)  
[Keith Henson](#)
- [Re: Schneier's book "Applied Cryptography"](#)  
[Y. Radaï](#)
- [Re: Fun with your phone company](#)  
[Geoff Kuenning](#)  
[Russell Stewart](#)
- [More on network file race condition](#)  
[Andrew Koenig](#)
- [Rights and Responsibilities of Participants in Networked Communities](#)  
[Herb Lin](#)

- [Searching RISKS et al.](#)  
[Frederick B. Cohen](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## "High-Tech Can Hinder Policy Work"

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

Fri, 9 Dec 94 10:15:03 PST

The Supreme Court is divided over a case involving false arrest due to erroneous computer data, attributed to human error. Ruth Bader Ginsburg was quoted thusly: "As automation increasingly invades modern life, the potential for Orwellian mischief grows." Antonin Scalia countered that nothing is gained by excluding evidence of true wrongdoing because some subordinate did not purge outdated information from a computer system.

The case arose after Isaac Evans was stopped in 1991 in Phoenix for a minor traffic violation; he was arrested because of a hit identifying an outstanding warrant --- although though that warrant had been previously "quashed" and should have been removed from the database. Furthermore, the arresting officer then detected the presence of marijuana. The Court is reviewing whether, under the circumstances, that evidence can be used in a trial for drug possession in light of the false arrest.

[Source: A Washington Post item appearing in the San Francisco Chronicle, 8 Dec 1994]

---

## Laptop proscription

<RMorris@DOCKMASTER.NCSC.MIL>

Thu, 8 Dec 94 20:42 EST

Act 4 of Shakespeare's 'Julius Caesar' opens with Mark Antony, Octavius, and Lepidus meeting to work out the proscription that is to follow Caesar's murder. To be proscribed means that you are rubbed out and your property confiscated by the people doing the proscribing. Clearly, proscription is a significant data processing problem since both the rubbing out and the division of spoils have to be worked out to the satisfaction of the proscribers.

In a recent production of Julius Caesar by the Folger Shakespeare Theater in Washington, D.C., there was only a modest amount of tittering when one of the proscribers arrived on stage to do the necessary work with a laptop.

Bob Morris

[I presume the character was ProScribe rather than ProLaTeX?

Was Folger in his Cups? or Caps?

(Sorry. That multipun is only for OLD Washington logicians.) PGN]

[Marc Rotenberg added, out of band, i.e., not in [RISKS-16.63](#) as mailed:

If Caesar lived until proscribed at the Folger,

he was obviously good to the last drop.]

---

## Our police and media in action

Lynn Gold <figmo@netcom.com>

Wed, 7 Dec 1994 22:46:34 -0800

I got the following from ba.broadcast today and felt it was worth sharing here....

The following is an INEXACT quote from KCBS, one of our all-news radio stations:

...the police have called the bomb squad to defuse the hand grenades. Until the grenades are defused, the police have prohibited the use of 2-way radios in the vicinity of the scene here, so we are reporting by cellular phone instead of radio.

Somebody needs to tell the folks at KCBS the meaning of "radio."

Somebody also needs to give the police a clue.

--Lynn

---

## Digital cash on the web -- comments?

justin wells <rjwells@undergrad.math.uwaterloo.ca>

Wed, 7 Dec 1994 23:13:14 -0500

There are a lot of people over in the comp.infosystems.www.\* newsgroups who are seriously talking about using the World Wide Web (WWW) as a digital cash system. I get the impression they want to do this in some number of months or a year.

Apparently they want to use the FORMS feature supported by most web browsers in conjunction with some sort of encryption algorithm. The idea is you connect to a commercial site, see something you want to pay for, fill your credit card number in on the form, and transmit it back to the http server with some kind of encryption. They're talking about using some encryption technique present or expected in the Netscape browser.

As far as I can tell this method will not involve any sort of authentication, and it will only secure data after it has left your browser and before it gets decrypted.

Are these people for real? This has to be one of the most foolish things I've heard in a long time, but I'd like to hear some comments from RISKS readers -- I'm no expert in these matters. It might also be an idea to crosspost a bit of the discussion back to \*.www.\* to wake these folks up.

Justin Wells rjwells@uwaterloo.ca

---

## **New printer font: Sloppy Handwriting 14pt**

*"Norman H. Cohen" <ncohen@watson.ibm.com>  
Fri, 9 Dec 94 09:43:21 EST*

I received an envelope in the mail yesterday that was immediately identifiable as junk mail by the word "URGENT" printed in large red letters imitative of a rubber stamp. Thus I was taken aback that the envelope appeared to be hand-addressed with a felt-tip pen.

Closer examination revealed that the apparently sloppily scrawled capital N in my first name was identical to that in "NY", the even sloppier lower-case A in my first name was identical to those in my street name and city name, and so forth. Nonetheless, to the casual observer, the effect was quite convincing.

The risk is an old one--the use of computers to perpetrate a deception.

---

## **Multicast backbone blunder [risks of hidden transmission]**

*Alan Clegg <abc@black-ice.gateway.com>  
Thu, 8 Dec 1994 13:14:57 -0500 (EST)*

While watching the multicast of the current IETF session [Automatic Address Configuration], I was presented with a message imposed by the broadcasting group of "susanp@spinnaker please stop broadcasting".

I looked at the monitor, and sure enough, there was *\*another\** video session being broadcast. For the next ~5 minutes, everyone on the multicast backbone was allowed to watch as susanp worked on some html markup [using hotmetal], then responded to a bit of e-mail.

The risk turns out to be that the newest version of the NV video transmission software allows you to transmit video across the mbone without a camera... any window or cursor-followed region will be happily transmitted to the world... It is not obvious in ANY way that you are actually transmitting any information...

I called the person listed in the WHOIS database for the address range that Susanp was in and the session went away, BUT... what would have happened if susanp had started doing something that was more company confidential? Since folks are recording the multicast digitally, all it would take is one screen shot with private information..

- abc

---

## **A Question for the Community regarding National Crypto Policy**

<CRYPTO@nas.edu>

Fri, 09 Dec 94 10:30:00 EST

As many of you know, the National Research Council is undertaking a study of national cryptography policy (description available on request to CRYPTO@NAS.EDU). This note is the first of a number of questions that will be posted to the Internet community in our attempt to solicit input on a broad scale. Please circulate this request to anyone that you think might be able to contribute.

The question of this posting is the following:

How, if at all, do capabilities enabled by new and emerging technology in telecommunications (e.g., key-escrow encryption technologies, digital telephony) and electronic networking make it *easier* for those who control that technology to compromise and/or protect the interests of individual end users? Please use as the standard of comparison the ease *today* of compromising or protecting these interests. We are interested in scenarios in which these interests might be compromised or protected both individually and on a large scale. Please be sure to tell us the interests you believe are at stake.

Please send your comments on this question to CRYPTO@NAS.EDU.

---

### **Problems with compiler optimisation (Pentium related)**

<mpoole@heac006.gb.ec.ps.net>

Wed, 7 Dec 1994 11:59:51 +0000 (GMT)

You may amused/horrified to hear of an incident that occurred at a major city bank last week here in the UK.

On hearing of the Pentium bug, they decided to test all of their machines to see which had the problem. They compiled up a test program and checked all of their Pentium based machines and discovered that all of them had the fdiv bug. They decided to be extra cautious and run the same program on all the other machines. To their horror all of the 486 machines exhibited the same problem.

After several days of headless chicken impersonations, a more-level head decided that something must be awry and called in a good friend of mine who in short order discovered their mistake.

The test program was compiled on a Pentium box and had the sum performed with constants. The compiler had noticed the use of constants and had performed the sum there and then, putting the result in the executable to be printed on demand on whichever box it was run on.

The risks involved are obvious but the solution is less so. Even if the sum is done using variables, what is to stop the compiler from noticing that the values do not change between initialisation and the time of performing the calculation, and cause the same problem ?

(Yes, I know. Use functions, pass parameters. But what if it gets in-lined, and then optimised ?)

Admittedly this only normally occurs on binaries that are shipped for alternative platforms, but how many software houses use the smaller chips (386/486) as the main compile engine before shipping ? And of course, users who have Pentiums without the bug, but use software compiled by a chip with it are also susceptible.

The effects and problems of this are going to be with us for a long time.

Martin Poole, Perot Systems Europe  
mpoole@heac006.gb.ec.ps.net mpoole@cix.compulink.co.uk

---

### **Risk of `_not_` using floating point.....**

*David Leshner <wb8foz@netcom.com>  
Fri, 9 Dec 1994 10:38:27 -0500 (EST)*

I spent 3 hours holding in the queue for XXX tech support before I got to speak to a person. When I did, I mentioned my wait. He apologized for the delay, then observed that his 'hold-time' counter had overflowed at 99 minutes.....

Such invalid data should do wonders for their staffing projections.

---

### **Re: Formal methods and the Pentium FDIV (Stalzer, [RISKS-16.62](#))**

*Tim Bradshaw <tfb@edinburgh.ac.uk>  
Fri, 9 Dec 94 00:57:01 GMT*

> Many formal approaches would not have caught this kind of error ...

I haven't followed all the arguments about random testing, but it's also the case that random testing is not appropriate for this sort of problem. If you have something like a lookup table in there, it really does make sense to make sure that you test *\*all\** the entries in that table: trying to do this with random numbers is crazy. As to trusting it because it was generated by computer: well, I wouldn't trust *\*anything\** that was easy to check if I was about to make millions of dollars worth of it.

--tim

---

### **It's all my fault, really [re: Good Times]**

*Martin Minow <minow@apple.com>  
Thu, 8 Dec 1994 08:04:59 -0800*

You may have received a few messages recently regarding a supposed computer

virus spread through the mail. Unfortunately, it's nothing new -- in fact, it was announced in a RISKS submission not too long ago. With the kind help of the RISKS moderator (no doubt, digging out from under his own avalanche of reports), I am enclosing it for your consideration.

Martin Minow minow@apple.com (note new address)

RISKS-LIST: RISKS-FORUM Digest Friday 1 April 1988 Volume 6 : Issue 53

FORUM ON RISKS TO THE PUBLIC IN COMPUTERS AND RELATED SYSTEMS  
ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator  
[...]

Date: 1 Apr 88 00:00

From: minow%thundr.DEC@decwrl.dec.com

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922)

Subject: Virus attacks RISKS

Today, I'm afraid I must confess that one of my recent postings to RISKS contained a Virus that Peter (no doubt inadvertently) distributed to the RISKS audience. The virus doesn't infect your programs or data files directly, but in a manner analogous to the "Christmas card" virus discussed here a few months ago, it causes increased network traffic.

As the virus establishes itself, you will note its affect by the increased amount of electronic mail you receive every day. For some of you, the increase is linear; but for others, I'm afraid you're on the early part of a exponential curve.

Although the virus was easy to create, I'm afraid that I don't know how to cure it. In fact, I believe I'm beginning to note its effects on my own system.

Humbly, Martin Minow

[PS: No avoid another visit from corporate security, please take careful note of the date of the original submission.]

[PPS: No, I didn't hack the mail protocol to get that date: I just stayed up late that evening.]

---

### Good Times is a \*meta\*virus ([RISKS-16.62](#))

*Ad absurdum per aspera* <JTCHW@lbl.gov>

Wed, 07 Dec 1994 16:54:35 -0800

Naah -- "Good Times" is the first \*meta\*virus. The target is available bandwidth itself; it acts by getting well-meaning users to send virus warnings to huge, massively overlapping mailing lists. :)

Joe "Dyn-o-mite!" Chew

---

### Good Times is a Meme (Keith Henson)

<hkhenson@cup.portal.com>

Thu, 8 Dec 94 11:26:38 PST

In [RISKS 16.62](#) Zygo Blaxell (zblaxell@miranda.uwaterloo.ca) and Reuven Lerner <reuven@hpwadck.wal.hp.com> both make good points re the "Good Times" 'virus' where the message about a virus is *\*itself\** a virus! (With possibly bad long term effects.) Computer viruses & human fads (like passing on the Good Times warning) both fit the model of a meme. (See *\_Selfish Gene\_* by Richard Dawkins.) A meme is one type of *\*replicating information pattern\**, genes are the other main class. Putting a class name such as "meme" on Good Times helps us group things/events into classes where we can expect analogous effects.

What computers and fast communications have done is to radically change the replication constants for memes, and to make unworkable the controls society has tried to put on such things.

Keith Henson (whose articles on memes are widely available on the net.)

[Re: Joe Chew's previous item: *\*Meme chose?\** PGN]

---

### Re: Rob Slade's review of Schneier's book "Applied Cryptography"

Y. Radai <RADAI@vms.huji.ac.il>

Thu, 8 Dec 94 14:32 +0200

> ... the book contains a substantial number of typos ...

This is all too correct. I should like, however, to add three points:

(1) The book contains not only many typos, but also a number of serious errors in its descriptions of some of the algorithms. (I pointed out several of these last June; copies of my posting are available from me by e-mail.)

(2) While Schneier himself maintains a cumulative errata sheet, the publisher (Wiley) apparently refuses to include it with copies of the book which have been distributed since the appearance of the errata sheet.

(3) The good news is that Schneier is preparing a second edition, which will, of course, correct all known errors. It will also contain several new sections not present in the first edition.

Y. Radai, Hebrew Univ. of Jerusalem, Israel, RADAI@VMS.HUJI.AC.IL

---

### Re: Fun with your phone company (Stewart, [RISKS-16.61?](#))

Geoff Kuenning <geoff@FICUS.CS.UCLA.EDU>

Wed, 7 Dec 94 17:47:36 -0800

As one who worked on bill-payment ("remittance processing") systems many years ago, I find this conclusion [take the phone number off the check, not the stub] highly implausible, to put it mildly. A phone, utility, or credit-card company in a moderately large city must process literally

hundreds of thousands of payments every day (divide the phone population by 30). The return portion of the bill is carefully encoded with many things, including both the account number and the amount due. That way, when the human operator types in the amount of the check, it is assumed correct if it matches the amount due, saving a costly verification step. Since the bill stub \*has\* to be OCR'ed, why would anyone build a complex and expensive system to scan the check for a phone number, printed in an unknown location in an arbitrary typeface (if it's present at all) instead?

It is far more likely that Russell accidentally sent in the wrong half of the stub, or no stub at all, and a human somewhere was faced with trying to credit the proper account with his payment. Since the phone number was on the check, the human assumed it represented the proper account -- an unjustifiable assumption, but an understandable one when you consider that there are thousands of these errors to deal with every day, so that it's not practical to make a phone call to verify the assumption, and the customer would probably get very upset if you mailed the check back without cashing it.

The RISK here is not a computer risk, but simply that it is always unfortunate to fall through the cracks of a system that is too big to give individualized service.

Geoff Kuenning g.kuenning@ieee.org geoff@ITcorp.com

---

**Re: Fun with your phone company (Kuenning, [RISKS-16.63](#))**

*Russell Stewart <diamond@RT66.com>*

*Wed, 7 Dec 94 21:06:35 MST*

>As one who worked on bill-payment ("remittance processing" systems many >years ago, I find this conclusion highly implausible, to put it mildly.

So would I! But I am only repeating to you what the woman at the phone company told me; and my \$150 \*was\* credited to my dad.

Actually, on further reflection, I've come to the conclusion that it probably \*wasn't\* an automatic scanner, but a human being. I suppose that sort of invalidates this as a Technological RISK.

>It is far more likely that Russell accidentally sent in the wrong half >of the stub, or no stub at all, and a human somewhere was faced with >trying to credit the proper account with his payment.

No, I sent in the correct portion of the bill, as I always do. Believe me, if you'd had the experiences I've had with the local US West office, you wouldn't be so skeptical.

Russell Stewart Albuquerque, New Mexico diamond@rt66.com

---

## More on network file race condition ([RISKS-16.62](#))

<ark@research.att.com>

Thu, 8 Dec 94 13:40:35 EST

Several people have suggested to me, some rather haughtily, that my corrupted /etc/hosts file would not have come about had I been using an operating system that supported file locking by default--that is, if only one process could have a file open for writing at a time.

Looking over the code to see if this was true revealed Cause 4. It turns out that the file is built up in several phases:

1. Generate the entries for 'localhost' and 'loghost' in a temporary file.
2. Append the entries for machines I am likely to use often to the temporary file.
3. Append all the other entries to the temporary file.

Because this is done as a shell script, each phase opens the file, appends to it, and then closes it. That means that file locking would not have avoided the race condition.

One person suggested to me that I should have built /etc/hosts in a temporary file rather than immediately overwriting the good copy. In fact, I did just that. However, since I 'knew' that the program would never run more than once at a time, I used a fixed name for the temporary file. Since that name was in my home directory, each process on each machine used the same file.

Finally, I will note that I know how to make the program safe against multiple accesses, even without file locking: use a separate temporary file for each invocation and then, instead of copying the file to its final place, move it there atomically. I don't know how to make such things automatic, though, and it's far from clear that one should always take such precautions, even for programs one believes will be run only on one's own behalf.

--Andrew Koenig ark@research.att.com

---

## Rights and Responsibilities of Participants in Networked Communities

"Herb Lin" <hlin@nas.edu>

Fri, 09 Dec 94 10:27:00 EST

The Computer Science and Telecommunications Board (CSTB) is pleased to announce the availability of a new report entitled \_Rights and Responsibilities of Participants in Networked Communities\_. Given increasing public interest and concern over the behavior of people on electronic networks, the report seeks to illuminate, to question, and to articulate difficult issues that arise in this context, and thus to help to

lay a foundation for a more informed public debate and discussion of the rights and responsibilities of those who operate in this domain.

The report is based on a workshop and a public forum involving technologists, lawyers, policy analysts, network service providers, and network operators in the exploration of several hypothetical but plausible scenarios in four areas (free speech, electronic vandalism, intellectual property interests, and privacy). The report illustrates how disagreements in these areas are rooted in value judgments; for example, the extent to which continuity with past precedents is desirable. Lawyers and policy-makers often argue that rights and responsibilities in a new domain inherently derive from existing rules, the report says. By contrast, technologists with extensive network experience often assert that with a new medium and a new form of human expression should also come new rules of social intercourse. The report notes that these four areas have always been inherently contentious, but over time certain compromises and understandings have evolved that guide what people do when communicating via traditional media such as print, telephone, radio, and television. Today the proliferation of networking technology threatens this state of understanding because it changes the environment in which previous compromises were achieved, leading to a re-examination of the same fundamental issues.

The report is available from the National Academy Press for \$25.00 (prepaid) plus \$4.00 shipping for the first copy and \$.50 shipping for each additional copy; tel. (202) 334-3313 or 1-800-624-6242. It will also be available soon on the WorldWide Web at <http://www.nas.edu>; via Gopher at <gopher.nas.edu>; and via FTP at <ftp.nas.edu>.

The National Research Council is the principal operating arm of the National Academy of Sciences and the National Academy of Engineering. It is a private, non-profit institution that provides independent advice on science and technology issues under a congressional charter. CSTB addresses national scientific and policy issues in computing science, telecommunications, and computer technology and their applications.

---

## Searching RISKS et al.

*"Dr. Frederick B. Cohen" <fc@all.net>  
Fri, 9 Dec 1994 07:16:40 -0500 (EST)*

I have recently setup a Mosaic server with on-line copies of the RISKS Digest and other on-line material on similar topics. This server allows the user to search full text for any given word, and produces a listing of all occurrences (in context). The user then selects the desired item(s) and views the files they occur in.

I am writing to RISKS for 2 reasons. One is to ask permission to use the Risks Forum in this way (after all, it is copyrighted as of its creation), and the other is to inform your readers of the proper URL (<http://all.net:8080>).

Please don't search for anything like "and". You will find that

the search produces a LOT of useless results.

FC

[FRED: Many thanks for doing this! I'll add it to the Info.  
Yes, you have my permission. But I trust that your home page will  
request users to respect any copyrights (explicit or implicit) and  
fair-reuse practices. Also, suggest that folks should remember to  
scan for subsequent corrections... 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 16: Issue 64**

**Sat 10 December 1994**

## Contents

- [Re: Interesting product claim \(more Pentium stuff\)](#)  
[Paul N. Hilfinger](#)
- [Re: Formal Methods ... Intel FDIV bug and verifying FPU's](#)  
[Miriam Leeser](#)
- [Re: Formal verification of the AAMP5](#)  
[Srivasa](#)
- [Re: Multicast backbone blunder](#)  
[Derek Atkins](#)
- [Re: Digital Cash](#)  
[A. Padgett Peterson](#)
- [Re: Cellular One roaming in NYC](#)  
[Alan Clegg](#)
- [Re: "Good Times" virus](#)  
[Steve Summit](#)  
[Susanne Forslev](#)
- [Re: Fun with your phone company](#)  
[Andy K](#)
- [Re: Digital cash on the web](#)  
[Hal Pomeranz](#)
- [German Telecom: technical risks/crime](#)  
[Klaus Brunnstein](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ **Re: Interesting product claim (more Pentium stuff)**

"Paul N. Hilfinger" <[hilfinger@CS.Berkeley.EDU](mailto:hilfinger@CS.Berkeley.EDU)>  
Fri, 09 Dec 1994 16:31:47 -0800

Well, William Kahan informs me that

(1) Inmos used formal methods for the FP on the T800, but that they got the specification wrong.

(2) Intel actually had in its possession a test that Kahan had designed that uncovers the flaw after about 2 minutes of testing. The test (as I understand it) is sort of "gray box" in that it makes certain assumptions about the class of algorithm used.

These points notwithstanding, however, Kahan still agrees that there is no substitute for formal proof in these cases.

Paul Hilfinger

---

## ✂ Formal Methods ... Intel FDIV bug and verifying FPUs

Miriam Leeser <mel@ultrastar.EE.CORNELL.EDU>

Thu, 8 Dec 94 13:33:22 EST

The Intel FDIV bug occurs both in single and in double precision divide. It is NOT a double precision error. The best source of information on this is the web site:

<http://www.mathworks.com/Pentium/README.html>

The Pentium uses a subtractive division algorithm based on a radix-4 Booth SRT algorithm. Similar algorithms are used for square root and division in this and several other processors. (We are in the process of working on a survey article of division and square root implementations in recent microprocessors.)

The closest verification work I know of is a proof of a radix 2 subtractive square root chip I did with some students here at Cornell. The paper describing this proof appeared in the Conference on Theorem Provers in Circuit Design in September 1994. We are working on a proof of a radix 2 subtractive division implementation. The two proofs are very similar.

The square root paper is available by anonymous ftp from  
tesla.ee.cornell.edu:~pub/hw-verify/sqrt-tpcd94.ps.Z

Verification of radix 4 is somewhat more difficult, largely because the implementation depends on a lookup table to guess the next digit. I have heard rumors that the error is in the translation of a table used for digit selection, but no substantiation that this is the case. It is highly likely that the error is related to using the output of the carry-save adder. Since we have not done a proof of a radix 4 algorithm, we do not consider the lookup table in our proof.

Our proof shows that the basic algorithm does in fact perform a square root, and then relates this to the register-transfer level implementation of the hardware. We do not prove the correctness of the implementation of each of the blocks of hardware (adders, shifters, etc.) As several people have pointed out, errors occur at several different levels. Formal verification is very useful at high levels, but will not preclude the need for lower level testing or simulation.

Miriam Leeser Cornell University mel@ee.cornell.edu

---

**Re: Formal verification of the AAMP5 (Rushby, [RISKS-16.62](#))**

srivas <srivas@csl.sri.com>  
Fri, 9 Dec 94 13:07:00 -0800

[John Rushby was incorrect when he said that the AAMP5 did not have floating point. The following message from the authors of the cited report gives a more accurate summary of the project. PGN]

Recently, John Rushby sent a message to this forum giving a reference to a paper about an application of mechanized verification to a commercial microprocessor. I am giving below a summary of the work reported in the paper. For those interested in finding out more details about the project, the paper is available over the web through

<http://www.csl.sri.com/aamp5.html>

or by ftp from

ftp.csl.sri.com/pub/reports/postscript/aamp5.ps.gz

(Note that name of the ftp site has an "ftp" at its head.)

\*\*\*\*\*

Formal Verification of AAMP5 Microprocessor:  
A Case Study in the Industrial Use of Formal Methods

Steve Miller	Manadayam Srivas
Collins Commercial Avionics	Computer Science Laboratory
Rockwell International	SRI International
Cedar Rapids, Iowa 52498	Menlo Park, CA 94025

The AAMP5 verification was a project conducted to explore how formal techniques for specification and verification could be introduced into an industrial process. Sponsored by the Systems Validation Branch of NASA Langley and Collins Commercial Avionics, a division of Rockwell International, it was conducted by Collins and the Computer Science Research Lab at SRI International. The project consisted of specifying in the PVS language developed by SRI a portion of a Rockwell proprietary microprocessor, the AAMP5, at both the instruction set and register-transfer levels and using the PVS theorem prover to show the microcode correctly implemented the specified behavior for a representative subset of instructions. The formal verification was performed in parallel with the development of the AAMP5 and did not replace any production verification activities.

The central result of this project was to demonstrate the feasibility of formally specifying a commercial microprocessor and the use of mechanical

proofs of correctness to verify microcode. This is particularly significant since the AAMP5 was not designed for formal verification, but to provide a more than three-fold performance improvement while remaining object code compatible with the earlier AAMP2. As a consequence, the AAMP5 is one of the most complex microprocessors to which formal methods have been applied. The AAMP architecture is specifically designed for use with block-structured, high level languages like Ada in real-time embedded applications. It is based on a stack architecture and provides hardware support for many features normally provided by the compiler run-time environment, such as procedure state saving, parameter passage, return linkage, and reentrancy. AAMP5 supports floating point calculations implemented via microcode.

Besides demonstrating the verification of a subset of AAMP5 microcode, an equally important accomplishment of the project was the development of an effective methodology that can be used by practicing engineers to apply formal verification technology to a complex microprocessor design. This includes techniques for decomposing the complex microprocessor verification problem into a set of verification conditions that the engineers can formulate, and proof strategies to automate the proof of the verification conditions.

This methodology was used to formally verify a core set of eleven AAMP5 instructions representative of several instruction classes. The core set did not include floating point instructions. Although the number of instructions verified is small, the methodology and the formal machinery developed are adequate to cover most of the remaining AAMP5 microcode. The success of this project has led to a sequel in which the same methodology is being reused to verify another member of the AAMP family of processors.

Another key result was the discovery of both actual and seeded errors. Two actual microcode errors were discovered during development of the formal specification, illustrating the value of simply creating a precise specification. Both errors were specific to the AAMP5 and corrected prior to first fabrication. Two additional errors seeded by Collins in the microcode were systematically uncovered by SRI while doing correctness proofs. One of these was an actual error that had been discovered by Collins during testing of an early prototype but left in the microcode provided to SRI. The other error was designed to be unlikely to be detected by walkthroughs, testing, or simulation.

---

### **\*Re: Multicast backbone blunder (Clegg, 16.63)**

*<warlord@MIT.EDU>*

*Fri, 9 Dec 94 16:05:31 EST*

- > The risk turns out to be that the newest version of the NV video
- > transmission software allows you to transmit video across the mbone
- > without a camera... any window or cursor-followed region will be happily
- > transmitted to the world... It is not obvious in ANY way that you are
- > actually transmitting any information...

This is not true. Having played with the latest version of nv last night, trying to get Multicast to work with Linux 1.1.72, I can attest to the fact that nv does provide you with a clue that it is transmitting.

First, the button on the bottom of the nv window will change between "click to start sending" and "click to stop sending", depending on the current state. Second, when you are transmitting, you should see your transmission in the nv session window, which displays all the video feeds currently in progress.

Also, it is possible to configure everything such that nv will be started with the -recvOnly flag, in which case it wont even let you send video (our version of sd does this automatically).

I don't think this is necessarily a program error or a program bug, although it is clearly an interface issue and possibly a clueless user not knowing what all these neat buttons do!

-derek

---

**✉ Re: Digital Cash (Wells, [RISKS-16.63](#))**

*A. Padgett Peterson <padgett@tcslr.dnet.mmc.com>  
Fri, 9 Dec 94 15:27:15 -0500*

Sounds a lot like some things I was discussing with some friends. Consider the following (going to use PGP for an example). A store sends out a catalogue via E-Mail at the start of the catalogue is the store's PGP public key (package obtained from ViaCrypt (plug) so legal for commercial use).

The subscriber has a program that on choosing a selection from a menu is able to use the header to encrypt the selections, credit card number, and shipping instructions with the store's public key and sign it with the shopper's private key (Addison Fisher was discussing this sort of thing quite a few years ago, just now technology has (almost) caught up).

The completed order is then sent to the store. Note that since the shopper just signed the message, it does not need the shopper's public key to extract the order, just to authenticate it if repudiated later, but the store's private key is needed to read it.

Concerned that the header key is someone else's and the whole thing is a scam ? Call this 800 number and press 9 to get a voice mail certificate number (eight hex digits and built into PGP now). And the "Home Shopping MIME" will flash it every thirty seconds on the bottom of the screen. Spice will know the most popular by heart anyway.

Of course this leads to the question of revoking a key that is compromised - obviously with the age-old tradition of a classified ad: "I will no longer be responsible for any debts incurred by..." - not so much a revocation as a divorce.

Padgett

---

**✉ Re: Cellular One roaming in NYC**

Alan Clegg <abc@black-ice.gateway.com>

Thu, 8 Dec 1994 13:44:18 -0500 (EST)

Recently, pjd@cne.gmu.edu wrote about Cellular One turning off roaming in NYC.

A friend of mine, after reading the article had this response:

Funny thing is the fact that the same people that are scanning the ESN are also getting that Credit Card number when you make the call. :)

Hummm... guess that does not burn the cellular company... Caller Beware.

--abc [tuning out of NYC]

---

**✉ "Good Times" virus ([RISKS 16.62](#))**

Steve Summit <scs@eskimo.com>

Fri, 9 Dec 1994 14:56:10 -0800

I'm also not sure where the real virus is. I have now received more copies of the "it's a hoax" message from well-meaning friends (and my own spouse) than the original "warning."

We should also be careful about shouting too loudly that "There's no such thing as an e-mail virus!" As RISKS readers know, there are several perfectly workable ways of wreaking mayhem via e-mail, and "active" e-mail is such a seductively attractive concept that sooner or later some misguided person will actually implement it (with inadequate safeguards), and then the fun will really begin. (Nat Borenstein has written a few papers about the idea of active e-mail, although his papers of course DO mention the glaring risks, and propose methods of implementing active e-mail reasonably safely, if anyone dared to.)

Steve Summit scs@eskimo.com

---

**✉ AOL "Virus"**

Susanne Forslev <sforslev@mcs.net>

Fri, 9 Dec 1994 16:57:30 -0600 (CST)

After reading in RISKS about the supposed AOL virus, I logged on to my

account to see if I had any mail. I didn't and I was pleased to find a button on my opening screen for e-mail information. I pushed it and found a very coherent explanation from the management of what can and cannot be done with e-mail and what to do if someone sends you a questionable file attachment. Now I just hope people bother to push the button and read the message. With luck, the AOL "Inoculation" has worked.

Sue Forslev sforslev@mcs.com sforslev@well.com

---

**✦ Re: Fun with your phone company**

*<andyk@e-mail.com>*

*Fri, 09 Dec 1994 18:27:47 EST*

A RISK uncovered here is the weakness of the underlying Data Model utilized by the phone company in question. Phone companies, in general, seem to have insisted on a business rule that requires that the telephone number itself also be the customers account number.

If one were to make an entity-relationship model of this enterprise there would be several entity-types that utilize the same identifier. CUSTOMER-ACCOUNT, CUSTOMER, SERVICE-ACCESS, FRAME-ASSIGNMENT, are each expected to be uniquely identifiable by the telephone number. Overwhelmingly this is the case, but there are enough exceptions - multiple lines for one customer, people moving, etc. that it weakens the data model (or increases its complexity unnecessarily) that the business processes begin to suffer. What ought to be merely a change to a relationship between two entities, or perhaps a value change to an attribute, results in a change to the existence of the entity itself.

I imagine, in the eyes of the Data Model, that when Russell Stewart moved - one CUSTOMER entity was deleted (or marked inactive) and another instance was created. No wonder they couldn't allocate the money properly! Each customer service rep probably has developed their own individual set of business rules to apply in the case of finding an appropriate instance of a CUSTOMER entity when the original one no longer exists.

---

**✦ Re: Digital cash on the web [Wells, [RISKS-16.63](#)]**

*Hal Pomeranz <hal@netmarket.com>*

*Fri, 9 Dec 1994 23:52:52 -0500*

In [RISKS-16.63](#), Justin Wells confuses two different methods of paying for goods and services over the Internet.

First, he talks about submitting credit card information via the FORMS interface supported by most recent Web browsers. Assuming both the client and server support some secure encryption mechanism, it is safe to transmit your credit card information over the Internet. The

NetMarket Company, for which I work, is the first company to do secure encrypted commercial transactions via the Web, though several other companies are also providing this functionality now.

Note that this is distinct from "digital cash". The scheme described above is simply a mechanism for transmitting your credit card information and is in fact not very different from simply calling a mail-order house on the phone and using your credit card.

Okamoto and Ohta ["Universal Electronic Cash", Crypto '91] propose six properties for an "ideal" digital cash system. Of these properties, credit card transactions are neither private (anonymous or untraceable), transferrable (a merchant can't pay somebody else with your "credit" without a bank doing arbitrage), nor divisible (you can't "make change" with credit).

Note that there are several competing digital cash standards under development at this very moment. Not all of these standards implement all of the features that Okamoto and Ohta outline in their paper. I fervently hope that we will end up with an "ideal" digital cash standard, but I am not hopeful.

Hal Pomeranz, Engineering Project Leader, The NetMarket Company

---

### **German Telecom: technical risks/crime**

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.d400.de>  
Sat, 10 Dec 1994 13:33:11 +0100*

German media's awareness about Telecom related crimes was raised significantly when International Herald Tribune reported on its front page earlier this week that "several thousands of German Telecom employees" are suspected to have participated in criminal activities which damaged German Telecom in the order of 500 million DM. According to this report, telephone lines were switched to service providers in areas such as Netherlands Antillas where services such as astrologic reports (horoscopes) and taped sex conversations are regularly offered at high prices (up to 12 DM/minute); such services are usually announced in German boulevard newspapers on specific pages.

Income from such telephone calls is usually divided between German Telecom which bills it's resp. international tariff, and the related PTT (e.g. NL-Antillas PTT) which subtracts its tariff from the amount sent and distributes the rest to the service provider. This trade between the PTTs is calculated by counting the \*total volume of connect time\* between related Telecoms. This implies that Telecom pays more to another PTT than it can charge to individual customers if some pirates succeed to generate communication between PTTs even when a real connection was NOT established, or with other criminal tricks. In cases reported by Herald Tribune, Telecom employees and service providers worked together to generate a significant volume of communication. Such procedures are a modern version of earning

real money with "virtual communication" :-)

As German media (with few exemptions) are not well informed about details of Telecom procedures and systems, much noise was generated, where some "experts" (e.g. a misinformed member of the Chaos Computer Club :-)) said that hackers may have hacked Telecom computers (which is nonsense, both in the sense of telephone hacking=phreaking and computer hacking). While Telecom admitted that investigations were underway (one day later, 2 Telecom employees and 1 service provider were jailed, being accused with having damaged German Telecom in the order of 2 million DM), spokesmen immediately rejected that damage be in the order of 500 million DM. More cases are evidently underway (both in jailing and reporting :-).

Since some time, public is growingly concerned about Telecom bills as steadily growing numbers of Telecom customers complain about unexpectedly high telephone bills. With estimated 600,000 customers (of 35 mio private customers) complaining this year, and a roughly estimated mean damage of 1,000 DM (as many customers report too high figures over months, with single bills adding to over 200,000 DM!), the \*overall damage for private customers\* may sum up to about 600 million DM! Despite of some recent damages to enterprise switching systems, discussion concerning potential economic damage has not reached the media so far.

Unfortunately, German telecom customers so far cannot control their bills amount and so argue whether they really connected to such service providers. Different from other technically advanced countries, German customers receive monthly bills with \*sums of telephone units and the total price which they have to pay\*. This is a relic from ancient technologies when units were counted in electromechanical counters whose actual figures were photographed for documentation purposes; the photos of a new and the last month were compared to calculate the difference as the basis of the new bill. Since some time, digital switching systems (esp. Siemens' EWSD and Alcatel' S12) are installed in most regional switching offices (Vermittlungsstellen), where a log-record is stored for each call containing all essential billing data. While German Telecom only recently offered to list details of each telephone call if customers apply for this service and pay a monthly price in the order of 10 DM), a federal parliament's commission (Petitionsausschuss) recently suggested to the ministry of Telecommunications that detailed bills should be given and that such service should be free of a fee (as e.g. in US and Canada).

Presently, a growing number of customers are seeking legal help against such Telecom bills. In few cases, courts (assisted by technical expertises about potential faults and points-of-attacks) have sentenced the bills as irregular. As in many cases of digital technologies, complexity of Telecom networks has grown so rapidly that new risks have appeared, e.g. in software and management of complex switching systems. In several cases, software bugs were not detected in Telecom's very detailed test process; in one case, billing records were store doubly, which was only detected "in the field". Management of such systems has never been analysed for any reasonable "quality" (even an ISO 9000-based analysis which is not very adequate would lead to improvements).

In cases of growingly complex systems with growing bugs and management

faults, more customer protection is needed. As customers are rarely able to relate overly high bills to technical problems of any kind, it should belong to the professional duties of related experts and their organisations (international as IFIP; national as ACM, BCS, GI/Germany, IEEE) to provide expertise for the public in cases such as Telecom criminality (from which side whatsoever). This may also help to produce better insight of public media about technologies.

Klaus Brunnstein (Dec.10,1994)



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 16: Issue 65

Thursday 15 December 1994

## Contents

- [Info on RISKS \(comp.risks\)](#)
- [No, I'm not Newt.](#)  
"GingrichN" alias Steve Barr
- [Oral Hackers](#)  
Mark Colan via John Markoff
- [Technology Under the Weather](#)  
Gordon Symonds
- [Wendy's Stock](#)  
Charles R Trew
- [Re: Formal Methods and Exhaustive testing](#)  
Tony Lauck
- [Re: Mailing-list deadman switch](#)  
John Gardiner Myers
- [Re: Self-extracting emacs elisp code](#)  
Morgan Jones
- [RISKS demonstrates more RISKS in mailing list software](#)  
Sidney Markowitz

---

## No, I'm not Newt.

<GingrichN@aol.com>

Tue, 13 Dec 1994 18:56:01 -0500

AOL's software just makes it easy to pick a `screen name,' any screen name (up to 5 screen names, in fact).

For the record, I am Steve Barr, reachable at  
GingrichN, SarahBrady, BARRST, etc. @aol.com,  
barrst@iris.uncg.edu, and barrsx@turing.uncg.edu.

AOL did seem to go through federal agencies. IRS, [B]ATF, CIA, and FBI were all unavailable.

BTW, someone else registered BClinton@aol.com.

Just a cautionary note. Now all you need to spoof mail is a credit card (stolen?) and a '10 free hours on AOL' disk.

Steve Barr

---

## Oral Hackers

<neumann@csl.sri.com>

Wed, 14 Dec 1994 19:09:08 -0800

John Markoff thought the following item might amuse some of you.

>From: Mark Colan <Mark\_Colan.LOTUS@crd.lotus.com>

>Date: 14 Dec 94 12:42:23 ES

>Subject: Oral Hackers

>

>from PC Week, 12/12/94, "Some Outrageous, and Not So Outrageous, Predictions

>

>PC audio's next push into the world of corporate computing will be dealt a

>major blow when a disgruntled layoff victim at General Motors destroys

>hundreds of hours of work by running through a floor of cubicles yelling,

>"FILE! CLOSE! NO!" The tactic, which will come to be known as oral hacking,

>obliterates unsaved work on speech-enabled systems by closing files without

>saving.

---

## Technology Under the Weather

Gordon Symonds <gsymonds@hpb.hwc.ca>

Mon, 12 Dec 1994 13:37:42 -0500 (EST)

>From the Dec 11 edition of the Ottawa Citizen:

MONTREAL - Myopic weather observation machines installed at Edmonton and Dorval airports to replace human observers as a cost-cutting measure can't tell rain from snow and are being withdrawn from service. Marc Gelinis, a weather specialist at Environment Canada's St. Laurent office, said the machines also cannot tell when there are clouds above 10,000 feet. "At 6:15 PM Friday, it was completely overcast and snowing at Dorval but the automatic weather system issued a report saying there were only scattered clouds at 4,000 feet," Gelinis said. The system at Dorval airport has been providing pilots with inaccurate weather reports since it was installed Nov. 15. Humans will remain on the job at the two airports until the machine can produce accurate weather reports. But the equipment will remain in place at another 48 smaller airports across the country.

---

## WENDY'S STOCK

"CHARLES R TREW" <CTREW@MAIL.LOC.GOV>

13 Dec 1994 14:10:14 GMT

Here's an expensive little mistake: American Stock Transfer and Trust Co. of NY, which handles the stock dividend reinvestment program of Wendy's, recently gave out double dividends to Wendy's shareholders. The company had to reprint and re-mail account statements to thousands of investors nationwide. I don't know if those receiving dividends via check were given double stuff, if so, that would have generated additional headaches I'm sure. Charlie Trew

---

## Re: Formal Methods and Exhaustive testing

Tony Lauck <[arlauck@CERF.NET](mailto:arlauck@CERF.NET)>

Thu, 15 Dec 1994 09:12:22 -0800

Those who build computational hardware or software have a responsibility to ensure that their artifacts produce correct results, because these artifacts are used in many applications, some of which are extremely critical to life or property. I can't imagine any valid excuse for shipping a CPU which deterministically gives incorrect results due to a bad algorithm or logical fault in its implementation. Computer arithmetic algorithms and math libraries are simple enough to permit complete verification by a combination of formal methods and exhaustive testing.

Here's a story that illustrates the lengths to which it is possible to go. In the late 60's I worked in the PDP-10 group at DEC. Digital had lost a benchmark to its then arch-rival, Scientific Data Systems. It seemed that the PDP-10 square root routine was too slow. I rewrote the routine and speeded it up by 25%, putting the new result on the master disk for subsequent distribution. Part of my speed up included removing unnecessary rounding in the early steps of Newton's method. Being concerned that the resulting code might produce different results from its predecessor, I tested the mantissa processing code exhaustively, verifying in each case that the resulting value was less than one LSB off of the exact answer. I also tested all possible values of the exponent and sign fields. A very little formal work showed that the combined routine was correct. (I would have felt even better if I had had the several months of computer time to test all  $2^{36}$  cases directly.)

I was prepared to swear that my new routine always gave the same answer as the old. As it turned out, this was NOT true. In exactly one case my new routine did a better job of rounding the square root to single precision. I found this out several years later when Mary Payne called my square root routine "brilliant". My rejoinder was that it was merely "lucky". It seems that Mary had been working to a stricter criteria than mine and wanted the rounding to always give the closest possible value.

For a long time, Mary Payne was responsible for Computational Quality at Digital. She consulted in the design of processors or math libraries, or anything else which was likely to result in bad numbers coming out of Digital's computers. It seems most unlikely that the Pentium bug would have gotten past her.

---

## Re: Mailing-list deadman switch

John Gardiner Myers <jgm+@CMU.EDU>

Sat, 10 Dec 1994 18:33:56 -0500 (EST)

As a postmaster at a large site, I have to say I have a real problem with mailing lists which have this "must actively resubscribe" feature.

The feature assumes that all recipients of the list are live humans, who can interpret the resubscribe message and reply. That assumption is not always true. At our site, we encourage users to *\*not\** subscribe to lists directly, instead we prefer to gateway mailing lists into our bulletin board system. This approach saves disk space, mail delivery time, and most importantly administrator time dealing with expired or abandoned accounts.

When some list sends out a resubscription request, at least one reader of the associated bboard has to forward it to an administrator, who has to manually respond. This is a waste of expensive staff time. Many times, the subscription just expires and any user who later becomes interested in the list sees what incorrectly appears to be an inactive list.

On a different topic: after spending some time composing a reply to the list-looping query in [RISKS-16.59](#), including technical information as to what the standards state various mail agents should do in various situations. In 16.60, I read a reply by Peter da Silva which gave information on the topic that was in fact *\*completely incorrect\**. Later I was horrified to find my name included in an editorial comment as having given a "similar response" on the topic.

I suppose this is a RISK of RISKS; by contributing to an edited forum I ended up having my name attached to a position I completely disagree with. I hope the editor will post this retraction: it is my professional position that error (and other) notifications be sent to the envelope return path as the standards specify, that sending them to Errors-to: violates the standards and should not be done.

[Yes, indeed. Sorry for the guilt by association. I try wherever possible to prune items with similar messages. Here I elided a little too smoothly. Thanks. PGN]

---

## Re: Self-extracting emacs elisp code (Blob, [RISKS-16.62](#))

Morgan Jones <morgan@algorithmics.com>

Tue, 13 Dec 1994 19:26:06 -0500

And here is a good example of not RTFM'ing before sending an alarm:

>With all this talk about self extracting mail "viruses", a friend showed me  
>that in emacs (which I use to read mail, along with vm) has the ability to  
>self-extract elisp code. This feature seems to be turned on by default, and

>it not only applies to mail read with emacs, but rather every file visited  
>(when the feature is on, of course).

There are actually two mechanisms at work here. First, emacs supports a per-file variable initialization mechanism. Whenever a file is loaded, emacs scans the end of the file for a special section of "comments" which provide emacs with values to set in certain buffer variables. Enabled by default, this mechanism only allows literal values and so does not constitute any significant risk.

In Emacs 19, lisp forms may be included as the value for certain variables, and a special 'eval' construct is allowed which simply evaluates its form. By default, emacs shows you the code and asks if it should be evaluated.

The risk is that emacs is a very complicated product and generally requires a fair amount of configuration and customization to be usable by a power user. When a less experienced user sees the "cool stuff" that the power user does, he simply copies the power user's emacs configuration file. Unfortunately, the inexperienced user cannot read the file and so picks up many unwanted changes. If the power user made use of the 'eval' feature, he would probably disable the execution query; the inexperienced user would then be unwittingly susceptible to trojan attacks.

Being the primary emacs disciple at my site, I am usually the one responsible for propagating annoying functionality to coworkers. To avoid this problem, I have separated the benign functionality of my configuration to a centrally available file for other users to execute. Dangerous or annoying customizations are stored in my local configuration file which other users no longer need to copy.

Morgan W. Jones -- morgan@algorithmics.com  
Algorithmics Incorporated, Toronto, Canada

---

## **RISKS demonstrates more RISKS in mailing list software**

*Sidney Markowitz <sidney@apple.com>  
Tue, 13 Dec 1994 14:03:25 -0800*

I just received something that I guess was sent directly to the RISKS digest LISTSERV remailing address, thus bypassing the normal moderation process of mail sent to risks@csl.sri.com. If I'm correct, those of you not receiving RISKS via the LISTSERV distribution did not see it.

It was an ad for some computer hardware. Some people have been sending commercial e-mail messages to lists of mailing list addresses, ignoring the lack of relevance of their ad to the lists' topics. That is called "spamming" and is considered by many on the Internet to be antisocial behavior.

This particular message apparently was sent from e-mail address LIONEL GOLDBERG <actuary@ix.netcom.com> (But read RISK #3 below!). I contacted netcom and was told that they have an explicit policy against spamming from

their customers' accounts.

RISK #1: The LISTSERV system used by RISKS for automating list distribution on BITNET allows this kind of bypassing of the moderator.

RISK #2: If [actuary@ix.netcom.com](mailto:actuary@ix.netcom.com) really sent this message to RISKS and a bunch of other mailing lists indiscriminately, complaints to [sysadmin@netcom.com](mailto:sysadmin@netcom.com) can lose him his account.

RISK #3: E-mail can easily be forged. The LISTSERV software conveniently removed all traces of the actual path that the message took before it arrived at the list server and was redistributed, so I could not tell if the message was even a crude forgery sent from someone other than the account in the "From" header. So please don't jump the gun in accusing [actuary@ix.netcom.com](mailto:actuary@ix.netcom.com).

RISK #4: The ad asks for people to send checks or money orders, no COD or credit cards, to some unknown company for unseen equipment. Anyone want to buy a bridge?

RISK #4.9999721: Some of the items listed are Pentiums :-)

-- sidney markowitz <[sidney@apple.com](mailto:sidney@apple.com)>

[Comments from too many of you to name on this, including some who got multiple copies, and some of whom got copies from lists to which they are not even subscribed. netcom has disabled the account. RISKS was not the only list hit.

As you all know, the BITNET LISTSERV is wide open to the world. I have no control over what goes gets redistributed, although perhaps one of its wizards will change that soon? Perhaps it should have been set up that ONLY RISKS can cause E-mail to be distributed to the list, but that is not the way it works. Occasionally some overly moronic individual spams our BITNET readers. Perhaps the automated server that we are trying to set up might induce some of you to switch over, although my system does not really need the added burden... Stay tuned. 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 16: Issue 66**

**Tuesday 20 December 1994**

## Contents

- [Microsoft has no plans to acquire Catholic Church from EDUPAGE](#)
  - [Mistaken Identity](#)  
[Tom Knoedler](#)
  - [Emergency Broadcast System Goes Automatic?](#)  
[Darrell F. Oresky](#)
  - [Brands Burn the Bull's Behind](#)  
[Peter Wayner](#)
  - [Followup to "No I'm not Newt"](#)  
[Ted Koppel](#)
  - [Re: Oral Hackers](#)  
[Steve Holzworth](#)
  - [Re: Technology Under the Weather](#)  
[Ross Oliver](#)
  - [Intel announces new Pentium replacement policy](#)  
[Rich Kulawiec](#)
  - [Pentium bug as data management problem](#)  
[Rob Aitken](#)
  - [Testing the Pentium bug](#)  
[Daniel Essin](#)
  - [Mary Payne and "Good to the last bit!"](#)  
[Paul A. Karger](#)
  - [Pentium FDIV problem - so what's new ?](#)  
[A. Padgett Peterson](#)
  - [Spreadsheet Errors Study](#)  
[Ray Panko](#)
  - [The Status of Disclaimers](#)  
[Dick Nickalls](#)
  - [CFP: New Security Paradigms Workshop](#)  
[Catherine A. Meadows](#)
  - [CFP: Safety and Reliability of Software Based Systems](#)  
[Stella Page](#)
  - [Info on RISKS \(comp.risks\)](#)
-

## Microsoft has no plans to acquire Catholic Church (from EDUPAGE)

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

Mon, 19 Dec 94 11:43:01 PST

The latest Internet hoax has Microsoft acquiring the Roman Catholic Church, including exclusive electronic rights to the Bible. The story, written under an Associated Press byline, says the agreement provides for Pope John Paul II becoming the senior vice president of the company's new Religious Software Division, and two Microsoft senior vice presidents being invested in the College of Cardinals. The fake story included a promise from Bill Gates to "make the sacraments available online for the first time." Officials at Microsoft and AP said they didn't know where the story originated. (Tampa Tribune 12/17/94 B&F10)

[FROM EDUPAGE, 18 Dec 1994, which concludes thusly:]

[EDUPAGE is what you've just finished reading. To subscribe to Edupage: send a message to: listproc@educum.edu and in the BODY of the message type: subscribe edupage Count Dracula (assuming that your name is Count Dracula; if it isn't, substitute your own name) ... To cancel subscription to Edupage: send a message to: listproc@educum.edu and in the BODY of the message type: unsubscribe edupage.]

[Several folks submitted the original hoax to RISKS. It was not run here for a variety of reasons. The omission was not a sacramental lapse on my part. Fakes Vobiscum. PGN]

---

## Mistaken Identity

"Knoedler, Tom" <knoedler@eagle.sangamon.edu>

Wed, 14 Dec 94 13:50:00 PST

In the 19 December 1994 edition of \*Newsweek\*, read the 'My Turn' column entitled 'A Case of Mistaken Identity: On the Information Highway, you are guilty until proven innocent' by Michael W. Klein. Mr Klein, an attorney in New Jersey, was falsely identified as a reckless driver because a police clerk made a mistake on an address search. Law enforcement personnel were prepared to lock him up even though the physical descriptions did not match, even though the demographics did not match, just because the warrant had come out of the computer.

Thomas Knoedler knoedler@sangamon.edu

[... A familiar kind of case for long-time RISKS readers. PGN]

---

## Emergency Broadcast System Goes Automatic?

Darrell F. Oresky <dforesky@jumbo.Read.TASC.COM>

Fri, 16 Dec 94 14:48:28 EST

I heard a short note on the local all news radio station recently about a

planned upgrade to the Emergency Broadcast System (EBS). This upgraded service would allow the EBS to reach radio and TVs that were not actually turned on when the broadcast was sent. The intent is to inform even those misfortunates who were not actively listening or watching at the time of an emergency. I assume such an upgrade would require changes to radios and TVs to allow them to be turned out remotely via some sequence of commands carried over the airwaves? One potential risk of this configuration is that one could remotely activate speakers or video devices that may be part of the television or radio, and use this mechanism to listen in without anyone knowing.

Darrell Oresky dforesky@tasc.com

---

## Brands Burn the Bull's Behind

*Peter Wayner <pcw@access.digex.net>*

*Tue, 20 Dec 1994 09:36:51 -0500*

The Sports Monday of the NYT (12/19/94) ran a headline calling one basketball team the "Pentium" of basketball teams. It wasn't because they were playing 2-3 times faster than last year's team.

This illustrates the RISKS of imprecise technical language. There was no real meaning to the word "Pentium" before. The Intel, AMD and other clones were all supposed to be interchangeable. The brand name was just a marketing ploy that was even more hollow than the work of the folks at P&G, Coke or Pepsi. After all, there is a difference between colas. So, if there is no meaning to the word, it shouldn't be surprising that the first hint of a meaning, no matter how irrational, rushes in to fill the vacuum.

---

## Followup to "No I'm not Newt"

*Ted Koppel <tkoppel@carl.org>*

*Fri, 16 Dec 1994 18:50:38 -0700 (MST)*

To add to Steve Barr's comments about AOL and how anyone can have any name on that system:

My real name is Ted Koppel. There happens to be another fellow, a broadcaster, who has the same name as I do. I took my "ten free hours" on AOL, and explored the system. Not surprisingly, I used my name (actually Tkoppel, which is a reasonable login variation).

One of the places to visit on AOL is an area 'owned' by ABC News. I was in there, reading some of their stuff, and talking in one of the forums there, when I was told, in no unambiguous terms, to either get off the forum or change my name. Since my name is, after all, on my driver's license, I figured that I had a pretty good right to use it :-). So I told the fellow that.

It turns out that he is/was some sort of a staff person working for the ABC

Ted Koppel, and he was concerned that people would mistake ME for his Ted Koppel (a legitimate risk, I suppose). On the other hand, I'm not convinced that threatening me rudely was the appropriate way to go about it.

By the way, I subsequently dropped AOL, partially for this reason, but primarily because there was no 'killer app' that made me want to stay.

Ted Koppel \* The UnCover Company \* The CARL Corporation \* tkoppel@carl.org  
Work: 404 242 8733 Fax: 404 242 8511

---

**Re: Oral Hackers ([RISKS-16.65](#))**

*Steve Holzworth <sch@unx.sas.com>*

*Tue, 20 Dec 1994 04:40:19 GMT*

Mac 840AV machines (and presumably other AV machines) have a voice recognition feature. When we got ours, shortly after they had been released, and before anyone started doing useful work, we used to have great fun popping into someone's office and stating:

"Computer, Restart, Yes."

whereupon the Mac would dutifully reboot. ("Shutdown" was another option...).

Steve Holzworth, SAS Institute, SAS/Macintosh Development Team, Cary, N.C.

---

**Re: Technology Under the Weather (Symonds, [RISKS-16.65](#))**

*Ross Oliver <rosso@roscoe.csd.sgi.com>*

*Fri, 16 Dec 1994 22:01:46 GMT*

This article is biased and oversimplified view of a complex set of requirements. I wonder whether the weather specialist quoted in the article has an axe to grind against automated weather reporting systems.

The fact that the weather station report did not match current conditions is not unusual, regardless of who or what is making the report. Most airport weather reports are made once per hour, so if the weather is changing rapidly (for example, a storm front is moving in), actual conditions may be quite different from what is reported in the last hourly observation. This is not the fault of the automated observation system. Pilots must take into account when the observation was made, and how likely it is that conditions may have changed.

The article also stated, "the machines also cannot tell when there are clouds above 10,000 feet," implying a crippling limitation. In reality, clouds more than 5,000 or 6,000 feet above the ground are not particularly relevant to airport operations (i.e. takeoffs and landings), so less effort is expended to gather data on high clouds.

Ross Oliver

---

## Intel announces new Pentium replacement policy

*Rich Kulawiec <rsk@gynko.circ.upenn.edu>*

*Tue, 20 Dec 94 08:55:07 EST*

Public radio's "Marketplace" show is carrying a story this morning announcing that Intel will now replace, on request, any and all Pentium processors. This is a revision of their earlier policy, which required that Pentium owners justify the replacement to Intel staffers. I suspect that they could no longer afford the bad publicity or the manpower cost associated with the phone banks used to screen replacement requests.

[I suppose it is the corrected chip that will be called RePentium. PGN]

---

## Pentium bug as data management problem

*Rob Aitken <aitken@kokanee.dtc.hp.com>*

*Fri, 16 Dec 1994 12:44:26 -0800*

With all the discussion of verification, formal or otherwise, it seems to me that another explanation is being overlooked. Given the immense amount of data associated with a given chip design, it could be that the hardware implementation of the Pentium divide unit and the software representation which was verified (by whatever techniques Intel uses) were not the same.

Before a chip is fabricated, it exists as a huge software database, often including several mutually incompatible representations, with a large number of people using and changing it. Version control is a serious problem. If a design change was made after verification, or if verification was inadvertently performed on an earlier design, it is easy to see how a bug could slip in, even with formal verification.

If something like this did in fact happen, then the Pentium bug is an example of a much more mundane data management RISK than it has been made out to be, both in this forum and elsewhere.

Rob Aitken

---

## Testing the Pentium bug

*Daniel Essin <essin@hsc.usc.edu>*

*Sat, 17 Dec 94 1:10:26 PST*

I need a new, faster computer so I went to some computer stores to look at the Pentium 90's. Knowing of the fpu bug, I took my trusty formula snared off the net to test them.

>put in 5505001/294911. The correct answer is 18.66665197297. The Pentium

>produced 18.666092939000.

I carried out this test on two Pentium machines in the store using windows calculator. they both produced the wrong answer. A 486/66 of the same brand produced the correct answer.

When I asked the sales people about the bug, they said that the also had a test routine so we tried it. The instructions were to perform the use qbasic and run the following program:  
PRINT (4195835 \* 256)/(3145727 / 256)

Their instructions say that the correct answer is 87413.2569545927.

Both Pentiums produced the correct answer - however - they also produced the correct answer to 5505001/294911. I suspect that since qbasic has to run on oldx86 machines that lack fpu's, all floating point is probably done with a software emulator. Using this test, the store will never identify a single chip as defective creating a false sense of security with the customers and avoiding the difficulty of getting chips that are actually defective replaced.

caveat emptor

---

## Mary Payne and "Good to the last bit!"

*"Paul A. Karger" <pak0@gte.com>  
Fri, 16 Dec 94 10:06:30 -0500*

Tony Lauck commented on Mary Payne's work on assuring that DEC's computational routines always gave good results. I also worked with Mary at DEC, and was VERY impressed with her commitments to mathematical accuracy. Her motto at the time was that the computations should be "Good to the last bit!"

I have to agree that between Mary's work on algorithmic analysis and DEC's VERY extensive testing of instruction sets on each new processor model, it would have been very unlikely for a bug of the severity of the Pentium FDIV problem to have gotten out on a VAX or an Alpha processor.

---

## Pentium FDIV problem - so what's new ?

*A. Padgett Peterson <padgett@tcslr.dnet.mmc.com>  
Fri, 16 Dec 94 09:23:39 -0500*

Might point out that there is nothing new in the FDIV problem, 80x86 chips are notorious for "different" microcode - for a semi-complete list see the "86BUGS.LST" file in Ralf Brown's interrupt list.

For just one example, the operation of the instruction AAA ("ASCII Adjust for Addition" hex code 37) is noticeably different when executed on an 8088 as opposed to an 80386 - with initial value of AX=FFFF on an 8088 the result will be 0005h while on a 386, 0105h will result.

As a consequence any financial programs using BCD addition and requiring the AAA instruction may have different values on different systems.

Padgett

PS. Of course, I do not know of any program using either BCD or AAA and AX=FFFFh should never result from BCD addition, but what does that matter (AAM 37 now... 8\*) ?

---

## Spreadsheet Errors Study

"Ray Panko" <PANKO@busadm.cba.hawaii.edu>

Fri, 16 Dec 1994 10:02:15 -1000

I have recently completed a study on the types of errors that people make when they use spreadsheet programs. I am currently writing up the results. If you know of previous research that looked at spreadsheet errors other than the Michigan work of Olson and others or the Brown and Gould study at IBM, I would be grateful for citations or other information.

Basically, we found that student spreadsheeters have about the same error rates as professional programmers. About five and a half percent of their cells have errors before debugging. The problem is that they did not spontaneously debug, a lack seen in the Brown and Gould lab study and also in two ethnographic studies of real world spreadsheeters.

Given these error rates and apparent lack of deep debugging, the question is not what fraction of spreadsheets have errors but rather how many errors the typical large spreadsheet has.

Aloha, Ra3y (the 3 is silent)

Prof. Raymond R. Panko, Decision Sciences Dept, College of Business Admin. U of Hawaii, 2404 Maile Way, Honolulu, HI 96822 Panko@hawaii.edu (808) 956-5049

---

## The Status of Disclaimers

<mtzrwn@vaxb.ccc.nottingham.ac.uk>

17 Dec 1994 10:28:18 GMT

This is a HELP message. Can anyone out there direct me to any info/archive which will tell me the current state of disclaimers. I am writing some programs for medical use, and have come across the problem of how to phrase the disclaimer so that it stands up in court. The problem seems to be, at least in the UK, that one cannot say "..we disclaim all liability.." since apparently one has to put a sensible and realistic liability limit in the disclaimer. Perhaps some folk can help me here.

Dick Nickalls,, Dept Anaesthesia, City Hospital, Nottingham, UK

dick.nickalls@nottingham.ac.uk 100115.1010@compuserve.com

---

## **CFP: New Security Paradigms Workshop**

*Catherine A. Meadows <meadows@itd.nrl.navy.mil>*

*Thu, 15 Dec 94 19:33:40 EST*

CALL FOR PAPERS  
NEW SECURITY PARADIGMS '95

A Workshop Sponsored by ACM SIGSAC, DoD, and the Aerospace Institute

Residence Inn  
University of California at San Diego  
La Jolla, CA  
August 22-25, 1995

Paradigm shifts disrupt the status quo, destroy outdated ideas, and open the way to new possibilities. This workshop explores radical new models for computer security, trusted system integration, and intercomputer networking security. The goal is to develop transcendent solutions that provide the flexibility and interoperability users require in trusted systems.

We offer a creative and constructive workshop environment for about 25 participants at a small campus inn in scenic La Jolla adjacent to San Diego. Dress is casual. The tone is exploratory rather than critical. The refereed papers will be printed in a workshop proceedings.

To participate, submit preferably via email a research paper or a 5-10 page position paper to Program Chairs John Dobson and Catherine Meadows at the email addresses listed below by April 1, 1995. Alternatively, submit five copies of a hard-copy paper to either program chair by March 24, 1995. The Program Committee will referee the papers and notify authors of acceptance status by June 9, 1995.

Cost of the workshop, lodging, and meals will be about \$550. Scholarships are available.

### **WORKSHOP ORGANIZERS**

#### **Workshop Chair:**

Hilary Hosmer, Data Security, Inc., 58 Wilson Road, Bedford, MA  
+1 (617)-275-8231 (voice and fax) Hosmer@dockmaster.ncsc.mil

#### **Program Co-Chairs**

John Dobson, Computing Science Department, University of Newcastle  
Newcastle NE1 7RU, UK +44 91-222-8228 John.Dobson@newcastle.ac.uk

Catherine Meadows, Naval Research Laboratory, Code 5543, Washington, DC 20375  
+1 (202)-767-3490 (voice) +1 (202)-404-7942 (fax)

meadows@itd.nrl.navy.mil

Program Committee:

Thomas Haigh, Secure Computing Corporation

Deborah Hamilton, Hewlett Packard

Leonard LaPadula, MITRE

Ruth Nelson, Information System Security

Pierangela Samarati, Universita di Milano

Marvin Schaefer, Arca Systems

Bruce Schneier, Counterpane Systems

Olin Sibert, Oxford Systems

Adrian Spalka, University of Bonn

Daniel Sterne, Trusted Information Systems

Local Arrangements: Dr. Thomas Lincoln (Rand) +1 (310)-393-0411

Publications: Deborah Hamilton (Hewlett Packard)

Scholarships: Prof. Ravi Sandhu (George Mason Univesrity) +1 (703)-993-1659

Treasurer: Janet Haley (Haley Computer Services) +1 (609)-266-1471

Registration Chair: James Williams (MITRE) +1 (619)-223-2301 ext 31

ACM SIGSAC Liaison: Dixie Baker (Aerospace) +1 (310)-336-7998

---

## **CFP: Safety and Reliability of Software Based Systems**

*Stella Page <sp@csr.city.ac.uk>*

*Tue, 20 Dec 94 12:53:26 GMT*

European Network of Clubs for Reliability and Safety of Software

Centre for Software Reliability

**SAFETY AND RELIABILITY OF SOFTWARE BASED SYSTEMS**

Reims, France, 12-15 September 1995

**ANNOUNCEMENT & CALL FOR PAPERS**

12th Annual CSR Workshop

1st Annual ENCRESS Conference

Supported by the EC ESSI Programme and Lloyd's Register

In the past decade, there have been enormous advances in the use of computers - and hence software - in areas where safety and reliability are of significance both to individual users and to society at large. Examples can be found in all sectors of industry: railway signalling is increasingly computerised; fly-by-wire aircraft are the current technological trend in civil aviation; motor car engines and braking systems are computer-controlled; programmable logic controllers (PLCs) used in the process industries have increasingly complex software embedded within them; and commercial companies of all sizes become ever more dependent on the reliable

operation of their computer systems.

These systems do not always deliver the levels of safety and reliability which users and society are entitled to expect. There are many reported examples of software-related failures which have caused, or had the potential to cause, death, injury, environmental damage, or significant economic loss. These include deaths in hospitals of patients undergoing radiotherapy treatment, software-defect induced release of sufficient water from a reservoir to flood a valley, lost space-craft, and company failures.

Very often, these incidents could have been prevented, or their consequences reduced, by better awareness of safety and reliability issues as they apply to computer-based systems. Ideally, developers of systems should have evidence that their approach to system development is likely to lead to the required levels of safety and reliability. Often, evidence of this sort will form part of a safety case, or other justification for system reliability and/or safety, that has to be presented for approval or acceptance by an appropriate authority.

Many projects in the ESSI programme aim to produce evidence to support the use of particular technologies, in the development of safe and reliable systems. These projects are particularly encouraged to submit papers to this conference, which has been selected as one of the events at which ESSI Application Experiments can present their results for peer review and evaluation.

This is an open call for papers: we also seek other papers which argue for the suitability of particular technologies, methods or management approaches for use in developing reliable and safe systems, especially those which present the results of industrial experience.

Topics that could be addressed include:

A historical perspective on safety cases, and on how the current regulations requiring the production of safety cases have arisen.

How do software engineering methods and tools contribute to product safety, reliability, etc.?

What evidence is there to support the use of particular technologies to achieve reliable systems?

How do organisations deal with the safety and reliability of PES? Do different industrial sectors deal with PES safety and reliability in a similar manner?

Should we focus on management procedures more and technology issues less? (Some accident reports suggest this is so.)

Are tightly coupled time critical systems inherently less safe or reliable than other systems?

How do software metrics, software reliability models, etc., relate to dependability attributes?

How do we deal with the integrity of evidence used in safety arguments?

What is the impact of organisational rules and work practices  
on safety and reliability?

#### Dates for Authors

=====

Authors are invited to submit extended abstracts (two A4 pages),  
or near full papers, to Carol Allen at the address given below.  
Papers should be written in English which will be the language  
of the Workshop/Conference. The following dates have been set:

Submission of abstracts/papers	31st January 1995
Notification of acceptance	28th February 1995
Announcement of provisional programme	31st March 1995
Workshop version of paper available	31st May 1995

The proceedings will be published following the Workshop. As  
there is a requirement for the proceedings to be edited changes  
may be requested of authors after the papers have been  
presented.

#### Organising and Programme Committee

=====

Roger Shaw	Chair	Lloyd's Register
Carol Allen	Administration	City University
Ole Anderson		DELTA (Denmark)
Tom Anderson		Newcastle University
Robin Bloomfield		Adelard
Sandro Bologna		ENEA CRE-Casaccia (Italy)
Annie Combelles		Objectif Technologie (France)
Chris Dale		ENCRESS Project Manager
Norman Fenton		City University
Bev Littlewood		City University
Bob Malcolm		Malcolm Associates
Francesca Saglietti		ISTec (Germany)
Peter Scharbach		Lloyd's Register

#### Contacts:

=====

Chairman: Roger Shaw	Administration: Ms Carol Allen
Lloyd's Register	Centre for Software Reliability
Lloyd's Register House	City University
29 Wellesley Road	Northampton Square
Croydon	London
CRO 2AJ	EC1V 0HB

Tel: +44 (0)181 681 4818	Tel: +44 (0)171 477 8421
Fax: +44 (0)181 681 4839	Fax: +44 (0)171 477 8585
email: roger.shaw@aie.lreg.co.uk	email: c.a.allen@csr.city.ac.uk



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 16: Issue 67**

**Friday 23 December 1994**

## Contents

- [Software glitch snares Social Security Administration](#)  
[Mike Manos](#)
- [Cancelbot Derails Online Promo](#)  
[WSJ via Edupage](#)
- [Ben & Jerry's expects first loss](#)  
[Arthur D. Flatau](#)
- [Proliferation of Cockpit Warning Signals](#)  
[David Walter](#)
- [Year 2000 date problems already happening now](#)  
[Elana](#)
- [Re: Prevention of Oral Hacking](#)  
[Brad G. Parks](#)
- [Re: Pentium FDIV problem - so what's new?](#)  
[Mark Brader](#)
- [Intelligent Commentator on McNeil-Lehrer](#)  
[D.P. Schneider](#)
- [Financial Payment Systems](#)  
[Jeff Stapleton](#)
- [Possible solution to the \(electronic\) meme problem](#)  
[Bob Mehlman](#)
- [Advertising on the Net](#)  
[Mich Kabay](#)
- [Risk Takers Among Management](#)  
[Tom Kaiser](#)
- [Re: Koppel et al.](#)  
[Peter da Silva](#)
- [Re: Microsoft and the Catholic Church](#)  
[John Stevenson](#)
- [EDUPAGE on the WWW](#)  
[Timothy Hunt](#)
- [Public CM WAIS Server to end operation](#)  
[WAIS Admin](#)
- [Call for Papers and Panels: National Information Systems Security Conf.](#)  
[Jack Holleran](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Software glitch snares the Social Security Administration

Mike Manos <MMANOS@uhd2.uhd.com>

Wed, 21 Dec 1994 14:49:13 EST

[from Federal Computer Week, 21 Nov 1994]

The Social Security Administration has uncovered a software coding error that over the years nicked and dimed Social Security recipients out of \$478.5 million. The problem occurred in 1978, when SSA wrote new code because employers began reporting earnings annually rather than quarterly. The software program, with its 76 sets of variables, had a few holes in it. Over 16 years, about 426,000 people did not receive appropriate payment increases.

---

## Cancelbot Derails Online Promo (WSJ via Edupage 12/20/94)

Edupage <info@ivory.educom.edu>

Tue, 20 Dec 1994 18:15:26 -0500

### CANCELBOT DERAILS ONLINE PROMO

Messages promoting "Netchat," a new book by Michael Wolff, have been unceremoniously wiped out by someone calling him/herself "Cancelmoose." The vigilante, who used a program called a cancelbot, worked through a computer in Finland that enables a mail sender to remain anonymous, and claims to have performed similar services more than a dozen times in the past. (\*Wall Street Journal\*, 20 Dec 1994, p. B7)

---

## Ben & Jerry's expects first loss

Arthur D. Flatau <flatau@cli.com>

Wed, 21 Dec 94 08:52:14 CST

According to an article (page F2) in the Tuesday December 20, 1994 issue of the Austin American Statesman (from the Associated Press) Ben & Jerry's Homemade Inc. is going to report its first quarterly loss since it went public. Quoting some of the relevant to risks part of the article:

Adding to the bad news, the company said Monday that recurring problems in a computerized handling system will force it to delay opening a new, more efficient manufacturing plant in St. Albans, Vt. until the middle of next year. [...]

"While our earnings have been negatively impacted in 1994 by the inefficiencies in the company's production planning, purchasing and inventory management systems ... the anticipated loss in the current quarter is due primarily to lower than expected sales level," [Ben & Jerry's President Chuck] Lacy said in a written statement. [...]

At the new St. Alban's plant, a computerized system that was supposed to automate handling of ice cream after it has been packed into pints has software problems, forcing the company to substitute a more conventional system.

That likely will require installation of different equipment and more employees for handling, although the company said it will still be more efficient than current manufacturing.

The St. Albans plant is designed to consolidate all of Ben & Jerry's manufacturing in Vermont again. The company hires Edy's [a major competitor] of Fort Wayne, Ind. to make about 37 percent of its ice cream, [Ben & Jerry's spokesman Rob] Michalak said.

Art flatau@cli.com Computational Logic, Inc. Austin, Texas

---

## Proliferation of Cockpit Warning Signals

<D.Walter@sheffield.ac.uk>

Wed, 21 Dec 94 13:54:23 GMT

The avionics thread seems to have gone quiet, perhaps because none of the several recent airliner crashes has involved an A320 aircraft. Here is an account of an incident I came across recently which highlights the problem of proliferation of warning signals in complex human-machine interfaces.

The incident involved a Continental Airlines 727 which came perilously close to landing gear-up at Chicago O'Hare about a year ago.

Initial investigation indicated that the crew had become distracted from their landing check-list by TCAS (Traffic Collision Avoidance System) warnings which sounded repeatedly as they flew through the busy airspace around O'Hare. The 727's gear warning did not trigger because the flap setting was 25 degrees instead of the usual 27.5 (in order to maintain speed on approach as requested by air traffic control). A ground proximity warning did sound at 500 ft, but lack of gear is only one of a number of possible causes for this warning.

A taxiing American Airlines pilot saw the 727 on short final with no gear. The tower radio transcript makes hair-raising reading:

American: "Tower, Continental's got no gear!"

Tower: "Who's got no gear?"

American: "Continental, just about ready to touch down on two-seven left"

The ground controller shouted to his colleague who was controlling Continental's approach, who warned:

"Go around, go around Continental. No gear!"

The 727 succeeded in executing a go-around, but not before scraping the rear third of the fuselage on the runway. It landed normally out of the second approach.

David Walter

---

## Year 2000 date problems already happening now

*Elana who? <elana@netcom.com>*

*Fri, 23 Dec 1994 05:48:33 GMT*

A few months ago, there was an excellent article in RISKS about the problems of the year date rolling from xx/xx/99 to xx/xx/00 and how it could affect computer systems. Today I mentioned the article in passing to a rep at my local bank as I was making a routine deposit. She said: "It's happening already." Apparently there is a problem with some of the credit cards they have been issuing to their customers. The expiration date on them is the year 2000, and for some tech reason she could not explain, two major stores here in town refuse to take them "because that weird date messes up their computers."

I regret that I cannot offer more info than this, but it is serious food for thought...

-Elana

[See the latest American Scientist, Jan-Feb 1995, which has a very nice article by Brian Hayes, spanning the entire subject. (Much of it is drawn from the RISKS Archives.) PGN]

---

## Re: Prevention of Oral Hacking

*Brad G. Parks <bparks@intcorp.com>*

*Thu, 22 Dec 94 11:21 CST*

I am a big fan of Voice Recognition Technology, however trite and useless people may say it is. And one thing that people have failed to mention so far that there are ways to prevent/discourage oral hacking (at least with Macintosh's general program).

With the Mac program there is an option that allows the user to name the computer something other than "Computer." There is another option for setting an "Attention Key" to basically give the program earplugs until that key is pressed again. There is also a voice recognizing option that sets how precise your language must be.

It is doubtful, at least to me, that somebody running around the office yelling "Computer, Restart, Yes" would restart my Mac, whose name is Alfred, has the precision level set rather high, and also has the voice recognition asleep until i press Keypad-0.

Brad G. Parks (bparks@intcorp.com) [Software Engineer, O-Programmer]  
Introl Corporation (612)-631-7810 2675 Patton Rd. St.Paul, MN 55113

[Ah, now we know! And we can record your normal voice and replay it. PGN]

---

## Re: Pentium FDIV problem - so what's new? (Peterson, [Risks-16.66](#))

<msb@sq.com>

Wed, 21 Dec 1994 14:03:47 -0500

It occurs to me that the English vocabulary might be related to why people have reacted so strongly to the existence of this bug -- which, let's face it, is not all that devastating \*relative to other bugs\*. The term "computer" suggests that computation is the most important and fundamental thing that the machine does, and because of this, any bug directly related to computation is seen as more serious than others.

In French the machine is called an "ordinateur", which is related to our word "ordinal" and conveys connotations of \*organizing\* data. What we mostly call computer science, they call "informatique" -- the study of information. And if you think about what computers are used for today, you will see that these terms are at least as fitting as the English ones. In English when we really mean that computation is the important part of the work, we use terms like "numerical" in addition to "computing".

Would English speakers have reacted equally strongly to a -- no pun intended -- comparable bug in the instructions for comparing and branching? I think they would not.

(No, you don't need to tell me that a large part of the reaction in this case was to Intel's reaction, not to the original problem.)

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

---

## Intelligent Commentator on McNeil-Lehrer

<d\_schneider@emulex.com>

Thu, 22 Dec 94 16:34:00 PST

A recent McNeil-Lehrer report (I'm pretty sure it was Tuesday night's -- 12/20/1994) had an intelligent commentator as an interviewee on the Pentium situation.

I agree with his comments about the Pentium (that the problem was probably more severe than Intel admitted and less severe than IBM trumpeted), but the reason I'm pointing this interview out is because Robin McNeil asked something to the effect, "So the issue is also that we shouldn't trust an answer just because the computer gave it to us?" The interviewee answered that this was just so, and that we should keep asking for and demanding proof that the computer is giving good answers.

There were also what I thought were intelligent comments on the difficulty of thoroughly testing such complex parts, and that testing had to involve strategies to maximize the confidence obtained.

I hope that one of your other submitters has given (or will give) the identity of the interviewee, and some exact quotes. I was impressed by his grasp of the big picture, and that he managed to convey it to the interviewer, too. (I think the choice of interviewer helped, but even intelligent interviewers can't be prepared to understand all issues, and McN-L tend to have more news on political and economic issues than on technical issues).

Hope you caught the interview, too!

/dps

---

## Financial Payment Systems

<mc!Jeff\_Stapleton@mhs.attmail.com>

Thu, 22 Dec 1994 10:56:25 -0600

In regards to [RISKS-16.64](#) here are some thoughts and concerns about financial payments on the World Wide Web, CommerceNet, the Internet, and electronic media in general:

Debit card payments today require an additional piece of authenticating data - the Personnel Identification Number or PIN. There are ISO (9564) and ANSI (X9.8) standards which tell us how to securely formulate a PIN block and encrypt it using the Data Encryption Algorithm or DEA (X3.92). Credit card payments may soon also require the PIN. However, we have no standards today telling us how to encrypt PINs using public key algorithms. True, the advent of the smartcard may eliminate the transmission of PINs, but not for a while yet (years?).

Speaking of public key cryptosystems, there ARE existing ISO and ANSI standards available today:

- ISO-CD 11568 parts 4 and 5 just completed the public ballot process.

- ANSI X9.30 part 1 - The Digital Signature Algorithm (DSA)

- ANSI X9.30 part 2 - The Secure Hash Algorithm (SHA)

- ANSI X9.30 part 3 - Certificate Management for the DSA is completing its public ballot process.

However, due to the legal problems between Cylink Corporation and RSA Data Security on fair licensing agreements for the RSA patents, the matching set of ANSI standards (X9.31 parts 1, 2, and 3) for RSA may be put on hold by the Accredited Standards Committee (ASC) X9 - for further details, call:

- X9 secretariat, American Bankers Association (ABA), 202-663-5284

- X9F chairman, Marty Ferris, 202-622-1110

- X9F1 chairman, Blake Greenlee, 203-762-8580

Although the standard addresses the DSA, X9.30-3 Certificate Management is rather generic and deals with the roles and responsibilities of the

asymmetric key pair owners, the certificate authority(s), and the public key users. Interesting stuff and can (and should be) used for implementing any public key cryptosystem. Copies can be purchased from the ABA (plug).

Jeff J. Stapleton - MasterCard International

---

## Possible solution to the (electronic) meme problem

<rmehlman%grumpy.decnet@UCLASP.IGPP.UCLA.EDU>

Wed, 21 Dec 1994 18:43:08 PST

Keith Henson ([RISKS 14.63](#)) points out that computer viruses and human fads fit Richard Dawkins' concept of a meme, adding

What computers and fast communications have done is to radically change the replication constants for memes, and to make unworkable the controls society has tried to put on such things.

In "Mind Viruses" (American Scientist, Jan-Feb 1995, p.26), Michael Szpir discusses 'human information parasites', such as the St. Jude 1 chain letter, likened to memes by Dawkins and Oliver Goodenough (Nature, Sept 1, 1994).

Some years ago, I received an electronic chain letter, complete with lengthy sequential history of previous senders. These letters differ from the old-fashioned kind -- they always have return addresses. It occurred to me that the appropriate response was to SEND IT BACK, and encourage the sender and all others to do likewise, hoping an avalanche of returned mail would eventually swamp the original sender, if it didn't bring the network to its knees.

No such luck. I actually tried it, forwarding the letter back to the sender with subject LET'S SEND IT BACK. Unfortunately, he returned it immediately, longer by two headers, with subject THAT'S NOT FAIR...IT'S GOT TO BE 5 OTHER PEOPLE. I did not repeat the experiment, though I tried unsuccessfully to get others to do so.

Still, I wonder, next time a chain letter or other intentional meme spreads through the Internet, if everyone returned their copies to the sender ...

Bob Mehlman, UCLA/IGPP

---

## Advertising on the Net

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>

22 Dec 94 14:25:04 EST

In the 05 Dec 1994 issue of *\_Network World\_* on p. 41, "John Doe" recounts his tale of woe after advertising on the Internet ("Ad leads to a nightmare on Cyber-Street). In brief, his main points are

- \* Placed ads in several USENET groups.
- \* Swamped with email abuse and flames in the groups as a result.

- \* Someone posted his 800- number in alt.sex groups as a phone-sex #.
- \* Switchboard swamped with requests for phone sex; operators horrified.
- \* One switchboard op quit because of what callers were saying.
- \* All 800- calls switched to the originator of the advertising as punishment.
- \* Impractical to cancel 800- service because of special letter combinations.

Moral: don't advertise on the Net.

<<Comments by MK:

One issue is whether it's good or bad to advertise on the Net.

Another is whether it's good or bad to respond to advertising on the Net in the ways demonstrated in this case.

Yet another is that exactly the same techniques could be used against any organization even if it \_doesn't\_ advertise on the Net.<>

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn

---

## Risk Takers Among Management

*Tom Kaiser <Tomkaiser@aol.com>*

*Thu, 22 Dec 1994 23:22:43 -0500*

Subject: Upper Managements View of Information Security(Infoworld 12/19/94)

The following extract from INFOWORLD 12/19/94 demonstrates some of the risks inherent in human management. (I read this shortly before reading [RISKS 16.66](#) and the posts calling for papers and serious work in all areas of network and computer security).

42% of senior management at U.S. companies consider information security to be only "somewhat important" or "not important," according to a survey by Ernst and Young LLP, with 15% of companies devoting no full time resources to security. This though even more than half the respondents reported information-related losses. Also , among respondents who said they were running "mission-critical applications" on their LAN's, half reported that security was unsatisfactory. What will it take to make security a priority in industry? The Stealth bomber blueprint on place mats in Pizza Hut? (end copy)

We can only hope that some of the recent antics and activities on the network cause these top managers to focus some their energies, and resources on the protection of their (our?) data. Analysis of all probable problems and or threats should precede implementation of any changes to or introduction any systems. I think most readers of RISKS would enjoy reading the entire poll and possibly having helped in phrasing some of those obscure questions, and "open to interpretation answers."

Thomas Kaiser Tomkaiser@aol.com

---

**Re: Koppel et al. ([RISKS-16.66](#))**

*Peter da Silva <peter@nmti.com>*

*Thu, 22 Dec 1994 17:51:54 -0600*

I seem to recall someone with the name of "Hughes" being forced to change the name of his hotel because Howard Hughes objected. Be glad your name doesn't match someone like that.

---

**Re: Microsoft and the Catholic Church ([RISKS-16.66](#))**

*John Stevenson <john@mtnbike.demon.co.uk>*

*Fri, 23 Dec 1994 22:53:37 +0000*

>Microsoft has no plans to acquire Catholic Church (from EDUPAGE)

Surely the big RISK here is that the world is infested with people who lack even a trace of a sense of humour. Hoax? I believe 'Microsoft to acquire Catholic Church' was what we writers call 'a joke'.

John Stevenson john@mtnbike.demon.co.uk mbuk@cix.compulink.co.uk

[I would call it a \*parody\*. RISKS readers seem to be a cut above the average in terms of not being fooled so easily, especially by such obvious parodies. But remember there are a lot of nontech folks out there with very bad spoof-suspicion thresholds. Even the most \*obvious\* humor sometimes gets taken seriously. Remember what happened to Piet Beertema's Chernenko hoax! Many people took it very seriously. Some might have even attempted to spoof the spoofer by pretending to take it seriously. At any rate, best wishes for a happy new year, with its own collection of good humor. PGN]

---

**EDUPAGE on the WWW**

*"Timothy Hunt [Assistant Unix Systems Manager]" <timothy@icr.ac.uk>*

*Wed, 21 Dec 94 14:55:07 +0000*

Noticing the article that made reference to EDUPAGE [Microsoft has no plans to acquire Catholic Church], RISKS readers may be interested to know that EDUPAGE is available via the Web, with URL : <http://www.ee.surrey.ac.uk/edupage>

Timothy J. Hunt, Joint Dept. of Physics, The Inst. of Cancer Research, Downs Road, Sutton, Surrey England SM2 5PT Timothy@icr.ac.uk +44(0)181 642 6011 x3312

---

**Public CM WAIS Server to end operation**

*Wais Administrator account <waisadm@cmns.think.com>*

*Thu, 22 Dec 94 11:36:41 EST*

The Public CM WAIS Server, which has provided a searchable database of past RISKS traffic as risks-digest.src, will cease operation on 27 December 1994. Please update the "Info on RISKS" item and inform your readers of the change.

[Here we come a-WAIS-ailing! And many thanks for your past serv-ice! PGN]

---

## Call for Papers and Panels: National Information Systems Security

Jack Holleran <Holleran@DOCKMASTER.NCSC.MIL>

Thu, 22 Dec 94 20:13 EST

CALL FOR PAPERS AND PANELS  
18TH NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE  
(formerly the National Computer Security Conference)

Co-sponsored by the National Computer Security Center and  
the National Institute of Standards and Technology

Baltimore Convention Center, Baltimore MD  
October 10-13, 1995

The National Information Systems Security Conference audience represents a broad range of information security interests spanning government, industry, commercial, and academic communities. Papers and panel discussions typically cover:

- ( research and development for secure products and systems presenting the latest thinking and directions;
- ( practical solutions for real-world information security concerns;
- ( implementation, accreditation, and operation of secure systems in a real-world environment;
- ( evaluation of products, systems, and solutions against trust criteria;
- ( security issues dealing with rapidly changing information technologies;
- ( network security issues and solutions;
- ( management activities to promote security in IT systems including security planning, risk management, and awareness and training;
- ( international harmonization of security criteria and evaluation;
- ( social and legal issues such as privacy, ethics, investigations, and enforcement;
- ( tutorials on security basics and advanced issues; and
- ( highlights from other security forums.

We invite the submission of papers and proposals for panel discussions in any of the above areas as well as other topics related to IT system security. We especially encourage student papers written by individuals in degree programs. The student should not have been previously published, and the paper shall be endorsed by an academic advisor.

BY MARCH 1, 1995: Eight (8) copies of your draft should arrive at the following address. See instruction on reverse side regarding the format of your submission and accompanying information required.

National Information Systems Security Conference

Attn: Conference Secretary, APS XI  
National Computer Security Center  
Fort George G. Meade, MD 20755-6000

BY JUNE 1, 1995: Authors and Panel chairs selected to participate in the Conference will be notified and advised when final papers and panel statements are due.

For additional information on submissions, please call (410) 850-0272 or send Internet messages to NISS\_Conference@DOCKMASTER.NCSC.MIL. For other information about the National Information Systems Security Conference, please call (301) 975-2775.

#### PREPARATION OF CONFERENCE SUBMISSIONS

Cover Sheet: Type of submission (paper, panel, tutorial)

Title or Topic  
Abstract (not to exceed 250 words)  
Author(s)  
Organizational Affiliation  
Phone numbers (voice and fax, if available)  
Internet address, if available  
Point of Contact, if more than one author

Submissions related to work under U.S. Government sponsorship must also include the following information:

U.S. Government Program Sponsor or Procuring Element  
Contract Number (if applicable)  
U.S. Government Publication Release Authority

Classified material or topics must NOT be submitted.

Draft Papers:

10 page maximum, including figures and references.  
Include title, abstract, and keywords on first page.  
No more than 12 characters/inch and 6 inches/line.  
One-inch margins all around.

Since the paper referee process will be anonymous, names and affiliations of authors should appear only on the separate cover sheet. All submissions are treated as proprietary information belonging to the authors.

Release for Publication and Copyright: Authors are responsible for obtaining government or corporate releases for publication. Written release will be required for all papers to be published. Papers developed as part of official U.S. Government duties may not be subject to copyright. Papers that are subject to copyright must be accompanied by written assignment for multi-media publication to the National Information Systems Security Conference Committee.

#### PANEL PROPOSALS:

( Panels are limited to 90 minutes, including time for prepared remarks, discussion, and audience interaction.

- ( Proposals are not to exceed two pages but should summarize the topic, issues, viewpoints and questions that will be addressed by the panel.
- ( Proposals are to include the names of panelists, panel chair, and affiliation of each participant.
- ( Each panel is limited to **\*five (5)\*** persons, including panel chair and four (4) panelists.
- ( Panels will be selected by the Conference Committee. Panel chairs and panelists will be expected to provide written statements for inclusion in the Conference Proceedings.
- ( Panel proposals **\*must be\*** received by March 1, 1995.



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 16: Issue 68**

**Tuesday 27 December 1994**

## Contents

- [Washington Post flubs stock prices](#)  
[William C. Fenner](#)
- [Sorcerer's Apprentice Hits Medicare](#)  
[Mich Kabay](#)
- [\\$25m power bungle: Automation at Australian electricity plant](#)  
[Tom Worthington](#)
- [Buy a country for \\$1200](#)  
[Amos Shapir](#)
- [Re: Mary Payne and "Good to the Last Bit"](#)  
[Jim Haynes](#)
- [Rate Hike For Universal TouchTone?](#)  
[Leonard Erickson](#)
- [Re: Year 2000 date problems already happening now](#)  
[Scot E. Wilcoxon](#)
- [Re: American Scientist article on the year 2000](#)  
[Brian Hayes](#)
- [RISKS of guessing at Fair Use](#)  
[Mich Kabay](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Washington Post flubs stock prices

"William C. Fenner" <[fenner@cmf.nrl.navy.mil](mailto:fenner@cmf.nrl.navy.mil)>  
Tue, 27 Dec 1994 09:01:22 -0500

The Washington Post printed a full page of old stock prices one day last week in their business section. According to their explanation, the data is normally stored in a file named "ap stox 2". In preparing the erroneous page, a user saw "ap stox2" (i.e. no space) "elsewhere in the machine" and used it instead.

The article also says that "Steps have been taken to prevent a recurrence". I wonder what kind of steps? Educating users? Probably the most useful thing to do would be to have the date in the filename, so an old file could

not be mistaken for current data.

Bill Fenner            fenner@cmf.nrl.navy.mil

---

## Sorcerer's Apprentice Hits Medicare

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
26 Dec 94 16:37:59 EST*

The Associated Press newswire for 94.12.26 @ 02:43 EST (via CompuServe's Executive News Service) reports a case of failed identification and authentication:

Sting Backfires.

MIAMI (AP) -- FBI agents thought they were setting a trap by buying copies of 35 Medicare cards and selling them to a suspected fraud operation.

But now the cards are being used to buy expensive leg braces and other medical equipment -- and the FBI can't track them.

"The FBI lost control of the cards. Now they have a monster on their hands," a government investigator familiar with the case told The Miami Herald for a story in Sunday's issues.

According to the story, Medicare spokesperson "Faye Baggiano, associate administrator of the Health Care Financing Administration in Washington," admits that they have used the social insurance number as the Medicare identifier; therefore "Medicare says it can't cancel the copied cards, which have been circulating for 16 months, because that would wipe out legitimate federal benefits to the people whose names are on those cards."

Normally, Medicare "provides phony numbers that can be canceled; it is unclear why the FBI used real numbers.

An analysis of just 10 of the 35 stolen cards shows "a total of \$163,745 for services that the real card holders say they never got or tried to get."

<<Comments by MK: yet another case where inadequate identification and authentication leads to problems--not to speak of the design error of using production data for test purposes!<>

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn.

---

## \$25m power bungle: Automation at Australian electricity plant

*Tom Worthington <tomw@ccadfa.cc.adfa.oz.au>  
Tue, 27 Dec 1994 12:13:02 GMT*

The attached is from the headline story Tuesday 27 December of the

Courier-Mail newspaper (ph: +61 7 2526011, fax: +61 7 2526696) in the state of Queensland, Australia. I thought it may be of interest to readers of "Risks" as it covers a number of themes discussed before:

**\$25m power bungle - Report slams hi-tech move**  
Exclusive by Ed Southern

A \$25 million project to turn one of the state's power stations into an automated plant created an unsafe workplace requiring twice the number of engineers to run, a confidential report reveals. The new automatic control systems also caused more than \$1.5 million damage to machinery at the Swanbank station near Ipswich.

...The audit found the Swanbank automatic control system had failed to protect the plant from damage. The system had been unable to prevent a "trip" (temporary shutdown) cutting oil flow to a turbine. This had resulted in a bent shaft leaving the turbine with reduced generating capacity. ...The automatic alarm system which tells operators how the plant is functioning was not properly operating almost two years after it was installed. ...The report found lack of adequate testing before commissioning and "waving of proper commissioning and acceptance testing procedures" and "a single-minded drive to meet target dates."

[Posted by Tom Worthington, Director of the Community Affairs Board,  
Australian Computer Soc. Inc. tomw@adfa.oz.au <http://www.peg.apc.org/~tomw>

---

## **Buy a country for \$1200**

*Amos Shapir <amos@cs.huji.ac.il>*  
*25 Dec 1994 17:21:07 +0200*

Police in Israel have started an investigation last week to determine how the entire population registry of the country has ended up being offered for sale by a private company, on a CD ROM disk for \$1200.

Political parties are entitled to get the voters registry (which includes people's names, addresses, birth dates and ID number) from the Ministry of the Interior. The latest elections in 1992 were the first time this information was disseminated on a CD ROM and not just printouts; these disks should have been returned to the Ministry after the elections, and were coded and numbered, but it's not clear from newspaper reports here how this coding was done, and how this was supposed to prevent the parties or their employees from keeping their own copies.

In addition to the registry (which is actually public information, though not freely available) the government-owned phone company sells a disk containing all phone books, and the government's companies registry is also available (I'm not sure if it is sold legally).

All this information enabled a TV reporter to demonstrate getting the list of all companies privately directed by the minister of Finance (including the names of all other directors), or the private address and phone number

of the chief of the Mossad and all of his neighbors (which were shown on screen, though with illegible resolution).

Israel is a small country, but it's only a matter of time and computing power before this kind of personal information processing is available everywhere.

Amos Shapir, The Hebrew Univ. of Jerusalem, Dept. of Comp. Science,  
Givat-Ram, Jerusalem 91904, Israel +972 2 585706,586950 amos@cs.huji.ac.il

---

## Re: Mary Payne and "Good to the Last Bit"

*Jim Haynes <haynes@cats.ucsc.edu>*

*Fri, 23 Dec 1994 17:31:13 -0800*

Perhaps it didn't happen on Mary Payne's watch; but I do recall there was a problem with floating point in early VAX-11/780 machines. Believe it required a microcode change, and a board swap for machines equipped with a floating point accelerator. Then there was the early production G.E. 635 floating point problem which resulted from truncating, rather than rounding, a 2's complement number, giving a negative bias to the results. Supposedly (urban legend alert!) this was recognized as important when a tape calculated on one of the machines was used to operate a numerically-controlled cutting torch. The torch was supposed to cut a circular plate out of a thick piece of steel. The actual cut had a jog in it, resembling (coincidentally, I'm sure) the "Intel Inside" logo. Then there was the floating point problem early in the life of the IBM 360 series. As I recall this was not so much an error as a surprisingly sudden loss of significance resulting from the base-16 fractions, such that a shift for exponent alignment shifted four bits at a time. And I recall some allegation about an early CDC machine (1604? 3600?) in which fixed point  $-1 \times -1 = -1$ .

---

## Rate Hike For Universal TouchTone? (nonincluded message, Pelletier)

*Leonard Erickson <Leonard.Erickson@f51.n105.z1.fidonet.org>*

*Sun, 25 Dec 1994 07:34:20 -0800*

> Is this just a ploy to line their pockets from their captive market?

No. Take another look at the figures you quoted. It costs *\*more\** to support pulse dialing. They can't go 100% touchtone until all their subscribers quit using old gear. So they have to keep the "pulse counters" around (and maintained) until then. Therefore, if you want pulse dialing, they are going to charge you \$2 extra each month.

This is the most *\*sensible\** thing I've seen a phone co. do in a long time. It encourages folks to quit using pulse/rotary phones. And it gives them hard figures on how many folks still can't use touchtone.

---

## Re: Year 2000 date problems already happening now (Elana, [RISKS-16.67](#))

Scot E. Wilcoxon <sewilco@fieldday.mn.org>

Sat, 24 Dec 94 16:26 CST

A local newspaper in Minneapolis recently ran a short article about the year 2000 problems, and pointed out that in 1995 any five-year planning programs are at risk.

Scot E. Wilcoxon sewilco@fieldday.mn.org +1 612 936 0118

---

## American Scientist article (PGN, [RISKS-16.67](#))

Brian Hayes <bhayes@mercury.interpath.net>

Sat, 24 Dec 1994 13:12:38 -0400

[With regard to Brian's "Computing Science" column in the Jan-Feb 1994 issue of *\_American Scientist\_* (Vol. 83, No. 1, pp. 12-15), <P.O. Box 13975, Research Triangle Park, NC, 27709, 800-282-0444>, which PGN noted in [RISKS-16.67](#), Brian has made the following offer:]

For net denizens who don't read ink on paper, I can supply a plain-ASCII version of the article's text by E-mail. Send me a request at bhayes@mercury.interpath.net.

[The column is based largely on material that has appeared in the RISKS Forum over the years. (Thanks, folks!) BH]

---

## RISKS of guessing at Fair Use

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>

26 Dec 94 22:15:12 EST

In an article by Andrew Lawler in *\_Science\_* magazine (94.11.25; 266:1315) entitled "Court says no to copying articles," we read of a recent case which may affect anyone who collects news, newspaper, magazine and journal articles:

Thinking of photocopying an article from your favorite journal? Think again. Last month [in October 94] a three-member federal appeals court in New York ruled that a Texaco Corp. scientist violated copyright laws by making one copy each of eight articles in a scientific journal and placing them in his files. The 2-1 ruling dramatizes the uncertainty over what constitutes fair use of copyrighted material, say lawyers familiar with the case, adding that the ruling should prompt companies and universities to review their policies toward copying.

According to the author, the suit was launched by the American Geophysical Union (AGU) and more than 80 other plaintiffs. They accused Texaco of "copying and distributing hundreds of scientific articles to hundreds of

researchers" and picked a sample case for the civil suit.

The court ruled that because the scientist in the sample case (David Chickering, who copied the eight articles from the journal *Catalysis*) filed the papers away in his library rather than use them immediately, he was in violation of the fair use laws governing copyrighted materials.

The dissenting judge wrote that because the defendant used the copied materials for research only, that use fell under existing fair use doctrine.

"Jon Baumgarten of Proskauer, Rouse & Gpetz & Mendelsohn in Washington," one of the lawyers for the plaintiffs, said that it's not true that "all educational use is fair use." He advised academic researchers to "Consult with your university counsel before making copies."

<<Comments by M.K.: This ruling has serious implications for anyone who uses online databases of bibliographic material; e.g., the Computer Database Plus owned by Information Access Company (IAC) and available on CD-ROM and online via CompuServe. The terms of use for the online service include the following text:

#### TERMS AND CONDITIONS

Computer Database Plus and its contents are copyright (c) 1988-1994 by Information Access Company (IAC) and/or its data suppliers. Copying, retransmitting, redistributing or publishing any part of this database, either in hardcopy or electronically, is prohibited.

The material contained in this database is provided only to individual users. Users may electronically store downloaded material only to facilitate changing the format or presentation of the material. If the user is retrieving information on behalf of another, the user may supply only one (1) printed copy. Copyright notices must not be removed from any material retrieved from this database.

Judging from the ruling described above, the IAC may very well be able to argue that its rules are not superseded by fair use doctrine. Thus storing specific articles in files on one's own hard disk for later search and use may be prohibited regardless of intention or actual use.

Similarly, the Executive News (ENS) Service on CompuServe, which provides news wire feeds in real time, allows users to store captured stories ("clippings") for a maximum of 14 days, after which they are discarded automatically. The introductory text for this service makes no specific restrictions on storage.

In ENS, individual newswires have different copyright wording:

\* AP includes, "All rights reserved. The information

contained in this news report may not be republished or redistributed without the prior written authority of The Associated Press."

\* Reuter's entries state, "Copyright Reuters America Inc. 1994. All rights reserved."

\* UPI articles include only, "Copyright 1994 United Press International"

\* Washington Post has, "Copyright 1994 The Washington Post."

It may be that storing copies of these articles in one's own online archives is actionable.

For those unfamiliar with fair use doctrine, I include the following commentary to stimulate further thought and discussion:

----- %<>== -----

#### US COPYRIGHT OFFICE CIRCULAR ON FAIR USE (1993)

One of the rights accorded to the owner of copyright is the right to reproduce or to authorize others to reproduce the work in copies or phonorecords. This right is subject to certain limitations found in sections 107 through 120 of the copyright act (title 17, U.S. Code). One of the more important limitations is the doctrine of "fair use." Although fair use was not mentioned in the previous copyright law, the doctrine has developed through a substantial number of court decisions over the years. This doctrine has been codified in section 107 of the copyright law.

Section 107 contains a list of the various purposes for which the reproduction of a particular work may be considered "fair," such as criticism, comment, news reporting, teaching, scholarship, and research. Section 107 also sets out four factors to be considered in determining whether or not a particular use is fair:

- (1) the purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes;
- (2) the nature of the copyrighted work;
- (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- (4) the effect of the use upon the potential market for or value of the copyrighted work.

The distinction between "fair use" and infringement may be unclear and not easily defined. There is no specific number of words, lines, or notes that may safely be taken without permission. Acknowledging the source of the copyrighted material does not substitute for obtaining permission.

The 1961 \_Report of the Register of Copyrights on the General Revision of the U.S. Copyright Law\_ cites examples of activities that courts have regarded as fair use: "quotation of excerpts in a review or criticism for

purposes of illustration or comment; quotation of short passages in a scholarly or technical work, for illustration or clarification of the author's observations; use in a parody of some of the content of the work parodied; summary of an address or article, with brief quotations, in a news report; reproduction by a library of a portion of a work to replace part of a damaged copy; reproduction by a teacher or student of a small part of a work to illustrate a lesson; reproduction of a work in legislative or judicial proceedings or reports; incidental and fortuitous reproduction, in a newsreel or broadcast, of a work located in the scene of an event being reported."

Copyright protects the particular way an author has expressed himself; it does not extend to any ideas, systems, or factual information conveyed in the work.

The safest course is always to get permission from the copyright owner before using copyrighted material. The Copyright Office cannot give this permission.

When it is impracticable to obtain permission, use of copyrighted material should be avoided unless the doctrine of "fair use" would clearly apply to the situation. The Copyright Office can neither determine if a certain use may be considered "fair" nor advise on possible copyright violations. If there is any doubt, it is advisable to consult an attorney.

\*\*\*Last update 6/10/93 (raa)\*\*\*

-----%<>==-----

Another useful document is the following:

(DRAFT VERSION) COPYRIGHT LAW AND MULTIMEDIA DEVELOPMENT IN EDUCATION

Section 106 of the Copyrights Act (P.L. 94-553) describes the exclusive rights of copyright owners.

"[T]he owner of copyright...has the exclusive rights to do and to authorize any of the following:

1. To reproduce the copyrighted work in copies or phonorecords;
2. To prepare derivative works based upon the copyrighted work;
3. To distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
4. In the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly; and
5. In the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display

the copyrighted work publicly."

The fair use provision of the Copyrights Act is found in Section 107 which is reproduced below.

"Notwithstanding the provisions of section 106, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include--

1. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
2. the nature of the copyrighted work;
3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. the effect of the use upon the potential market for or value of the copyrighted work."

The legislative history which speaks to the fair use provision acknowledges:

"The judicial doctrine of fair use, one of the most important and well established limitations on the exclusive right of copyright owners, would be given express statutory recognition for the first time in section 107. The claim that a defendant's acts constituted a fair use rather than an infringement has been raised as a defense in innumerable copyright actions over the years, and there is ample case law recognizing the existence of the doctrine and applying it."

It should be noted that at this point, the legislative history reiterates the four points listed above from section 107. Fair use must meet all four criteria to be a protected activity.

"Although the courts have considered and ruled upon the fair use doctrine over and over again, no real definition of the concept has ever emerged. Indeed, since the doctrine is an equitable rule of reason, no generally applicable definition is possible, and each case raising the question must be decided on its own facts. On the other hand, the courts have evolved a set of criteria which, though in no case definitive or determinative, provide some gauge for balancing the equities. These criteria have been stated in various ways, but essentially they can all be reduced to the four standards which have been adopted in section 107...."

There are no definitive standards or guidelines governing the use of copyrighted materials in the preparation of multimedia courseware for instruction, or classroom presentations utilizing multimedia. However, while developing these products, faculty should be governed by the same criteria which are prescribed for the use of copyrighted print materials. In essence,

the use of copyrighted print materials is governed by three criteria:

**Spontaneity:** The "fair use" of copyrighted materials in an educational setting should be at the "instance and inspiration of the individual teacher...." Further, the "inspiration and decision to use the work and the moment of its use for maximum teaching effectiveness" must be so close together in time "that it would be unreasonable to expect a timely reply to a request for permission." In other words, the decision to use the material must be the instructor's and not dictated by management or administration and it must be a spontaneous decision.

**Brevity:** With regard to print media, the guidelines are specific even to the point of specifying the maximum length of an excerpt from poetry or prose. Though these limits do not apply to non-print media, they clearly indicate that the intent is for a small portion of the original to be copied under fair use, and not a substantial portion of the work.

**Cumulative Effect:** "...copying of...material is for only one course in the school in which the copies are made." The guidelines for copying of print media, states "[n]ot more than one short poem, article, story, essay or two excerpts from the same author, nor more than three from the same collective work or periodical volume during one class term" is permitted. Even though the media may be different, faculty can best avoid copyright infringement by following the spirit of these guidelines when dealing with other forms of media in a multimedia presentation. For instance, using 8 minutes from a 10 minute video tape (in a multimedia presentation) would appear to violate the fair use guidelines by diminishing the "potential market" and value of the copyrighted work.

Instructors should be aware that when relying on the fair use provision, the use of copyrighted materials must meet all three tests (spontaneity, brevity, and cumulative effect). Instructors are encouraged to procure copyright releases for materials which they anticipate using for longer than one term.

Finally, the guidelines (developed by the Ad Hoc Committee on Copyright Revision, the Author-Publisher Group, and the Association of American Publishers) also indicate that

1. "Copying shall not be used to create or to replace or substitute for anthologies, compilations, or collective works..."
2. Copying is not allowed from consumable works such as "workbooks, exercises, standardized tests and test booklets and answer sheets..."
3. "Copying shall not substitute for the purchase of books, publisher's reprints or periodicals...(and shall not) be repeated with respect to the same item by the same teacher from term to term."

It should be noted that clip art, clip video, and clip audio are marketed and available for use in developing multimedia materials. These forms of "clip media" are licensed to the purchaser (individual, school, or faculty member) for use in multimedia presentations. In many cases, clip media can be used to substitute in a presentation for copyrighted materials that might

violate the fair use provision.

Assembled by the Academic Computing Technologies Group, Johnson County  
Community College, Overland Park, KS 66210.

----- %<>== -----

Given the nature of the RISKS FORUM and NCSA FORUM membership, I think these  
issues warrant further clarification. I invite legal counsel with expertise  
in the field to comment.<>

Mich M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn



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 16: Issue 69**

**Tuesday 3 January 1995**

## Contents

- [Gov't Recommends Electronic Copyright Restrictions](#)  
[Edupage](#)
- [One for the GIFFer \(CompuServe-Unisys GIF Tax Protest\)](#)  
[Pat Clawson](#)
- [Mail repeatedly returned to sender](#)  
[Curtis Keller](#)
- [Dates in a 4GL](#)  
[name removed](#)
- [Dates and Times Not Matching in COBOL](#)  
[Fred Ballard](#)
- [Testing and the Sources of Dates and Times](#)  
[Fred Ballard](#)
- [Dates in "Ancient" Systems](#)  
[Fred Ballard](#)
- [COBOL's Two-Character Year Field](#)  
[Fred Ballard](#)
- [Last call for papers for COMPASS 95](#)  
[John Rushby](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Gov't Recommends Electronic Copyright Restrictions (Edupage)

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Tue, 3 Jan 95 14:12:52 PST

From Edupage, 27 Dec 1994:

### GOV'T RECOMMENDS ELECTRONIC COPYRIGHT RESTRICTIONS

The draft report on copyright law issued last July is drawing fire from some academics and librarians, who say it gives copyright holders too much power and "ought to maintain the balance that is maintained in the print world," according to a law professor who moderates an Internet forum on copyright law. One particular sticking point is U.S. Patent & Trademark Office Commissioner Lehman's opposition to allowing libraries to ship books

electronically to patrons, because an extra copy would show up in each recipient's computer. "To me, the burden on those who would say that ought to be a fair use is extraordinarily high. You would see massive dislocation of the market for that work," says Lehman. The draft report was used to represent the U.S. position in recent meetings of the World Intellectual Property Organization, and Lehman says a basically unaltered final report will be ready in the spring. (Wall Street Journal 12/27/94 B5)

[To subscribe to Edupage: send a message to: listproc@educom.edu and in the BODY of the message type: subscribe edupage YourName (assuming that your name is YourName; if it isn't, substitute your own name) ... To cancel subscription to Edupage: send a message to: listproc@educom.edu and in the BODY of the message type: unsubscribe edupage.]

---

### **One for the GIFfer (CompuServe-Unisys GIF Tax Protest, Pat Clawson)**

*"Peter G. Neumann" <neumann@csl.sri.com>  
Tue, 3 Jan 95 13:27:49 PST*

An Open Letter to Our Colleagues In the Online Communications Community:

The announcement by CompuServe and Unisys that users of the GIF image format must register by January 10 [1995] and pay a royalty or face lawsuits for their past usage, is the online communications community's equivalent of the sneak attack at Pearl Harbor.

The announcement of the CompuServe-Unisys GIF Tax on December 29, during the lull between Christmas and New Year's Day, was clearly timed to cause maximum damage while an unsuspecting public celebrated the holidays.

We at TeleGrafix Communications have no quarrel with those who seek to protect their intellectual property and profit from it. Indeed, we are in business to do the same. We believe those who develop software are entitled to reap financial rewards from their labors.

But in our opinion, the timing and circumstances of the CompuServe-Unisys action indicates this is a shakedown of the online communications community by two powerful corporations, rather than a reasonable effort to protect intellectual property.

The GIF format has been in widespread public use since 1987. Its widespread use and royalty-free licensing has been encouraged by CompuServe for years. Neither CompuServe or Unisys have made any significant improvements to GIF or its underlying LZW algorithm and compression process to justify charging for what has been free.

Giving GIF users only 14 days to comply with sudden, unexpected demands to pay the private CompuServe-Unisys GIF Tax or face prosecution for past usage of what had been promoted for seven years as free, open standard software is unconscionable. It is especially outrageous since CompuServe and Unisys admit in writing that they decided to require licensing SIX MONTHS AGO in June, and didn't announce it to the public until now.

According to the CompuServe-Unisys GIF licensing agreement, the settlement of the patent dispute was executed on June 21, 1994. CompuServe agreed to implement the agreement "as soon as reasonably practicable and in no case later than six (6) months after the date this Agreement is executed..." That six month period ended on December 21, 1994 -- but CompuServe did not make the licensing terms public until December 28. Indeed, CompuServe appears to have violated the terms of its own settlement agreement with Unisys.

While many of the messages we have read online in reaction to the CompuServe-Unisys GIF Tax decree express both dismay and disbelief, virtually none have analyzed the actual provisions of the licensing agreement. It is in this area that TeleGrafix Communications wishes to contribute to the dialogue.

In our opinion, the CompuServe-Unisys licensing agreement is both illogical and overly broad. Let's examine some of its key provisions. All quotes cited are directly from the agreement.

1. CompuServe will license Developers who want to use GIF technology. The term "developer" is defined as "the other undersigned party to the agreement," and it seems to apply to ANYONE who contemplates distributing any product that uses the GIF format.
2. Developers will be licensed to sell or distribute "Products" that "use and exploit GIF...solely within the Field of Use." The term "Field of Use" is defined as "primarily for accessing the CompuServe Information Service and for manipulating and viewing data received through the CompuServe Information Service." The licensing agreement further defines the term "Products" as being "software that is developed or distributed...which is designed for and used primarily for accessing the CompuServe Information Service and for manipulating and viewing data received through the CompuServe Information Service." IT APPEARS THAT THE ONLY LAWFUL USE OF GIF WILL BE FOR COMPUSERVE-RELATED PRODUCTS. Using GIF images in any other manner, such as on CD-ROMs or bulletin board systems, is prohibited. Most of the thousands of products that have used GIF in some manner are henceforth contraband.
3. Developers may no longer "use, copy, modify or distribute the GIF specification, except as expressly permitted by CompuServe." This states that the GIF specification can no longer be shared, published or uploaded in any manner without the express consent of CompuServe.
4. Members of the public are prohibited from using any software product containing GIF until they have become a REGISTERED user of the product. The customer also must agree to use the product "primarily for accessing the CompuServe Information Service and for manipulating and viewing data received through the CompuServe Information Service." This virtually eliminates the concept of freeware or shareware containing GIF capabilities, since prospective customers can no longer try out these software products without registering them first.
5. Software developers must pay \$1.00 for a license to use GIF, PLUS a fee

equal to the GREATER of 1.5% of the selling price of the product, or \$0.15 per "Disposition." Disposition is defined as "the sale, lease or license or any other grant of rights to a Product or any new Product." All royalties must be paid quarterly. Noncommercial and freeware usage of GIF technology is NOT exempted from the royalty requirement. Because the royalty provisions and definition of "Disposition" are so broad in scope, it appears that a GIF Tax payment may be due to CompuServe-Unisys each time a GIF image is transmitted via BBS or Internet. The operators of a BBS or World Wide Web site with hundreds or thousands of GIF images online could easily be bankrupted by these licensing requirements.

6. CompuServe must be notified of ANY new product using GIF when it is first offered to customers.

7. Persons using GIF must keep records of its use, and CompuServe has the right to audit those records every year upon seven days notice. Persons using GIF must pay the cost of the audit if a royalty underpayment of 10% or more is discovered, along with 12% interest on any underpaid royalties.

8. Even if the patent is later found by the courts or the U.S. Patent Office to be invalid and unenforceable, or if the patent expires, any developer must "return all copies of the GIF specification and any confidential information of CompuServe then in its possession or control to CompuServe, (ii) stop using the Licensed Technology, and (iii) stop distributing Products." This states that EVEN IF THE PATENT IS OVERTURNED OR EXPIRES, YOU MUST STOP USING OR DISTRIBUTING GIF.

9. Even though CompuServe has publicly disseminated the text of the agreement it wants GIF users to sign, the terms of the agreement are to remain confidential. This is illogical, to say the least, since they have posted it for public download on their own system.

10. Developers have to indemnify and hold CompuServe harmless for any damages if their CUSTOMERS somehow use GIF technology in a way not permitted by the licensing agreement.

11. Unisys has the right to enforce the agreement, as well as CompuServe. Further, Unisys has the right to pursue legal action or seek damages against Developers even after the agreement has terminated.

TeleGrafix Communications Inc. will not sign such a licensing agreement. We think most other software developers, BBS sysops and Web site operators also will refuse to sign.

We encourage our colleagues in the online communications community to evaluate the CompuServe-Unisys action, and to lodge appropriate protests directly with those companies.

We believe that the CompuServe-Unisys GIF Tax drives a stake through the heart of Internet development. It will cripple the World Wide Web, NCSA Mosaic, and other Internet multimedia technologies that rely heavily on GIF imaging.

Fortunately, we at TeleGrafix Communications do not depend on GIF imaging in our new RIPscrip 2.0 online multimedia technologies. We chose to implement the JPEG image format and only recently decided to add GIF support as a convenience to our customers. Due to the restrictive conditions of the CompuServe-Unisys GIF Tax and licensing agreement, we must now reevaluate our plans for supporting GIF use in the upcoming release of RIPscrip 2.0.

While our company hopes to profit financially from our advanced RIPscrip 2.0 technology, we will not demand royalties from those who have used the freeware versions of our earlier RIPscrip 1.54 products and/or technical specifications. The RIPscrip 2.0 specification also will be made public for third-party use after it is finalized.

We expect that the CompuServe-Unisys action will spell the death of GIF as a commercially viable technology, shifting the attention of the online communications community to JPEG imaging.

Sincerely,

Pat Clawson  
President & Chief Executive Officer  
TeleGrafix Communications Inc.  
Huntington Beach, CA

Voice: (714) 379-2140  
Fax: (714) 379-2132  
BBS: (714) 379-2133  
Internet: rip.support@telegrafix.com

---

### **Mail repeatedly returned to sender**

*Curtis Keller <curtis@Starbase.NeoSoft.COM>  
Mon, 2 Jan 1995 22:05:11 -0600*

"You are invited to discover Wired magazine - free"

I received a pretty snazzy advertisement for Wired magazine 2 weeks ago and I decided to order the "free sample copy". I have placed the postage paid reply card in the mail 3 times, and 3 times a day or so later the same reply card has returned. It turns out that the reply card has my name and address on the flip side in the same position as the address of Wired magazine on the "correct side." Additionally the postal service 5+4 bar coding is on both sides of the card - once for Wired magazine and once for "me". I'll toss it in the mail once again.

Curtis Keller 713-953-8309 curtis@neosoft.com curtis@kinesix.com

---

### **Dates in a 4GL**

<[Name removed at submitter's request]>

*Tue, 3 Jan 95 12:12:12 XST*

I am currently using a fourth-generation language called NOMAD2. NOMAD2 stores dates internally as the number of milliseconds since a date in the 1580s when the Gregorian calendar was first put into use. At least the version of NOMAD2 that I use does (1).

For the most part, this seems to work out very well. Much of the fears about what happens with computer-stored dates on January 1, 2000 are groundless for NOMAD2. But perhaps not all of them. Using an appropriate date data type may have led to a false sense of security.

Most years are entered in the application system I'm working with as two digits. NOMAD2 allows this and effectively adds 1900 to years entered as two-digit years. When the system date changes to 2000, I'm not sure whether NOMAD2 will start adding 2000 to the years entered. (There may even be a system variable for setting this.) Regardless, on 1-Jan-200, it will still not be appropriate to add 2000 to years from the now previous century or 1900 to years from the now current century. Any arbitrary scheme to treat, say, the entered years 30 through 99 as 1930 through 1999 and 00 through 29 as 2000 through 2029 would lead to problems (2) since the system I'm working with could involve birthdates of 1929 and before.

Since the department I am working in has chosen to stay with the current version of NOMAD2 (1), any new schemes for handling this problem may be lost to my application. The whole topic of staying with a stable release of a system and not getting improvements or fixes to existing errors versus going to new releases that have improvements, may fix existing faults, but may introduce new ones is a rich risk management topic.

#### NOTES:

1. A new application system in another operating environment is replacing the one I am maintaining. As a consequence, no further upgrades are being planned for NOMAD2 in our operating environment. The vendor of NOMAD2 continues to make upgrades. The vendor's most release dealt with a date problem from one its clients. The client was storing uninitialized dates on its DB2 database as something like January 1 of the year 0 which DB2's date data type allows. NOMAD2 can map DB2 databases, but its date data type did not allow dates before the introduction of the Gregorian calendar. (I assume they haven't had any clients who wanted to store archaeological data.) The client was stubborn and the new release of NOMAD2 contains a fix for the problem. I'm not aware of the implementation details.

2. As Brian Hayes noted in "Waiting for 01-01-00" on p. 14 of January-February 1995's *\_American Scientist\_*.

---

## Dates and Times Not Matching in COBOL

*Fred Ballard <72400.1525@compuserve.com>*

*01 Jan 95 21:31:03 EST*

There is no way to obtain the system date and time in one statement in COBOL. A program could get the date just before midnight and then get the time relative to the day after the date it got. A timestamp of 31-Dec-1994 00:00:01 indicates just after midnight between 30-Dec-1994 and 31-Dec-1994, but it could have been obtained from a COBOL program running around midnight between 31-Dec-1994 and 1-Jan-1995.

The only way in a COBOL program to assure that the time obtained is for the date obtained is to loop getting the date, then the time, and then the date again until both dates match (as would usually be the case).

No one knows how often such a check is performed in existing COBOL code, but I would guess it is very rare. No one knows how likely such an error would occur or what consequences it might have. But it certainly is not desirable. (It's a little like the Pentium FDIV bug.)

I haven't heard of any problems actually caused by this, but the potential risk is there as it is in any language that makes accessing the date and time simultaneously impossible. (I believe BASIC shares this problem with COBOL.)

---

## Testing and the Sources of Dates and Times

*Fred Ballard <72400.1525@compuserve.com>  
01 Jan 95 21:31:02 EST*

Application software typically draws the current date and time directly from the system. Not using data hiding, that is, drawing the current time from another application module, may cause problems with testing and could lead to faults due to the difficulty of testing if it is not possible to change the system date and time during a test.

A realtime financial application may want to close the books for the now previous day when the time goes past midnight. I've heard of such an application and the developers did not use data hiding. As a result they had to run their tests when the system (and actual) time changed to midnight. Therefore, only one test could be run each night and in this case they had to rearrange their normal 8-5 working hours to center around midnight. Introduction of changes and fixes were more easily introduced when the programs were modified to access the "current" date and time through a common module that could shift the time during a test.

However, as with most things, the tradeoff of using data hiding instead of directly accessing the system date and time opens up the potential risk of accidentally using test times in a production environment. (This risk might still be present if a test was allowed to alter the system date and time thereby moving data hiding to another level.)

---

## Dates in "Ancient" Systems

*Fred Ballard <72400.1525@compuserve.com>*

*01 Jan 95 21:30:55 EST*

In a few IBM 1401-based programs at the insurance company I was working at in the late 1960s, the year was stored as a one-character field! Fortunately the problem of going from 1969 to 1970 in these programs was recognized in time, the programs were few in number and modest in size (our 1401s had a maximum main memory of 8K), and the programs were corrected in time.

---

## **COBOL's Two-Character Year Field**

*Fred Ballard <72400.1525@compuserve.com>*

*01 Jan 95 21:30:57 EST*

Stating the fact that COBOL has a default date format used in its special-registers bypasses the fact that COBOL has no date data type for the storing of dates (Freudian-slip, make that dates).

This has left the coders of the billions of lines of existing COBOL code free to invent as many date formats as human creativity will allow. In my reading, use, and maintaining of COBOL code in over twenty-six years of information system programming, this is a surprisingly large number.

This is one of the reasons "dusty deck" COBOL systems are such a problem as the year 2000 draws near. No assumptions can be made as to how dates are stored in COBOL-based systems and files. Also, the manipulation of a given format varies from one COBOL program to the next. There is no guarantee that any installation-wide modules are used for date manipulation. (Installation-wide is pretty much the best you can hope for; COBOL itself has no date manipulating modules.)

Actually, there is no guarantee that date routines will even be concentrated and re-used within a given COBOL program. Date processing is often scattered throughout the program, with each date variable having not only its own unique processing but different code for the same operations on a given date at different points in a program.

Obviously, some of this date code may contain errors. In many cases the errors are compensated for, consciously or unconsciously, by the program's developers or maintainers. So correcting a date computation at one point may lead to an error because the next use of the date has an existing correction for the previous error.

[Thanks to Fred, who also pointed out an error on Page 88 of my RISKS book, which should have read "COBOL uses a two-character YEAR field" (instead of DATE). Sorry! PGN]

---

## **Last call for papers for COMPASS 95**

*John Rushby <RUSHBY@csl.sri.com>*

*Fri 30 Dec 94 12:08:49-PST*

Typeset copies of the CFP are available via anonymous ftp from ftp.csl.sri.com in /pub/compass95-cfp.{txt|tex|dvi|ps} and /pub/compass95-cfp-a4.{dvi|ps} or via WWW from <http://www.csl.sri.com/compass95.html> .

CALL FOR PAPERS  
COMPASS '95

10th Annual IEEE Conference                      June 26--30, 1995  
on COMPuTer ASSurance (COMPASS)              Gaithersburg, MD USA

Sponsored by IEEE Aerospace and Electronic Systems Society  
and IEEE National Capital Area Council  
In cooperation with The British Computer Society

The purpose of this conference is to bring together researchers, developers, integrators, and evaluators who work on problems related to specifying, building, and certifying high-assurance, high-consequence computer systems. What distinguishes COMPASS from similar conferences is its emphasis on bridging the gap between research and practice. For researchers this provides an opportunity to present new results, theories, and techniques both to other researchers, and to practitioners who can put them to use. They can also learn from practitioners of issues and problems encountered in building real systems. Practitioners have an opportunity to share lessons learned, to hear of new research, and to influence future research directions.

The conference will be held at the National Institute of Standards and Technology in Gaithersburg, Maryland, which is a suburb of Washington DC (4 miles from the Shady Grove Metro Station). The proceedings will be published by the IEEE.

Papers should present advances in the theory, design, implementation, evaluation, or application of high-assurance systems, or report on experiments, evaluations, and open problems in the use of new technologies for computer assurance. Special consideration will be given to presentations (either single papers or paper pairs) by practitioners and researchers who have worked on the same problem. There will also be a tools fair and the conference will be preceded by one or two days of tutorials. Papers, panel session proposals, tutorial proposals, and tools fair proposals are solicited in relevant areas including the following:

Software Reliability	Software Safety	Computer Security
Formal Methods	Tools	Human-Computer Interfaces
Real-Time Systems	Networks	Embedded Systems
V&V Practices	Certification	Standards
Measurement and Metrics	Organization Theory	Lifecycle Processes

Representative application areas of interest include but are not limited to: communications, military systems, avionics, road and rail transport, space systems, nuclear and conventional power generation,

plant and process control, and medical systems.

#### INSTRUCTIONS TO AUTHORS:

Send five copies of your paper, panel session proposal, tutorial proposal, or tools fair proposal to John Rushby, Program Chair, at the address given below. Abstracts, electronic submissions, late submissions, overlength papers and papers that cannot be published in the proceedings will not be considered. Papers submitted from outside North America should be sent via overnight courier service or express mail. Exceptionally, authors in countries where copying or printing facilities are limited may submit a single copy in any form available to them (including electronic mail).

Papers must be received by January 17, 1995 and must not exceed 7,500 words. Authors are responsible for obtaining prior to acceptance any and all necessary permissions and clearances for publication and are expected to present their paper in person if it is accepted. Authors will be notified of acceptance by March 14, 1995. Camera-ready copies are due not later than April 17, 1995.

Papers that describe use of technology presented at a previous COMPASS conference are eligible for a special award. Papers of exceptional quality and appropriate subject matter are eligible for inclusion in a special issue of the Journal of High Integrity Systems or the Journal of Computer Security.

Limited financial assistance will be available for student authors.

#### PROGRAM COMMITTEE

Robin Bloomfield Adelard, UK  
Connie Heitmeyer Naval Research Laboratory, USA  
John Gannon University of Maryland, USA  
Rich Gerber University of Maryland, USA  
Jon Jacky Radiation Oncology, University of Washington, USA  
Jeremy Jacob York University, UK  
John Knight University of Virginia, USA  
Carl Landwehr Naval Research Laboratory, USA  
Keith Marzullo University of California, San Diego, USA  
John McLean Naval Research Laboratory, USA  
Jon Millen MITRE Corporation, USA  
Steve Miller Collins Commercial Avionics, USA  
Peter Neumann SRI International, USA  
Hans Rischel Technical University Denmark  
Jeannette Wing Carnegie-Mellon University, USA

#### FOR FURTHER INFORMATION CONCERNING THE SYMPOSIUM, CONTACT:

Bonnie Danner, General Chair	John Rushby, Program Chair
	Computer Science Laboratory
TRW Systems Division	SRI International
One Federal Systems Park Drive	333 Ravenswood Avenue
Fairfax, VA 22033, USA	Menlo Park, CA 94025

Tel: (703) 876-4383                      Tel: (415) 859-5456  
Fax: (703) 876-4304                      Fax: (415) 859-2844  
BONNIE.DANNER@trw.sprint.com              Rushby@csl.sri.com

Paul Anderson, Publicity Chair  
Space & Naval Warfare Systems Command  
SPAWAR 224-1B  
Washington DC 20363  
Tel: (703) 602-3179  
FAX: (703) 602 4485  
andersop@smtp-gw.spawar.navy.mil

Additional and typeset copies of this call for papers are available via  
anonymous ftp from ftp.csl.sri.com in /pub/compass95-cfp.{txt|tex|dvi|ps}  
or via WWW from <http://www.csl.sri.com/compass95.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 16: Issue 70**

**Weds 4 January 1995**

## Contents

- [GIF, UNISYS, and CompuServe](#)  
[Tim Oren](#)
- [Datastream may be charged in Jan 1995](#)  
[Mich Kabay](#)
- [Common Criteria Draft \(0.9\) on CD-ROM](#)  
[Klaus Brunnstein](#)
- [Computer Addiction](#)  
[Mich Kabay](#)
- [Virus Creation Labs](#)  
[Andy S. Lopez](#)
- [Don't plot murder via cordless phone](#)  
[Mich Kabay](#)
- [Cell phones in Israeli army](#)  
[Mich Kabay](#)
- [Dense ordinateurs](#)  
[Mark Stalzer](#)
- [Re: COBOL's 2-Character Year Field](#)  
[Mark Brader](#)  
[Walter Murray](#)  
[Paul Robinson](#)
- [Info on RISKS \(comp.risks\)](#)

---

## GIF, UNISYS, and CompuServe

*Tim Oren* <[TIMOREN@csi.compuserve.com](mailto:TIMOREN@csi.compuserve.com)>  
04 Jan 95 14:51:09 EST

In 1987, CompuServe designed the Graphics Interchange Format (GIF) specification for graphics files. The GIF specification incorporated the Lempel-Zev-Welch (LZW) compression technology on which Unisys Corporation was independently pursuing a patent filing. In early 1993, Unisys notified CompuServe of patent rights granted to LZW. At that time, CompuServe began negotiating with Unisys to secure a licensing agreement. This agreement was reached in mid-1994, and CompuServe then initiated a process to secure a

similar license that would benefit its GIF developer community.

Following the agreement reached between CompuServe and Unisys, CompuServe announced the Graphics Interchange Format (GIF) Developer Agreement, shortly after its completion, on December 29, 1994. This agreement is aimed at GIF developers who are developing programs and shareware primarily for use in conjunction with CompuServe. The service offers a license to these developers to use LZW technology in programs written to the GIF specification.

CompuServe remains committed to keeping open the GIF 89a specification both within CompuServe and in areas outside CompuServe. CompuServe continues to strongly support the use of the GIF specification in the entire online community including the Internet and World Wide Web. This agreement will be transparent to end-users and will not result in any charges for people using viewers or transmitting GIF images.

The agreement offers software and shareware developers who use the LZW technology in their GIF programs protection under a software license that CompuServe is authorized to grant under the agreement with Unisys. Developers who choose to take advantage of this service would acquire the rights to use the LZW technology in certain software and shareware developed primarily for use in conjunction with CompuServe. Developers who choose to participate in this agreement within the implementation period will also benefit in that Unisys has agreed not to pursue royalty claims for past use of the LZW technology in GIF. The implementation period has been extended to January 31, 1995.

CompuServe has presented this new agreement as a service to its GIF developer community. Cost to developers will be a \$1.00 one-time licensing fee and a royalty payment of 1.5 percent or \$0.15, whichever is greater, per registered copy of a program containing the LZW technology. CompuServe will not profit from this service.

CompuServe encourages developers to work with Unisys directly if the GIF Developer Agreement does not meet their needs. Unisys is continuing to make the LZW technology available to any interested parties under reasonable and non-discriminatory terms. Developers are not required to register with CompuServe. Registering with CompuServe is simply one option for addressing the Unisys LZW patent issue. Developers may want to consider consulting with legal counsel.

CompuServe is committed to keeping the GIF 89A specification as an open, fully-supported, non-proprietary specification for the entire online community including the World Wide Web. Whether they choose to register with CompuServe or not, developers are encouraged to continue use the GIF specification within their products.

A copy of the GIF Developer Agreement is available in the Library section of the CompuServe Graphics Support Forum (GO GRAPHSUP) and will shortly be posted to CompuServes World Wide Web page ([HTTP:\\WWW.COMPUERVE.COM](http://WWW.COMPUERVE.COM)). Developers who are not developing software primarily for use in conjunction with CompuServe should contact Unisys directly at: Welch Patent Desk, Unisys Corp., P.O. Box 500, Bluebell, PA 19424 Mailcode C SW 19.

Sincerely,

Tim Oren, CompuServe Vice President, Future Technology

---

## Datastream may be charged in Jan 1995

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
04 Jan 95 06:16:28 EST*

The Reuter newswire reports on last year's Datastream case:

RTw 94.01.03 05:55 EST  
Teenage hacker taps into U.S. defence secrets

LONDON, Jan 3 (Reuter) - A British teenager allegedly hacked into sensitive U.S. government computers and was able to monitor secret communications over the North Korean nuclear crisis last spring, the Independent newspaper reported on Tuesday.

The boy tapped into several defence computers for seven months in what U.S. officials conceded was one of the most serious breaches of computer security in recent years, the paper said.

The article continues with the following key points:

- \* The youngster posted the data on the Internet and was labelled "Datastream" because of the volume of information he supplied.
- \* He "was finally caught by special U.S. investigators because he left his terminal on-line to a U.S. defence computer overnight."
- \* The child was arrested in July in Britain.
- \* "...[P]rosecutors are expected to decide this month whether he can be charged, the Independent said."
- \* "...[T]he U.S. Air Force Office of Special Investigations acknowledged the hacker could have accessed and read the Korean files."

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn

---

## Common Criteria Draft (0.9) on CD-ROM

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.d400.de>  
Fri, 30 Dec 1994 13:58:25 +0100*

German Information Security Agency (GISA, in German: Bundeasamt fuer Sicherheit in der Informationstechnik, BSI) has prepared a CD-ROM containing the draft (version 0.9) of the Common Criteria presently being issued by a committee of experts from USA, Canada and European Union. This

(unclassified) version will be sent to every interested person together with accompanying material guiding comments (deadline of comments: March 1,1995). Interested experts should send a fax to

German Information Security Agency  
Attention Dr. Kreuz  
Post Box 20 03 63  
D 53133 Bonn  
FAX: +49-228-9582-427

Most regrettably, the CD-ROM is designed for PC work. When trying to mount the CD-ROM in the mode usually adapt to read PC CD-ROM formats, we succeeded to crash our SUN OS 4. As our SOLARIS systems have no CD-ROMs, we could not test whether this may work. (Nice to crash insecUNIX with INFOSEC material :-).

Klaus Brunnstein (Dec.30,1994)

PS: I asked BSI whether we may offer the CDROM material via our ftp-site. BSI informed me that they wish to be sure that the letter with guidance to the comment process accompanies the CD-ROM so I cannot offer this material via ftp :-)

---

## Computer Addiction

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
26 Dec 94 16:38:07 EST*

The Associated Press newswire (via CompuServe's Executive News Service) reports on addiction to computers on an article datelined 94.12.26 @ 00:00 EST:

Computer Addiction

By PATRICE GRAVINO, Associated Press Writer

KANSAS CITY, Mo. (AP) -- It answers immediately and makes few demands. It can introduce you to new friends and lovers, entertain you, organize your bills and provide expert information about almost any topic.

It's the nearly perfect companion: your computer.

But many people, from industry experts to social scientists, are beginning to ask -- and debate -- whether there's such a phenomenon as "computer addiction" and whether it's becoming a problem.

The author goes on to cite several anecdotal cases:

- o A "former computer instructor in Kansas City" explains the breakup of his 16-year marriage in part to the time he spent at his computer.
- o "[F]uturist Andre Bacard, a physicist and author based at Stanford University in California, where he researches the social impact of

technology," reports several acquaintances who spend an inordinate amount of time online. Some "belong to a half-dozen computer networks, and they log-on to one after another. Their entire social world is vicarious." He adds, "I think it both encourages and cultivates psychosis in many people."

- o Some psychologists report having to help parents pull their children away from their computers because they are neglecting schoolwork and withdrawing from social interactions not mediated by computers.

- o "Steve Spaw, a computer graphics consultant in Kansas City," reports that he has to force himself not to spend all his time with his system.

- o "Dr. James Donley, medical director of outpatient psychiatry at the University of Kansas Medical Center in Kansas City, Kan.," reports few obvious cases of computer addiction so far, but feels that there's certainly a potential. He draws parallels with the potentially excessive involvement in the world of pets that some enthusiasts display. He also points to the "inherently self-centered" activity where "people have a fairly simple relationship, where you can kind of predict or dictate what happens.... It can be used as an avoidance of social relationships." He argues that susceptibility to computer addiction "more to do with their personalities than with computers."

<<Comments by M.K.: As I have mentioned before, computer addiction, if it exists, conforms to what University of Chicago Professor Mihaly Csikszentmihalyi has defined as "autotelic" behaviour. He describes this complex of behavioural cues in his book, Flow: The Psychology of Optimal Experience (1990). Harper & Row (New York). ISBN 0-06-016253-8. xii + 303.

Basically, his research suggests that highly enjoyable activities share certain attributes (p. 48 ff):

- o Challenging activity that requires skills
- o Merging action and awareness
- o Clear goals and feedback
- o Concentration on the task at hand
- o Sense of control
- o Loss of self-consciousness
- o Transformation of time.

Flow is certainly not inherently dangerous; however, as in any human experience, some outliers will cross the fuzzy boundaries from wholesome involvement and commitment into crazy excess. Perhaps it would be appropriate for such people to glue timers to their computers! I can imagine someone writing a TSR which alerts them with a voice warning: "Susan, it's time to stop using your computers now: you've been working steadily for [fill in appropriate time limit] hours." <grin>

Have any RISKS readers experienced such involvement with computer programs that they worry about the possibility of harmful effects on their relations with others? Do social relations through network communications supplant live interactions? Is there any reason to be any more concerned about spending, say, three hours online in a multi-user dimension than three hours

chatting on the phone or--for that matter--three hours in one's own living room serving a friend tea?<>

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn

---

## **Virus Creation Labs**

"ANDY S. LOPEZ" <75713.2205@compuserve.com>

04 Jan 95 12:12:43 EST

I recently bought a copy of a book called "The Virus Creation Labs" by George C. Smith (American Eagle, ISBN 0-929408-09-8) and it contains material, bulleted below, which may be of interest.

----The hiring of a hacker called Priest (who programmed the Satan Bug and Natas viruses) by Norman Data Defense, the developer of anti-virus software. The author writes that the initial job offer was carried by US Secret Service agents questioning the hacker after the agency's network was trashed by Satan Bug in 1993.

----A look back at the AIS Security Branch bulletin board system and the bruhaha surrounding its archive of hacker utilities and virus code. The coverage by the Washington Post and Associated Press is reviewed, and there are some interviews and comment from some of the people involved.

----A revealing look at the cozy relationship between some virus writers (who were looking for a little press) and some anti-virus software producers (who were looking for even more press and copies of the viruses in question).

---

## **Don't plot murder via cordless phone**

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>

31 Dec 94 06:50:38 EST

The AP newswire (via CompuServe's Executive News Service) for 94.12.30 @ 20:02 EST reports on a murder plot ruined by use of a cordless phone:

### Scanner Plot

MEMPHIS, Tenn. (AP) -- A woman listening to a police scanner she had gotten for Christmas picked up a conversation over cordless telephones and heard what turned out to be a murder plot unfolding, investigators say.

The article explains that Donna McGee heard a woman and her boyfriend plotting to kill the woman's husband and then collect insurance money. As the family gathered around in horror, "Mrs. McGee's daughter recognized a playmate's name" and the family figured out "the identity of the intended victim."

Law enforcement officials said that because Mrs McGee was not purposely

zeroing in on a specific conversation but only scanning across the bands, she had broken no laws in listening to the murder plot.

<<MK: People who live in glass houses shouldn't throw binoculars.>>

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn

[Also noted by rjones@oz.net (Ry Jones).]

---

### Cell phones in Israeli army

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
31 Dec 94 06:51:09 EST*

>From the Reuter newswire 94.12.29 @ 15:07 EST (via CompuServe's Executive News Service):

JERUSALEM, Dec 29 (Reuter) - The Israeli army has taken its best shot at a formidable new foe -- an insatiable craze for cellular phones, which have fast become an essential extra in soldiers' kit.

The article explains that cell phones have become a problem for the army because "soldiers, especially reservists, have begun taking them on army duty, vexing commanders by making stock market deals and chatting to loved ones even during live-ammunition exercises."

It is now forbidden to carry cell phones on duty and officers may "forbid a soldier from having a cellular phone at all."

<<Comments from MK: The article did not say, but RISKS and NCSA Forum readers will agree, that using unencrypted cellular phones for military matters would be a serious mistake.>>

M.E.Kabay,Ph.D./DirEd/Natl Computer Security Assn

---

### Dense ordinateurs (Mark Brader)

*Mark Stalzer <stalzer@macaw.hrl.hac.com>  
Tue, 3 Jan 1995 15:55:21 +0800*

>Would English speakers have reacted equally strongly to a -- no pun intended  
>-- comparable bug in the instructions for comparing and branching? I think  
>they would not.

On the contrary, it would be far worse: the computer would be accused of not being able to make up its mind!

-- Mark

## Re: COBOL's Two-Character Year Field (Ballard, [Risks-16.69](#))

Mark Brader <msb@sq.com>

Wed, 4 Jan 1995 01:50:34 -0500

->-> Date: 01 Jan 95 21:30:57 EST

From: Fred Ballard <72400.1525@compuserve.com>

Hmm... <grin> do you think the mail program that generated that header was written in COBOL? In fact, 8 out of 9 articles accepted for that issue of Risks had Date lines with 2-character years!

Mark Brader msb@sq.com SoftQuad Inc. Toronto

---

### COBOL addresses date risks

Walter Murray <walterm@hprctbs3.rose.hp.com>

Wed, 4 Jan 95 10:18:53 -0800

I'd like to respond to a few statements made in [RISKS-16.69](#).

Fred Ballard pointed out the risk of a COBOL program running near midnight and retrieving the system date and time as two separate operations. He suggests looping, getting the date, the time, and the date again, to make sure the date and time came from the same day. I have used that technique in all the code I have written, and have wondered whether anyone else worried about such things.

The good news is that the COBOL language now provides a way to get the date and time in a single statement. The ANSI COBOL 1985 standard was officially updated in 1989 with the Intrinsic Function module, which I believe many vendors have implemented. There is now a CURRENT-DATE function that provides, with a single function reference, the system date, time, and local time differential from Greenwich Mean Time (if known).

Several other of Mr. Ballard's concerns were also addressed in the same addendum to the COBOL standard. The CURRENT-DATE function returns the date and time in a standard 21-character format that includes four digits for the year.

Addressing the multiplicity of date formats in use, the updated standard defines three: standard date form (YYYYMMDD), Julian date form (YYYYDDD), and integer date form (a numeric value representing the number of days counting from January 1, 1601, of the Gregorian calendar). The standard addresses date processing by providing functions to convert between integer date form and the other two forms.

In summary, the COBOL language has addressed the problems. Now it's up to COBOL programmers to learn and start using what the language provides.

Walter Murray

---

## Re: Dates and Times Not Matching in COBOL

Paul Robinson <paul@tdr.com>

Tue, 03 Jan 1995 22:41:12 -0500 (EST)

Fred Ballard <72400.1525@compuserve.com> writes:

> There is no way to obtain the system date and time in one statement in COBOL.

Because most operating systems separate the request for time from the request for date. I can't think of any system where the date and time are returned in a single request; there probably are but I can't think of any. OS/MVS on IBM mainframes, Decsystem 20 on Digital Mainframes, RSTS/E and RT11 on Digital Minicomputers, MSDOS, VS/9 on Univac Mainframes, none of these returned date in the same call as time.

> The only way in a COBOL program to assure that the time  
> obtained is for the date obtained is to loop getting the date,  
> then the time, and then the date again until both dates match  
> (as would usually be the case).

I guess it's because with the exception of batch jobs being run at that time, most jobs run at some time other than exactly midnight - usually it's during business hours - and thus the problem only exists for two minutes of the day, e.g. during the one minute before midnight and the one minute after. The other 1438 minutes of the day, it's not a problem. Actually it's less than that. The problem is during the last one second of the last minute of the day and the first second of the first minute of the next day, since unless the call for date and time occurs exactly at that precise instant, and that one of them occurs just before 00:00:00 and the other just after. This means, that during 86,398 seconds of the day this isn't an issue, and is during "alpha and omega, the first and the last", is when the problem occurs.

This sort of issue pops up so rarely that it's not something one thinks about much. In fact, a lot of reports print date only, so the time doesn't matter one way or the other.

> I haven't heard of any problems actually caused by this, but the potential  
> risk is there as it is in any language that makes accessing the date and  
> time simultaneously impossible. (I believe BASIC shares this problem with  
> COBOL.)

I captured a print out from running GW Basic:

```
Ok
PRINT TIME$
22:33:44
Ok
PRINT DATE$
01-03-1995
Ok
```

The question is how fast is the timing here. Just how many date and time requests can a basic program issue in one second. Using an MSDOS version of BASICA under MSDOS 6.0 running on an AMD 386 DX 40 with turbo on, I wrote the following program, called "TICK.BAS":

```
110 REM FIRST START WITH A NEW SECOND
120 T1$=TIME$
130 IF T1$=TIME$ THEN 130
135 REM NOW COUNT NUMBER OF ACTIONS IN ONE SECOND
140 J = 0 : T1$=TIME$ : D1$=DATE$
150 T$=TIME$ : D$=DATE$
160 J = J+1 : IF T$=TIME$ THEN 160
170 PRINT J
```

When I ran this program, twice, the printed result was:

```
3023
```

Basica typically isn't fast, yet in one second, this program, running in Interpreted basic, issued 3023 date and time requests. Actually, it issued 3023 date requests and 6046 time requests. This means that, for example, on a computer such as mine, it has to be issuing a request for the date and the time during the 1/3023rd of one second between the last second of one day and the first second of the next. If there is even 2/3023rds of a second before midnight, there would be enough time to get both date and time in the same second:

```
A#=1/3023 : PRINT USING "##.#####";A#
0.0003307972
```

Or a 3 in 10,000 chance of this happening in the cases of someone running a program in Basic which would hit within the time required to cause an error of this type. And in a compiled language the chance is even less since the time to do two MSDOS calls.

Using Turbo Pascal 6, I wrote the following file called "TICK.PAS":

```
uses dos;
var yr,mo,day,dow,
    hr,min,sec,tick,
    hr2,min2,sec2,tick2:word;
    l:longint;

BEGIN
  getdate(yr,mo,day,dow);
  gettime(hr,min,sec,tick);
  repeat
    gettime(hr2,min2,sec2,tick2);
  until sec2<>sec;
  l := 0;
  repeat
    gettime(hr,min,sec,tick);
    inc(l);
  until sec <> sec2;
```

```
writeln(i:1);  
end.
```

The results I got for this were: 6767, 6229, 6229, 6575, 6571, 6201, 6205, 6202, 6228, 6575, 6229, 6228, 6229, 6574, 6229, 6575, 6229, 6571.

Figuring worst case at 6200 tests, it means that there would have to be less than  $2/6200$  of one second before midnight for the possibility of this happening.  $1/6200$  of one second means that if a program of this type was executed every day in such a manner as to cross midnight, during the moment the date and time were collected, the chances are an error of this type happening would strike one execution every 16.9 years, since it can only happen once a day, and it can only happen during the  $1/6200$  of a second before midnight.

No wonder I never thought about such a thing. It may be crass to put it this way, but how many people worry about an error that *might* happen once every 16.9 years?



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 16: Issue 71**

**Thursday 5 January 1995**

## Contents

• [A Whole Bunch of Date-Time Stuff](#)

[Fred Ballard](#)

[Paul Robinson](#)

[John Cavanaugh](#)

[Dave Moore](#)

[Chuck Karish](#)

[Jerry Leichter](#)

[Richard Schroepel](#)

[Craig Everhart](#)

[Erann Gat](#)

[Wayne Hayes](#)

[Walt Farrell](#)

[Stanley F. Quayle](#)

[Marc Horowitz](#)

[Peter Capek](#)

[Lars Wirzenius](#)

[Phil Rose](#)

[David Jones](#)

[Jonathan I. Kamens](#)

[Andrew W Kowalczyk](#)

[Barry Jaspan](#)

[Joe Morris](#)

[Lord Wodehouse](#)

---

## Adopting Programming Improvements

*Fred Ballard* <72400.1525@compuserve.com>

05 Jan 95 00:08:23 EST

I'm glad to see (and embarrassed as well) that, as Walter Murray describes in [RISKS-16.70](#), ANSI COBOL addressed the problems I described with COBOL dates in [RISKS-16.69](#) in the 1985 standard.

He further says that, "Now it's up to COBOL programmers to learn and start

using what the language provides."

That brings me to the subject of how fast improvements are actually adopted. I attended a meeting where Gerald Weinberg (author of *The Psychology of Computer Programming*, among many other excellent books) spoke. He told a story illustrating how long it takes to introduce improvements. It was determined in the nineteenth century that surgeons could drastically reduce the mortality rate among their patients by washing their hands before operations. It took a full generation of surgeons from the older, who couldn't be bothered, to the younger, who wouldn't do it any other way, for the improvement to find widespread use. (What's really frightening is a radio story I just heard on a children's burn unit in Russia that mentioned a doctor there who could not be persuaded to wash his hands between examining patients' dressings.)

All in all, I think we face the same thing in computer programming. (For instance, in my case, although I'm not currently using COBOL, I should have checked a current manual before commenting. Should the opportunity arise, I will welcome and use the improvements.) I'm pessimistic about wide improvements in programming techniques and how fast they spread to programmers in information systems software and applications. I'll give some examples:

- o In the area of reuse (and sticking with dates), in the 4GL I use, the ADDDATE function correctly adds to and subtracts from dates before its epoch date, but allowed arithmetic operations (addition and subtraction) on the same dates fail.

- o In program control, because the 4GL formerly lacked a generalized loop structure, GOTOs had to be used to construct them and were also used to code spaghetti bowls of code throughout the 1980s and 1990s, ignoring the precepts of structured programming introduced at least as early as 1968.

- o The use of modularization is haphazard; in one instance, a manager dismissed the coupling and cohesion of structured design from the early 1970s as impenetrable. (Well, actually he said he never got it and didn't want to get it.)

- o Code inspections, programming teams, and software metrics are never used or even mentioned.

- o Data hiding has been impossible in the 4GL because all variables have had global scope. When local variables were introduced in the current version, they can only be automatically allocated variables whose use is restricted in many commands. Most programmers haven't missed local variables and welcome everything being global.

- o Object-oriented development is viewed as a distant, experimental possibility.

>From what I've seen, most of the improvements in programming from the last quarter century of computing science are still viewed as tentative innovations: usually unexplored, unknown, or unused.

---

## Mea Culpa!

*Paul Robinson <paul@tdr.com>*

*Thu, 05 Jan 1995 03:23:19 -0500 (EST)*

As too many people have informed me, in regards to the message regarding dates and times, Unix (and the C language) return the number of seconds since 1970 as the date field.

[... and POSIX and Standard C systems, etc. This was noted, in many messages NOT included in RISKS, including those by (among others),

karish@mindcraft.com (Chuck Karish)

jepstein@cordant.com (Jeremy Epstein)

Marc Horowitz <marc@MIT.EDU>,

"Barry Jaspan" <bjaspan@cam.ov.com>,

scotte@center.uscs.com (L. Scott Emmons),

jra@IntNet.net (Jay Ashworth)

Just for kicks, I surveyed the 30 messages that were candidates for this issue, and 10 of the DATE: fields had two-character fields. PGN]

Someone else informed me that under VM, one can issue a form of the DIAG instruction and get the time since a certain epoch. (There is an issue here which the person who pointed it out to me may be unaware of; DIAG is a privileged instruction if you were running under anything EXCEPT VM, so the only place you can use that instruction is for stuff that runs in machine emulation.)

Someone else informed me that in assembly language on a Decsystem 20, you can get the date and the time in a single call. I never used assembly on a DEC 20, so I was unaware of this.

Someone else pointed out that my comparison on a 386 DX 40 isn't quite the same as conditions on other computer systems because a 386/40 is a relatively recent development in what is available for the average person, e.g. the old mainframe computers used to only accept batch jobs and a job might take hours or {days} to run. I remember my days of punching jobs on cards some twelve or fifteen years ago, and waiting 20 minutes to 1/2 an hour for a job to complete. Cheap terminal access made card punch access obsolete.

---

## Re: Year 2000 date problems already happening now

*John Cavanaugh <johnc@msc.edu>*

*Thu, 29 Dec 1994 12:30:04 -0600 (CST)*

Indeed, year 2000 date problems have already been happening for quite some time. The first report I remember seeing was in a Computerworld article in 1975, when some programs that did projections 25 years ahead started failing.

John Cavanaugh, Minnesota Supercomputer Center, Inc., 1200 Washington Ave. S

Minneapolis, MN 55415 johnc@cray.com +1 612 337-3556

---

## Re: Dates in a 4GL

Dave Moore <davem@garnet.spawar.navy.mil>  
Wed, 4 Jan 1995 09:56:20 -0500 (EST)

I just wanted to point out that this system of time storage will differ from World Time (UTC) by the number of leap seconds prior to the stored time. Currently this is 10 or 11 seconds. The most recent leap second was added the end of June 94. I expect that most non-real-time applications don't care about 10+ seconds. However it's interesting to note that the internal storage is in milliseconds. This difference can become quite critical in real-time applications.

---

## Re: Dates and Times Not Matching in COBOL

Chuck Karish <karish@mindcraft.com>  
4 Jan 1995 22:52:34 GMT

>This sort of issue pops up so rarely that it's not something one thinks  
>about much. In fact, a lot of reports print date only, so the time doesn't  
>matter one way or the other.

And this is exactly why we discuss this sort of issue in RISKS: because people don't think about this sort of issue much. As a buyer of computing services, are you happy to have a bug report answered with "Aw, that almost never happens!?" Or maybe "Nobody cared much thirty years ago; why worry now?"

Chuck Karish Mindcraft, Inc. 415 323 9000 x117 karish@mindcraft.com

---

## Date and time

Jerry Leichter <leichter@lrw.com>  
Wed, 4 Jan 95 18:04:40 EDT

In a recent RISKS, Paul Robinson makes two points I'd like to disagree with.

The first is minor. Mr. Robinson lists a variety of operating systems, all of which he says return the date and time separately, thus leaving programs open to the danger that, if they sample across a midnight boundary, they may get a time from one day and a date from another. All the OS's he lists are rather old. All versions of Unix since the very beginning have returned, on request, a unified date/time value, represented as the number of seconds since a fixed time (in 1970). Even the usual ASCII converted date/time routine returns a string containing both time and date.

Similarly, VMS, since it was first introduced, has used a unified date/time

value, this time a (64-bit) value indicating 100-nanosecond "ticks" since a fixed time (in 1858).

While I don't have the appropriate documentation here to check, I'd bet that such recent designed systems as Windows NT and OS/2 also use a combined offset.

He is right about MSDOS, however. Once a toy, always a toy.

The second point is more significant, even if the particular application is trivial. He points out that the problem can only arise if the program happens to execute the first of the call in a short period of time just before midnight - a period determined by the time needed to issue the two calls one after another. He estimates, then measures, this interval, and computes the fraction of 24 hours that it represents. This fraction he claims is the probability of seeing the bug.

Probabilistic arguments can sound very convincing, but are all too often very poorly made - so poorly made as to be essentially meaningless. This argument is an example of that class. What Mr. Robinson has calculated is the probability that a program which runs at times evenly distributed throughout the day will happen to get caught by such a bug. However, I submit that there are almost no programs with this property. Many programs are much more likely to run during the day than near midnight; many never run at midnight at all. They will have essentially no chance of seeing a problem. On the other hand, there exist programs that regularly run near midnight - programs that roll files over for the new day, for example. Their probability of seeing the problem are much, much higher - though without more information, it's impossible to estimate the real probability.

Probabilistic arguments look strong because they look so objective. However, there's often a great deal of subjectivity in estimating the underlying distributions on which the calculations are based. We need only recall the orders of magnitude that distinguished the Intel and IBM estimates of the probability of running into the Pentium divide bug. Intel assumed the divisors and dividends were chosen at random from all possible 64-bit values. IBM made various assumptions, such as that the divisors and dividends were the best representations of numbers that, in decimal, had one digit before and two digits after the decimal point. There are completely different distributions, and the resulting "objectively calculated" probabilities are wildly different. Which is "right"? Both, and neither. Both correctly describe a possible use of a Pentium. Neither exactly describes any likely real set of calculations performed by any real Pentium user. Which one is more useful? Ah, well that all depends on what you are trying to do.

Finally, I'll point out that the underlying problem - of accurately reading a field that cannot be accessed atomically - recurs at multiple levels. Many contemporary chips provide a 64-bit hardware-updated clock, but can only access its value 32 bits at a time. Reading such a clock requires care! Leslie Lamport published an algorithm a couple of years back - essentially the trick that others have mentioned, of reading high order, then low order, then high order again, and retrying if the high order bits changed - that can be proved to get the correct time without requiring interlocking. The proof is non-trivial.

-- Jerry

[And don't forget the delightful old SRI stuff, which Lamport, Shostak, Pease, Rushby, and others have contributed to, showing that the old-faithful three-clock fault-tolerant algorithms do not work under Byzantine fault modes; you need FOUR clocks! PGN]

---

## Getting Date & Time in synch

*"Richard Schroepfel" <rsc@cs.arizona.edu>*

*Wed, 4 Jan 1995 16:32:59 MST*

Walter Murray <walterm@hprctbs3.rose.hp.com>:

Fred Ballard pointed out the risk of a COBOL program running near midnight...

I used it in 1969 in assembly code written under ITS, which had separate Date and Time calls. I think I read about it in Datamation.

At the hardware level, the manual for the IBM 360 discussed (in 1965) the 64-bit clock, a new feature of the architecture. The clock was represented as two 32bit words in memory, and was automatically updated by the hardware, every X microseconds. The application programmer might read the clock value while the hardware was propagating a carry to the high word, and the program would see mismatched upper & lower data. The manual promised that, if you used a certain Move instruction to read the clock, the hardware would hold off clock ticks while the Move completed. Moreover, the same promise applied if you were Moving a new value into the clock memory.

This problem's been around a long time.

Rich Schroepfel rsc@cs.arizona.edu

---

## Re: Dates and Times Not Matching in COBOL (Robinson)

*<Craig\_Everhart@transarc.com>*

*Thu, 5 Jan 1995 10:57:44 -0500 (EST)*

I have to interpret this line of reasoning as having been intended to draw flames--if not by Mr. Robinson, then by our beloved editor/moderator. I can make the Pentium analogy as well as most folks, and this one is far easier to understand.

One of the big reasons for the RISKS list effort is to allow us to understand what we're buying in to when we allow machines to do our work for us. To the extent that we trust machines to do the right thing, we had better see to it that they do. To the extent that we cannot trust such machines, we need to be aware of the likelihood of problems, and adjust our trust accordingly.

There are so many time-based calculations going on all the time, that it

boggles the mind to imagine the impact of this carelessness. So many of these calculations are embedded so deeply that you'll never bother to verify them.

So what if you're charged for another day of rent, even for an expensive object? So what if you're charged another day's interest on money? Or so what if it happens, as long as it's not likely to happen to you but rather to somebody else?

(What is wrong with this attitude?)

I'm reminded of a story told me by a buddy some time around 1974, wherein he had labored hard and long to isolate the cause of a machine freeze-up that hit his timesharing system (a Sigma, I think) once every few days. He had finally traced the problem to a race condition that would have been solved by inverting the order of two machine instructions. Upon reporting this to the manufacturer's engineers, they answered with "but that problem will almost never happen, so it's not worth fixing," regardless of the periodic machine freezes that it had in fact caused.

Craig

---

## Re: Dates and times not matching in COBOL

Erann Gat <gat@aig.jpl.nasa.gov>

Wed, 4 Jan 95 19:06:13 PST

```
135 REM NOW COUNT NUMBER OF ACTIONS IN ONE SECOND
140 J = 0 : T1$=TIME$ : D1$=DATE$
150 T$=TIME$ : D$=DATE$
160 J = J+1 : IF T$=TIME$ THEN 160
```

Paul Robinson <paul@tdr.com> writes:

> ... but how many people worry about an error that \*might\* happen  
> once every 16.9 years?

A lot of Pentium users were pretty upset about a bug that was purported to turn up only every 27,000 years. Paul's blase attitude about this problem is particularly ironic in light of the fact that his BASIC benchmark program contained a bug:

```
135 REM NOW COUNT NUMBER OF ACTIONS IN ONE SECOND
140 J = 0 : T1$=TIME$ : D1$=DATE$
150 T$=TIME$ : D$=DATE$
160 J = J+1 : IF T$=TIME$ THEN 160
      ^^^ Should be 150
```

I didn't check the Pascal version.

Erann Gat gat@jpl.nasa.gov

---

## Re: Dates and Times Not Matching in COBOL (Robinson)

Wayne Hayes <wayne@csri.toronto.edu>

Wed, 4 Jan 1995 18:09:17 -0500

Once ever 16.9 years \*per computer\*. That means that with just 17 computers, the error \*might\* occur once per year. 17000 computers, and it's probably happening once a day somewhere in the world. Obviously it's not, though, otherwise we would've heard about it sooner, but that's not the point.

The point is program correctness. This is a trivial problem to fix, and so it should be fixed. The low probability of it happening will be little consolation when your VISA card gets 2 months worth of interest rather than just 1, or the life support system issues an overdose because it finds a discrepancy of 86,399 seconds between two readings occurring 1 second apart, at midnight.

[There were numerous comments on the 16.9-ness monster, a few of which are included for diversity. Others, omitted here, include those from Duncan Booth <Duncan@rcp.co.uk>, "Stanley F. Quayle" <QUAYLE@scriptel.com>, "Jonathan I. Kamens" <jik@cam.ov.com> "Peter Capek 914-784-6721" <capek@watson.ibm.com> the last three of whom noted the Intel similarities (e.g., once in 27,000 years). PGN]

---

## Dates and Times Not Matching in COBOL

"Walt Farrell" <wfarrell@VNET.IBM.COM>

Thu, 5 Jan 95 09:41:22 EST

IBM's MVS and its predecessors (at least for the last 20-25 years) have always returned the date and time in a single system call. Whether the COBOL compiler has made that information available in one call is another question. But when the system's TIME service is used, you can get both the time and the date with one invocation.

Paul further detailed some experiments he ran to see how severe the problem might be of having a program running that makes two requests, one just before midnight and the other just after midnight. His conclusion, for a program written in Pascal, was that:

> ... but how many people worry about an error that \*might\* happen  
> once every 16.9 years?

I'm afraid this conclusion ignores the multi-programming aspects of today's systems. When multiple programs are running, one program may be suspended by the operating system to service a program with a higher priority. It's conceivable that a program might be suspended for several seconds (or even minutes if it has a very low priority and the system is running many

programs of higher priority) such that the first request could occur well before midnight, then the program would be suspended until after midnight.

-- Walt

---

## **RE: Dates and Times Not Matching in COBOL**

*"Stanley F. Quayle" <QUAYLE@scriptel.com>*

*Thu, 05 Jan 1995 10:46:36*

I've done a lot of process control work, and while I'd \*NEVER\* use COBOL for such an application, it's important to eliminate windows of failure. Why live with Murphy's Law when you can prevent it?

Stanley F. Quayle Scriptel Holding Inc. 4145 Arlingate Plaza, Columbus, OH 43228 quayle@scriptel.com +1 614 276-8402

---

## **Re: Dates and Times Not Matching in COBOL (Robinson)**

*Marc Horowitz <marc@MIT.EDU>*

*Thu, 05 Jan 1995 00:15:37 EST*

You're using a reasonably modern PC, which is, relatively speaking, a really fast machine. I've used timesharing machines which were so overloaded that simple jobs took hours. I wouldn't be at all surprised to find out that seconds or even minutes elapsed between "consecutive" date and time requests. This is still unlikely, but I wouldn't stake my million-dollar application on it.

1/6200 is also substantially more likely than the 1/10<sup>9</sup> which is often cited for "critical" applications.

Marc

---

## **Date and Time not matching... (2)**

*"Peter Capek (TL-863-6721)" <capek@watson.ibm.com>*

*Thu, 5 Jan 95 01:47:13 EST*

The Rexx programming language includes separate built-in functions for obtaining the date and time. However, the defined semantics for these is that the first call to either within a clause (informally: statement) causes a record to be made which is then used for ALL calls to these functions within that clause. Hence, if multiple calls to DATE and/or TIME are made in a single clause, they are guaranteed to be consistent with one another.

Peter Capek

---

## **Split up date and time calls vs an atomic operation (Robinson)**

Lars Wirzenius <wirzeniu@cc.helsinki.fi>

Thu, 5 Jan 1995 15:32:31 +0200

Paul Robinson suggested in [RISKS-16.70](#) that COBOL has separate statements for getting the date and time "[b]ecause most operating systems separate the request for time from the request for date".

To me, this indicates that most operating systems have not been designed with reliability in mind (or if they have, then they are buggy in this regard). One example of an operating system that does provide the date and time of day in a single call is Unix; it's interface has been copied to the C language. Even when the operating system does not provide an atomic time call, it's not a good idea for a language to `_mandate_` the split calls, since this always puts the burden on the language user. In C, for instance, if the operating system does not support an atomic call, the `time()` function can hide this by using a `"do { get date1; get time; get date2; } while (date1 != date2);"` loop as suggested by an earlier RISKS entry. The C programmer then gets an atomic operation anyway. This is the approach to take for all systems and languages, and I'm glad to hear the COBOL now does take it.

In addition to the race condition introduced by separate date and time of day calls in an operating system, remember that if the operating system returns the date, then it must know something of calendars. A very simple understanding of the Gregorian calendar is simple to code (one needs a table containing the lengths of months, and a simple formula that tells whether a year is a leap year). Even so, there are a lot of programs that can't handle it correctly. A more complete understanding of calendars in general (not just the Gregorian one) would need a lot more code, which is better kept outside the kernel. I think the Unix design, where the kernel keeps track of some universal time and the programs convert this into dates and local time as they wish, is the best solution.

Lars.Wirzenius@helsinki.fi (finger wirzeniu@klaava.helsinki.fi)

Publib version 0.4: <ftp://ftp.cs.helsinki.fi/pub/Software/Local/Publib/>

---

## re Dates and Times not matching (Robinson)

Phil Rose <pvr@wg.icl.co.uk>

Thu, 5 Jan 95 14:30:34 GMT

One more example: ICL's VME provides them.

Surely that's the whole point about RISKS: Yes, it mayn't happen very often, but will do so and in safety critical situations will probably do so at the most dangerous time. (Sodd's law aka Murphy's law)

Anyway, Mr Robinson's analysis overlooks one important fact - jobs do not always run randomly. If I set a job to start at 5 minutes to midnight to do some housekeeping or such and it tends to run for 4 min 59.9 secs +/- 0.1 sec before reading the date and time it is probably much more likely to fall over this problem than if I set it off to run randomly after I go home. It's

a problem with reliability calculations - they tend to assume life is random!

Phil Rose pvr@wg.icl.co.uk P.V.ROSE@UK03.wins.icl.co.uk G3ZZA

---

## Atomic time/date access

*Robinson <David Jones <dej@eecg.toronto.edu>*

*Thu, 5 Jan 1995 11:11:32 -0500*

The Unix `gettimeofday()` and AmigaDOS `CurrentTime()` calls return both time and date. Both these systems combine time and date into a single 32-bit number (which has other problems, which I'll get to later).

He then goes on to estimate the probability of a time/date rollover error by running tests on GW-BASIC on a MS-DOS machine. This environment allows reasonably well-controlled execution time behavior. In contrast, heavily loaded Unix systems short on real memory may swap your program out between the time and date instructions, leading to a window of vulnerability much larger than the 1/3023 s window that he gives.

Unix isn't completely off the hook. Most systems use a signed integer for time/date values. The highest value that can be stored in such an integer is  $2^{31}-1$ , which corresponds to Mon Jan 18 22:14:07 2038 EST. So Unix gives us another 38 years.

David Jones, M.A.Sc student, Electronics Group (VLSI), University of Toronto  
email: [dej@eecg.toronto.edu](mailto:dej@eecg.toronto.edu), finger for PGP public key

---

## Re: Dates and Times Not Matching in COBOL (Robinson)

*"Jonathan I. Kamens" <jik@cam.ov.com>*

*Thu, 5 Jan 1995 12:16:53 -0500*

From the start, the UNIX concept of time has been the elapsed time since January 1, 1970, the "UNIX system time". Any UNIX program which needs to get the current time or the current date from the system does so by first asking for the UNIX system time (using `time(3)` (`time(2)` on older systems) or `gettimeofday(2)` and then using a UNIX library function to convert it into the appropriate human-interpretable data (current date, current time, etc.). The operation of getting the UNIX system time is atomic, and always has been.

Just so that people don't think I'm claiming that UNIX was the first to get this right, I'll point out that Multics had similar functionality -- a function for getting the current system time as a 72-bit binary number, functions for converting that number into human-readable representations, and a function for converting a human-readable date string into such a 72-bit binary number.

Just so that people don't think I'm claiming that no one has gotten it

right since UNIX, I'll point out that MacOS uses the same concepts, although it has the different problem of assuming that the system time is always local time (i.e., it has no concept of time zones).

The fact that the current date and the current time are intertwined and should not be treated separately by an operating system trying to achieve reliability is not new knowledge, and the technology to "do it right" is not new technology. Just because COBOL and DOS got it wrong doesn't mean that we should live with it being done wrong.

Jonathan Kamens | OpenVision Technologies, Inc. | jik@cam.ov.com

---

### **COBOL date at midnight issue (Ballard)**

*Andrew W Kowalczyk <AKOWALCZ+aLIFDR1%Allstate\_Corp+p@mcimail.com>*

*Thu, 5 Jan 95 11:27 EST*

Regarding Fred Ballard's suggestion of bracketing the time of day inquiry between two date inquiries.

In the various large organizations I have worked for I have never seen a "production" "batch" program that relies on the system date for any processing decisions or calculations. Nearly all programs use a "run date" which is entered as a parameter or is in a common file read by all programs that need a date.

Besides addressing the "after midnight" problem it also allows retroactive processing when problems happen or anticipatory runs to spread out workloads or compensate for postal delays.

Of course there is the problem of entering the wrong control date. A clever approach is to utilize the system date as a reasonableness check on the entered control date (this would be especially likely to catch the common error we all commit of not incrementing the year digits in our head until sometime in February :) )

As we replace these old systems with real time client-server systems then the use of system date and time becomes more enticing - but then we confront the headache of which clock to use on a network of processors.

Also a potential risk in relying on programming language facilities that return the date and time in a single request - how do we know that the language implementors have applied Fred Ballard's carefulness to the extraction - as Paul Robinson points out: most of the underlying operating systems would require separate calls.

Andy Kowalczyk Allstate Life Insurance Company - Direct Response  
3100 Sanders Road Suite N3A Northbrook, IL 60062-9266 voice: (708)402-4457

---

## Re: Dates and Times Not Matching in COBOL (Robinson)

"Barry Jaspan" <bjaspan@cam.ov.com>

Thu, 5 Jan 95 12:33:00 EST

[...]

Paul is missing one of the basic lessons of RISKS (even though he states the source of the problem): the coupling of seemingly unrelated events. The probability distribution of the time of day at which jobs run is not flat. There are a LOT of batch jobs out there in the world that run automatically at "midnight." This bug will almost certainly occur eventually, probably already has, and with a frequency much higher than once every 16.9 years. Maybe it will even happen on the A320 he is flying in...

Barry

---

## Dates and times (Robinson, [RISKS-16.70](#))

Joe Morris <jcmorris@mwunix.mitre.org>

Thu, 05 Jan 1995 13:11:19 -0500

MS-DOS certainly has the problem, but OS/360 and its successors (including MVS) don't. I can't speak for the other systems cited.

In the OS/360 world, the time and date have always been available in the single operating system call SVC 11 (optionally through the TIME macro). Time is returned in GPR0; date in GPR1. Optionally, on S/370 and later systems the program can use the SVC 11 call to obtain the 64-bit TOD clock and do its own conversion to date-and-time. (The TOD clock, maintained by the hardware, gives time from 0000 hours 1 January 1900 and is the datum from which all time and date information on the system are derived.)

Of course, none of this makes any difference if the language in use doesn't provide a mechanism for the application to retrieve both time and date returned by the same OS invocation.

Joe Morris / MITRE

---

## Midnight rollover risks

Lord Wodehouse <w0400@ggr.co.uk>

Thu, 5 Jan 1995 11:02:12 +0000 (GMT)

As much as the various contributors who have worked to show that the chances of a problem with the time/date at midnight are less than 1 in  $10^6$  in any one day, I am afraid that if one was depending on the software to fly a 747, that would not be a great comfort!

However I have seen a wonder example of such a problem with a large VAX cluster of six machines. The batch subsystem and job controller runs on all

the CPUs. Jobs set to run at midnight will be started by the first machine to reach midnight and to schedule the job. However the job may well not run on that machine, but on another. If the clocks are not in step and they \_never\_ are, that machine may resubmit the job to run the next midnight. The result - well as opposed to one job running once at midnight, you can end up with lots of them and unless the code handles this, the data files can become interesting. As machines get faster, the jobs can run quicker, so the window for such a problem becomes more significant. With an old 11/750, getting the job to start might take seconds, while a 6660 it might take less than 1/100th of a second. So with the 11/750 cluster. the clocks can be a few seconds adrift, while with 6660's, that margin is much smaller.

Lord John - The Programming Peer +44 181 966 2109 w0400@ggr.co.uk



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 16: Issue 72

Friday 6 January 1995

## Contents

- [Computing error at Fidelity's Magellan fund](#)  
[Kathy Godfrey](#)  
[Arthur Flatau](#)
- [Phone system problems in Santa Fe](#)  
[Bruce Wampler](#)
- [LZW/GIF flap on RISKS](#)  
[Tim Oren](#)
- [Re: CompuServe-Unisys GIF Tax Protest](#)  
[Peter Bishop](#)
- [Software math errors](#)  
[Chris Phoenix](#)
- [Rutherford Effect: term for particular class of failures](#)  
[Bill Thomas](#)
- [Re: Cancelbot Derails Online Promo](#)  
[Andrew Haley](#)
- [Re: Soldiers and Cellular Telephones](#)  
[Linden B. Sisk](#)
- [Re: Computer Addiction](#)  
[Mary Shafer](#)  
[John C. Rivard](#)  
[Steven D. Brewer](#)
- [Re: Date and Time](#)  
[Leslie Lamport](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Computing error at Fidelity's Magellan fund

*Kathy Godfrey <[kgodfrey@BBN.COM](mailto:kgodfrey@BBN.COM)>*

*Wed, 4 Jan 95 17:44:41 EST*

There was a big flap recently over Fidelity's Magellan fund estimating in November that they would make a \$4.32/share distribution at the end of year, and then not doing so. A letter of explanation was sent to the shareholders (including me) from J. Gary Burkhead, the President of Fidelity, including

the following pertinent items:

"During the estimating process, a tax accountant is required to transcribe the net realized gain or loss from the fund's financial records (which were correct at all times) to a separate spreadsheet, where additional calculations are performed. The error occurred when the accountant omitted the minus sign on a net capital loss of \$1.3 billion and incorrectly treated it as a net capital gain on this separate spreadsheet. This meant that the dividend estimate spreadsheet was off by \$2.6 billion....

"Some people have asked how, in this age of technology, such a mistake could be made. While many of our processes are computerized, the requirements of the tax code are complex and dictate that some steps be handled manually by our tax managers and accountants, and people can make mistakes. The error in this case was not caught in the initial review, but was detected in our normal process--which includes a review by outside auditors--as we prepared to make the actual distribution calculation.

"We have taken several steps designed to ensure that this error should not happen again. We will subject initial estimates to the same rigorous verification process that we use in preparing the distributions that the funds actually pay. This will include a thorough review not only by our own fund accountants but also by the fund's treasurer and independent auditors. In addition, estimates will be reviewed by each fund's portfolio manager."

I'm still not clear as to exactly why a spreadsheet or other program couldn't be developed to make the estimation calculation, since the problem seems to have been a transcription error and not a failure to understand the complexities of the tax code. It also occurred to me to wonder what sort of testing the software they do use undergoes, and whether those procedures will also be upgraded in the wake of this mistake.

I see two RISKS: The implication that this mistake only happened because manual steps were involved, and the risk of having infrequent but highly important tasks that require non-standard procedures (like "manual" calculations in a largely computerized environment).

<>Kathy Godfrey kgodfrey@bbn.com

---

### **Only Wimps use minus signs (Magellan/Fidelity Investments)**

*Arthur D. Flatau <flatau@cli.com>*

*Fri, 6 Jan 95 12:31:47 CST*

[Arthur sent us an excerpt from the 5 Jan 1995 edition of the \*Austin American Statesman\*, p D8 (omitted here), with the following comment. PGN]

Even after reading risks all these years, I am still amazed that these kind of errors can slip by. The last time I entered a \$1.3 billion check as a deposit in my checkbook, it was only a short time before I was bouncing checks left and right. It also was quite apparent when I balanced my check book at the end of the month.

Art flatau@cli.com Austin, Texas

---

## Phone system problems in Santa Fe

<wampler@cs.unm.edu>

Thu, 5 Jan 95 10:46:12 MST

>From the January 4, 1995 Albuquerque Tribune front page:

Hello? Hello? Phones go haywire in Roundhouse

Your state government has been disconnected. Please check the number and call again some other time.

As if Gov. Gary Johnson's call for the mass resignation of about 350 state officials weren't enough to confuse citizens in search of bureaucrats, the state's phone system on Tuesday began to arbitrarily shifting many 827-prefix calls to an erroneous recording that declared the number was not in service.

The 827 prefix is state government's main prefix in Santa Fe.

"I'm quite uncomfortable about the current situation," John Dawson, deputy director of the state Office of Communications, said Tuesday.

"It's manifesting itself very seriously today for some reason. But I'm hopeful that it will be over in the next 24 hours."

Dawson said a glitch in the software that controls the state office phone system was at fault for the complications. He said it appeared to be affecting only Santa Fe offices with the 827 prefix.

The state was aware of the computer problem a year ago, and removed the software because of it, he said. But two weeks ago the state allowed its contractor, Fijitsu Business Communication Systems, to reinstall the software because the glitch supposedly had been removed."

The article went on to describe the confusion, and the fact that our new governor was not getting calls. As might be expected, this happened right when a new administration was moving in to Santa Fe. So, if it was broken once, try to break it again at the most critical time possible. Sigh...

Bruce Wampler, Ph.D. Adjunct Professor, Department of Computer Science  
University of New Mexico wampler@cs.unm.edu

---

## LZW/GIF flap on RISKS

Tim Oren <oren@well.sf.ca.us>

Tue, 3 Jan 1995 22:15:24 -0800

[A longer message from Tim is floating around the well. This one seems quite succinct, and helps to clarify further the situation discussed in [RISKS-16.69](#) and .70. PGN]

Because the RISKS list gets pretty wide distribution, I wanted you to know

that the original posting contains some pretty serious misinterpretation of a messy situation. Briefly,

- CompuServe is asserting no proprietary rights in the GIF spec, and couldn't even if we wanted to, since it has long been openly published.

- The LZW algorithm was incorporated from an open publication, and without knowledge that Unisys was pursuing a patent. The patent was brought to our attention, much to our displeasure, after the GIF spec had been published and passed into wide use.

- We found it necessary to take a license to the patent from Unisys, and since a number of our developers had used GIF in good faith, we also negotiated a pass-through license for their benefit. Clawson has distributed parts of this license, with a poor interpretation, outside of its original context, which was to developers of CompuServe-related products alone. GIF is included in this license because we are unable to pass through a general license to practice LZW.

- It is not the intent of CompuServe to attempt to enforce proprietary rights in GIF against users or developers, including those of Web technology. We cannot and do not speak for Unisys' intent in this matter.

- Having and transmitting GIF images is not an infringement of the patent, since 'practicing' LZW means running code which accomplishes the compression of the graphics.

Tim Oren, Vice President, Future Technology CompuServe, Inc.

---

## Re: CompuServe-Unisys GIF Tax Protest

*Peter Bishop <p\_bishop@adelard.demon.co.uk>*

*Thu, 05 Jan 95 18:01:30 GMT*

The recently announced patent restriction by UNISYS/COMPUSERVE on the use of GIF files poses a potentially serious problem. The Internet community needs to protect itself from such arbitrary constraints by establishing a new public domain standard for graphics interchange.

This standard needs to:

- 1) Be compact
- 2) Decode fast
- 3) Be free from patent/copyright restrictions
- 4) Be rapidly available

JPEG is certainly a candidate as it is a public standard. The only drawback is the slow decoding time.

However there is an alternative based on existing 'standards' that should give similar performance to GIF files.

We can do this by:

a) Representing the picture using the Portable Bit Map (PBM) format

b) Compressing using the Free Software Foundation GZIP method.

I have been trying this idea out to see if the performance is OK. Unfortunately I do not have PBM support on my machine, but I have been testing the approach using the Windows bitmap format (BMP). The tests were done on an PC 386/DX33 machine using 8 bit (256 color) files. The GIF and JPEG measurements were based on the LVIEW 3.1 public domain graphics package. Standalone DOS GZIP and PKZIP v1.1 packages were used for the other measurements.

Results:

Test file Cathedra.bmp

Format	Size (bytes)	Encode (secs)	Decode (secs)
BMP	307,994	-	-
ZIP	185,866	14	6
GZ	173,314	15	6
GIF	197,548	8	9
JPEG	56,167	25	30

Test file simba.bmp

Format	Size (bytes)	Encode (secs)	Decode (secs)
BMP	265,398	-	-
ZIP	109,760	15	5
GZ	99,748	14	4
GIF	113,895	9	8
JPEG	34,638	21	20

Assuming that BMP and PBM formats are of similar size, it would seem that a compressed PBM file format (GZF?) has advantages over the equivalent GIF file since it is smaller and decodes faster. The encoding time is slower - but this is a 'one-off' operation so it is not too important.

It is also interesting to note that GZIP gives better compression than my rather elderly V1.1 version of PKZIP, and I think that GZIP will stand up pretty well against current compression methods such as those in PKZIP 2.04.

I hope this starts a useful debate on defining a 'rapid hack' to provide a substitute for GIF format files.

Obviously it is important that we get something that people are happy with - but quickly. One option is to set up a forum of current GIF providers and users who would hammer out a new format. The other more direct (and rapid) approach is to nominate a volunteer to define the format and provide the C

sources so that the new format can be readily incorporated into existing graphics tools.

The obvious choice here is the Free Software Foundation. It is part of their remit to provide good quality free software, and they are the authors of GZIP, so they should be in a good position to define the format and publish it via the usual GNU distribution channels (together with a GIF to GZF converter).

Peter Bishop, Adelard, 3 Coborn Rd, London E3 2DA, England

Tel : +44-81-983-0219 p\_bishop@adelard.demon.co.uk

---

## Software math errors

*"Chris Phoenix" <Chris.Phoenix@efi.com>*

*Wed, 4 Jan 1995 18:18:00 -0800*

Along with the historical-interest postings on hardware math errors, it may be interesting also to consider software math errors. Here's one:

The built-in BASIC on the TI 99/4A computer uses a certain shortcut for boolean calculations: it uses \* for and and + for or. Operations such as ">" return numeric values, and the IF statement tests for zero or non-zero.

Here's the problem: the 'numeric values' mentioned above are 0 for false, and -1 for true.

So `` 10 IF (((1 > 0) \* (1 > 0)) + (1 > 0)) PRINT "It Works" `` won't print anything, since -1 \* -1 is 1, and 1 + -1 is 0.

Chris Phoenix chris@efi.com 415-286-8581

---

## Rutherford Effect: term for particular class of failures

*Bill Thomas <billt@core.rose.hp.com>*

*Wed, 4 Jan 95 20:38:30 PST*

While resolving a problem involving interactions of multiple systems we found we had a set of failure conditions which had a very low probability of happening, lacked any work around or avoidance strategies, and had very unexpected results when one occurred. We gave the name "Rutherford Effect" to such situations.

The reason for the name "Rutherford Effect" comes from the experiment Rutherford and two of his students, Geiger and Mardsen did. They made a beam of particles project onto a thin metal foil. Most particles when through with no problem. However, a few hit the nucleus in of a atom in the foil and bounced back. According to legend, Rutherford said, "I would not have been more surprised if I had shot a cannon ball at tissue paper and it bounced back." The similarity of a computer mostly working but having a very small number of unpredictable and unavoidable failures inspired us to say it suffered from a "Rutherford Effect".

The Pentium also suffers from a Rutherford Effect.

Bill Thomas billt@core.rose.hp.com

---

**Re: Cancelbot Derails Online Promo (WSJ via Edupage 12/20/94)**

*Andrew Haley <aph@atml.co.uk>*

*Thu, 5 Jan 1995 13:57:27 GMT*

The excerpt from the Wall Street Journal about this incident reproduced in [RISKS-16.67](#) is inaccurate.

This incident involved Michael Wolff posting nearly 150 virtually identical messages to different newsgroups. (Actions of this kind are called "spamming", where "spam" is defined as the posting of 20 or more substantially identical messages to Usenet. The content of these messages is irrelevant.) These messages were cancelled by Cancelmoose.

After the cancellation, the issue of these messages was discussed at length in alt.current-events.net-abuse, and a vote was taken, which was overwhelmingly in favour of the cancellation. There was nothing special about the Wolff postings; all mass postings to Usenet that fit the criteria of spam are cancelled.

Cancelmoose is not a "vigilante", as he does not act alone; there is substantial agreement amongst the Usenet administrators that have contributed to this debate that these actions are necessary.

Wolff claims to be an expert on the Internet; if this were true he shouldn't have been "stunned and amazed" by the response.

Andrew

---

**Re: Soldiers and Cellular Telephones**

*Linden B. Sisk <sisklb@texaco.com>*

*Thu, 5 Jan 95 09:47:41 CST*

Cellular phones, when powered up, periodically transmit to the nearest cell, even when someone is not talking on them. For soldiers, that represents a risk that enemy troops will be able to locate them using direction-finding equipment and attack them, or call in artillery fire or air strikes on their position. That, I presume, is why the Israeli command structure is concerned about their troops carrying cell phones - and should be - notwithstanding the issue of time being spent on non-military tasks.

Linden B. (Lindy) Sisk sisklb@texaco.com

---

**Re: Computer Addiction**

Mary Shafer <shafer@nasp.dfrf.nasa.gov>

Wed, 4 Jan 95 17:18:53 PST

Try the "leave" command if you're a UNIX person. It not only warns you that the time to logout is coming up, but proceeds to nag you after the set time passes.

I've been using this since about 1988, since I'm in a carpool.

Mary Shafer, SR-71 Chief Engineer, NASA Dryden Flight Research Ctr, Edwards, CA  
shafer@dfrc.nasa.gov URL <http://www.dfrc.nasa.gov/People/Shafer/mary.html>

---

## Re: Computer Addiction (Kabay, [RISKS- 16.70](#))

John C. Rivard <jcr@garnet.msen.com>

Wed, 4 Jan 1995 21:43:43 -0500

Actually, there was (and perhaps still is) such a product for the Apple Macintosh called LifeGuard.

It was reviewed in the February 1991 issue of *\_MacUser\_* magazine. According to the reviewer, the memory-resident program produced an audible and visual alarm on the Mac after a length of time that the user specifies. It then reminded the user to take a break:

"You control the frequency of breaks as well as the interval allowed before it's time to resume work."

It also provided the user with a "snooze" function to temporarily override the alarm. It even offers suggestions for exercises and basic information on ergonomics, according to the reviewer.

LifeGuard's publisher was Visionary Software, Inc., P.O. Box 69447, Portland, OR 97201 (800-877-1832 or 503-246-6200). I have never actually seen the product, just read the review. I wonder if it caught on and whether it is still available today (version 1.0 was reviewed).

John C. Rivard      jcr@garnet.msen.com      JCR Design and Consulting  
Copyright (c)1994 John C. Rivard (just in case) :^)

---

## Re: Computer Addiction

Steven D. Brewer <brewer@cs.wmich.edu>

Thu, 5 Jan 95 13:37:55 EST

Such things already exist. Coffee Break, a program for the Mac by Thomas Reed, was written to help reduce repetitive stress injuries. It allows you to set how much time you want to work between breaks and how long your breaks should be. It will then come to the foreground when you have exhausted your work time and will not relinquish control of your computer

until after the break time has passed. I haven't used the program myself and can't speak in any detail about its features. It is available from the typical Mac ftp sites (I downloaded it from the umich archives: /mac/util/organization/coffeebreak1.1.sit.hqx.)

Steve Brewer <brewer@cs.wmich.edu> [http://141.218.91.93/WWW/l\\_sbrewer.html](http://141.218.91.93/WWW/l_sbrewer.html)  
Science Studies WMU Kalamazoo MI 49008

---

**Re: Date and Time (Leichter, [RISKS-16.71](#))**

<lamport@pa.dec.com>  
Thu, 05 Jan 95 15:57:51 -0800

Jerry Leichter said

Leslie Lamport published an algorithm a couple of years back - essentially the trick that others have mentioned, of reading high order, then low order, then high order again, and retrying if the high order bits changed - that can be proved to get the correct time without requiring interlocking. The proof is non-trivial.

Despite the assortment of trivialities that have been published as "Lamport's bakery algorithm", I am still not inured to the defamation of my algorithms. Please inform the Risks list that my clock-reading algorithm, published in

AUTHOR = "Leslie Lamport",  
TITLE = "The Concurrent Reading and Writing of Clocks",  
journal = tocs,  
volume = 8,  
Number = 4,  
Month = nov,  
Year = 1990,  
pages = "305--310"

requires no retrying.

Leslie



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 16: Issue 73**

**Friday 6 January 1995**

## Contents

- [My life as an international arms courier \[longish, but good\]](#)  
[Matt Blaze](#)
- [Work monitoring](#)  
[Phil Agre](#)
- [GRE by computer, the sequel](#)  
[Cris Pedregal Martin](#)
- [More on "Cell phones in Israeli army"](#)  
[Heinz Wrobel](#)
- [Re: Adopting Programming Improvements](#)  
[Douglas W. Jones](#)
- [Re: CompuServe-Unisys GIF Tax Protest](#)  
[Kenneth Albanowski](#)
- [Info on RISKS \(comp.risks\)](#)

---

## My life as an international arms courier

*Matt Blaze <mab@research.att.com>*

*Fri, 06 Jan 95 16:58:50 -0500*

[This is admittedly a bit long, but I thought this experience might be of some interest to RISKS readers. -matt]

[Matt, Struggling as we are with export controls in the NRC crypto policy review, this is quite interesting. Thanks. PGN]

Under an obscure provision of US law, devices and computer programs that use encryption techniques to hide information from prying eyes and ears are considered "munitions" and subject to the same rules that govern the international arms trade. In particular, taking such items out of this country requires the approval of the State Department, which decides whether exporting something might endanger national security. In the past, these restrictions were of little concern to the average citizen; encryption found most of its application in military and diplomatic communications equipment. Today, however, growing concern over electronic fraud and privacy

means that encryption techniques are starting to find their way into more conventional commercial products like laptop computers and portable phones.

Mostly to find out what the process was like, I recently applied for a temporary export license for a portable telephone encryption product that I wanted to take with me on a business trip to England and Belgium.

The item in question is more properly called a "telephone security device." This is a little box that scrambles telephone conversations to protect them against eavesdroppers; this sort of protection is sometimes important when discussing confidential business matters from faraway places. The particular model I bought was already approved for export; it employs a cipher algorithm that the government has already decided is not a threat to national security even should it fall into the hands of some rogue government. This model is aimed primarily, I presume, at international business travelers who want to communicate in a reasonably secure manner with their home offices in the states. In other words, a typical user buys two of them, leaving one at the home office and carrying the other when traveling abroad. The options that came with my device included a James Bond-ish looking acoustic coupler and handset to facilitate its connection to the hardwired phones that are still common in European hotel rooms.

It turns out that there was recently some discussion in the government about exempting products like my secure phone from the licensing paperwork requirements. Unfortunately, however, this exemption never actually took effect. So even though the device I had was already approved for sale abroad, I still needed to get a temporary export license before I could take it with me. But I was assured that "this is an easy, routine process". Well, sure enough, about two weeks before I was to leave I got back my official US State Department "license for the temporary export of unclassified defense articles". So far, so good.

>From what I was able to figure out by reading the license (and having a few conversations with an export lawyer), I'm required to leave from an international airport with a Customs agent present (no problem there, although Customs is geared to arriving, rather than departing, travelers). At the airport, I'm supposed to fill out a form called a "shipper's export declaration" (SED) on which I have to declare that "these commodities are authorized by the US government for export only to Belgium and the United Kingdom. They may not be resold, transhipped, or otherwise disposed of in any country, either in their original form or incorporated into other end-items without the prior written approval of the US Department of State". Then I'm to present the SED and export license to a Customs official at the airport before I leave. The Customs officer is supposed to take my SED and endorse my license to show what I'm actually taking out of the country.

On the way back in, I'm supposed to "declare" my item at Customs (even though it was manufactured in the US) and show them my license, and they're supposed to endorse the license again as proof that I

have, in fact, returned the "defense article" to the safety of the United States.

The first hitch I ran into was that no one could actually tell me where I could get an SED form. But when I called Customs they assured me that this was no big deal. "Just come by when you get to the airport and we stamp the license. I guess you can just fill out the SED there," they said.

I made sure to get to the airport early anyway.

Although there was moderately heavy traffic near the airport, I made it to JFK two and a half hours before my 10pm flight. I was flying United, which has their own terminal at JFK, so Customs has an office right there in the same building from which I was to depart (JFK is awful to get around, so I was glad for this). I checked in for my flight (and got upgraded to first class, which bolstered my expectation that everything was going to be really easy from here on). Then, luggage, license and phone in hand, I made my way downstairs to Customs, expecting to fill out the SED form and "just have my license stamped" as they had assured me earlier on the telephone. I explained my situation to the security guard who controls entry to the Customs area, and he led me to "the back office" without much argument or delay. The head uniformed Customs guy in the back office (which I think is same office where they take the people suspected of being "drug mules" with cocaine-filled condoms in their stomachs) looked approachable enough. He had a sort of kindly, grandfatherly manner, and he was playing a video game on a laptop computer. I got the impression that most of the people he encounters are suspected drug smugglers, and he seemed pleased enough to be dealing with something a little different from the norm. When I explained what I was doing he looked at me as if I had just announced that I was a citizen of Mars who hadn't even bothered to obtain a visa.

He explained, carefully, that a) I really do need the SED form; b) not only that, I should have already filled it out, in duplicate; c) he doesn't have blank SED forms; d) he, like everyone else in the entire US government that I had spoken to, has no idea where one gets them from, but people must get them from somewhere; and e) it doesn't really matter, because I'm in the wrong place anyway.

I asked him where the right place is. "The cargo building, of course," he told me, patiently. I remembered the cargo building because I passed it in the taxi just as the traffic jam began, about half an hour before I got to the United terminal. The airport shuttle bus doesn't stop there. I'd have to call a taxi. "But I think they're closed now, and even if they were open you'd never make it before your flight" he helpfully added, saving me the trip. He also complimented me for going to the trouble to get the license.

I must have looked hurt and confused. Eventually he called in some fellow in a suit who I presume to have been his boss.

"Are you the guy who wants to export the fancy gun?" the fellow in the suit asked me.

"It's not a gun, it's a telephone," I responded, with a straight face.

"Why do you have a license to export a telephone?" Good question, I thought. I explained about the export law and showed him the thing. He agreed that it looked pretty harmless.

The fellow in the suit reiterated points a through e almost verbatim (do they rehearse for these things?) and explained that this isn't really their department, since my license was issued by the State Department, not Customs, and my situation doesn't come up very often because exports usually go via the cargo building. He'd love to help me, but the computer in which these things get entered is over in Cargo. "That's how the records get made. But you do have a valid license, which is nice." He also suggested that I would have had an easier time had I shipped the device instead of carrying it with me.

I asked what I should do, given that my plane was scheduled to leave in less than an hour. Neither was sure, but the fellow in the suit seemed willing to leave it to the discretion of the uniformed guy. "How does this thing work, anyway?" he asked. I explained as best as I could, trying to make it sound as harmless as it is. "You mean like that Clipper chip?" he asked.

At this point, given that he has a computer and knows something about the Clipper chip, I figured that maybe there was some hope of making my flight. Or maybe I was about to spend the night in jail. In my mind, I put it at about a 90:10 hope:jail ratio.

Then he asked, "Do you know about this stuff?"

So we chatted about computers and cryptography for a while. Finally, the two of them decided that it wouldn't really hurt for them to just sign the form as long as I promised to call my lawyer and get the SED situation straightened out ASAP. They assured me that I won't be arrested or have any other trouble upon my return.

I made my flight, validated license in hand.

An aside: Throughout my trip, I discovered an interesting thing about the phone and the various options I was carrying with it. Under X-ray examination, it looks just like some kind of bomb. (I suspect it was the coiled handset cords). Every time I went through a security checkpoint, I had to dig the thing out of my luggage and show it to the guard. I almost missed the new "Eurostar" chunnel train (3hrs 15mins nonstop from London to Brussels, airport-style checkin and security) as the guards were trying to figure out whether my telephone was likely to explode.

Coming back to the US was less eventful, though it did take me an extra hour or so to get through Customs. Expecting a bit of a hassle

I didn't check any luggage and made sure to be the first person from my flight to reach the Customs line. The inspector was ready to wordlessly accept my declaration form and send me on my way when I opened my mouth and explained that I needed to get an export license stamped. That was obviously a new one for him. He finally decided that this had to be handled by something called the "Ships Office". I was sent to an unoccupied back room (a different back room from before) and told to wait. I thought about the recent Customs experiences of Phil Zimmermann. (Zimmermann, the author of a popular computer encryption program, was recently detained, questioned and searched by Customs officials investigating whether he violated the same regulations I was trying so hard to follow.) After about half an hour, an officer came in and asked me what I needed. I explained about my export license that had to be endorsed. She just shrugged and told me that she had to "process the flight" first. As best as I could tell, her job was to clear the airplane itself through Customs, that being, technically speaking, a very expensive import. It would take a little while. She was pleasant enough, though, and at least didn't look at me as if she intended to send me to jail or have me strip searched.

Finally, she finished with the plane and asked me for my form. She studied it carefully, obviously never having seen one before, and eventually asked me what, exactly, she was supposed to do. I explained that I had never actually gone through this process before but I understood that she's supposed to record the fact that I was re-importing the device and stamp my license somewhere. She told me that she didn't know of any place for her to record this. After some discussion, we agreed that the best thing to do was to make a Xerox copy of my license and arrange for it to go wherever it had to go later. She stamped the back of the license and sent me on my way. It was a little over an hour after I first reached the Customs desk.

My conclusion from all this is that it just isn't possible for an individual traveler to follow all the rules. Even having gone through the process now, I still have no idea how to obtain, let alone file, the proper forms, even for a device that's already been determined to be exportable. The export of export-controlled items is ordinarily handled by cargo shipment, not by hand carrying by travelers, and the system is simply not geared to deal with exceptions. Technically speaking, everyone with a laptop disk encryption program who travels abroad is in violation of the law, but since no one actually knows or checks, no mechanism exists to deal with those who want to follow the rules. While (fortunately) everyone I dealt with was sympathetic, no one in the government who I spoke with was able to actually help me follow the rules. I was permitted to leave and come back only because everyone involved eventually recognized that my telephone was pretty harmless, that my intentions were good, and that the best thing to do was be flexible. If anyone had taken a hard line and tried to enforce the letter of the law, I simply wouldn't have been able to take the thing with me, even with my license. Had I just put my telephone in my suitcase without telling anyone instead of calling attention to myself by trying to follow the rules, chances are no one would have

noticed or cared.

Unfortunately, however, these absurd rules carry the full force of law, and one ignores them only at the risk of being prosecuted for international arms trafficking. While it may seem far-fetched to imagine US citizens prosecuted as arms smugglers simply for carrying ordinary business products in their luggage, the law as written allows the government to do just that. At the same time, anyone who is aware of and who tries to follow the regulations is made to jump through pointless hoops that are so obscure that even the people charged with enforcing them don't know quite what to make of them.

Copyright 1995 by Matt Blaze. All rights reserved.

Electronic redistribution permitted provided this article is reproduced in its entirety.

---

## Work monitoring

*Phil Agre <pagre@weber.ucsd.edu>*

*Fri, 6 Jan 1995 16:36:05 -0800*

The *\*Wall Street Journal\** has a couple of articles about work monitoring:

Amy Stevens, Clients second-guess legal fees on-line, *The Wall Street Journal*, 6 January 1995, page B1.

This article discusses several law firms whose clients get daily updates on their bills, including explanations for each billed bit of time. Not all lawyers are happy about this, as one might imagine. They probably won't get a lot of sympathy, but imagine a world in which everyone billed by the minute in real time and had to explain any given minute to the customer on demand.

This trend may be relevant to another article on the same page:

Barbara Carton, What's up doc?: Stress and counseling, *The Wall Street Journal*, 6 January 1995, page B1.

It's about the growth of stress management programs for doctors who can't handle being made to see a new patient every fifteen minutes regardless of the nature of the cases.

Phil Agre, UCSD

---

## GRE by computer, the sequel ([RISKS-15.30](#), Dec 1993)

*Cris Pedregal Martin <pedregal@eon.cs.umass.edu>*

*Fri, 6 Jan 1995 15:17:07 -0500 (EST)*

GREetings! Just over a year ago *\*The New York Times\** reported that the GRE would be (partially) administered with the use of computers. The system was

to be "adaptive" (i.e., questions were selected by the computer based on previous answers by the person tested). I pointed out some RISKS in the use of computers for this in general, and the "adaptive" strategy in particular.

I overlooked a simpler RISK. According to a story by Alice Demnner in today's *\*Boston Globe\** (1995 Jan 6, p.4), the computerized GRE has problems because of *\*recycled questions\**.

Apparently questions repeated so frequently that they could be memorized and given to other test takers.

The Educational Testing Service (ETS, the private entity that administers GRE) is "eliminating about three-quarters [!] of the test dates scheduled in the next five months;" ETS is also "adding questions to the exam." [Which I interpret to mean that they won't change the length but will add more questions to the pool from which the program draws its questions--CPM] [Well, I interpreted an earlier article to suggest merely that they would cut down on the opportunities for people to reuse the same answers! PGN]

The problem was identified by Kaplan Educational Centers, which expressed doubts that the ETS would be able to cope with the demand for testing with their reduced schedule.

I guess the lesson is to never underestimate the simplest risks. The other lesson, not to base a lot on the GRE scores, was always there.

Cris Pedregal Martin                      pedregal@cs.umass.edu  
Computer Science Department              UMass / Amherst, MA 01003-4610

---

## More on "Cell phones in Israeli army"

*Heinz Wrobel <heinz@hwg.muc.de>*  
*Thu, 5 Jan 1995 21:20:27 +0100*

>From the german newspaper "Starnberger Merkur", January 4th, 1995:

[Sorry, my translation and spelling may be inadequate. I try to get the meaning across.]

Pizza in the fields

Cellular phones make it possible: Israeli soldier's like to order pizza delivered even on delicate duty at the lebanon border. [...]  
Almost every night they order food at pizza places and restaurants in the neighbourhood. [...] Some pizza joints can already find out about troop movement by analyzing the orders.

Even if this currently an exaggeration, it might definitely be a risk for some.

Heinz Wrobel    heinz@hwg.muc.de

[Ah, yes, the old pizza inference strikes again. We have had various reports in the past relating to increased late-night activities in the White House, the Pentagon, etc. The intelligence term for preventing this kind of inference is OPSEC. I guess in the old days it was the apple vendors rather than the pizza parlors that were being watched. This of course led to OPSECing the apple cart. PGN]

---

## Re: Adopting Programming Improvements (Ballard, [RISKS-16.71](#))

*Douglas W. Jones <jones@pyrite.cs.uiowa.edu>*

*6 Jan 1995 16:35:44 GMT*

In [RISKS-16.71](#) Fred Ballard <72400.1525@compuserve.com> discussed the problems with getting programmers to use new features of programming languages in their code. He commented that the example of surgeons learning to wash their hands before surgery suggested that we should expect long delays between the introduction of a feature in a language, for example, the ANSI COBOL solution to the date problem, and the utilization of that feature by "front line" programmers.

I believe that there's a sound engineering reason for many programmer's failure to adopt new features of programming languages. It's more than just ignorance and cussed stubbornness that keeps some of us writing in, for example, Kernighan and Ritchie C instead of newer versions of the language!

If I am writing software for a specific system, I have no reason not to use the full language that happens to be supported on that system. On the other hand, if I am writing software intended to be portable, I have every reason to avoid new features and language extensions. Each such feature I use will add to the complexity of the instructions I must give for porting the program, and each such feature may prevent some potential user from running my code.

For example, if I want to write code using a sophisticated GUI on UNIX, you'd probably advise me to use C++ and Motif, or some similar combination of tools. On the other hand, not all UNIX systems have C++, and not all have Motif. If I want to minimize the work needed to port my code to new systems, I'd better stick to the older, more universally available standards, the Xt widget set and K&R C. Anyone with a UNIX system supporting X will have those!

Not all system administrators are technophilic, in the sense that they rush out to get the newest implementation of every language or toolkit as soon as it's released, and as system administration is decentralized, with each workstation user responsible for upgrading their software, more and more people will be running ancient compilers and toolkits simply because it's too much of a hassle to keep installing the newest versions of every language on their system.

Doug Jones jones@cs.uiowa.edu

---

## Re: CompuServe-Unisys GIF Tax Protest (Bishop, [RISKS-16.71](#))

Kenneth Albanowski <kjahds@kjahds.com>

Fri, 6 Jan 1995 16:38:12 -0500 (EST)

> This standard needs to:

> 1) Be compact

> 2) Decode fast

> 3) Be free from patent/copyright restrictions

> 4) Be rapidly available

>

> JPEG is certainly a candidate as it is a public standard. The only

> drawback is the slow decoding time.

I'm not saying that replacing GIF is the best solution, but I should point out some additional factors that would be useful in a generalized image format:

\* The image format should allow for commentary text.

\* The image format should be able to contain arbitrary binary data.

\* The image format should support "partial retrieval" where the image data can be used to construct a low-res version before the entire image is received. Currently I am only aware of one application, Netscape, that can make use of this feature, but it is invaluable on low-bandwidth connections.

GIF supports all of these features, although they aren't heavily used. Various applications make use of the comment field. Fractint uses custom "tagged" data to store fractal generation parameters in the image, and Netscape can use interlaced GIFs to support low-to-high resolution retrieval of an image.

GIF has turned out to be an extremely important and useful graphics format, with some of its features (like interlacing) only beginning to be used. Before replacement of something is considered, we must fully understand what it is we already have.

Kenneth Albanowski (kjahds@kjahds.com, CIS: 70705,126)



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 16: Issue 74

Sunday 8 January 1995

## Contents

- [Software sensitive to cold?](#)  
[Karol Fruehauf](#)
- [Revision Level, What Does It Mean???](#)  
[Mark Thorson](#)
- [Re: Cancelmoose, WSJ word usage, and vigilantism](#)  
[Steward](#)
- [Re: ETS Electronic Testing](#)  
[Simson L. Garfinkel](#)
- [Re: Fidelity error](#)  
[Barry Margolin](#)  
[Floyd Ferguson](#)
- [Re: My life as an International Arms Courier](#)  
[A. Padgett Peterson](#)
- [Re: Israeli army, cellular phones, pizza](#)  
[Michael Dahan](#)  
[David Wadsworth](#)
- [Re: GIF](#)  
[David Winfrey](#)  
[Simson L. Garfinkel](#)  
[John Mainwaring](#)  
[Garrett P. Nievin](#)
- [Re: Date/Time](#)  
[Steve Sapovits](#)  
[Mark Brader](#)  
[Erann Gat](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Software sensitive to cold? (Badener Tagblatt, January 7, 1995)

*Karol Fruehauf* <100411.1736@compuserve.com>  
07 Jan 95 09:46:38 EST

"The current extreme cold is causing troubles to the Rhatische Bahn (RhB)  
[a private railway company in Switzerland, Ff]; the brand-new locomotives

can't cope and mainly the service of the Albula-route in Engadin [eastern part of Switzerland, e.g. St.Moritz, Ff] suffers breakdowns. The main switch of the Ge 4/4 III type locomotives gets frozen and the oil supply control software goes out of service.

With a heating equipment for the main switch and a new version of the oil supply control software all problems should be resolved."

The new version of the software will be most likely delivered with cold resistant bits and bytes preventing them to shrink under low temperature conditions. Another solution could be to equip them with skates so that the bits and bytes can function on ice too.

Karol Fruhauf, INFOGEM AG, CH-5401 Switzerland

---

## Revision Level, What Does It Mean???

*Mark Thorson <eee@netcom.com>*

*Sat, 7 Jan 1995 17:27:43 -0800*

How should a revision level be interpreted? Here's a quick guide for anyone short of a clue:

0.1 WE GOT A REALLY GREAT NEW WAY TO DO THINGS !!!

<0.9 Not ready for prime time.

0.9 We think it works, but we won't bet our lives on it.

1.0 Management is on our case; seems like a low risk.

1.01 Okay, we knew about that. All known bugs are fixed.

1.02 Fixes bugs you won't see in 27,000 years, i.e. more than three times the age of the universe.

1.03 Fixes bugs in the bug fixes.

1.04 All right, this REALLY fixes all known bugs.

1.05 Fixes bugs introduced in rev 1.04.

1.1 A new crew hired to write documentation.

1.11 From now on, no comma after "i.e." or "e.g."

1.2 Somebody actually changed a functional feature.

2.0 New crew hired to write software. Old crew blamed for bugs.

2.01 New crew sending out resumes to placement agencies.

3.0 Re-write the software in another language, go back ten squares.

... return to line 0.1

---

## Cancelmoose, WSJ word usage, and vigilantism (Haley)

*<steward@shell.portal.com>*

*Fri, 6 Jan 1995 23:48:25 -0500*

>Cancelmoose is not a "vigilante", as he does not act alone; there is  
>substantial agreement amongst the Usenet administrators that have  
>contributed to this debate that these actions are necessary.

Not to be hopelessly pedantic, but as the post was disagreeing with

the WSJ's word choice:

vigilante- a member of a vigilance committee; any person executing summary justice in the absence or breakdown of legally constituted law enforcement bodies. Now also, a member of a self-appointed group undertaking law enforcement but without legal authority, operating in addition to an existing police force to protect property etc. within a localized area. - New Shorter Oxford Dictionary

It appears to this poster that, in fact, the operator of Cancelmoose -is- a vigilante, executing summary justice on behalf of the vigilance committee consisting of the USENET administrators among whom the 'vote' was taken.

steward@shell.portal.com

---

## ETS Electronic Testing

*Simson L. Garfinkel <simsong@pleasant.cambridge.ma.us>  
Sat, 7 Jan 1995 20:02:10 -0800*

Although I have seen much in the past week about ETS and its electronic testing system, I have seen little in the way of first-hand reports by people who took the test.

I am one of those people. Here is my report.

In the fall of 1992, I had the mistaken notion that I wanted to go to graduate school in the fall of 1993. I got the GRE application and discovered that it was too late for me to take the standard written test and still make my application deadlines. It was possible, however, for me to pay an additional fee (under \$100, but more than \$20) and take the electronic version. This seemed like a godsend, so I willingly parted with my money and awaited my response.

I got a form back from ETS approx. three weeks later. I was to call up the local testing center (in Cambridge, a few blocks from MIT), and make an appointment. I did this.

On the appointed day, I showed up at the ETS testing center. They seemed very disorganized. The center was a quarter of the floor of a medium-sized office building. There was a reception desk up front, a waiting area, and rows of offices with windows. Across from the offices was the "testing room" --- a long, narrow room. There were tables along the walls, computers on the tables, chairs, and windows that overlooked the offices. The arrangement, apparently, was to make it difficult for people taking the test to see other people's screens, and easy for people to look into the room and see if we were cheating.

I presented two forms of identification, which the receptionist scrutinized. I then waited in the reception area until the appropriate time. Three other people showed up. We were then led to the testing area. I

sat down at one machine, and the test began.

I should say here that I found taking the test on the computer to be a much more enjoyable experience than taking the test on paper. The test is self-paced. You have a little count-down timer in the corner of your screen showing you how many minutes and seconds are left in a particular section. You can abort the section at any point and go to the next section.

The test looks much the same as the regular test: diagrams or reading comprehension paragraphs, with questions. You answered the question by clicking on a bubble --- just as if you were filling it in with a pencil. You could also mark questions. You could switch to an outline view that showed every question how you had answered it, and whether or not it was marked. You could click directly to a question.

Was the test susceptible to cheating? Absolutely. Quite simply, we were not watched. There was intermittent talking between two of the test takers on the day of my test. I could see screens of other test-takers. Infact, one of the students seemed to doing the same questions that I was doing.

ETS said that one of the advantages of the computer-test is that the exam will be able to adapt to the student in real-time. This will make the exam more precise, allowing it to zero-in on the student's exact abilities. In my experience, though, I didn't see any such adapting. (I vaguely recall that ETS said that the adapting wasn't being used the year that I took the test, but it may be online now.)

Between each section, we were given a short break. At the end of the test, I was given the chance to cancel the entire test. If I didn't want to do that, I could view my result. However, if I viewed my result, that made it permanent.

I got my score and left. Instead of taking the regular 3 1/2 hours, I was finished in two.

As I said, it was a very enjoyable experience.

---

**Re: Fidelity error**

*Barry Margolin <barmar@nic.near.net>*

*8 Jan 1995 15:08:45 -0500*

On Godfrey: My interpretation of the letter was that the complexity of the tax code is what prevents them from automatic the transcription fully. It takes a human accountant to go through the financial records and determine what should be copied to the distribution calculation.

While I doubt that it's actually impossible to automate this, it's quite conceivable that the complexity has delayed implementation of such measures. Companies only have finite resources to automate their procedures.

On Flatau:

> ... It also was quite apparent when I balanced my check  
>book at the end of the month.

Isn't that precisely what happened? An accountant screwed up, and when the auditors reviewed the books they discovered the error and corrected it.

Frankly, I'm surprised at RISKS people flaming Fidelity for this error. IMHO, this is an example of a company whose procedures \*worked\*. As we all know, no process is infallible, and checks are necessary to catch the errors. Of course it would be nice if the checks always occurred before the failures became public, but the important thing in this case is that the checks occurred before checks were cut (sorry for the pun).

Barry Margolin BBN Internet Services Corp. barmar@near.net

---

### Re: Computing error at Fidelity's Magellan fund

Floyd Ferguson <floydf@iphase.com>

Sat, 7 Jan 95 10:07:45 CST

I see two RISKS: The implication that this mistake only happened because manual steps were involved, and the risk of having infrequent but highly important tasks that require non-standard procedures (like "manual" calculations in a largely computerized environment).

<>Kathy Godfrey kgodfrey@bbn.com

Maybe there is also a cultural RISK?? Magellan Fund does not expect to lose billions and billions of dollars. Manually entering data that is unexpected or unpleasant or unwelcome surely must be more prone to error. Perhaps a computer version of a Freudian slip?? So, procedures for manual entry of data need to take into account the potential emotional/affective content of the data being entered.

[What about Freudian slips? PGN]

Floyd Ferguson floydf@iphase.com

---

### Re: My life as an International Arms Courier (Blaze, [RISKS 16.73](#))

A. Padgett Peterson <padgett@tcslr.dnet.mmc.com>

Sat, 7 Jan 95 10:21:39 -0500

Unfortunately, the disclaimer at the end of Mr. Blaze's posting makes it impossible to extract the single paragraph I wished to comment on (another RISK in itself) so I will have to wing it. [Nice observance! PGN]

The RISK a government takes in enacting such laws is that people will try to act within them. To me one of the most powerful strengths of the USA is that a large portion of the citizenry feel free to point out just how absurd some laws are by insisting on their enforcement. If everyone did, whether out of

"creative anarchy" as here or pure fear of the consequences as exists in unnamed countries (fortunately regimes based on fear never seem to last very long since stagnation is inevitable).

IMHO, unenforceable laws are bad laws primarily because they degrade respect for all laws (look at speed limits for one example). Of course many laws are broken simply because they are unknown (does everyone have a leash for their alligator ?), obscure, and/or unenforced.

Further, where enforced, people quickly learn the right words to say (when I built a home for my hobby, on my first application I said "garage" and was told that for the size it needed steel doors and a commercial fire sprinkler system. It immediately became a "garage/workshop" and so came under less restrictive residential requirements).

The bottom line is that it takes people like Matt to take the time and trouble to point out the absurdities in order to get them "fixed" - after all in the best of worlds, that is what bureaucrats are for. IMHO doing something like this is worth it provided you never have to do it again.

Padgett

ps wonder what would be the RISK of making up an official appearing document for example from the "Department of Stepanographic Affairs" and using for the exportation of encoded ducks ?

---

### **Israeli army, cellular phones, pizza**

*Michael Dahan <msdahan@pluto.msc.huji.ac.il>  
Sun, 8 Jan 1995 12:15:26 +0200*

The flap here in Israel regarding cellular phones began when newly inducted soldiers brought the phones to basic training at boot camp. The concern had less to do with security risks but rather socio-economic concern: Soldiers who could afford cellular phones (which are ridiculously expensive in Israel and serve as status symbols) and those who couldn't. One of the most important features of the Israeli Army is that it is an army of the people: many and women from the age of 18 serve two (for women) and three (for men) years, and then do reserve duty once a month till the age of 55. The use of cellular phones by new recruits caused concern for the melting pot characteristic of the army and serves to introduce additional stress between those who can afford the phones and those who can't. The pizza on the other hand is another story....

Michael Dahan Dept. of Political Science Hebrew University Jerusalem, ISRAEL  
msdahan@pluto.msc.huji.ac.il

---

### **Re: Soldiers and Cellular telephones**

*David Wadsworth <dwadsw@etna.demon.co.uk>*

*Sun, 08 Jan 1995 10:53:03 GMT*

The problem with cellular telephones in Military/Emergency service use is that they work too well! In an emergency people get rather discouraged when their incredibly expensive radio system is overloaded, and unusable, but a simple cell phone works perfectly well. If you are in an emergency situation, and you are reduced to whistling into a microphone in morse code to try to get your message through an overloaded radio channel, then, if you have a cell phone, you will use it regardless of security.

Of course, in some cases the cell phone may be more secure than other means of communication!

David Wadsworth

---

### **Patent problems in replacing GIF**

*David Winfrey <dwinfrey@cpcug.org>*

*Sat, 7 Jan 1995 06:28:02 -0500 (EST)*

[RISKS-16.72](#) contains some discussion of the GIF/LZW patent problem, including a suggestion that some other standard (such as JPEG) be defined.

Unfortunately, JPEG contains patented (by IBM) compression code. Many compression algorithms, including the simplest form of run-length encoding, are patented.

See [rtfm.mit.edu:/pub/usenet/news.answers/compression-faq/part\[1-3\]](http://rtfm.mit.edu:/pub/usenet/news.answers/compression-faq/part[1-3]) for details, patent numbers, and excerpts from the mind-numbing legalese in which patents describe inventions.

The same FAQ also points out that LZW is patented by both Unisys and IBM, the patent office having failed to notice that both patent applications described the same algorithm.

David Winfrey [dwinfrey@cpcug.org](mailto:dwinfrey@cpcug.org)  
Capital PC User Group, Rockville MD

---

### **more on GIF (decompression)**

*Simson L. Garfinkel <simsong@pleasant.cambridge.ma.us>*

*Sat, 7 Jan 1995 20:02:16 -0800*

It is my understanding, based on a conversation with Richard Stallman two years ago, that the Unisys patent on LZW only covers compression, and not decompression. This is the reason that the GNU gunzip compression program can decompress "compressed" archives without violating any (known) patents.

This, of course, means that there is a simple and reasonably transparent solution to the current GIF crisis:

1. Adopt a new compression standard for GIF.
2. All newly created GIF files will be in this standard.
3. Continue to support decompression of GIF files compressed with LZW, because that does not violate the Unisys patent.

For a compression algorithm, we could use the simpler compression algorithm used by programs like PGP (I think that it is straight LZ, rather than LZW), or we could use the algorithm that gzip uses (which is better at compression than LZW, but executes more slowly).

Simson

---

### **Re: CompuServe-Unisys GIF Tax Protest**

*"john (j.g.) mainwaring" <crm312a@bnr.ca>  
Fri, 6 Jan 1995 18:31:00 -0500*

In [RISKS 16.72](#), Peter Bishop refers to the recently announced UNISYS/COMPUSERVE patent restriction and recommends switching over to use the Free Software Foundation's GZIP. This may not solve the problem. In the same issue of RISKS, Tim Oren of CompuServe pointed out that the restriction had been imposed entirely by Unisys, and that CompuServe wished as much as the rest of us that it would go away. I am not sure what compression algorithm ZIP & GZIP use, but I was under the impression that they use LZW, just like GIF. If so, I should imagine unisys will be leaning on the FSF and PKWare and anyone else they can find who uses LZW in their software.

It would be very interesting to see the opinion of someone with a knowledge of patent law on how a patent can be obtained on something that has been as widely published, apparently without notice of restriction, as LZW has been.

John Mainwaring crm312a@bnr.ca The usual disclaimers may apply

---

### **Error in CompuServe/Tim Oren's msg**

*Garrett P Nievin <gnievin@osf1.gmu.edu>  
Sat, 7 Jan 1995 18:35:06 -0500 (EST)*

I believe Tim Oren of CompuServe has made an error in chronology.

When the GIF standard was initially developed in 1987, Unisys was not "pursuing" a patent for the LZW algorithm; the patent had already been awarded, in 1985.

Garrett P. Nievin

---

## Re: Date/Time

Steve Sapovits <steves@telebase.com>

Thu, 5 Jan 1995 18:33:08 -0500 (EST)

This discussion brings several time-related bugs from my past to mind.

One of the more mundane was the October bug. We introduced some new date/time functions into our code sometime in the spring or summer. They all seemed to work fine. When October came around, things started behaving strangely (obvious "core walks" for you UNIX folk). The problem? Months were zero-based (0-11) but were displayed one-based (1-12). The code used the zero-based number to calculate the number of digits required for display. Simple coding error. The bigger problem was a lack of unit testers to test all ranges of dates instead of relying on the normal passage of time. When the problems first showed up it had been months since we had worked on the date/time code so it was not immediately suspected.

A more interesting bug which shows just how likely it is for time to not be accurate if it's not fetched atomically showed up when we had our product running on a 286-based UNIX (XENIX I think). I forget the exact details, but we had your basic C language MIN() type macro, which looked something like this:

```
#define MIN(x, y) (((x) < (y)) ? (x) : (y))
```

Simple enough. Until someone did something like this:

```
least_time = MIN(time((long *) NULL), old_time);
```

[ the time() function in UNIX returns the number of seconds since the epoch ].

This looks innocent enough, but it expands so that there are two time() calls -- one during the comparison and one to get the value the expression evaluates to. Our expectation was that either the original x or y would be the result of using the macro. Instead, some cases evaluated to x plus some number of seconds -- the number of seconds we gotted swapped out on that pathetic system between the two calls.

Steve Sapovits, Telebase Systems (610) 293-4724 steves@telebase.com

---

## Re: Dates in a 4GL (Moore, [Risks-16.71](#))

Mark Brader <msb@sq.com>

Thu, 5 Jan 1995 19:45:38 -0500

[I could not possibly use all of the responses received on this subject. I chose just a few, ignoring a few very fine points that would be useful to someone involved in a particular system. Mark Brader wrote a nice note on leap seconds, which, however, seemed gratuitous here. Pete Carah <pete@wakko.ent-img.com> noted we are now up to 18 accumulated leap seconds. Martin Ewing

<martin.ewing@yale.edu> warned about nonmonotonic clocks. Several folks had "fixes" for nonatomic clock reads. Paul Robinson's note generated a welter of messages. I recommend we wait until NEXT January, and try again. PGN]

Actually, it's even worse than Dave is saying. See, UTC was adopted in 1961, but the leap second system was not adopted until 1972. For at least some of the years in between, when adjustments in UTC were needed, the *rate of time* was changed. That is, instead of extra seconds, there would be *longer* seconds (and proportionately longer milliseconds). So the true conversion of a time stored in milliseconds since some time in 1582 is complicated indeed!

Recommended reading: "Greenwich time and the discovery of the longitude" by Derek Howse (1980, Oxford University Press, ISBN 0-19-215948-8).

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

---

## Re: Dates and times not matching in COBOL

*Erann Gat <gat@aig.jpl.nasa.gov>*

*Fri, 6 Jan 95 16:47:59 PST*

Actually, there are TWO bugs. The T\$ in line 160 [which should be 150] should be T1\$. The program specification was that it should make N calls to DATE\$ and 2N calls to DATE\$, so these really are bugs, not just alternative interpretations.

E.



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 16: Issue 75**

**Thurs 19 January 1995**

## Contents

- [Airline schedules in local time](#)  
[Matthew Kwan](#)
- [Car-radio security code nuisance](#)  
[Daniel P. B. Smith](#)
- [Bugs in Digital RAID Storage Subsystems](#)  
[Andy Ram](#)
- [Maryland Emission testing](#)  
[Paul Peters](#)
- [Computers in nuclear plant](#)  
[WB Whaley via Jonathan\\_Welch](#)
- [Anik E2 redux](#)  
[Luis Fernandes](#)
- [Shaky testing](#)  
[Mark Stalzer](#)
- [Re: Midnight Batch Run Bites](#)  
[Paul Robinson](#)
- [New Risk from the WWW](#)  
[John MacInty](#)
- [RISKS on the World Wide Web](#)  
[Lindsay F. Marshall](#)
- [Criminal hacker arrested in Winnipeg](#)  
[Mich Kabay](#)
- [Phone Phreaking Explored](#)  
[Steve O'Keefe](#)
- [International Cryptography Institute 1995](#)  
[Dorothy Denning](#)
- [12th Annual ISSA Conference & Exposition](#)  
[Jack Holleran](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Airline schedules in local time

*Matthew Kwan <mkwan@cs.mu.oz.au>  
Mon, 9 Jan 1995 11:53:35 +1100*

Anyone who has received an itinerary from a travel agent knows that airlines tend to publish their schedules with departure and arrival times expressed in local time.

While this is little more than an inconvenience for travelers who want to figure out flight durations, it can become a more serious problem when the airlines use local times in their internal computer systems (and inflict these files on third-party software developers!).

A case in point involves an airline who had a flight out of Athens at 0205 on 25sep94 (local time). Unfortunately, according to the airline's timezone information, Athens switches from daylight savings (UTC+0300) to standard time (UTC+0200) at exactly 0300 on 25sep94. In other words, 25sep94 0205 occurs twice, so when converting this time to UTC you have a 50/50 chance of being out by an hour.

In our particular case the only risk was that the system would report the cabin crew working hours as being one hour less than reality, but the results could potentially be more serious, especially if the computers at the airport get confused.

mkwan

---

### **Car-radio security-code nuisance**

*"Daniel P. B. Smith" <dpbsmith@world.std.com>  
Sun, 8 Jan 1995 20:04:39 +0001 (EST)*

I bought a used 1994 Geo Prizm with a factory-installed Delco radio that claims to have a "theft deterrent." The owner's manual says "the theft deterrent feature ... can be used or ignored. If ignored, the system plays normally. If it is used, your system won't be usable if it's ever stolen. The instructions below tell you how to enter a security code into the system. If your vehicle loses battery power for any reason, you must enter the security code again before the system will turn on."

I was tempted to ignore it, but decided, what the heck, I suppose I'd better use it. Well, of course, I discovered that the previous owner had entered a security code, and had not removed it when the car was sold. So if anyone were to leave the car headlights on overnight and drain the battery (why, no, \_I\_ certainly couldn't be so stupid as to do that :-)) the radio would become unusable.

The used-car dealer had no idea what to do, but suggested I call a Chevy dealer. The Chevy dealer hadn't ever heard of the situation and wasn't aware the radio had such a feature, and suggested I call a Chevy 800 number. The Chevy 800 number know nothing, and suggested I call a Delco 800 number. At every stage, of course, I had to explain the security feature, which apparently was new to the 1994 model. And at every stage I had to endure further misunderstandings, because at each stage, they were initially unable to understand why there was any problem given that the radio worked.

Delco said, "sure, no problem, we'll fax the dealer the directions, a lot of them don't know about it." I asked how long the fix took and was told, "it depends how good they are at following directions. If the radio isn't inoperative yet it's easy, otherwise it gets pretty involved."

I took the car to the dealer. I had a chance to glance at the faxed instructions but not read them carefully. I have the impression that if the radio isn't inoperative, removing the security code just requires entering a complicated, but fixed series of digits and button-pushes. (A savvy radio thief would have to remember to do this BEFORE stealing the radio). After it has had power removed and decided to become inoperative, there is a much longer procedure, involving calling Delco to get a dealer code, leaving the radio unpowered for a long time, etc.

Later that morning the dealer called me and said, "We think your ignition lock security system must be interfering with your radio because we tried your radio and everything works fine, including the cassette player." So I explained the problem once again. I came by at noon as agreed to pick it up and was told it would take a little longer, "because we are waiting for Delco to call us back with a dealer code." When I picked it up, they HAD removed the old security code (and installed a new one, but they told me what it was). It had forgotten all the station settings. I suspect that they either did the complicated procedure when they only needed to do the simple one, or someone disconnected the radio as part of their troubleshooting, or someone couldn't resist disconnecting it to see what would really happen...

What's the RISK? Well, given that people do sell used cars, and that many people may not even bother to read that part of the manual--especially if the radio is working--what has been achieved overall is to take a highly reliable car radio and reduce its life expectancy to the same as that of a car battery.

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

---

## Bugs in Digital RAID Storage Subsystems

*"Andy Ram, x1783, Hong Kong" <ARAM%11305@gs.com>  
Sun, 08 Jan 1995 20:48:05 -0500 (EST)*

Does any one know anything about reported bugs in the Digital RAID Storage System ? One tends to hear so much of this bug.. nothing about it ?

---

## Maryland Emission testing

*Paul Peters <PPeters@DOCKMASTER.NCSC.MIL>  
Mon, 9 Jan 95 09:55 EST*

The following article appeared in the 8 Jan 1995 Washington Post:

## Maryland Delays New Auto Tests

A computer glitch has forced the delay of Maryland's tough new auto emissions testing program.

The state Motor Vehicle Administration announced Friday that the start-up of the program would be delayed for several weeks to fix the problems in the software used to measure emissions. The MVA had planned to start mailing notices Friday to about 25,000 drivers to get their cars and trucks tested.

"it's not going to start until we're satisfied we can give a quick and accurate test." MVA Administrator W. Marshall Rickert Jr. said.

The General Assembly passed the tougher testing program after the federal government ordered the state to reduce smog.

Comments heard on this topic include the opinion that it might be an excuse to delay this testing which includes having a state driver test your car at 55 mph on a dynamometer. The test will be more costly than the present test and is expected to result in a high failure rate.

---

## Computers in nuclear plant

*Jonathan\_Welch <JHWELCH@ecs.umass.edu>  
Mon, 09 Jan 1995 08:34:04 -0500*

I read this in comp.os.vms this morning and it made me wonder just how well this plant in Georgia is managed.

Jonathan Welch VAX Systems Manager Umass/Amherst JHWELCH@ecs.umass.edu

-----

Newsgroups: comp.os.vms  
Subject: VAX 4000 Upkeep/Maintenance  
From: wbwhaley@aol.com (WBWhaley)  
Date: 9 Jan 1995 06:33:26 -0500

At work recently we just installed a Vax 4000 with 2 model 100's as our hosts and numerous model 60's, VLC's, and a few model 90's as our basic system workstations. Approx 20 workstations total along with an assortment of LAN Bridge 150's / 200's, local segment repeaters all tied together on thick wire ethernet and fiber optic cable. Its primary use is being our plant computer for the nuclear power plant I work at, so it is in constant use. A vast majority of the extra network equipment is for redundancy being that we hate to lose any plant info/data in case of a failure. Anyway, I was curious to see what other system users performed on their systems as regular preventive maintenance and the such being that we are new to the system. Defrag HD, cleaning bridges/repeaters/servers, host cpu's, etc. Right now, we are tied to using built in VMS utilities and I would like your suggestions. I have gotten a good bit of info from the system managers manual, but wasn't sure if there were any other tricks I may have missed. VMS is totally new to me, so pardon my simple

description. <G> Any help would be appreciated.

Bill Whaley Augusta, Ga

---

## Anik E2 redux

*Luis Fernandes <elf@eccles.ee.ryerson.ca>*

*Tue, 17 Jan 1995 14:47:07 +0500*

Excerpts from the July, 4, 1994 Aviation Week and Space Technology follow:

"Telesat Canada engineers have succeeded in a five-month rescue effort by reestablishing pointing control over the Anik E2 satellite without the use of its failed momentum wheel systems, thus salvaging a \$203-million asset."

This is the first time that a rescue of a geosynchronous, 3-axis stabilized satellite without a serviceable momentum wheel on board has been successful (other satellites with this type of problem have been abandoned, in the past). No one is certain why the integrated circuits in the control systems failed, but it is believed that electrostatic discharge during an intense solar storm is to blame.

"...during the five months that the satellite was out of action, Telesat Canada lost about \$15 million. Engineers devised an alternative pointing system...and installed two entirely separate ground-based systems for redundancy. A software program developed by Telesat Canada engineers...keeps track of the satellite in three axes and calculates adjustments in pointing."

Anik E2 service life will be shortened by one year because of the extra fuel used in re-positioning the satellite during its life.

---

## Shaky testing

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

*Thu, 12 Jan 1995 11:43:49 +0800*

In the Jan. 12 LA Times, Pacific Bell, the US Geological Service, and CalTech, announced an 18 month trial of a new system for measuring the effects of earthquakes. The system uses sensors placed around Southern California that relay data to CalTech's computers during a 5+ magnitude earthquake. The data is reduced to give emergency crews the location of large ground accelerations so that they can tailor their responses. (Large ground motion can occur far away from the epicenter, e.g. Filmore is about 20 miles from Northridge yet it was severely damaged in the 6.8 quake.)

One interesting issue is testing the system: a 5+ quake is required. A Pacific Bell official said they would extend the test period if an appropriate quake doesn't occur. Talk about waiting a long time

for test runs...

Mark Stalzer, mas@acm.org

---

### Midnight Batch Run Bites (Kowalczyk, [RISKS-16.71](#))

<ROBINSON\_PAUL@tandem.com>

9 Jan 95 10:16:00 -0800

Not so many years ago, I needed a certified check from my large Boston-area bank. I arrived at my branch office at 9:05am, gave a teller appropriate paperwork to transfer funds from savings to checking, and then had the necessary incantations performed to transform my normal everyday check into a certified check. Among other things, this caused the check amount to be immediately debited from my checking account; but since I'd just requested a transfer of the necessary amount into checking, the teller did not complain about the apparent overdraft. So far so good.

Within a week I received an overdraft penalty notice, because my transaction at the teller window to do the transfer was not processed until after midnight thus leaving my checking account short that day. I had to show my transfer receipt, with its 9:05am timestamp, to an actual human before the bank would clear the penalty.

The incident taught me to avoid teller transactions whenever possible, though, because the nice human who cleared the penalty told me that all the ATM transactions were cleared first, before teller transactions, each evening. A RISK of avoiding new technology??

Paul T. Robinson

robinson\_paul@tandem.com (NOT the Paul Robinson of paul@tdr.com)

---

### New Risk from the WWW

<jmacinty@mv.us.adobe.com>

Tue, 17 Jan 95 07:55:55 PST

At the end of January middle of February this year Microsoft will be introducing Internet Assistant. A HTML creator and WEB browser for Word for Windows 6.0.

The WEB browser will read Word 6.0 documents directly and therefore the risk.

Word documents can come with programming that will activate on opening. While this has always been a problem document distribution hasn't generally been widespread until soon from now.

Three types of things I can see happening.

1. Viral type documents. These are documents that will change your normal.dot and copy itself from document to document.

2. Trojan Horse type 1 documents. These are documents that do something on opening, like delete files etc....And possible even harmless things.

3. Trojan Horse type 2 documents. Really scary documents that communicate BACK to the web-server without your knowing it and sending additional information gleaned from your machine and or network. There are some truly scary things that could be done with a creative VBA/CGI programmer.

It is unfortunate that these risks exist, because otherwise the ability to have "programmable" documents on the web is a really cool concept. But nonetheless risks like these have to be dealt with

John

---

## RISKS on the World Wide Web

*"Lindsay F. Marshall" <Lindsay.Marshall@newcastle.ac.uk>  
Tue, 17 Jan 1995 15:29:07 GMT*

You can now read the complete RISKS archives on the World Wide Web (apart from the very earliest issues which will appear as soon as I have hand converted them...) Individual issues have a file name of the form volume.issue.html where issues is always a two digit number:

<http://catless.ncl.ac.uk/Risks/16.01.html>

is the first issue of volume 16. The URL <http://catless.ncl.ac.uk/Risks> gives you an introduction page and leads you to the indices for previous issues. The latest issue can always be found via the URL

<http://catless.ncl.ac.uk/Risks/latest>

The translation from RISKS to html is automatic so there may be errors. Please report any that you find to me so that I can fix them. Currently the text of messages is left as pre-formatted text. I have hand converted issues 16.74 to use the html formatting commands. Any feed back on what people would like to see and any improvements that I could make will be most welcome.

Lindsay

MAIL : Lindsay.Marshall@newcastle.ac.uk  
URL : <http://catless.ncl.ac.uk/Lindsay.html>  
POST : Dept. of Comp. Science, U of Newcastle, Newcastle upon Tyne, UK NE1 7RU  
VOICE: +44-191-222-8267 (FAX: -8232)

---

## Criminal hacker arrested in Winnipeg

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>*

09 Jan 95 13:35:38 EST

According to a Canadian Press reported printed in The Globe and Mail (955.01.07, p. A4),

Police crack illegal access to Internet

WINNIPEG -- Police have made what they believe is one of Canada's first arrests for breaking into the Internet....

a 31-year-old man was arrested...after an eight-month police investigation into illegal access to the Internet computing system at the University of Manitoba....

...[T]he man will be charged with two counts of unauthorized use of a computer service....

The article states that the Crackerjack program "was used to decrypt the access codes of legitimate users" and that the accused is alleged to have stored stolen software and porn online.

M.E.Kabay,Ph.D.

DirEd/Natl Computer Security Assn (Carlisle, PA)

Mgmt Consultant/LGS Group Inc. (Montreal, QC)

---

## Phone Phreaking Explored

Steve O'Keefe <okeefe@olympus.net>

18 Jan 1995 17:37:20 GMT

HarperCollins has just released *MASTERS OF DECEPTION: The Gang That Ruled Cyberspace*, a new book by New York Newsday journalists Michelle Slatalla and Joshua Quittner. You might recall the book from a cover story in the December issue of *WIRED*. Slatalla and Quittner unravel the story of gang warfare between the Legion of Doom (LOD) and the Masters of Deception (MOD), a turf battle fought through the phone system that led to one of the most high-profile hacker prosecutions ever.

Slatalla and Quittner followed the Masters of Deception story for five years at Newsday. When the *WIRED* excerpt appeared, their phone service was hacked and their e-mail attacked by a group calling themselves the Internet Liberation Front, or ILF. A police investigation is still in progress.

The authors begin an 8-city tour in New York today. They are planning to kick off a "cybertour" in February. The book is available for purchase on Delphi (Online Bookstore) and CompuServe (Go HAR), or at your local bookstore. The *WIRED* excerpt is on HotWIRED at the following URL:

<http://www.hotwired.com/Lib/Wired/2.12/features/hacker.html>

For more information about the book -- including a tour schedule -- please send e-mail requesting a "digital flyer" to <okeefe@olympus.net>

STEVE O'KEEFE  
Electronic News & Reviews

---

## INTERNATIONAL CRYPTOGRAPHY INSTITUTE 1995

*Dorothy Denning <denning@cs.cosc.georgetown.edu>*  
*Fri, 13 Jan 95 11:25:27 EST*

Call for Participation (Deadline: March 15, 1995)

### INTERNATIONAL CRYPTOGRAPHY INSTITUTE 1995: GLOBAL CHALLENGES

September 21-22, 1995  
Washington, DC

Presented by  
The National Intellectual Property Law Institute

The International Cryptography Institute will focus on the cryptography challenges associated with meeting the information protection needs of users and the law enforcement and national security needs of nations.

The Institute will address such topics as:

- national encryption policies and regulations
- meeting user needs for information security and data recovery
- meeting law enforcement and national security needs
- national and global encryption markets and product availability
- international approaches and standards
- creating an international cryptography infrastructure
- the use of encryption technologies in different countries
- cryptography in the financial industry and other industries
- legal and policy issues of digital signatures and digital cash
- new developments in encryption policies and technologies

Persons interested in speaking at the conference are invited to submit a proposal to the Institute Chair:

Prof. Dorothy E. Denning, Chair ICI '95  
Georgetown University  
Computer Science Department  
225 Reiss Building  
Washington DC 20057-0997  
ph: 202-687-5703, fax: 202-687-6067  
e-mail: denning@cs.georgetown.edu

Proposals must be received by MARCH 15, 1995, and should include the following:

- Name, title, organization, address, phone, fax, and e-mail address
- Brief biography

- Title of presentation
- Abstract of presentation or paper
- Amount of time requested for presentation and discussion

Notification of acceptance will be made by April 15, 1995. Papers and materials for the proceedings will be due on August 15, 1995.

Inquiries about registration or the proceedings should be addressed to:

The National Intellectual Property Law Institute  
P.O. Box 27913, Washington, DC 20038-7913  
ph: 800-301-MIND or 202-962-9494  
, fax: 800-304-MIND or 202-962-9495

---

## 12th Annual ISSA Conference & Exposition

*Jack Holleran <Holleran@DOCKMASTER.NCSC.MIL>  
Tue, 17 Jan 95 09:46 EST*

Information Systems Security Association (ISSA) is pleased to announce  
LEARNING From EACH OTHER,  
the 12th Annual Conference & Exposition  
to be held  
April 2-5 1995 at Sheraton Hotel and Towers  
Toronto, Ontario, Canada

The cost is \$795 (ISSA Member), \$895 (nonmember); Full Day electives \$295.  
Canadians may pay in Canadian Dollars (same rates!)  
Brochure and registration form are available from:  
ISSA Headquarters, 4350 DiPaolo Center, Suite C, Glenview, IL, 60025  
Phone: (708) 699-6441; fax (708) 699-6369;  
or by sending E-Mail to: ISSA @ MCS.COM

The event begins with Pre-Conference Specialty Seminars on Saturday and Sunday

A Welcome Reception and Vendor Exhibition opening will be held Sunday evening  
- an excellent opportunity for networking! Each Day then begins with  
Registration at 7:30 and continental breakfast and Vendor Exhibition at 8:00.

April 1 - Saturday (Pre-conference Activities)  
Four elective Full Day Seminars to choose among

April 2 - Sunday  
The First CISSP Examination sponsored by (ISC)2  
Two elective Half Day Seminars to choose  
7pm Welcome Reception and Vendor Exhibition

April 3 - Monday's Highlights:  
Welcome and General Session will include "How to Handle Internal Investigation  
and Establish Successful Compliance Programs" by Terry F. Lenzner, a former  
member of the Board of Overseers of Harvard University with a broad range of  
experiences in public and private legal investigations.

AM Track Choices: 10:30-noon

- A1: Gale Warshawsky of LLNL will explore the merits and processes of Making Computer Security Information Available Electronically
- B1: Charles Blauner of Bellcore will introduce the security issues involved in the use of Distributed Systems.
- C1: Francis Labayen and Kimberly Clair of Andersen Consulting will discuss LAN Security issues by component, and their corresponding solutions.
- D1: Vendor panel: Viruses: an opportunity to see a virus contained and neutralized, as well as learn from leaders in the field how to avoid the beasties!
- E1: Lessons Learned: Richard Heffernan and William Haywood increase the participant's awareness of threats to intellectual property from industrial espionage.

Lunch in the Exhibit Hall

After Lunch Track Choices 1:30-3:00 pm

- A2: Rebecca Duncan of DataPro gives a blueprint for effective network security strategy.
- B2: Charles Blauner of Bellcore leads a discussion of OSF Distributed Computing Environment (DCE) and its security capabilities.
- C2: Robert Kane of Intrusion Detections describe Best Practices for Securing Novell Netware LANs.
- D2: Vendor Panel: PC Security Solutions, and the extent of their effectiveness.
- E2: Lessons Learned: Jamie Trainer examines a real world example of securing a multinational 1400 heterogeneous node network of workstations and PCs.

Late PM Track Choices: 3:30-5:00 pm

- A3: Peter Davis' Manager's Guide to Internet Security
  - B3: Tsvi Gal, Bank of America; discusses protecting "the network is the computer."
  - C3: Ed Blackwell presents "Primer for PBX and Voice Mail Fraud"
  - D3: Vendor Panel: Disaster Recovery - Business Resumption
  - E3: Lessons Learned: L. Dain Gary, CMU SEI, Internet Security and CERTSM
- Late-Late Birds of a Feather and Committee meetings

April 4 - Tuesday Highlights:

Plenary: Crossroads, by Steven J. Green, University of Houston; application and development of computer and communications security responsibility with in the work setting.

AM Track choices: 10:30-noon

- A4: Teresa Donatelli and Ann McHoes present a detailed discussion of Developing a Security Awareness Program
- B4: Will Ozier moderates a panel discussion of the activities of the ISSA GSSP committee in establishing Generally Accepted System Security Principles.
- C4: John Clark, Andersen Consulting discusses risks introduced by Frame Relay technology.
- D4: Vendor Panel; Pros and Cons of Encryption; determining your need for it.
- E4: Sadie Pitcher Department of Commerce Disaster Plans.

Lunch in the Exhibit Hall

After Lunch Track Choices: 1:30-3:00 pm

A5: Charlotte Greig, Wells Fargo Bank; How to get (management's) Attention for Information Security Awareness Part I.

B5: Allan Cobb, York University; The Architecture of Audit Facility for a Distributed Application: using OSF DCE in university student application processing.

C5: Douglas Conorich, RAXCO, Strengths and weaknesses of TCP/IP Network Security.

D5: Vendor Panel: What a network manager should consider in Distributed Informations Systems Security Management.

E5: James P. Litchko; Internet Threats and Countermeasures.

Late PM Track Choices: 3:30-5:00 pm

A6: How to Get Attention for Information Security Awareness - Part II

B6: Gary Baker, Ernst & Young; "Distributed Computing and Client Server - An Auditor's Perspective"

C6: Ed Blackwell, "Value Added Networks Security Pitfalls" Using the security features provided by VANs.

D6: Vendor Panel: Discuss the security ramifications of network components (routers, bridges, etc.)

E6: Fred Sanborn, Booz, Allen and Hamilton; Securing the Enterprisewide Network.

Late-Late Birds of a Feather and Committee meetings 5:00-6:30 pm

Special ISSA Social Event 7-9 pm

April 5 - Wednesday Highlights:

Annual Meeting of The Information Systems Security Association

AM Track choices: 10:30-noon

A7: Alex Woda, "How to Secure, Audit and Control EDI" - a practical approach. An EDI audit program will available for participants

B7: Colin Rous, Cerberus, "Distributed Computing and Client/Server Security: What it means for the Security Administrator."

C7: Robert Clyde, RAXCO, "Multi-Platform Enterprise Security Management"

C8: Panel: Security Issues for Electronic Commerce", Loreto Remorca and David Lyons, moderators.

D7: Vendor Panel: Awareness and Training; ideas and solutions you can incorporate into your program.

E7: Bart Burrton, Auditor General Canada, "A Top Down Computer Security Assessment for Senior Management."

After Lunch Committee Meetings 1 - 3 pm

April 6 - Thursday: (Elective) CISSP Preparation Course. This session will assist in preparation for the CISSP exam and explain test contents as well as the tools and methods for preparation.

Make your room Reservations with the Sheraton, and tell them you will be attending the 12th Annual ISSA Conference and the rate will be \$127 (plus 15%)

For more information call ISSA headquarters (708) 699-6441.



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 16: Issue 76**

**Tuesday 24 January 1995**

## Contents

- [CERT Advisory CA-95:01.IP.spoofig.attacks.and.hijacked.terminal.connections](#)
- [More on the new CERT advisory](#)  
[Steve Bellovin](#)
- [Bouncemail](#)  
[Phil Agre](#)
- [Another post office stamp machine story \(they \\*almost\\* got it right!\)](#)  
[Jonathan I. Kamens](#)

---

## CERT Advisory CA-95:01.IP.spoofig.attacks.and.hijacked.terminal.connections

CERT Advisory <[cert-advisory@cert.org](mailto:cert-advisory@cert.org)>  
Mon, 23 Jan 1995 13:49:47 -0500

CA-95:01                    CERT Advisory  
                          January 23, 1995  
                          IP Spoofing Attacks and Hijacked Terminal Connections

The CERT Coordination Center has received reports of attacks in which intruders create packets with spoofed source IP addresses. These attacks exploit applications that use authentication based on IP addresses. This exploitation leads to user and possibly root access on the targeted system. Note that this attack does not involve source routing. Recommended solutions are described in Section III below.

In the current attack pattern, intruders may dynamically modify the kernel of a Sun 4.1.X system once root access is attained. In this attack, which is separate from the IP spoofing attack, intruders use a tool to take control of any open terminal or login session from users on the system. Note that although the tool is currently being used primarily on SunOS 4.1.x systems, the system features that make this attack possible are not unique to SunOS.

As we receive additional information relating to this advisory, we will place it, along with any clarifications, in a CA-95:01.README file. CERT advisories

and their associated README files are available by anonymous FTP from info.cert.org. We encourage you to check the README files regularly for updates on advisories that relate to your site.

## I. Description

This description summarizes both the IP spoofing technique that can lead to root access on a system and the tool that intruders are using to take over open terminal and login connections after they get root access. We are currently seeing attacks in which intruders combine IP spoofing with use of the tool. However, these are two separate actions. Intruders can use IP spoofing to gain root access for any purpose; similarly, they can hijack terminal connections regardless of their method of gaining root access.

### IP spoofing

To gain access, intruders create packets with spoofed source IP addresses. This exploits applications that use authentication based on IP addresses and leads to unauthorized user and possibly root access on the targeted system. It is possible to route packets through filtering-router firewalls if they are not configured to filter incoming packets whose source address is in the local domain. It is important to note that the described attack is possible even if no reply packets can reach the attacker.

Examples of configurations that are potentially vulnerable include

- routers to external networks that support multiple internal interfaces
- routers with two interfaces that support subnetting on the internal network
- proxy firewalls where the proxy applications use the source IP address for authentication

The IP spoofing attacks we are currently seeing are similar to those described in two papers: 1) "Security Problems in the TCP/IP Protocol Suite" by Steve Bellovin, published in *Computer Communication Review*, vol. 19, no. 2 (April 1989) pages 32-48; 2) "A Weakness in the 4.2BSD Unix TCP/IP Software" by Robert T. Morris. Both papers are available by anonymous FTP from

[ftp.research.att.com:/dist/internet\\_security](ftp.research.att.com:/dist/internet_security)

Bellovin paper: [ipext.ps.Z](#)

Morris paper: [117.ps.Z](#)

Services that are vulnerable to the IP spoofing attack include

SunRPC & NFS

BSD UNIX "r" commands

anything wrapped by the tcp daemon wrappers - site dependent; check your configuration

X windows

other applications that use source IP addresses for authentication

### Hijacking tool

Once the intruders have root access on a system, they can use a tool to dynamically modify the UNIX kernel. This modification allows them to hijack existing terminal and login connections from any user on the system.

In taking over the existing connections, intruders can bypass one-time passwords and other strong authentication schemes by tapping the connection after the authentication is complete. For example, a legitimate user connects to a remote site through a login or terminal session; the intruder hijacks the connection after the user has completed the authentication to the remote location; the remote site is now compromised. (See Section I for examples of vulnerable configurations.)

Currently, the tool is used primarily on SunOS 4.1.x systems. However, the system features that make this attack possible are not unique to SunOS.

## II. Impact

Current intruder activity in spoofing source IP addresses can lead to unauthorized remote root access to systems behind a filtering-router firewall.

After gaining root access and taking over existing terminal and login connections, intruders can gain access to remote hosts.

## III. Solutions

### A. Detection

#### IP spoofing

If you monitor packets using network-monitoring software such as netlog, look for a packet on your external interface that has both its source and destination IP addresses in your local domain.

If you find one, you are currently under attack. Netlog is available by anonymous FTP from

```
net.tamu.edu:/pub/security/TAMU/netlog-1.2.tar.gz  
MD5 checksum: 1dd62e7e96192456e8c75047c38e994b
```

Another way to detect IP spoofing is to compare the process accounting logs between systems on your internal network. If the IP spoofing attack has succeeded on one of your systems, you may get a log entry on the victim machine showing a remote access; on the apparent source machine, there will be no corresponding entry for initiating that remote access.

#### Hijacking tool

When the intruder attaches to an existing terminal or login connection, users may detect unusual activity, such as commands appearing on their terminal that they did not type or a blank window

that will no longer respond to their commands. Encourage your users to inform you of any such activity. In addition, pay particular attention to connections that have been idle for a long time.

Once the attack is completed, it is difficult to detect. However, the intruders may leave remnants of their tools. For example, you may find a kernel streams module designed to tap into existing TCP connections.

## B. Prevention

### IP spoofing

The best method of preventing the IP spoofing problem is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network. In addition, you should filter outgoing packets that have a source address different from your internal network in order to prevent a source IP spoofing attack originating from your site.

The following vendors have reported support for this feature:

Bay Networks/Wellfleet routers, version 5 and later

Cabletron - LAN Secure

Cisco - RIS software all releases of version 9.21 and later

Livingston - all versions

If you need more information about your router or about firewalls, please contact your vendor directly.

If your vendor's router does not support filtering on the inbound side of the interface or if there will be a delay in incorporating the feature into your system, you may filter the spoofed IP packets by using a second router between your external interface and your outside connection. Configure this router to block, on the outgoing interface connected to your original router, all packets that have a source address in your internal network. For this purpose, you can use a filtering router or a UNIX system with two interfaces that supports packet filtering.

NOTE: Disabling source routing at the router does not protect you from this attack, but it is still good security practice to do so.

### Hijacking tool

There is no specific way to prevent use of the tool other than preventing intruders from gaining root access in the first place.

If you have experienced a root compromise, see Section C for general instructions on how to recover.

## C. Recovery from a UNIX root compromise

1. Disconnect from the network or operate the system in single-user mode during the recovery. This will keep users and intruders from accessing the system.

2. Verify system binaries and configuration files against the vendor's media (do not rely on timestamp information to provide an indication of modification). Do not trust any verification tool such as `cmp(1)` located on the compromised system as it, too, may have been modified by the intruder. In addition, do not trust the results of the standard UNIX `sum(1)` program as we have seen intruders modify system files in such a way that the checksums remain the same. Replace any modified files from the vendor's media, not from backups.

-- or --

Reload your system from the vendor's media.

3. Search the system for new or modified `setuid` root files.

```
find / -user root -perm -4000 -print
```

If you are using NFS or AFS file systems, use `ncheck` to search the local file systems.

```
ncheck -s /dev/sd0a
```

4. Change the password on all accounts.
5. Don't trust your backups for reloading any file used by `root`. You do not want to re-introduce files altered by an intruder.

The CERT Coordination Center thanks Eric Allman, Steve Bellovin, Keith Bostic, Bill Cheswick, Mike Karels, and Tsutomu Shimomura for contributing to our understanding of these problems and their solutions.

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in Forum of Incident Response and Security Teams (FIRST).

If you wish to send sensitive incident or vulnerability information to CERT staff by electronic mail, we strongly advise that the e-mail be encrypted. The CERT Coordination Center can support a shared DES key, PGP (public key available via anonymous FTP on [info.cert.org](http://info.cert.org)), or PEM (contact CERT staff for details).

Internet E-mail: [cert@cert.org](mailto:cert@cert.org)

Telephone: +1 412-268-7090 (24-hour hotline)

CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4), and are on call for emergencies during other hours.

Fax: +1 412-268-6989

CERT Coordination Center  
Software Engineering Institute

Carnegie Mellon University  
Pittsburgh, PA 15213-3890  
USA

Past advisories, CERT bulletins, information about FIRST representatives, and other information related to computer security are available for anonymous FTP from [info.cert.org](http://info.cert.org).

CERT is a service mark of Carnegie Mellon University.

---

## More on the new CERT advisory

Steve Bellovin <[smb@research.att.com](mailto:smb@research.att.com)>

Tue, 24 Jan 1995 07:09:12 -0500

[The CERT advisory is the previous item in this issue.  
Also, see John Markoff's front-page story in yesterday's editions of The New York Times, 23 Jan 1995. PGN]

There's a great deal of confusion about what kind of attack the recent CERT advisory is referring to. Let me try to clear things up.

The specific attack is a sequence number guessing attack, originally described by R.T. Morris in Bell Labs Computer Science Technical Report #117, February 25, 1985. I generalized (and publicized) the attack in my 1989 paper "Security Problems in the TCP/IP Protocol Suite", Computer Communications Review 19:2, April 1989, pp. 32-48 (URLs below). Both his attack and my generalizations are special cases of a more general attack, IP source address spoofing, in which the attacker illegitimately uses a trusted machine's IP address in conjunction with some protocol (such as rsh) that does address-based authentication.

In order to understand the particular case of sequence number guessing, you have to look at the 3-way handshake used in the TCP open sequence. Suppose client machine A wants to talk to rsh server B. It sends the following message:

A->B: SYN, ISSa

That is, it sends a packet with the SYN ("synchronize sequence number") bit set and an initial sequence number ISSa.

B replies with

B->A: SYN, ISSb, ACK(ISSa)

In addition to sending its own initial sequence number, it acknowledges A's. Note that the actual numeric value ISSa must appear in the message.

A concludes the handshake by sending

A->B: ACK(ISSb)

The initial sequence numbers are intended to be more or less random. More precisely, RFC 793 specifies that the 32-bit counter be incremented by 1 in the low-order position about every 4 microseconds. Instead, Berkeley-derived kernels increment it by 128 every second, and 64 for each new connection. Thus, if you open a connection to a machine, you know to a very high degree of confidence what sequence number it will use for its next connection. And therein lies the attack.

The attacker X first opens a real connection to its target B -- say, to the mail port or the TCP echo port. This gives ISSb. It then impersonates A and sends

A->B: SYN, ISSx

B's response to X's original SYN (so to speak)

B->A: SYN, ISSb', ACK(ISSx)

goes to the legitimate A, about which more anon. X never sees that message but can still send

A->B: ACK(ISSb')

using the predicted value for ISSb'. If the guess is right -- and usually it will be -- B's rsh server thinks it has a legitimate connection with A, when in fact X is sending the packets. X can't see the output from this session, but it can execute commands as more or less any user -- and in that case, the game is over and X has won.

There is a minor difficulty here. If A sees B's message, it will realize that B is acknowledging something it never sent, and will send a RST packet in response to tear down the connection. There are a variety of ways to prevent this; the easiest is to wait until the real A is down (possibly as a result of enemy action, of course).

There are several possible defenses. Most obvious is to take advantage of topological knowledge: don't let packets purporting to be from a local machine arrive on an outside interface. That works very well if you only trust local machines. If trust is granted to outside machines (say, via .rhosts files) and if the attacker can identify the patterns of trust (which isn't that difficult), the topological solution won't work. In that case, you have to block all protocols that use TCP and address-based authentication. (UDP is a separate can of worms.)

Best of all, don't use address-based authentication; it's a disaster waiting to happen. The only real solution is cryptographic authentication.

Firewalls based on tcpd have a special problem: address-based authentication is their business. If you have a set of rules that grants special permission to inside addresses, and you don't use a screening router as well, you may be vulnerable. The question is this: can an attacker do damage by just sending commands and not seeing any output? If the answer is

yes, you are vulnerable.

--Steve Bellovin

For further information, see the two papers cited above:

[ftp://ftp.research.att.com/dist/internet\\_security/117.ps.Z](ftp://ftp.research.att.com/dist/internet_security/117.ps.Z)

[ftp://ftp.research.att.com/dist/internet\\_security/ipext.ps.Z](ftp://ftp.research.att.com/dist/internet_security/ipext.ps.Z)

---

## Bouncemail

*Phil Agre <pagre@weber.ucsd.edu>*

*Mon, 16 Jan 1995 19:05:36 -0800*

[Excerpted with permission from Phil's The Network Observer]

Bouncemail top ten.

In running a large mailing list for the past year or so, I have become acquainted with a depressing variety of dysfunctional mail handling software. I've gathered here my top ten least favorite phenomena in hopes that a Universal Union of Large List Maintainers might spring up to force them to get fixed:

10. Mailers that give intermittent "user unknown" messages for users who perfectly well exist, perhaps because they cannot detect transient local network problems well enough to postpone delivering mail.
9. The confusion over the Errors-To: field, which sure seems like a good idea to me but which apparently is not part of the standard. It is supported by most but not all mailers. If it didn't exist then I'd have to run my mailing list from a separate account.
8. Mailers that generate messages lacking well-formed headers, most commonly addresses like "someone@local" without proper domain information.
7. Mailers that tell me "Press F1 for help with VNM error codes" even though my function keys are unlikely to be programmed the same way as they are for users at the site that generates the bouncemail message. In general, mailers designed on the assumption that all senders and recipients of messages would use that same mailer -- particularly when the mailer in question does not think in terms of standard IP domain formats.
6. Mailers that complain that a certain message could not be delivered but do not specify who in particular the message could not be delivered to. Also, mailers that complain that a forwarded message could not be delivered without

providing any indication of what address(es) the message was forwarded from.

5. Vacation programs that respond to bulk or mailing-list mail or that do not keep track of who they've replied to, with the result that I get batches of spurious vacation messages (sometimes in German) as each holiday approaches.
4. Mailers that generate mail that cannot be replied to. Sometimes a message says "From: Fred\_Q\_Smith@foobar.com", even though the user's account is actually called "fqs". Sometimes I have no idea why I cannot reply to a message, and the mailer offers me no help in figuring it out. This is particularly annoying when the sender in question starts sending further messages to the effect of, "you should reply to my messages, you rude person!" It is even more annoying when the machine that generated the bogus message does not have a "postmaster" alias defined.
3. Mailers that take a month before giving up on the delivery of messages to a missing user, whereupon they initiate a monthlong stream of error messages, individually, for every one of the messages I've sent in the last month.
2. Mail-reading programs that automatically generate a little message to the effect of "so-and-so read your message about "routine administrative notes" on December 3rd at 08:41" -- even when the message was sent to a mailing list and not directly to the person reading it. The people whose mail readers generate these messages are usually not aware of them, and their site maintainers usually do not know how to shut them off.
1. The astoundingly baroque and uninformative error messages that I have gotten from the Novell mailer.

Of course errors happen. The basic point here is that the error messages are so incomprehensible, so incomplete, so inconsistent, and so difficult to adjust or control. The right way to do this, in my view, would be for mailers to be talking to one another and maintaining updated status tables for the process of delivering (or not delivering) each message. A reasonable amount of useful information could travel over these lines of communication, and my mailer could consequently provide me with some significantly more useful functionalities. Imagine a GUI interface with a window showing the messages that got bounced, deferred, and so forth. And imagine that I could just click on each one to say, in one nice clean operation, "okay, let's just take this person off the mailing list, send them a nice explanatory note in case they're magically back on-line, and expunge from the system all remaining traces of existing messages from me to them or error messages from these mailers about them".

## Another post office stamp machine story (they \*almost\* got it right!)

"Jonathan I. Kamens" <jik@cam.ov.com>

Thu, 19 Jan 1995 09:46:39 -0500

Some readers of RISKS will recall numerous previous articles about suboptimal behavior of the electronic postal stamp vending machines which have been appearing in United States Post Offices over the past few years. I am one of the many people who at one point or another has lost money in one of the machines. However, this message isn't about that; it's about a case I witnessed recently in which the vending machine \*almost\* got it right, but still has a few kinks that need to be worked out.

On the first business day after the recent US postal rate increase, I went to the Post Office to buy some new stamps. Of course, it was a madhouse, because everyone else had the same idea I did. However, although the line in front of the service windows was many people long, there were only one person using the vending machine, with no line behind him. I therefore decided to get in line behind him, since I had enough crisp bills (or so I thought) to buy stamps from the machine.

The man was standing in front of the machine, whose LED display claimed that he had a \$5.00 credit (presumably because of a five-dollar bill he'd inserted), trying to get the machine to take a one-dollar bill (he wanted to buy a book of twenty 32-cent stamps for \$6.40). The bill slot in the machine wasn't pulling in his bill part way and then rejecting it, as you might expect it to do if it could not verify the bill. The slot wasn't engaging at all, i.e., the man was pushing the bill into the slot over and over, and nothing was happening.

He did this five or ten times, then stopped, turned around to look at the service windows as if trying to attract someone's attention, wavered momentarily as if contemplating actually going over to the windows to ask for assistance, and then turned around and started shoving the bill at the bill slot again. He repeated this cycle three or four times, with me standing there thinking, "Look, idiot, if the slot wouldn't take the bill the first time, it isn't going take it the hundredth time either," and wondering why he didn't just buy a booklet of ten stamps and come back for more later. Finally, he got up the courage to go over to the windows and ask for help.

A few seconds after he walked away from the machine, it started beeping, with the LED display asking if he needed more time, and saying that if he didn't press the "YES" button he'd lose his money. Since I'm a nice guy, I pressed the "YES" button for him.

Meanwhile, the woman he was talking to at a service window was telling him something to the effect of, "Well, I don't know anything about the vending machine. You'll have to talk to <so-and-so>. She's in charge of it. She's in back right now. Hold on, I'll send her out. Go back to the machine and wait for her."

So, the man went back to the machine and stood there waiting. I said to

him, "Why don't you just buy a booklet of ten stamps and come back later for more?" He said, gesturing at the sign on the machine which says that change over a dollar is given in dollars, "Because then I'll lose money." I'm not sure what gave him that impression, but I explained to him that what the sign meant was that the machine issues Susan B. Anthony dollars when it has to issue change of more than a dollar.

Once he understood that, he went ahead and pushed the button sequence for the booklet of ten stamps. The machine then spit his five-dollar bill out of the bill slot and informed him on the LED display that it was currently unable to issue change of over a dollar. At this point, the woman "in charge of" the vending machine showed up and asked what the story was. The man told her what had happened, and she basically repeated everything he'd done (putting in his five-dollar bill, trying repeatedly to get the machine to take the additional one-dollar bill, giving up and trying to buy ten stamps, getting back the five-dollar bill), at which point she said, "Well, I don't know what's wrong. I guess you'll just have to get in line with everybody else."

At this point, I decided that trying to use the vending machine myself would not be a productive endeavor, so I picked up a copy of the USPS stamps-by-mail pamphlet and walked out. It was only when I'd made it out of the Post Office a few steps that I realized what astute RISKS readers have realized already -- the vending machine's behavior made perfect sense, and was in reality protecting the user from losing money, although its user interface needs some improvement. As I see it, the explanation for the machine's behavior is as follows....

Most bill readers, in vending machines, change machines, etc., can only return to the user the last bill inserted into the machine. I.e., if I insert a five-dollar bill into a reader and then a one-dollar bill, the reader can return the one-dollar bill to me if necessary, but the five-dollar bill is lost in the innards of the machine.

The stamp machine in this case was programmed to know that it couldn't give back more than a dollar in change (presumably because its supply of dollar coins was exhausted), and also to know that if it allowed the user to insert more than one bill, it might not be able to give back adequate change after the user completed his purchase. For example, if the user inserted two five-dollar bills and then purchased \$6.40 worth of stamps, the machine would have to issue \$3.60 in change, which it couldn't do. It therefore refused to accept the second bill.

So, what are the problems? I see several:

- 1) The machine should have told him on its display that it couldn't accept any more bills, after he inserted the first bill.
- 2) Instructions should have been displayed on the machine or on a placard within sight of the machine, explaining the machine's behavior when it runs out of dollar coins.
- 3) Better yet, there should be a light on the machine, with the words, "When lit, only one bill per purchase will be accepted, and money

deposited into machine must be less than one dollar above purchase price of desired item," and it should be lit at the right time.

4) The woman "in charge of" the machine should have a clue about how it works. I suspect that the USPS just wheels the machines into Post Offices, sets them down, says, "Here you go, a new vending machine!" and then periodically comes back to empty the money and restock them. Perhaps they should invest a little in training at least one person at each Post Office to know how the machines work.

5) The USA really needs a dollar coin in common circulation :-).

Jonathan Kamens | OpenVision Technologies, Inc. | [jik@cam.ov.com](mailto:jik@cam.ov.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 16: Issue 77**

**Monday 30 January 1995**

## Contents

- [UK Cabinet Secret on National ID Card Found in Surplus Store](#)  
[Li Gong](#)
- [Perils of Call Forwarding](#)  
[Stephen Thomas](#)  
[Quentin Fennessy](#)
- [Deutsche Telekom offices searched](#)  
[Mich Kabay](#)
- [My life as "uucp@aol.com"](#)  
[Uucp@aol.com](#)
- [Risks of reusing accounts](#)  
[Charlie Shub](#)
- [>From the cat file](#)  
[Andrew Koenig](#)
- [Another stamp machine story](#)  
[John Kriens](#)
- [The risks of Risks](#)  
[Fritz Knabe](#)  
[Haritini Kanthou](#)
- [ACSAC '95 Call for Papers and Participation](#)  
[Marshall D Abrams](#)
- [Info on RISKS \(comp.risks\)](#)

---

## UK Cabinet Secret on National ID Card Found in Surplus Store

*Li Gong <[gong@csl.sri.com](mailto:gong@csl.sri.com)>*  
*Wed, 25 Jan 95 10:02:56 -0800*

The Manchester Guardian Weekly (week ending 21 Jan 1995) reported that plans for the UK national ID card system was found in a government surplus store. The second-hand file cabinet was sold for about 35 pounds. It contained memos on investigation into the feasibility of smart-card technology, a detailed card design, as well as cabinet level letters exchanged on this topic. Whitehall has confirmed that the files are authentic.

Li GONG Email: gong@csl.sri.com Tel: 415-859-3232 Fax: 415-859-2844  
SRI International, Computer Science Lab, Menlo Park, California 94025, USA

---

## Perils of Call Forwarding [Plumbing the Depths]

*Stephen Thomas <stephen.thomas@tridom.com>*

*Mon, 30 Jan 1995 09:41:22 -0500*

I'm sure many eagle-eyed risks readers spotted this one, but just in case, here's an item from an AP story in Sunday's Atlanta Constitution.

Stephen A. Thomas, AT&T Tridom, email: stephen.thomas@tridom.com

>From The Atlanta Constitution, Sunday, January 29, 1995, page D7

Did he steal jobs, thanks to call forwarding?

Police say plumber grabbed rivals' calls [Abstracted starkly by PGN]

Michael Lasch, a plumber in Levittown, NY, is accused of calling Bell Atlantic to order Ultra Call-Forwarding for at least five of his company's competitors, which enabled him remotely to redirect their calls to his phone. He was charged with theft by deception, criminal attempt, unlawful use of a computer, criminal trespass and impersonating an employee. The scam was detected when a customer complimented another firm on work performed over Christmas weekend -- when in fact no one had been working! [The WRENCH that stole Christmas?]

[Also noted by "Whittle, Jerome SMSgt" <JWhittle@amclg.safb.af.mil> and Quentin Fennessy <Quentin.Fennessy@sematech.org>, from whom I include the following excerpt. PGN]

---

## Phone number hijacking with Bell Atlantic ultra-forwarding

*Quentin Fennessy <Quentin.Fennessy@sematech.org>*

*Sun, 29 Jan 1995 12:30:47 -0600*

[...] There is nothing new about this crime - except the use of a new medium to hijack a channel of communications. The risks are obvious - as more such services are available without verification the more this crime can occur. I suppose that if Lasch were more sophisticated he could have kept up his scheme for much longer. For example, if the ultra-forwarding were flexible enough he could enable it for the coldest days, in order to fill up his queue with work orders for frozen pipes, and then disabling the forwarding while he completed the jobs.

Quentin Fennessy

---

## Deutsche Telekom offices searched

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>*

27 Jan 95 10:50:59 EST

>From the Reuters newswire (95.01.25 @ 11:36 EST) via CompuServe's Executive News Service:

Deutsche Telekom Offices Searched in Fraud Probe, by William Boston

BONN, Jan 25 (Reuter) - Police searched offices of Deutsche Telekom AG on Tuesday to determine whether staff at the German state telephone monopoly had withheld proof of computer hackers tapping into private phone lines to call foreign sex hotlines.

Juergen Froehlich, chief prosecutor in Cologne, said in a statement that police went through Telekom offices in Bonn, Cologne and Duesseldorf as part of an investigation into a gang of hackers.

The author continues with the following key points:

- \* Legal authorities are investigating the possibility that D.T. employees concealed data on stolen phone services.
- \* Over 2M D.T. clients have complained about fraudulent phone calls charged to their accounts over the last 30 months.
- \* D.T. officials deny that its customers paid for any fraudulent calls, explaining that the criminals placed their calls from accounts obtained using false names.

M.E.Kabay, Ph.D., Director of Education, NCSA (Carlisle, PA)  
Mgmt Consultant, LGS Group Inc. (Montreal, QC)

---

## My life as "uucp@aol.com"

<Uucp@aol.com>

Sat, 28 Jan 1995 18:45:29 -0500

America Online allows its user accounts to specify up to five "screen names", which uniquely identify the user. AOL screen names consist of a capital letter followed by two to nine alphanumeric characters or spaces. The screen name is not case-sensitive, so "MR SMITH" and "Mr Smith" refer to the same account, and the AOL software forces uniqueness on new names by appending digits to the end of the name.

AOL accounts can also send and receive Internet e-mail. AOL converts its screen names to Internet-style addresses by dropping all spaces and appending "@aol.com", so our "Mr Smith" becomes "mrsmith@aol.com" to the outside world.

Which is where I come in. I was trying to come up with a unique screen name that did not end in randomly assigned digits -- AOL's membership stands at

1.5 million users, each of whom can reserve up to five names, so most common English words and names are already taken.

Idly searching for a name, I requested "root". (I always put this down as my first choice when requesting a new account. It never hurts to ask.)

The AOL software politely informed me that this name was taken, and said the same when I requested "postmaster", "webmaster", etc. In some cases it suggested an alternative like "webmast236", and in others it simply said "That name is taken."

Then I requested "uucp".

And the software asked me to enter my new password.

\*

Since then I've been getting a lot of strange e-mail, to put it mildly. Much of it is private correspondence from external addresses to accounts on AOL, or vice versa, that has been Cc:'d to uucp. (I don't know why. Is this happening due to user ignorance or carelessness, or is it the behavior of the mail software?) In no case so far has the sender suspected that "uucp@aol.com" is a live human being.

The RISK here is the assumption that "uucp" (or, for that matter, "root") is a trusted e-mail address on the remote machine. The only required e-mail address in RFC 822 is "postmaster" -- there is no requirement that the remote machine use the UUCP transport mechanism, the UNIX operating system, or that any e-mail address other than "postmaster" route e-mail to the system administrator. ("Postmaster@aol.com" does route e-mail to a person responsible for AOL's mail system, in compliance with RFC 822.)

AOL reserves certain screen names to prevent this kind of confusion, but "uucp" was not one of the reserved names. (Neither was "nuucp", if you were curious -- I've reserved that one too. I think I can retire both addresses permanently by deleting the screen names from my account, but I plan to make certain before doing so.) "Root@aol.com" and "webmaster" are already in use, but I can't say \*who\* is using them.

Of course these RISKS apply to any site, not just to AOL -- any site could have a user account named "uucp" and still be RFC 822 compliant. But as the net grows, and incorporates more and more diverse machines, the RISK becomes more dangerous. Don't assume that mail addressed to "uucp" or "root" on a remote machine is going to a trusted recipient, because for at least one large site this assumption isn't true.

Scott Forbes MSForbes@aol.com

---

## risks of reusing accounts

Charlie Shub <cdash@ludell.uccs.edu>  
Wed, 25 Jan 1995 23:47:46 +0700

Two years ago, i was on sabbatical at a large university, and picked up some support by teaching a course. Their division of computing services managed many computing accounts, and had a pretty reasonable scheme for class accounts. They used a 3 letter followed by 3 digit account names. The first two letters denoted the department, and the third letter was a for the first course, b for the second course, etc. 000 was always the instructor's account and 001 was student 1, 002 student 2, etc. A reasonably sane idea. I would guess that at the end of each semester they cleaned student accounts by deleting all files and reinserting initialization files. They would then generate new passwords for all accounts each semester. What is the risk? accounts may have state data that does not appear in the account or that is not normally cleansed.

The course i was teaching was on a machine i did not use for my personal work, so i had set up automatic mail forwarding to my machine here that I normally read mail on (by telnet from there when i was there). The between semester cleansing algorithm did not reset that forwarding address. Finally, the 5th course in the department again used that same machine, so account cse000 became the instructor's account. That instructor has apparently given the students a "use e-mail" assignment, and did not test the system with a self mailing.

Since the forwarding is still in effect, I have been receiving electronic mail intended for this instructor for the past few days. I thought of sending him/her email to let him/her know about this, but realized that such mail would immediately be forwarded to me. I thought of replying to the students, but if they are just learning about computers, that would also be fruitless. I thought of logging into the account to unset the forward, but the new instructor has obviously changed the password. I suppose I could have chosen to just wait until some interested party finds this in risks, or watch from the sideline until confusion reigns. I believe I have identified the instructor, and have sent her email. A blind copy of this note to risks is being sent to a friend at that institution who will, no doubt, follow up with the instructor and keep me (and perhaps risks readers) posted on how this shakes out.

charlie shub cdash@cs.colorado.edu -or- cdash@colospgs (BITNET)  
(719) 593 3492 (fax) 593-3369

---

### From the cat file

<ark@research.att.com>  
Thu, 26 Jan 95 16:56:42 EST

This morning I was sitting at my home terminal, reading mail. I got up for a few minutes. When I returned to the terminal, the screen showed a partial reply to the last message I had been reading. It looked something like this:

From: ark@research.att.com  
To: sender@machine.com



change for the five.

Luckily, there was no line, so I got my five \$1 bills and ran back downstairs. The money was still registered in the machine, so I proceeded to feed my \$1 bills in. Everything went fine until I got to the fifth bill--which the machine refused to take. Once again, the bill was in perfect shape. After trying a bunch more times, I realized that I would need exact change, so I walked down to the change machine in one of the break rooms to get the bill broken into coins..

Unfortunately, it took too long to get the coins and I arrived back at the machine just in time to see it finish telling me I had taken too long and reset itself, removing all traces of my money from the display.

As you have probably deduced by now, the machine had been programmed to not allow a person to put more than the next highest dollar amount into the machine from the purchase price of the stamps. Since all of the denominations of stamps were between  $\$(X).50$  and  $\$(X+1).00$  [books of \$.29 stamps were \$2.90 and \$5.80 and post card stamps were \$1.90 or \$3.80], the machine assumed that anyone putting in more than the next dollar would risk losing money--something they \*clearly\* would not want to do, since they would lose money. (Never mind that they would also lose the money they'd put in up to this point since once the bills go into the machine they don't come back out.) The sign about getting a maximum of \$.50 back was misleading since the machine gave no opportunity to lose that much.

Luckily the Post Office refunded my money without any hassle, but I still wish whoever programmed the machine hadn't thought they were being so damn clever.

-John Kriens jkriens@cc.bellcore.com

---

## The risks of Risks

*Fritz Knabe <Fritz.Knabe@ecrc.de>*

*Mon, 23 Jan 95 17:13:13 +0100*

As a frequent reader of the RISKS forum, I was very interested when "Computer-Related Risks" (our esteemed moderator's new book) was reviewed here. Using the information from the review, I faxed an order to ACM.

Two months later, with no book, I discovered that ACM had debited my credit card for \$34.50, rather than the \$22.25 + shipping that I was expecting. It seemed that not only did I not have the book, the book I didn't have wasn't even the one I wanted.

I called ACM and discovered that whoever processed my order completely ignored the title and author information in my fax and went right for the 6-digit order number, which it turns out was incorrect. (Interestingly enough, the order number identified a book on software quality.) I hadn't received the wrong book because it was out of stock (I had received no notification of this, either).

The lessons? Overworked order entry people will enter an order number and simply ignore the accompanying description, even though the description is much more likely to be correct. And next time I'll be sure to check the order number directly with ACM, or leave it off.

Fritz Knabe knabe@ecrc.de

---

### **The risks of Risks (Fritz Knabe)**

*Haritini Kanthou <KANTHOU@ACMVM.bitnet>*

*Wed, 25 Jan 95 12:18:23 EDT*

Thank you for bringing to our attention the fact that in one of the ads in CACM, the order number for Peter Neumann's Computer-Related Risks was incorrectly cited as 706943. The correct number is 704943, at \$22.25 plus shipping for ACM members or \$24.75 plus shipping to nonmembers.

[The incorrect number was first found in the original press release from ACM, and it got propagated to various other places. PGN]

Haritini Kanthou, Member Services Mgr. acmhelp@acm.org

---

### **ACSAC '95 Call for Papers and Participation**

*Marshall D Abrams <abrams@mitre.org>*

*Fri, 27 Jan 95 23:25:07 EST*

#### **CALL FOR PAPERS AND PARTICIPATION**

11th Annual Computer Security Applications Conference  
December 11-15, 1995  
New Orleans, Louisiana

#### **The Conference**

The phenomenal growth of the Internet is threatening our very notion of privacy and property. Information networks and computers are routinely processing private, proprietary, sensitive, classified, and critical information. The Internet has created an addiction to information and instantaneous information exchange in the military, government, and private sectors. Computers are making decisions ranging from the mundane to life threatening. To provide protection to this information, the information technology community must:

- o Develop methodologies and tools for designing systems capable of protecting the sensitivity and integrity of information, and assuring that expected services are available when needed.
- o Design safety-critical systems such that their software and hardware are not hazardous.
- o Develop methodologies and tools capable of assuring that

computer systems accorded trust are worthy of that trust.

- o Build systems of systems out of components that have been deemed trustworthy.
- o Build applications on evaluated trusted systems without compromising the inherent trust.
- o Include computer security in enterprise modeling and reengineering.
- o Extend computer security technologies to specifically address the needs of the civil and private sectors.
- o Develop international standards for computer security technology.

For the past 10 years the Annual Computer Security Applications Conference has been helping the IT community meet these challenges by providing a forum for information exchange that is unsurpassed. The Conference will explore a broad range of technology applications with security and safety concerns. Technical papers, panels, vendor presentations, and tutorials that address the application of computer security and safety technologies in the civil, defense, and commercial environments are solicited. Selected papers will be those that present examples of in-place or attempted solutions to these problems in real applications; lessons learned; and original research, analyses, and approaches for defining the computer security issues and problems. Of particular interest are papers that present descriptions of secure systems in use or under development, presenting general strategy, methodologies for analyzing the scope and nature of integrated computer security issues, and potential solutions. Papers will be judged for best paper awards. A prize will be given for the Outstanding Conference Paper and the Best Student Paper. For the Best Student Paper, expenses to attend the conference will also be awarded .

Panels of interest include those that present alternative or controversial viewpoints or those that encourage lively discussion of relevant issues. Panels that are simply a collection of unrefereed papers will not be selected.

Vendor presentations of interest should emphasize innovative product implementations, especially implementations involving the integration of multiple products. Vendor presentations that simply describe product features will not be selected.

Areas of Interest:

Security in Enterprise Modeling and Reengineering  
Trusted System Architectures and Technology  
Encryption Applications (e.g., Digital Signatures)  
Certification, Evaluation, and Accreditation  
Application of Formal Assurance Methods  
Trusted DBMSs, Operating Systems, and Networks  
Security Policy and Management Issues  
Electronic Document Interchange  
Open Systems and Composed Systems  
Software Safety Analysis and Design  
Risk/Hazard Assessments  
AIS Security Tools

#### Instructions for Submissions:

We provide blind refereeing of papers and ask that you put names and affiliations of authors on a separate cover page only. Substantially identical papers that have been previously published or are under consideration for publication elsewhere should not be submitted. Panel proposals should be a minimum of one page that describes the panel theme and appropriateness of the panel for this conference, and should identify panel participants and their respective viewpoints. Send 5 copies of your completed Papers and Panel proposals to Dr. Gary Smith (papers from Europe should be sent to Klaus Keus) by May 31, 1995. For panel/forum preparation instructions, please contact Jody Heaney at (703) 883-5837 or via e-mail at [heaney@smiley.mitre.org](mailto:heaney@smiley.mitre.org). Send five copies of your vendor presentation proposal to Steve Rome. Vendor presentation proposals should include an abstract that describes the product and example applications. Send one copy of your tutorial proposal to Daniel Faigin. It should consist of one- to two-paragraph abstract of the tutorial, an initial outline of the material to be presented, and an indication of the desired tutorial length (full day or half day). Electronic submission of tutorial proposals is preferred.

Authors will be required to certify prior to June 30, 1995, that all necessary clearances for public release have been obtained; that the author or qualified representative will be presented at the conference to deliver the paper, and that the paper has not been accepted or previously published elsewhere. Authors will be notified of acceptance by August 1, 1995. Camera-ready copies are due not later than September 30, 1995.

#### Instructions to Students:

Student papers must be authored 100% by students; no faculty authors are permitted. Send 5 copies of student papers to Dr. Gary Smith; please identify your paper as "Authored by Student." Contact Ravi Sandu, Student Paper Award Chair, to ensure that your paper is considered for the Best Student Paper Award. This award includes expenses to allow the student to travel to the conference and present the paper.

#### Contact Information

Send your papers to:

Dr. Gary Smith  
Technical Program Chair  
ARCA Systems, Inc.  
8229 Boone Blvd., Suite 610  
Vienna, VA 22182  
(703) 734-5611  
[smith@arca.va.com](mailto:smith@arca.va.com)

or

Klaus J. Keus  
BSI  
Bundesamt fuer Sicherheit in der Informationstechnik  
Kessenicher Str. 216  
53129 Bonn Germany

Phone: Germany-(0)228-9582-141

Fax: Germany-(0)228-9582-455

e-mail: keus@bsi.de

Send tutorial proposals to:

Daniel Faigin

Tutorial Program Chair

The Aerospace Corporation

P.O. Box 92957, MS M1/055

Los Angeles, CA 90009-2957

(310) 336-8228

faigin@aero.org

For information about Student Paper contact:

Ravi Sandhu

Student Paper Award Chair

George Mason University

ISSE Department, Mail Stop 4A4

Fairfax, VA 22030

(703) 993-1659

sandhu@isse.gmu.edu

Send vendor proposals to:

Steve Rome

Vendor Track Chair

NSA, V23

9800 Savage Rd.

Ft. Meade, MD 20755

(410) 684-7374

romes@romulus.ncsc.mil

Videos Still Available!

Video tapes of the 1989, 1990, 1992, 1993, and 1994

Distinguished Lecturers are still available. The titles and lecturers are:

1994 Donn Parker

"Computer Loss Experience and Predictions"

1993 H. O. Lubbes,

"COMPUSEC, A Personal View"

1992 James P. Anderson,

"Computer Security Myths and Myhtakes"

1990 Dorothy Denning,

"The Data Encryption Standard: Fifteen Years of Public Scrutiny"

1989 Stephen T. Walker,

"INFOSEC: How Far We Have Come! How Far Can We Go?"

The price for each tape is \$17.00. An additional \$5.00 will be charged for foreign orders for postage. Checks should be made out to Applied Computer Security Associates (ACSA). Send check to Dr. Marshall Abrams, 2906 Covington Road, Silver

Spring, MD 20910. Please indicate which tape you are ordering.

#### Conference Proceedings

Some copies of the 1992 and 1994 proceedings can still be purchased through Ron Ross for \$25 each. Contact him at The Institute for Defense Analyses, 1801 N. Beauregard Street, Alexandria, VA 22311, (703) 845-6617, e-mail: rross@ida.org. For 1991 & 1993 Proceedings, contact the Computer Society Press by dialing 1-800-CS-BOOKS or (714) 821-8380. The non-member price is \$80, the IEEE member price \$40.

#### Mailing List

To be added to the Annual Computer Security Applications Conference mailing list to receive future conference announcements, please send Name, Company, Address, City/State/Zip, Country, and e-mail address to Vince Reed, Publicity Co-chair, The MITRE Corporation, 1500 Perimeter Pkwy., Suite 310, Huntsville, AL 35806, phone: (205) 830-2606, fax: (205)830-2608, e-mail: vreed@mitre.org

Sponsored by Applied Computer Security Associates in cooperation with IEEE Computer Society Technical Committee on Security and Privacy, and ACM Special Interest Group on Security, Audit and Control.

#### Marshall D Abrams

telephone 703.883.6938 Information Systems Security Division  
secretary 703.883.5900 The MITRE Corporation, M/S Z202  
facsimile 703.883-1397 7525 Colshire Drive, Mc Lean, VA 22101-3481



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 16: Issue 78**

**Thursday 2 February 1995**

## Contents

- [Novel form of interference](#)  
[Mich Kabay](#)
  - [Attack on glasfibre cables causes Lufthansa delays](#)  
[Klaus Brunstein](#)
  - [Anonymous ?? Survey](#)  
[Dave Moore](#)
  - [Deep Faults with NYNEX default?](#)  
[Edward P. Ravin](#)
  - [Nynex glitch lets Call ID work even if blocked](#)  
[Dick Mills](#)
  - ["Protect Your Privacy" by Stallings](#)  
[Rob Slade](#)
  - [Identification technologies](#)  
[Phil Agre](#)
  - [Automatic file downloads in Seyon](#)  
[Bruce E. Wampler](#)
  - [Announcement of new mailing list on ethical issues](#)  
[Bashir Jiwani](#)
  - [CFP: 3rd International Workshop on Feature Interactions](#)  
[Nancy Griffeth](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

### Novel form of interference

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>*  
*31 Jan 95 11:22:34 EST*

An amusing tidbit on unexpected risks of technology:

The Reuters news wire reports on an odd form of interference from cell phones and pagers:

RTw 01/30 0425 Israeli rabbi pulls plug on cellular phones

JERUSALEM, Jan 30 (Reuter) - An Israeli rabbi has banned cellular telephones and pagers from synagogues, saying they interfered with worshippers' communication with God.

Rabbi Mordechai Eliahu, a renowned sage and a former chief rabbi of the Jewish state, published the edict on Monday.

Interestingly, the cell phones are called, "Miracle Phones."

Maybe G-d needs spread-spectrum channels.... <g>.

M.E.Kabay, Ph.D., Director of Education, NCSA (Carlisle, PA); Chief Sysop, NCSA CompuServe Forum, Mgmt Consultant, LGS Group Inc. (Montreal, QC)

---

### **Attack on glasfibre cables causes Lufthansa delays**

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.d400.de>  
Thu, 2 Feb 1995 10:38:43 +0100*

Unknown attackers interrupted, Wednesday Feb.1,1995, 7 glas fibre cables near Frankfurt/Main airport. As parts of the cables were cut out, about 15.000 telephone lines were interrupted. The cables also carried data for Lufthansa's booking computers; consequently, new reservations had to be made manually. As Lufthansa's main computers (installed at Frankfurt airport) were cut off for some time, delays of up to 30 minutes were caused. According to diverse German media, police has no information about backgrounds of this criminal attack.

Klaus Brunnstein (February 2,1995)

---

### **Anonymous ?? Survey**

*DAVE MOORE <dave.moore@tcbbbs.cais.com>  
Tue, 31 Jan 95 21:44:00 -0500*

I was recently asked to participate in an opinion survey feedback to management in order for them to compare their own views, superior views, peer views, and subordinate views. This data is then to be used by the reviewee as a self improvement tool.

In order to get honest feedback, a commercial P.C. software package called "2020" was used as a survey tool. This package is supposed to protect your anonymity. It also uses a user supplied password on each diskette to prevent anyone reading your responses. The responses are then collected by a master program and combined with everyone else's responses. Only the combined result is seen, individual responses are not ever seen or tracked. At least, that's the theory.

Since privacy and encryption have been a long time interest of mine, I decided to take a look at the files.

The first thing I saw was that both my name and my reviewee's name were embedded in the data area.

The next thing I saw was that free form comments were stored in clear ascii. You lose the formatting, but any file viewer could see the comments.

I used a hex editor to change some of the comments then reinvoked the program to see if it would detect the changes. It never noticed a thing. It obviously didn't use a digital signature or even a simple checksum.

The cherry on top was the password. It only uses 0-9 & A-Z (uppercase). The password was stored encrypted: down-1 and backward. Thus a password of "simple6" was stored as "5DKOLHR". This took me all of the commercial breaks while watching Star Trek Voyager to find and figure out.

The net result was that I chose not to participate in the anonymous feedback survey.

dave.moore@tcbbs.cais.com

---

### **Deep Faults with NYNEX default?**

*EDWARD P RAVIN <HFDG63A@prodigy.com>*

*Tue, 31 Jan 1995 22:42:54 EST*

Today I received an interesting letter from NYNEX (nee NY Telephone, the local telephone service provider in NY City):

Our records indicate that you requested All-Call Restrict Service on your telephone line...

During a recent system check, we discovered that All-Call Restrict Service was not in place on some lines which it had been requested. We are in the process of checking every All-Call Restrict line and correcting this problem where it exists. As soon as we complete the checking and correction process, we will confirm the status of All-Call Restrict on your line through a special notification.

In other words, you might have thought you had Caller-ID disabled when you make calls from your line, because you ordered it and NYNEX sent you a confirmation notice six or seven months ago, but unless you independently verified that it was in place, you might have been sending your number all this time.

I can tell whether my line is sending caller-ID because I can call a friend with a display and ask him. But as usual, there is no way the local telco can tell you what your lines settings are. Call the billing office, and they will describe what you have ordered and what was reported to have been installed, but what is actually on the line?

It would be nice if you could dial a number and have a voice robot read back to you the settings actually in place -- surely this is possible with

today's digital exchanges, if anyone thought to implement it. Given how many different settings you can have with today's phone lines in the USA (call forwarding, speed dialing, send or don't send Caller ID, choice of long distance carrier, etc), we already need it.

---

## **Nynex glitch lets Call ID work even if blocked**

*Dick Mills <dj.mills@pti-us.com>*

*Wed, 01 Feb 1995 08:19:53 -0500*

So reported the Schenectady, New York Gazette on 2/1/95. The report said

Now, [Nynex] has discovered that All-Call Restrict feature doesn't always work. "The company is indicating to our staff that roughly between 10 percent and 15 percent of people who believe they have All-Call blocking may have a situation where it doesn't work."

That means as many as 82,500 people's numbers are being divulged when the think those numbers are being blocked.

Nynex officials say they are investigating the problem and should have a cause identified sometime next week.

"After this, one of the important things we'll do after we identify the cause is implement new processes that will prevent this from happening again."

New England Telephone, Nynex's subsidiary, is checking to make sure its call blocking is working.

The problem was revealed by an Albany man who depends on anonymity for his livelihood. He tried for weeks to convince Nynex that his call blocking was not working, only to be told it was. Eventually [the man] took his story to the local press.

The company's routine maintenance tests in its 600 central switching offices hadn't discovered this glitch.

To me the risk here is the arrogance that allows people to argue that such large complex, distributed systems can ever be built flawlessly. Any claim that the system will always protect the customers privacy is fatuous. It happened already and it will certainly happen again sometime somewhere.

Dick Mills Power Technologies, Inc. P.O. Box 1058 Schenectady, NY  
12301-1058 dj.mills@pti-us.com +1(518)395-5154

---

## **"Protect Your Privacy" by Stallings**

*"Rob Slade, Social Convener to the Net" <roberts@mukluk.decus.ca>*

*Thu, 02 Feb 1995 12:47:47 EST*

[It didn't start out this way, but this seems to be the start of a "mini" series of reviews on the topic of PGP. Garfinkel's review is due to be sent in another two weeks, Schneier's a week after that; Peachpit has one due out in February while Zimmerman's own, I found out yesterday, is due out in April. - rms]

BKPRTPRV.RVW 941214

"Protect Your Privacy", Stallings, 1995, 0-13-185596-4, U\$19.95

%A William Stallings ws@shore.net

%C 113 Sylvan Avenue, Englewood Cliffs, NJ 07632

%D 1995

%G 0-13-185596-4

%I Prentice Hall PTR

%O U\$19.95 (515) 284-6751 FAX (515) 284-2607 camares@mcimail.com

%P 302

%T "Protect Your Privacy"

This is the first-released of at least three books on PGP (Pretty Good Privacy), the encryption and authentication package by Phil Zimmerman. It covers the concepts of encryption, public key encryption, authentication and key management, as well as the installation and operation of PGP on MS-DOS and Macintosh platforms. There is also some overview of front end shells for DOS and Windows, plus helpful supplementary information on password/phrase choice key servers, and where to get PGP. (The promise of coverage for Windows, UNIX, OS/2 and Amiga in the promotional literature is overkill, but these interfaces will be almost identical to those covered.)

Stallings' material is generally very clear and well written. Many times, however, concepts are introduced early in the book but not explained until much later. This is particularly true of key management. In most cases, I can assure the reader not to worry--all will be made clear, eventually. (In some few cases, the explanation may remain confusing until you actually run the program.)

The book echoes the assertion by many that PGP has become the de facto standard in Internet privacy and authentication. Certainly no commercial product has anything like the same range of use. Full acceptance of PGP, though, has been hampered by the version incompatibilities and the legal difficulties caused by the US weapons (!) export control laws. Given the touchy nature of this subject, it is not terribly surprising that both Stallings, and Michael Johnson in the access document, comment only briefly on the subject. These passages are somewhat calming, but hardly calculated to inspire confidence.

Solid background on the technology, if sometimes disjointed. Terse, but serviceable documentation on the program. Readable and informative.

copyright Robert M. Slade, 1994 BKPRTPRV.RVW 941214

Vancouver Institute for Research into User Security Canada V7K 2G6  
ROBERTS@decus.ca Robert\_Slade@sfu.ca rslade@cue.bc.ca p1@CyberStore.ca

## Identification technologies

Phil Agre <pagre@weber.ucsd.edu>

Wed, 1 Feb 1995 20:39:50 -0800

The journal "Information Technology and People" has just published a special issue, edited by Roger Clarke <roger.clarke@anu.edu.au> entitled "Identification Technologies and Their Implications for People". As the title suggests, it's about computer technologies that identify particular human beings, as well as applications of those technologies to automated tracking of highway traffic. Here are the contents:

Roger Clarke

"Human Identification in Information Systems:  
Management Challenges and Public Policy Issues"

Simon Davies

"Touching Big Brother:  
How Biometric Technology Will Fuse Flesh and Machine"

Marcus Wigan

"The Influence of Public Acceptance on the Realisability of  
the Potential Benefits of Intelligent Vehicle-Highway Systems"

Philip E. Agre and Christine A. Harbs

"Social Choice About Privacy:  
Intelligent Vehicle-Highway Systems in the United States"

Full details on the issue, including abstracts for the papers, are available on the web at:

<http://weber.ucsd.edu/~pagre/identification.html>

Or through e-mail by sending a message that looks like this:

To: rre-request@weber.ucsd.edu

Subject: archive send identification

Phil Agre, UCSD

---

## Automatic file downloads in Seyon

<wampler@cs.unm.edu>

Wed, 1 Feb 95 11:20:44 MST

I've recently started using the Seyon terminal program to dial in to my university account from my home Linux system, and have discovered an interesting risk that is found in Seyon, and perhaps other terminal programs.

One thing I use Seyon for is uploading and downloading files using the Zmodem protocol. To down load a file, you simply enter "sz filename" on the

host machine, and like magic, the file is downloaded. That is the risk. Apparently, the sz program used to download files sends some special character sequence that Seyon is set up to recognize, and then automatically start the download. While this makes downloading nice and easy, it is entirely possible that this sequence could take place without the user noticing what was happening - there are no confirmations from the user required for the download to take place.

It is not hard to imagine someone building a virus based on sending the Zmodem startup sequence, and then simply downloading a file to the remote system. I would imagine this could be even embedded into a regular text posting. Thus a naive or tired or busy user could have some unknown file downloaded to their system simply by reading some posting.

I imagine you can configure Seyon to avoid this behavior, but it is apparently the default mode -- and one that is likely to be used by bunches of people. It is likely that other downloading protocols and terminal emulation programs allow similar actions. I think it is important to recognize the risk in this, and at the least, any program that allows automatic downloading should by default require the user to confirm that it is OK to proceed. Power users can turn off the confirmation. New and casual users would have some protection from unintentional downloads.

Bruce E. Wampler, Ph.D. (wampler@cs.unm.edu)  
Adjunct Professor, Department of Computer Science, University of New Mexico

---

## **Announcement of new mailing list on ethical issues**

*Bashir Jiwani <bashir@ethics.ubc.ca>  
Mon, 30 Jan 1995 18:32:42 -0800 (PST)*

Hello. My name is Bashir Jiwani and I am a graduate student in philosophy at the University of British Columbia in Vancouver, Canada. I began looking into ethical issues of information technology for a course I was taking this past semester. I have developed an interest in these issues and have decided to pursue this interest further. To this end I am pleased to announce that with the help and support of the UBC Centre for Applied Ethics a new mailing list that is intended for discussion of topics in this area has been created.

This list is to be different from existing lists in this area in several important respects.

Firstly, the list is to be moderated. That is, all submissions to the list will not automatically be posted to the list members. Rather, they will first arrive at the moderator's mailbox. The moderator will then put together the various submissions, screening for length and administrative content, and then send them out to the list subscribers.

Secondly, and perhaps most importantly, there will be an established agenda of topics that will serve to guide discussion on the list. Rather than just waiting around for something to happen to get people talking, I have put

together a list of topics that the discussion will progress through. For each topic I have tried to gather a few relevant articles as background reading and have placed them at the list's WWW site. As well I have prepared some basic notes for each topic that fleshes out some of the issues that are thought to be of concern. In this way I have availed myself as the presenter of these topics. I have prepared so far presentations in three topic areas. My hope is that the role of presenter will be shared with the members of the group who are interested in specific issues in information technology ethics and who are willing to put together a small package of background materials for the group's benefit. So as we get to the last of the topics I have set out, I am hoping someone else will have a specific area of interest and will present this area to the list by sketching some of the arguments at issue and by locating various articles that will give participants some background information.

The third most significant difference is the WWW site that the list is associated with. The web site is to serve various functions. It is to make available the presenter's background materials either by providing links to copies which may be located here or at other sites. The web pages are also intended to archive list discussions. As well, any links that members might feel may be useful can also be set up on these pages through the administrative moderator. As I have mentioned, I will be both administrative moderator and topic presenter for the duration of the first three discussion topics after which it is my hope that other members will take on the role of topic presenter and I will refine myself to administrative duties.

I believe that the list will be attractive to all users of information technology. The participation of philosophers as well as business professionals is especially encouraged.

Due to the guided nature of the discussion, the list will officially open as soon as a critical mass of members have signed up. This mass has been set at 40. So as soon as forty people are subscribed to the list, the first set of moderator's discussion notes will be mailed to all members.

To subscribe to the list, send the one-word message "subscribe" in the body of an e-mail message to "infotech-ethics-request@ethics.ubc.ca". For a more detailed description of the list or to access the articles and moderator's notes on the various topics or just to surf some interesting waves, visit the web site at url: <http://ethics.ubc.ca/people/grads/bashir/infotech.html>.

Feedback on or about the list can be sent via the web pages or to the moderator directly at [infotech-ethics-moderator@ethics.ubc.ca](mailto:infotech-ethics-moderator@ethics.ubc.ca).

Bashir Jiwani [bashir@ethics.ubc.ca](mailto:bashir@ethics.ubc.ca) Vancouver, BC

---

### **CFP: 3rd International Workshop on Feature Interactions**

*Nancy Griffeth <[nancyg@thumper.bellcore.com](mailto:nancyg@thumper.bellcore.com)>*

*Wed, 1 Feb 1995 15:43:57 -0500*

Call for Participation  
Third International Workshop on Feature Interactions  
in Telecommunications Software Systems  
Kyoto, Japan  
October 11-13, 1995

Description

This workshop is the third in a series, whose mission is to encourage researchers from a variety of computer science specialties (software engineering, enterprise modeling, protocol engineering, distributed artificial intelligence, formal techniques, software testing, and distributed systems, among others) to apply their techniques to the feature interaction problem that arises in building telecommunications software systems (see the back page for a description of the problem). We welcome papers on avoiding, detecting, and/or resolving feature interactions using either analytical or structural approaches. Submissions are encouraged in (but are not limited to) the following topic areas:

- Classification of feature interactions.
- Modeling, reasoning, and testing techniques for detecting feature interactions.
- Software platforms and architecture designs to aid in avoiding, detecting, and resolving feature interactions.
- Tools and methodologies for promoting software compatibility and extensibility.
- Mechanisms for managing feature interactions throughout the service life-cycle.
- Management of feature interactions in PCS, ISDN, and Broadband services, as well as IN services.
- Management of feature interactions in various of the operations support functions such as Service Negotiation, Service Management, and Service Assurance.
- Feature Interactions and their potential impact on system Security and Safety.
- Environments and automated tools for related problems in other software systems.
- Management of Feature Interactions in various other enterprises, such as banking, medicine, etc.

Format

We hope to promote a dialogue among researchers in various related areas, as well as the designers and builders of telecommunications software. To this end, the workshop will have sessions for paper presentations,

including relatively long discussion periods. Panel discussions and tool demonstrations are also planned. The first day of the workshop, October 11, is devoted to tutorials and discussions on areas related to feature interactions.

#### Attendance

Workshop attendance will be limited to 100 people. Attendance will be by invitation only. Prospective attendees are asked to submit either a paper (maximum 5000 words) or a single page description of their interests and how they relate to the workshop. Proposals for tutorials and discussions are also requested (maximum 3000 words). About 16-20 of the attendees will be asked to present talks; a small number of tutorials and/or discussions will also be selected. We will strive for an equal mix of theoretical results and practical experiences. Papers will be published in a conference proceedings.

#### Submissions

Please send five copies of your full original paper or interest description to:

Kong Eng Cheng  
Department of Computer Science  
Royal Melbourne Institute of Technology  
GPO Box 2476V  
Melbourne, Victoria  
AUSTRALIA 3001

E-mail: [kec@cs.rmit.edu.au](mailto:kec@cs.rmit.edu.au)  
Tel: +61 3 660 3266  
FAX: +61 3 662 1617

Important dates are:

February 28, 1995: Submission of contributions.  
May 15, 1995: Notification of acceptance.  
June 26, 1995: Submission of camera-ready versions.

#### Workshop Co-chairpersons

Tadashi Ohta (ATR, Japan)  
Nancy Griffeth (Bellcore, USA)

#### Program Committee

Co-Chairpersons:  
Kong Eng Cheng (Royal Melbourne Institute of  
Technology, Australia)  
E. Jane Cameron (Bellcore, USA)

Jan Bergstra (CWI and University of Amsterdam,  
The Netherlands)

Ralph Blumenthal (Bellcore, USA)  
Rolv Braek (SINTEF DELAB, Norway)  
Bernie Cohen (City University of London, UK)  
Robert France (Florida Atlantic University, USA)  
Haruo Hasegawa (OKI, Japan)  
Dieter Hogrefe (University of Bern, Switzerland)  
Richard Kemmerer (UCSB, USA)  
Victor Lesser (University of Massachusetts, USA)  
Yow-Jian Lin (Bellcore, USA)  
Luigi Logrippo (University of Ottawa, Canada)  
Jan van der Meer (Ericsson, The Netherlands)  
Robert Milne (BNR, UK)  
Leo Motus (Tallinn Technical University, Estonia)  
Jacques Muller (CNET, France)  
Jan-Olof Nordenstam (ELLEMTEL, Sweden)  
Yoshihiro Niitsu (NTT, Japan)  
Ben Potter (University of Hertfordshire, UK)  
Henrikas Pranevicius (Kaunas University of Technology,  
Lithuania)  
Martin Sadler (HP, UK)  
Jean-Bernard Stefani (CNET, France)  
Greg Utas (BNR, USA)  
Jyri Vain (Institute of Cybernetics, Estonia)  
Hugo Velthuisen (PTT Research, The Netherlands)  
Yasushi Wakahara (KDD R&D Laboratories, Japan)  
Ron Wojcik (BellSouth, USA)  
Pamela Zave (AT&T Bell Laboratories, USA)

#### Workshop Statement

The feature interaction problem is a major obstacle to the rapid deployment of new telephone services. Some feature communications system. Telecommunications software is huge, real-time, and distributed; adding new features to a telecommunication system, like adding new functionalities to any large software system, can be very difficult. Each new feature may interact with many existing features, causing customer annoyance or total system breakdown. Traditionally, interactions were detected and resolved on a feature by feature basis by experts who are knowledgeable on all existing features. As the number of features grows to satisfy diverse needs of customers, managing feature interactions in a single administrative domain is approaching incomprehensible complexity. In a future marketplace where features deployed in the network may be developed by different operating companies and their associated vendors, the traditional approach is no longer feasible. How to detect, resolve, or even prevent the occurrence of feature interactions in an open network is now an important research issue.

The feature interaction problem is not unique to telecommunications software; similar problems are encountered in any long-lived software system that requires frequent changes and additions to its functionality. Techniques in many related areas appear to be applicable to the management of feature interactions. Software methodologies for extensibility and compatibility, for example, could be useful for providing a structured design that can prevent many feature interactions from occurring. Features

are typically design to suit the purposes of a user or business, hence Enterprise modeling will play a role in the identification of certain classes of interaction, in particular the solution of an interaction in one enterprise may not be desired by another. Formal specification, verification, and testing techniques, being widely used in protocol engineering and software engineering, contribute to the detection of interactions. Several causes of the problem, such as aliasing, timing, and the distribution of software components, are similar to issues in distributed systems. Cooperative problem solving, a promising approach for resolving interactions at run time, resembles distributed planning and resolution of conflicting subgoals among multiple agents in the area of distributed artificial intelligence. This workshop aims to provide an opportunity for participants to share ideas and experiences in their respective fields, and to apply their expertise to the feature interaction problem.

#### Workshop Announcement

3rd International Workshop on Feature Interactions in Telecommunications Software Systems, October 11-13, Kyoto, Japan, Sponsors: IEEE Communications Society. In cooperation with ACM SIGCOMM and ATR, Japan. Contact Tadashi Ohta, ATR, 2-2, Hikari-dai, Seika-cho, Soraku-gun, Kyoto, 619-02, Japan, Tel: +81 7749 5 1230, Fax: +81 7749 5 1208, e-mail: ohta@atr-sw.atr.co.jp.



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 16: Issue 79**

**Weds 8 February 1995**

## Contents

- [Proposed Virginia law on self-disabling software](#)  
[Jeremy Epstein](#)
- [Cellular Phone Security](#)  
[Chip Seymour](#)
- [Japanese bank workers steal 140 million yen by PC](#)  
[Mich Kabay](#)
- [Road pricing in Singapore](#)  
[Phil Agre](#)
- [InfoWar Level II in Miami](#)  
[Mich Kabay](#)
- [Phone switch bug causes alarm among NM officials](#)  
[Mich Kabay](#)
- [Telephone RISKS](#)  
[Ry Jones](#)
- [Risks in computerized cockpits](#)  
[Rob Horn](#)
- [Concatenating phrases produces confusing results in bank responses](#)  
[Daniel P. B. Smith](#)
- [More from the cat file](#)  
[Phil](#)
- [1996 ACM COCCS call for papers](#)  
[R.F. Graveman](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Proposed Virginia law on self-disabling software

*Jeremy Epstein <jepstein@cordant.com>*  
*Sun, 5 Feb 95 17:02:53 EST*

The "Washington Post" reported in Saturday's edition (4 Feb 95) that the Virginia legislature is considering a law requiring that companies notify customers if the software they sell has a self-disabling feature (e.g., after some period of time). The article was sketchy, but it's intended to head off people developing software and then demanding ransom to prevent the

software from self-destructing. The law would not \*ban\* such features, just require that they be disclosed.

The RISK? Does informing people that the software is self-disabling encourage them to try to subvert the feature? And if someone did and that triggered the disable feature, would that come under the law? And what if it were used in safety critical systems: "I'm sorry, but the license period on the software in your heart monitor has expired. Please contact the vendor to reenable."

---

## Cellular Phone Security

*Chip Seymour <cseymour@mbunix.mitre.org>*

*Mon, 6 Feb 1995 11:43:54 -0500*

Under the heading "CELLULAR PHONE SECURITY", EDUPAGE of 5 Feb 1995 mentions a \*Wall Street Journal\* article dated 3 Feb 1995 that states Cellular One of New York and New Jersey is starting to require new customers to enter a four-digit security code before placing calls.

This is in an effort to curtail cellular fraud, which is quoted as being \$482 million (3.7% of the industry's revenue) in 1994.

NYNEX began such a program last fall. I spoke with a NYNEX sales representative who told me the new system changes channels after a user enters the phone number and presses "Send". The four-digit PIN code is sent on a new frequency, and would-be ESN thieves now have the added task of determining which PIN goes with which ESN.

However, if your cellular telephone is equipped with a recall feature, pressing "RCL" displays, not the telephone number you've just dialed, but the four-digit PIN number. My Motorola DPL 550 recalls the PIN number even after a powerdown.

Just a word of warning. Recall your PIN and Clear the display before leaving your telephone, and consider enabling the automatic-lock feature, if available.

---

## Japanese bank workers steal 140 million yen by PC

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>*

*05 Feb 95 14:12:50 EST*

>From the Reuters news wire via CompuServe's Executive News Service:

RTw 02/05 0107 Japanese bank workers steal 140 million yen by PC

TOKYO, Feb 5 (Reuter) - A Japanese bank employee and two computer operators have been arrested and charged with allegedly using a personal computer money transfer system to steal 140 million yen (\$1.4 million), police said on Sunday.

Police said the 140 million yen was illegally sent in December last year from Tokai Bank Ltd to an account in another bank using a settlement system operated by personal computers. It was withdrawn the same day.

The following day, a total of 1,490 million yen (\$14.9 million) was sent from Tokai Bank to accounts in several other banks using the same system. But this time the fraud was discovered before any withdrawals could be made.

According to the article, the suspects include employees of the bank systems group and a computer services supplier. It seems that the scheme was driven in part by debts owed to organized crime groups.

M.E.Kabay, Ph.D., Director of Education, Natl Computer Security Assn (Carlisle, PA); Mgmt Consultant, LGS Group Inc. (Montreal, QC)

---

## road pricing in Singapore

*Phil Agre <pagre@weber.ucsd.edu>  
Sun, 5 Feb 1995 21:48:04 -0800*

The LA Times had an article about road pricing in Singapore:

Charles P. Wallace, Singapore in high-tech tangle to fight automobile gridlock, Los Angeles Times, 3 February 1995, page A5.

The story is that Singapore's streets are rapidly becoming jammed with cars, and so the authoritarian government is trying to impose a road-pricing scheme based on automatic vehicle identification (AVI). "Road pricing" means that every road, or at least every frequently clogged road, is a toll road. "AVI" means that your car carries a device that can be "pinged" by a radio signal from a roadside beacon, whereupon it broadcasts a number (its own serial number in most versions, but perhaps the car's identification number) that allows a charge to be made to an account. The LA Times article is basically sympathetic to the government's position despite the straightforward coercion that the system involves. It pays no attention to privacy issues. The only existing AVI toll-collection system mentioned is the voluntary Telepass system in Italy.

The basic argument behind road-pricing is a familiar market argument: when people can travel on roads for free, they naturally do so at a higher rate than if they had to pay the actual costs of providing roads. Road pricing, on this model, seeks to establish the most efficient level of road usage by letting people decide how much it's worth to them to drive.

In practice this argument generally runs afoul of reality in several ways:

(1) Road pricing schemes have generally required the collection of large amounts of data about individuals' travel patterns. So long as this data is accumulating, pressures to use it for other purposes, from marketing to

repression, are more or less inevitable. Digital cash payment schemes might alleviate this problem, but so far as I am aware they have not been seriously proposed, much less implemented.

(2) Unless you actually privatize the roads, in practice a "road price" is really a tax whose levels are set not by a market but by a legislature. One might argue that this is fine in a properly functioning democracy, but people often don't see it that way. A road-pricing scheme in Hong Kong failed a while back due in part to anti-tax sentiments.

(3) It's very difficult to establish a proper competitive market in roads, since in most areas it's an industry with extremely high barriers to entry.

(4) The whole geography of many countries -- maybe not Singapore, but certainly the United States -- has been shaped by the availability of free road travel. Introducing road pricing at this late date would cause great economic disruption. The resulting process would actually be very interesting to watch, and in the very long run might even reverse the flight from cities into the suburban sprawl. But it would be very messy.

(5) When it costs money to drive on roads, the poor cannot legally drive. When you're looking for a job, free roads are one of those little subsidies that keep the wolves from the door.

Enormous intelligent vehicle-highway systems (IVHS) including AVI-based toll collection are coming to most of the world. Singapore is the exception in declaring that the systems will be mandatory. But do you really believe that the IVHS in your region will remain voluntary? Will your insurance company require you to sign up for it? Will the availability of AVI encourage your local bureaucrats, faced with intractable budgetary woes, to propose road pricing schemes for the two dozen most overburdened roads in your region? Will you still refuse to sign up for the system when the alternatives are traveling strictly on free roads or stopping to pay thirteen tolls every day? These are questions worth thinking about now, before IVHS technical standards are established and deployment decisions get set in stone.

Phil Agre, UCSD

---

## InfoWar Level II in Miami

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
07 Feb 95 21:45:05 EST*

The following item does not involve high technology, but it does illustrate the risk from information warfare level II (inter-corporate):

WP 02/06 Dial and Save's Word-of-Mouth Toll;  
Chantilly Long-Distance Firm Battles False Rumors of  
Free Service to Cuba

By Kara Swisher, Washington Post Staff Writer

Executives at Dial and Save, a small long-distance company in Chantilly, never thought they would have something in common with corporate giants such as Procter & Gamble Co. and Kentucky Fried Chicken Corp. But recently the firm became a member of that unfortunate group of companies zapped by untrue rumors that spread out of control. ... Dial and Save is contending with thousands of angry customers who say they thought that certain calls placed through its network were free.

According to the author, over 10,000 people in the Miami area thought they were getting free calls to Cuba--and they placed over \$2 million in calls in a few weeks. Now people are reacting to unexpected bills (some as high as \$10,000).

The furious callers insisted that they had placed the calls only because they had heard they were using free test lines. Customers said they would never have made the calls if they had known the costs; they had believed that Dial and Save's access number was the code for a free ride to reach their relatives in Cuba.

The article continues with an extensive discussion of the public-relations nightmare caused by the angry customers (or perhaps I should say, "would-be non-customers") over their unexpected bills. In addition, the company has felt obliged to hire 20 extra Spanish-speaking operators to handle the thousands of angry calls they are currently receiving.

[Comments by MK: I don't want to discuss the possible motivations of people claiming they expected free service by calling an access number. My reason for posting this fairly low-tech story is to illustrate the economic consequences of a simple rumour. Now imagine this rumour spreading through cyberspace, aided by anonymous postings and repostings in innumerable news groups, e-mail messages and bulletin board systems.

This story reminds me of the lament recently posted by an anonymous executive in Network World 11(49):41 (94.12.05) entitled, "Ad leads to a nightmare on Cyber-Street." This poor fellow spammed the Net in a small way and got a slew of nastygrams e-mail and was publicly pilloried in many news groups.

Unfortunately, "someone uploaded a message to most of the alt.sex groups that listed my company's two 800 numbers as phone sex lines." The consequences of that rumour were horrendous: flooded phone lines, angry and embarrassed receptionists, and complete humiliation of the naive Internet advertiser.

Now, such childish pranks have already had expensive consequences, yet they are as nothing compared to the potential for economic terrorism posed by anonymity and pseudonymity on the Internet. As yet, I think, only some people on the Net have internalized the appropriate level of skepticism about any information gleaned from the Internet, let alone about anonymous postings. With a growth rate estimated by some at 10% per month in the number of people using IDs that can access the Internet,

we will see a natural increase in credulous newcomers. If thousands of people can believe that a phone-sex service would use an 800 number (or that a commercial phone service supplier would make free long-distance calls available), I think millions of people will be prepared to believe all sorts of other nonsense--and, alas for the victims, act upon those mistaken beliefs.

So what are we gonna do, eh? Even my usual leitmotiv (We need non-repudiatable identification and authentication for access to the Internet -- etc. etc. etc.) fails: the people using the "free" access codes for calls to Cuba were tracked unerringly by their normal phone company accounts. No doubt the gullible seekers after, ah, aural sex were equally traceable--but so what? The damage was done regardless of non-repudiation.

I dunno what we're going to do. Any ideas?]

M.E.Kabay,Ph.D., Director of Education, Natl Computer Security Assn  
(Carlisle, PA), Chief Sysop, CompuServe NCSA Forum

---

### Phone switch bug causes alarm among NM officials

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
07 Feb 95 21:45:39 EST*

>From the Washington Post news wire via CompuServe's Executive News Service:

WP 02/06 DIGITAL FLUBS

According to the brief report,

The Albuquerque Tribune reported that many calls placed to numbers that use the state government's main Sante Fe prefix, 827, were erroneously routed to a recording that announced that the number was not in service.

Since these events coincided with New Mexico Governor Gary Johnson's announced intention to replace many government officials, the bug in the phone switching software caused an unusual number of strong emotional responses.

M.E.Kabay,Ph.D., Director of Education, Natl Computer Security Assn  
(Carlisle, PA); Mgmt Consultant, LGS Group Inc. (Montreal, QC)

---

### Telephone RISKS

*Ry Jones <rjones@rjones.oz.net>  
5 Feb 1995 20:12:58 GMT*

Two items have recently become news in the PNW. One, we had an earthquake centered in Tacoma. According to articles in the Tacoma News-Tribune, the Seattle Post-Intelligencer, and The Daily Olympian, all three counties 911 systems were knocked out due to people calling to see if there had been an

earthquake, or to get information about the quake. All three articles mentioned very high call volumes; the Seattle article mentioned 350 calls in the first 10 minutes after the quake.

The RISKS are obvious. As a denial of service attack, this was perfect. Hundreds of well-meaning people (like rubberneckers on the information superhighway?) slowed or stopped vital services from being delivered. All three counties exhorted people to only call 911 after you have been hurt in an earthquake.

As an aside, I got on the net and hit `gopher://geophys.washington.edu:79/0quake` and had instant, up-to-date information. Much better than what was available on the radio or TV. Perhaps if someone made a VMB that recited the most recent event to all callers? Then we could lose access to one switch somewhere, instead of to the 911 switch.

Two: page A9, Saturday Feb 4 1995 issue of The Daily Olympian.

#### LOSER: AUTOMATIC CALLING

Poor Kenneth Calkins. The retired South Sound resident has received the same call once a week, every week, for nearly a year. The call, made through the Employment Security Department, is for a job opening Calkins has no interest in. Officials say the call, portions of which are in spanish, was meant for another person at another number. ...

They go on to talk about how he didn't know how to remove himself from whatever list was generating the calls.

The RISKS here are the annoyance of the voting elderly by newfangled computers with Automatic Calling Units. You could get voted out of office if enough people get angry...

Finest handcrafted code since 1987.

---

## Risks in computerized cockpits

*Rob Horn 6-4365 <horn%temerity@cliffy.polaroid.com>  
Wed, 08 Feb 1995 10:04:00 -0500 (EST)*

Last week's (30 Jan 1995) and this week's (6 Feb 1995) Aviation Week & Space Technology have two moderately large sections on investigations, theories, and practices with the new computerized cockpits. In general the articles are good. The authors take the perspective of pilots. They discuss how pilots interact with the computerized systems and how these interactions improve or decrease effectiveness and safety.

R Horn

[Also noted by `wb8foz@netcom.com` (David Leshner), who added that the first issue includes "detailed (make that *very* detailed) discussions on some of the [in]famous Airbus incidents." PGN]

---

## Concatenating phrases produces confusing results in bank responses

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

*Thu, 2 Feb 1995 22:56:33 +0001 (EST)*

BayBank, a Massachusetts chain, has recently started offering "linked accounts." For example, a recent ad shows the former hockey player, Bobby Orr, using his telephone to transfer money from his account to his son's. I figured it would be neat to have something in common with Bobby Orr, so I had them set up the same thing for me and my daughter who's at U. Mass. Before setting up the link, my accounts, as shown at ATM machines or over the phone, were identified as "savings" and "checking."

BayBank has a feature which they call "custom account names." You might think this means you can pick any name you want, but what it actually means is that you can select from a list of about a hundred names, with highly personalized choices like "daughter 1" and "son 2." The BayBank rep who set up my account suggested the "custom" names "my checking," "daughter's checking," "my savings," and "daughter's savings," which sounded sensible to me.

The first time I tried to be like Bobby Orr, here's what the confirmation dialog I got over the phone was: "Seventy dollars have been transferred from your my savings account to your daughter's checking account. The reference number for this transaction is one thousand eight hundred and four." This caused me to say "huh?" three times. The (British?) grammar of "seventy dollars have" isn't bad; I would have preferred that the transaction number be read as "one eight zero four;" but the phrase "your my savings account" stopped me cold.

So, next month my daughter gets her bank statement and, yep, you guessed it: her statement shows this as "BayBank XP24 Transfer From BB Boston My Savings." See, it's my daughter's statement, but it's not her my savings, it's my my savings.

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

---

## More from the cat file

*<phil@hyphen.equinox.gen.nz>*

*Fri, 3 Feb 95 14:35:45 +1300*

You think *\*you've\** got problems...

We have three little furry friends. The other morning (about 5 am) I was obliged to remove one of them from my bedroom in response to demands for food. Said mammal was carried to the kitchen and fed in an attempt to get some more sleep.

On the return trip to my room I was alerted by the distinctive sound of the dial tone from the 'handsfree' phone in my study. Then I heard it dial...

It had only rung twice by the time I cancelled the call (it's a long hall, ok? :-). It appears that the kitten was asleep in the empty paper box on the corner of my desk and had been aroused by the sound of cat biscuits hitting the food bowl. In the process of heading for the easy way off my desk (via my chair) he had managed to stand on my phone and take advantage of the 'one-touch hands-off dialing' facility.

Later that morning I used the redial function to see who had been disturbed and to apologise profusely for the obscenely early call. Luckily, the recipients were somewhat amused and quite forgiving.

There is now an empty box over my phone whenever I'm not sitting right next to it...

phil

---

### 1996 ACM COCCS call for papers

*"R.F. Graveman" <rfg@ctt.bellcore.com>*

*Sat, 4 Feb 1995 10:50:03 -0500*

Call for Papers

Third ACM Conference on Computer and Communications Security

Hyatt Regency, New Delhi, India

March 14-16, 1996

Sponsored by ACM SIGSAC

Hosted by Indian NIC and AIMIL,

Bell Atlantic, and George Mason University

High quality, original, and unpublished (and not submitted elsewhere) research and practice papers in the area of computer and communications security are solicited. All aspects of computer security are relevant, such as theories, techniques, applications, and practical experiences. They include:

access control, accounting and audit, applied cryptography (block ciphers, hash functions, digital signatures, key escrowing, cryptographic protocols), authentication, authorization, data/system integrity, electronic commerce, intrusion detection, key management, open systems security, privacy, protection of software and intellectual property, secure networking (LANs, WANs, firewalls, ATM, Internet, mobile, wireless, and telecommunications), secure operating systems and APIs, security architectures and models, security management, security of distributed systems and databases, security protocols, and smart-cards and secure PDAs.

Instruction for authors:

Submit seven (7) copies of your paper (not exceeding 7500 words or 25 pages) to either of the Program co-Chairs, in a form suitable for anonymous review

(no author names, affiliations, obvious references), with a cover letter including author names, email and postal addresses, phone and fax numbers. Electronic or late submissions will be rejected without review. Where possible all further communications to authors will be via email.

Paper submission: July 1, 1995  
Acceptance decision: September 1, 1995  
Camera-ready papers due: December 1, 1995

General Chairs:

Ravi Ganesan, Bell Atlantic, USA  
Ravi Sandhu, George Mason University, USA

Program Chairs:

Li Gong  
SRI International  
Computer Science Laboratory  
333 Ravenswood Avenue  
Menlo Park, California 94025, U.S.A.  
Tel: + 1-415-859-3232  
Fax: + 1-415-859-2844  
Email: gong@csl.sri.com

Jacques Stern  
ENS-DMI  
45 Rue d'Ulm  
75230-05 Paris, France  
Tel: + 33-1-44322029  
Email: Jacques.Stern@ens.fr

Local Arrangement:

N. Seshagiri, National Informatics Center, India  
H.C. Verma, AIMIL, India

Awards: Raymond Pyle, Bell Atlantic, USA  
Publication: Clifford Neuman, U. of Southern California, USA  
Publicity: Richard Graveman, Bellcore, USA

Program Committee Members:

Aditya Bagchi, Indian Statistical Institute  
Elisa Bertino, University of Milan, Italy  
Matt Blaze, AT&T Bell Laboratories, USA  
Claude Crepeau, Universite de Montreal, Canada  
Matthew Franklin, AT&T Bell Laboratories, USA  
Virgil Gligor, University of Maryland, USA  
Richard Graveman, Bellcore, USA  
Sushil Jajodia, George Mason University, USA  
Kwok-Yan Lam, National University of Singapore  
E. Stewart Lee, University of Toronto, Canada  
Arjen K. Lenstra, Bellcore, USA  
Kaicheng Lu, Tsinghua University, China  
Shyh-Wei Luan, IBM Almaden Research Center, USA

Tsutomu Matsumoto, Yokohama National University, Japan  
Catherine Meadows, Naval Research Laboratory, USA  
Clifford Neuman, University of Southern California, USA  
Luke O'Connor, DSTC, Australia  
Bart Preneel, K.U. Leuven, Belgium  
Jean-Jacques Quisquater, UCL-MathRIZK, Belgium  
Lakshmi Raman, Bellcore, USA  
Michael Reiter, AT&T Bell Laboratories, USA  
Nachum Shacham, SRI International, USA  
Y.K. Sharma, National Informatics Center, India  
Shiuh-Pyng Shieh, Chiao-Tung University, Taiwan  
Stuart Stubblebine, AT&T Bell Laboratories, USA  
Paul Syverson, Naval Research Laboratory, USA  
Paul Van Oorschot, Bell-Northern Research, Canada  
Vijay Varadharajan, University of Western Sydney, Australia  
Gio Wiederhold, Stanford University, USA  
Michael Wiener, Bell-Northern Research, Canada  
Rebecca Wright, AT&T Bell Laboratories, USA  
Moti Yung, IBM T.J. Watson Research Center, USA

More information, access <http://www.csl.sri.com/acm-ccs/ccs.html> or  
email to [acmccs3@isse.gmu.edu](mailto:acmccs3@isse.gmu.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 16: Issue 80**

**Monday 13 February 1995**

## Contents

- [German Railway Wage Woes](#)  
[Debora Weber-Wulff](#)
- [Risks of modern newspaper article composing or editing?](#)  
[Thomas A. Russ](#)
- [Portuguese E-cash](#)  
[Kent Borg](#)
- [Long-Distance Debit Cards](#)  
[Len Bauer](#)
- [Risks of remote printing through a network](#)  
[Skyruner](#)
- [Risks of Third-Party-Billed Calls](#)  
[Micah Altman](#)
- [Re: Info War II in Miami](#)  
[Jim Huggins](#)
- [Re: Road pricing in Singapore](#)  
[Mats Ohlin](#)
- [New service for Risks Forum members](#)  
[Frederick B. Cohen](#)
- [Security and Privacy Program](#)  
[Catherine A. Meadows](#)
- [Info on RISKS \(comp.risks\)](#)

---

## German Railway Wage Woes

*Debora Weber-Wulff* <[weberwu@tfh-berlin.de](mailto:weberwu@tfh-berlin.de)>

9 Feb 1995 17:02:43 GMT

There was an article on the business page of the "Tagespiegel" this morning on the problems plaguing the German railway company. I had meant to post the problems to risks when it began, but you know how it goes.... So anyway, it is now the fourth month that the railway has not correctly met its payroll because of software problems and the natives, er, workers are rather restless.

The railway has just recently been privatized and the employees transferred from civil service to private contracts. Calculating a civil service payroll in Germany is not for the faint at heart, there are all sorts of little additions and deductions. The unions had insisted that the pay remain more or less the same, and worked out a new, different but still complicated schedule of pay adjustments. Now the fun begins.

Some people don't get paid at all. One who now longer works for the railway received a notice that he owes them 1.61 DM. Many people that normally make 3000-4000 DM a month receive only 900. And then there are the apprentices who normally make just 1000 a month - they seem to be getting somewhere on the order of 15000 DM a month... interestingly enough, the Bahn manages to call the overpayments back lickety split. The other direction is not so easy. Last month they offered to give everyone 2000 DM extra until everything gets straightened out. That didn't work either, with some being asked to pay the Bahn money and others having big payroll deductions wipe most of it out.

What did the Bahn do? Amazingly, this is being programmed in-house. And since there is no responsible leader of the programming department (!), they have hired someone for that job (probably so that they can fire him next month...). "It's just a software problem" they say. And the payroll is so large, it cannot be done by hand. Employees are being asked to keep track of what they get and what they think they should get.

[Ah, did I mention, they jacked up the prices for travelling by train the beginning of February? That's another story, but I think I know what they need the money for now....]

Debora Weber-Wulff, Technische Fachhochschule Berlin, FB Informatik,  
Luxemburger Str. 10, 13353 Berlin, Germany weberwu@tfh-berlin.de

[I suppose if they get rid of the new leader,  
we have a Bahn-fire of the Sanities? PGN]

---

## **Risks of modern newspaper article composing or editing?**

<tar@ISI.EDU>

Wed, 8 Feb 1995 16:05:41 -0800

I noticed an interesting AP newswire story in the LA Times Business section (p. D2) on January 31, 1995. The only problem was that it appeared to have a final paragraph from a much earlier story appended to the end. The phrasing matched well enough that it took a while to realize that we did not, indeed, invade Japan over the issue. I enclose the last two paragraphs:

Headline: Japan Worker's Pay Surges to New High; U.S. Trails

...

Some of the increas in Japan reflects the decline value of the dollar against the yen, and the effect of Japan's higher wageds is

offset by generally higher prices for consumer goods.

Indeed, the U.S. forces that begin landing on the island today will depend explicitly on Cedras' cooperation for their success. One of the first tasks of the commander of the U.S. expeditionary force, Lt. Gen. Henry Hugh Shelton, will be an official call on Cedras.

A risk of ghost stories in the machine?

Thomas A. Russ, Senior Research Scientist, USC/Information Sciences Institute  
4676 Admiralty Way, Marina del Rey, CA 90292 tar@isi.edu (310) 822-1511x775

---

## Portuguese E-cash

*Kent Borg <kentborg@borg.org>*

*Wed, 08 Feb 1995 23:07:49 -0500*

The Wednesday, 8 Feb 1995, International Herald Tribune has a very short item on "Portuguese Plastic". The AP picture shows a pair of open hands holding both a few pretty coins and a single less pretty smart card.

The card has snappy graphics (including a picture of coins) and I count about 9-electrical contact pads for getting at the smarts.

Some details:

- o "Spending limit of \$375". (Presumably 60,000 Escudos.)
- o "Does not have a user's name on it".
- o "Requires no secret codes".
- o It can have new value put in it using an automatic teller machine.
- o Written on the card is: "Porta Moedas Multibanco" and "Caixa Geral de Depositos".
- o The picture seems to show a dark fuzzy printed serial number, maybe 12-digits long.
- o For incidental purchases, merchants' readers will be cheap and autonomous if it really can be used to buy "newspapers, cigarettes, or a cup of coffee".

Missing Details:

- o Is the system publicly documented and secure, or is it security through obscurity?
- o Does it have the user's name \*in\* it? (Is it anonymous, or not?)
- o Who issues it? (Who will get burned if it is hacked?)
- o When will it start running?
- o What \*is\* the underlying system?

Risks issues? I think the most interesting will be the public's sense of the risks, what they are told, and whether they "buy" it.

-kb

Kent Borg +1 (617) 776-6899 kentborg@borg.org kentborg@aol.com

---

## Long-Distance Debit Cards

"Len Bauer" <lab1@rfc.comm.harris.com>

Wed, 08 Feb 95 14:43:42 -0500

My father is a security investigator for a major national "Less-Than-Truckload" freight carrier. Recently a string of major shippers have been hit by weekend thefts up and down the North Atlantic seaboard. The most recently pilfered items were \$270,000 of long distance prepaid calling cards. These apparently are gaining acceptance as both a debit card and/or collectible item depending upon the picture on the card.

When the trucking firm contacted the owner of the shipped cards and told them of the theft, they had no way of de-activating the stolen cards. Even knowing the lot numbers, etc., they do not have the software in place to render the cards obsolete. So goodbye \$270,000 in calls, and assuming they are sold for 50 cents on the dollar at the Port Authority Terminal, hello \$135,000 for the bad guys.

Len Bauer Rochester NY. Harris RF Communications

---

## Risks of remote printing through a network

<SKYRUNER@delphi.com>

Thu, 09 Feb 1995 01:30:32 -0500 (EST)

I'm submitting this to illustrate the RISKS of trying to print a document from a remote laptop through a network and assuming that it will come out on the right device.

I work at a small daily newspaper which uses Macs, PCs, and a mainframe in its network. In addition to small laser printers and dot-matrix printers we have output devices that can produce 13 x 21.5" pages on regular paper, "RC" paper, or film negative. The film costs \$1 per inch of depth so we're always being admonished to be careful not to waste it.

We have two reporters who started a self-publishing project last year, a fiction zine called *\_Sludgecone\_*. They have been using the newspaper's facilities to produce their camera-ready pages, although their actual printing was done at a copy shop.

The other day one of them decided to print out all the raw, unedited copy (24 pages) for the second issue. He was at his house with his laptop, and logged in to our system intending to print them out on 8.5 x 11" paper on one of the small laser printers. Unfortunately for him it did not go there, but rather to film. Each page came out on 13 x 21.5" film. 24 pages at \$1 an inch, with 4 inches between pages, added up to \$600 worth of wasted film.

At this time I don't know what's going to happen but I'd guess that this unfortunate person and his partner will be forbidden from using the

newspaper facilities to produce \_Sludgecone\_, and they might have the \$600 taken out of their paychecks.

skyruner@delphi.com

---

## RISKS of Third-Party-Billed Calls

*Micah Altman <micah@cco.caltech.edu>*

*7 Feb 1995 21:56:41 GMT*

The following is a summary of a recent personal experience with PacBell. While I have not seen this precise RISK mentioned in the digest, it is a variant on a theme familiar to risk readers.

While reviewing my January residential local phone bill I noticed an unfamiliar entry under the heading of "Operator and System-Assisted Calls". Listed under this heading was a short call, marked as a "system assisted 3rd party call". Both destination and source numbers were listed, but I recognized neither.

This afternoon I called the PacBell billing center for an explanation and correction. The service representative, Brian, was straightforward and polite. He informed me of the following:

- This call was made from another residential number, the person who made the call simply requested that it be billed to my number.
- When a 3rd-party-billed call is made from a residential number, "9 times out of ten the operator making the call will NOT ASK FOR ANY VERIFICATION (emphasis added)"

Let me stress that this was not a case of a pilfered PIN, or "calling card" number. I have never requested or received a "calling card" from PacBell, so there there should be no such account number to steal. It would seem that PacBell simply allows calls to be billed to other numbers with no verification at all.

While PacBell offered to credit the call they did not offer to block such calls until I explicitly asked whether there was any way to prevent the situation from recurring.

While I consider myself to be a reasonably well-informed consumer, prior to this incident I was neither aware of the procedures used for 3rd party billing, nor of the blocking service available for such calls (at the time I initially ordered phone service I explicitly requested all blocks that were then offered).

With the plethora of phone calling cards with, at least, weak authentication, third-party billing seems to be a service of little value. Making such a service available without verification is unconscionable.

The RISKS of the situation are obvious.

---

**Re: Info War II in Miami (Kabay, [RISKS-16.79](#))**

*Jim Huggins <huggins@eecs.umich.edu>*

*Wed, 8 Feb 1995 14:36:38 -0500*

> I think millions of people will be prepared to believe all sorts of other  
> nonsense--and, alas for the victims, act upon those mistaken beliefs.

One problem is that what constitutes "nonsense" is a floating target. There are (or have been) for-pay phone-sex lines which operate from 800 numbers, much to the dismay of concerned parents who have already blocked 900 numbers on their home phones with the help of their telco and have no way to screen for 800 numbers, too. (It should be noted that many telcos are working now to eliminate this sort of bait-and-switch.)

It's not unlikely that a commercial phone service could make free long-distance phone calls available; I've seen booths in shopping malls from various long distance vendors encouraging you to try a free phone call to anywhere to check the quality of their phone line.

The RISK, as with all urban legends, is that of poor authentication -- either of the purported author or of the content of the message. Relying on "common sense" in a rapidly changing age is not necessarily as easy as sounds (if it ever was that easy...).

Jim Huggins, University of Michigan (huggins@umich.edu)

---

**Re: Road pricing in Singapore (Agre, [RISKS-16.79](#))**

*<Mats.Ohlin@itsec.fmv.se>*

*Mon, 13 Feb 1995 17:27:22 --100*

In [RISKS-16.79](#) Phil Agre mentioned Digital cash payment schemes for road tolls but assumed that such systems have not yet been proposed, much less implemented. Fact is that in Sweden there is an undergoing major national road toll project which in 1996/97 will introduce such a system, based of transponders plus smart cards. Cards may be filled with cash at various places, gas stations etc. Privacy issues are of concern, so a Digital cash system is necessary; still there remains the potential (risk) for systematic tracking of travel patterns. This will be of considerable concern from the Data Inspectorate. The system will be able to make the recording at speeds around 80 km/h (50 mph). Cars without the right equipment will be photographed - unless you pay at the manual gate of course.

Mats Ohlin

---

**New service for Risks Forum members**

*"Dr. Frederick B. Cohen" <fc@all.net>*

*Wed, 8 Feb 1995 23:20:06 -0500 (EST)*

Management Analytics is offering (in a test mode only) the ability to scan sites over the Internet for well-known over-the-wire security holes.

The service is available from Mosaic (via W3) at the URL:

<http://all.net:8080>

Comments are welcomed, and a lively debate is anticipated.

How does the attack scanning process work?

We have collected and written a set of attack programs that automatically probe systems in the same way as many attackers probe them. When you request an attack, the computer at all.net launches the attack against the specified machine, logs the results, and E-mails the results out.

How do you keep this process safe? </h2>

Since the attacks are launched from all.net, we don't give out the attack code in the process of testing. The results are E-mailed to postmaster@the.attacked.machine so that only the systems administrator responsible for dealing with postal problems at the machine under scan gets the result. These results are posted along with the identifying information about the person and site that requested the attack so that the action is traceable. Finally, all.net is identified as the source in a separate posting to the systems administrator of the machine. All of the attacks are well known and the programs we use are widely available in source form for free over the Internet.

FC

---

## Security and Privacy Program

*Catherine A. Meadows <meadows@itd.nrl.navy.mil>*

*Thu, 9 Feb 95 17:56:34 EST*

PLEASE NOTE: THE PRINTED VERSION OF THIS INFORMATION WILL NOT ENTER THE US MAIL SYSTEM BEFORE FEBRUARY 28, 1995. PARTICULARLY IF YOU ARE OUTSIDE THE CONTINENTAL U.S., CONSIDER USING THIS FORM TO REGISTER.

1995 IEEE SYMPOSIUM ON SECURITY AND PRIVACY

May 8-10, 1995  
Claremont Resort,  
Oakland, California

  //  
  //  //  
  //  //  
  //  //  //  
  //  //

Sponsored by the  
IEEE Technical Committee on Security and Privacy  
In cooperation with the  
International Association of Cryptologic Research

  //  //  
  //  //  
  //  //  //  
  //  //  
  //  //  
  //  //

Symposium Committee

  //  //



11:00-12:30 COVERT CHANNEL CONTROL

A Network Version of the Pump  
M. Kang and I. Moskowitz (NRL)

An Architecture for Covert Channel Control in  
Realtime Networks and Multiprocessors  
R. Browne (Independent Consultant)

Version Pool Management in a Multilevel Secure Multiversion  
Transaction Manager  
A. Warner and T. Keefe (Penn State)

2:00-3:30 PANEL: Selling Cubic Zirconia on the Internet:  
Security for Electronic Commerce

Chair: S. Kent, (BBN)  
Panelists: TBA

4:00-5:00 SHORT TALKS

WEDNESDAY MAY 10

9:00-10:30 ANALYSIS OF SECURITY VULNERABILITIES

Capacity Estimation and Auditability of Covert Channels  
B. Venkatraman and R. E. Newman-Wolfe (U. of Florida)

Supporting Security Requirements in Multilevel Real-Time  
Real-Time Databases  
R. David, S. Son, (U. of Virginia), R. Mukkamala (Old Dominion U)

The Intel 80x86 Processor Architecture:  
Pitfalls for Secure Systems  
O. Sibert, (Oxford Systems), P. Porras, R. Lindell (Aerospace)

11:00-12:30 PROTOCOL ANALYSIS

Recent-Secure Authentication:  
Enforcing Revocation in Distributed Systems  
S. Stubblebine (AT&T)

Reasoning About Accountability in Protocols for  
Electronic Commerce  
R. Kailar (Secureware)

The Interrogator Model  
J. Millen (MITRE)

12:30 SYMPOSIUM ADJOURNS

1995 IEEE Symposium on Security and Privacy //

//

REGISTRATION FORM //

// //

Dates strictly enforced by postmark [not E-mail] //

//

Name: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Affiliation: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

Postal Address: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Phone: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Fax: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

E-mail: \_\_\_\_\_

[Note: Address information will be distributed to attendees]

Please enter the appropriate registration fee below:

Advance Member (to 3/31/95)...\$310 |

| --IEEE Member # (REQUIRED) \_\_\_\_\_

Late Member (4/1/95-4/21/95)..\$370 |

Advance Non-Member (to 3/31/95)...\$385

Late Non-Member (4/1/95-4/21/95)..\$460

Advance Full-Time Student.....\$100

Late Full-Time Student.....\$100 Total amount due: \_\_\_\_\_

Do you wish to present at a poster session or lead an evening discussion?

[ ]Yes [ ]No

Do you have any special requirements? \_\_\_\_\_

Please indicate your method of payment by checking the appropriate box:

Check in U.S. funds drawn on a U.S. bank (PLEASE ENCLOSE WITH THIS FORM)

Credit card authorization:

(Charges will appear on your statement as made by IEEE COMPUTER SOCIETY)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Credit Card Number:

\_\_\_\_\_

Card Holder Name: \_\_\_\_\_ Expiration Date: \_\_\_\_\_

Signature: \_\_\_\_\_

Mail registration to:

Dale M. Johnson  
The MITRE Corporation

Or fax this form (CREDIT CARD

REGISTRATIONS ONLY) to:  
fax #: (617)271-3816

M/S: A156                      voice #: (617)271-2386  
202 Burlington Road  
Bedford, MA 01730-1420    <>>SORRY, NO REGISTRATIONS BY E-MAIL<<

### Evening Sessions

The 1995 IEEE Symposium on Security and Privacy will accommodate poster sessions and evening discussions. There will be rooms with blackboards and bulletin boards for interested parties to post presentations on work in progress, recent research results, and innovative proposals, or to lead discussions on topics of current interest. These rooms will be available Monday and Tuesday, May 8 and 9, from 8 pm to midnight. If you are interested in posting a presentation or organizing a discussion on a particular topic, please indicate so on the registration form.

### Hotel Reservations - The Claremont Resort

The Claremont Resort in Oakland, California is 20 minutes from San Francisco and just over an hour from Napa Valley. It is situated in the Oakland-Berkeley hills overlooking the San Francisco Bay on 22 acres of beautifully landscaped lawns and gardens. Facilities include the Claremont Pool and Tennis Club and The Spa at the Claremont.

Oakland Airport is 14 miles from the hotel, or attendees may choose to fly into San Francisco and rent a car. Bay Area Shuttle (415/873-7771) provides service from the San Francisco Airport or the Oakland Airport to the Claremont Resort. The charge is \$10 per person one way. Parking is available at the hotel at a cost of \$8 per day for guests and a maximum of \$8 per day for non-guests.

Hotel reservations must be made under the group name IEEE Symposium on Security and Privacy. The group rate is \$99 single, \$111 double occupancy, plus 11% tax. The cut-off date for reservations is Saturday, April 8, 1995. Reservations made after this date will be accepted on a space available basis. Reservations must be accompanied by an advance deposit or credit card guarantee. You may cancel your individual reservations up to 72 hours prior to arrival, after which your deposit becomes non-refundable. Please be advised the check-in time is after 3:00 pm; check-out is 12 noon.

For reservations and information, contact: The Claremont Resort, Ashby and Domingo Avenues, Oakland, CA 94623-0363; Phone: 800/551-7266 (7 a.m. to 8:30 pm, PST) or 510/843-3000; Fax: 510/549-8582.



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 16: Issue 81**

**Tuesday 14 February 1995**

## Contents

- [Stolen ATM Card nets \\$346,770](#)  
[David Tarabar](#)  
[Jerome Whittle](#)
  - [Sweden-Pedophiles-Internet](#)  
[Mich Kabay](#)
  - [A RISKy place on the Web](#)  
[Stephen R. Savitzky](#)
  - [Rumors in Cyberspace](#)  
[Adam Shostack](#)
  - [Priests told to keep cell phones out of confession](#)  
[Mich Kabay](#)
  - [Cellular phones](#)  
[Chaim Seymour](#)
  - [Web Page copying reader's system information](#)  
[Brian Leibowitz](#)
  - [RISKS of posting to newsgroups](#)  
[A. Padgett Peterson](#)
  - [Good Pentium Followup](#)  
[Martin Minow](#)
  - [Invisible blue zone](#)  
[Jeff Jonas](#)
  - [RISKS of third-party-billed calls not uncommon](#)  
[Tony Yip](#)
  - [Self-disabling software](#)  
[Jerry Leichter](#)  
[Bob Brown](#)
  - [What "RISKS of Third-Party-Billed Calls"?](#)  
[Gary Beckmann](#)  
[PGN](#)  
[GB](#)
  - [Re: attack scanning](#)  
[Stephen Kelley](#)  
[Frederick B. Cohen](#)
  - [Info on RISKS \(comp.risks\)](#)
-

## Stolen ATM Card nets \$346,770

David Tarabar <dtarabar@hstbme.mit.edu>

Sun, 12 Feb 95 16:39:56 -0500

Thieves broke into a van and stole an Oregon woman's ATM card and discovered her PIN number written on her Social Security card. They then made repeated withdrawals, covering 100 miles and visiting 48 ATM machines over a three day period. (Friday night - Monday 2 AM)

They were able to get \$346,700 in cash with the help of some questionable computer systems.

1) Ordinarily there is a \$200 daily limit for withdrawals, However, "because of a computer program change at the Oregon TelCo Credit Union, the limit was not in effect that weekend."

2) When the account was down to zero, the thieves fed empty deposit envelopes into the machine and credited the account with bogus deposits of \$825,000 -- and then made withdrawals against this sum.

Technology did work in at least one respect. At least 5 of the machines had taken photos of the people using the stolen card. Three persons are in custody and are facing Federal charges.

[From an AP report in the New York Times 12 Feb 1995.]

[Also noted on-line by

Jerry Whittle, Belleville, Illinois <jwhittle@amclg.safb.af.mil>, szabop@tualatin.pen.tek.com (Paul Szabo), "Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>, schaller@hsi.com (Dave V. Schaller), and olsen@Rational.COM (David Olsen), and by snail-mail from Ed Coover at MITRE-McLean VA. PGN]

---

## Stolen ATM Card nets \$346,770

"Whittle, Jerome SMSgt" <JWhittle@amclg.safb.af.mil>

Sun, 12 Feb 95 12:05:00 cst

I see a number of mistakes/risks here.

1. Smith wrote left her purse in a van overnight and wrote down her PIN number.
2. The bank's software allowed withdrawals of over \$200 per day.
3. The bank immediately credited someone's account for a deposit - even a huge amount like \$820,500. My bank doesn't credit my account until the next business day.
4. Only about 10% of the ATM machines had hidden cameras. Had the crooks been a little more lucky, they may have never been caught.
5. Karen Smith isn't liable for the theft even though she left her card and PIN number unsecured. I believe that she should shoulder some of the blame and loss.

Jerry Whittle, Belleville, Illinois <jwhittle@amclg.safb.af.mil>

---

## Sweden-Pedophiles-Internet

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
10 Feb 95 07:42:36 EST

>From the Associated Press news wire via CompuServe's Executive News Service:

APn 02/06 1228 Sweden-Pedophiles-Internet  
By THOMAS GINSBERG  
Associated Press Writer

STOCKHOLM, Sweden (AP) -- Pedophiles have found a home on the Internet and exchange hundreds of pictures a week through anonymous conduits, a researcher said Monday.

The statistics provided a glimpse at the scope of the potentially illegal activity, which police fear can lure kids into sex. It came from a study by Mats Wiklund, a researcher at Stockholm University's Institute of Computer and System Science.

During a seven-day period in late December and early January, Wiklund counted 5,651 messages or postings about child pornography in four electronic "bulletin boards."

The author makes the following key points:

- \* Many graphics showed what appeared to be "adolescents engaged in sexual acts." A few showed young children, apparently to attract the interest of other pedophiles.
- \* The messages tracked and counted were a fraction of the total traffic, since Wiklund was unable to track private e-mail and scanned only about half of the porn-related groups he knew of.
- \* Most of the pornographic messages were sent through the anonymizing server located in Finland.
- \* The Internet offers advantages to pedophiles:

"The Internet has become a channel of communication for pedophiles," Wiklund said. "From their point of view, they've found a green technology. You can be anonymous and still be reached."

- \* Exchanging pornography electronically is a crime in many areas of the world:

In most countries the distribution of child pornography is illegal. Two years ago, U.S. police raided about 40 locations

where people were exchanging child pornography by computer. Two Danes were convicted in 1993 of transmitting child pornography to an estimated 6,000 people worldwide.

\* 85% of the messages Wiklund scanned were fantasies about sex with children or technical tips on how to transmit pornographic pictures.

\* Law enforcement officials are still unsure of how to handle this traffic:

Finnish detective Sgt. Timo Laine said it was unclear whether the country's laws would apply to "electronic smuggling" by computer. He said did not know whether police would take action against the computer owner in Finland.

"We've never had this kind of case before," Laine said. "If I transmit this information through the Internet, is it considered smuggling?"

M.E.Kabay, Ph.D., Director of Education, Natl Computer Security Assn (Carlisle, PA); Mgmt Consultant, LGS Group Inc. (Montreal, QC)

---

## A RISKy place on the Web

*Stephen R. Savitzky <steve@cache.crc.ricoh.com>*

*Tue, 14 Feb 95 15:14:36 -0800*

There was an announcement in misc.kids.computers yesterday that, at first glance, appeared to be just what it said: "a communication playground for children ages 8-12". The full text of the announcement is quoted below:

KidsCom, a communication playground for children ages 8-12 is up and running. Kids can find key pals, get help with Internet questions from an Internet guru, talk about what they'd like to be when they grow up, explore links to other children's sites, enter sweepstakes to win prizes, and give feedback on what they'd like to see and do on the Internet.

<http://www.spectracom.com/kidscom/>

For more info, please email [kidscom@spectracom.com](mailto:kidscom@spectracom.com)

What they didn't mention, however, was that before you can "play" you have to fill out a form that asks for: name, address, e-mail address, demographic information, \*and a password\*! Some people are already advising kids against giving out their names and addresses on the Net; this goes \*much\* farther.

There are at least two risks here, the most obvious being the risk (almost a certainty) of ending up on some direct marketer's mailing list. The other one is the usual one of sending passwords in the clear: what if the kid has an account on a Unix system somewhere (mine does, on our Linux box at home), and what if they use the same password in both places?

Now, the folks at SpectraCom may simply not have thought about the potential

consequences of what they're doing; their description of the company as

a full service research, strategic planning and communications company that specializes in conveying information in an understandable and actionable way. ^^^^^^^^^(sic)

would seem to indicate as much. But the same technique could be used by someone trolling for easy systems to crack. It would work even better on adults, of course, and the next bunch might ask for a 4-digit number instead of a password...

Hey, kid, want a free lollypop? Just fill out this form...

Steve Savitzky h:steve@starport.com 408-294-6492 <http://www.rahul.net/starport/w:steve@crc.ricoh.COM> 415-496-5710 <http://www.crc.ricoh.com/~steve/>

---

### Rumors in Cyberspace (Kabay, [RISKS-16.79](#))

*Adam Shostack <adam@bwh.harvard.edu>  
Thu, 9 Feb 1995 16:15:32 -0500 (EST)*

In [RISKS-16.79](#), Mitch Kabay writes:

> ... Now imagine this rumour spreading through cyberspace, aided by  
> anonymous postings ...

While there may be risks in anonymous postings, spread of rumors really doesn't seem to be one of them. The "Good Times" virus of a few months back spread without going through anonymizing services. This is to be expected of the way rumors spread. People who saw and spread the virus did so because they heard it from people they knew.

Attempts to spread rumors through anon. services will be subject to much more fact checking and consideration than 'normal' rumors. News and mailing lists do just fine in causing runaway rumor spread. There's no little that anonymous servers will do to change that.

Adam

---

### Priests told to keep cell phones out of confession

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
09 Feb 95 07:51:57 EST*

>From the Reuters news wire via CompuServe's Executive News Service, yet another unexpected technological interference with a religious process:

RTw 02/08 0749 Priests told to keep cell phones out of confession

ROME, Feb 8 (Reuter) - Even Italians who religiously carry their cellular phones while dining in restaurants or jogging

in forests might draw the line against priests using them in the confessional box.

An Italian Catholic magazine has told priests who own such phones to keep them out of the confessional box or at least turn them off while administering the sacrament to the faithful.

It seems the February editorial in *\_Vita Pastorale\_*, a monthly magazine for parish priests, cited a case in which a woman complained after her priest's cell phone rang during her confession.

A cartoon in the left-leaning daily *La Repubblica* showed a priest in a confessional box holding a cellular phone to his ear while simultaneously hearing a member of the faithful confess.

"Say three Our Fathers and three Hail Marys...No, no I wasn't talking to you," the priest says to the caller.

M.E.Kabay, Ph.D., DirEd, Natl Computer Security Assn (Carlisle, PA);  
Mgmt Consultant, LGS Group Inc. (Montreal, QC)

---

## Cellular phones

*Chaim Seymour <seymour@ashur.cc.biu.ac.il>*  
*Sun, 12 Feb 1995 15:28:20 +0200*

Re: M.E. Kabay's posting. The official Israeli term for Cellular phones:

The term 'pelephone' means 'wonder phone' and not 'miracle phone'.

It is generally used and is not peculiar to Rabbis.

Chaim Seymour, Chairman, Cataloguing and Classification Dept, Wurzweiler Library, Bar-Ilan University, Ramat Gan 52100 Israel Tel: 03-5318127

---

## Web Page copying reader's system information

*Brian Leibowitz <bml@netcom.com>*  
*Fri, 10 Feb 1995 09:40:37 -0800*

I found this on the edupage newsletter.

\*\*\*\*\*

Edupage, a summary of news items on information technology, is provided three times each week as a service by Educom -- a Washington, D.C.-based consortium of leading colleges and universities seeking to transform education through the use of information technology.

\*\*\*\*\*

### ONLINE SPYING

While you're connected to your favorite Web page, it's also connected to you, and could be copying all sorts of information off your hard drive, say

industry experts. In fact, it happened last year when Central Point Software used registration software developed by Pipeline Communications, and inadvertently also gathered descriptions of the users' systems -- the type of microprocessor, the version of DOS and Windows, the type of display and mouse, and the amount of free space available on the hard drive. Customers squawked, and Central Point had Pipeline change the software. However, Pipeline reports that at least one of its clients is using the scanning feature now -- but only after getting the owner's permission. The lesson? "If you can't trust it, don't connect to it." (Forbes 2/13/95 p.186)

Brian Leibowitz bml@netcom.com

---

## RISKS of posting to newsgroups

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>

Thu, 9 Feb 95 11:43:59 -0500

>From: UVS1::"daemon@anon.penet.fi" 8-FEB-1995 22:25:48.89

>To: padgett@tccslr.dnet.mmc.com

>CC:

>Subj: Anonymous code name allocated.

>You have sent a message using the anonymous contact service.

>You have been allocated the code name an199742.

>You can be reached anonymously using the address

>an199742@anon.penet.fi.

>If you want to use a nickname, please send a message to

>nick@anon.penet.fi, with a Subject: field containing your nickname.

>For instructions, send a message to help@anon.penet.fi.

This arrived in my morning mail. Seems someone has either subscribed to the FIREWALLS newsgroup or set up a mail forwarder such that anyone posting to the FIREWALLS group is automatically granted an "anonymous" account.

Since ANON.PENET.FI is generally believed to have been compromised some time ago and all accounts/real user names extracted, this could be an attempt by someone wanting to discredit any such list (wonder if the numbers are assigned sequentially).

Personally, I have no use for such an account and did not request it (why I did not bother to obscure the account number), just one reason being that "Security by Obscurity" has been proven not to work in the long term, another being that I would consider certain domestic agencies lax if they were not monitoring international gozintas and gozoutas. Of course, on the gripping hand (literary plug) this may have a plus in that anyone who receives an account this way probably did not have one before. 8\*)

Padgett

---

## Good Pentium Followup

*Martin Minow <minow@apple.com>*

*Thu, 9 Feb 1995 16:45:22 -0800*

In IEEE Spectrum, February 1995, there's a good overview of the Pentium problem, including a reasonable amount of technical detail and links to several technical papers.

Of particular interest to Risks readers is the author, Linda Geppert's, conclusion:

"These scientists and others did all of us a service by digging deep into the causes and ramifications of the bug and so precipitating Intel's no-questions-asked replacement policy. But in the process they spent valuable time and effort on something that could have been a non-problem, had Intel been more forthcoming."

Martin Minow minow@apple.com

---

## Invisible blue zone

*Jeff Jonas <jeffi@panix.com>*

*Tue, 14 Feb 1995 18:29:13 -0500 (EST)*

With all the outcry about people not knowing what phone calls cost, this is somewhat related in that people are assumed responsible for knowledge that is not readily available.

In a TV "Shame On You" report, it was shown that an entire area of lower Manhattan, New York is a "Blue Zone" where the curb is SUPPOSED to be painted blue and have signs that tell that there's no parking and it's a tow away zone. Well, there are entire blocks with NO signs or paint on the curbs. The traffic department issued tickets from US \$55 to \$200 if towed. Appeals are useless as even a reporter with the parking commissioner was told that "leaflets were distributed". Yea - back in 1988. Traffic court simply found everyone 'guilty'. So now the leaflets are being distributed, along with the parking ticket. So even when there's no notification or warning, New York City's Parking Violations Bureau doesn't back down and gets to keep your money. At least with the phone companies, folks seem to be getting refunds.

Now jump to the computer network world. There are many newcomers spamming USENET with posting to EVERY newsgroup (some apparently use some script as they're too thorough to post to EVERY newsgroup so fast, and some even crosspost to 8-10 groups at a time). When informed "you should not do that", some reply "nobody told me it was wrong, were was I to find out?".

I'm not sure of the balance of abiding by the rules that you never read vs "how was I supposed to know?". (Ex: "I never knew murder was illegal" is no defense anywhere I know.)

There are cancel-bots used to filter out internet abusers. I'm concerned about a denial of service attack. Let's say somebody forges my header and spams the network. The cancelbots then cancel those postings and I'm essentially barred from the internet. Unless I get replies that I'm being blocked, I have no way to know to appeal (let alone to whom) and I must get a new network identity to ever reachieve connectivity. My apologies if the cancelbot control is already centralized and fair, but I fear that I may be blocked with no way to appeal, even if wrongly accused. I guess this boils down to internet connectivity being a privilege, not a right.

-- Jeffrey Jonas jeffj@panix.com

---

### **RISKS of third-party-billed calls not uncommon (Altman, [RISKS-16.80](#))**

*"Tony Yip, 431-3183, F13" <TONYY@ola.bc.ca>  
Mon, 13 Feb 1995 15:06:16 -0800 (PST)*

I find that a reader's experience with PacBell's third party billed policy not uncommon. Living in Vancouver, BC, I've had to call BC Tel periodically (meaning once every year or two depending on my luck) to credit my bill with third party calls that I did not make.

It appears that BC Tel rarely verifies third party calls. In other words, anybody can pick up a pay (or any other) phone, dial the operator and request a long distance call to be billed to a third phone number that they make up. The operator may ask for the caller's name but, again, that is not verified so any name will do.

I am not certain but I believe the route BC Tel takes is that if they cannot collect from the caller (i.e. the person who gave a phony name and third party number), they will try to collect from the number that was called.

The first risk is the overall reactive approach to chase down fraud after it has occurred with no attempt to prevent it. In other words, the onus is on the customer to check if his/her telco has made a billing mistake. In a large family with several teenagers, this type of bill checking for erroneous third party calls is quite impossible.

The second risk is attempting to collect from the called party. What if the long distance call is a nuisance call from an ex-spouse? Or a \$200 long distance call from old school mates or friends or whoever (and you thought they were so nice to call you!)... The list goes on. And what about the legal implications of asking people to pay for calls that they did not initiate nor authorize?

But...there is no outcry so I guess the problem is not serious enough to warrant drastic action.

---

### **Self-disabling software (Epstein, [RISKS-16.79](#))**

Jerry Leichter <leichter@lrw.com>

Mon, 13 Feb 95 17:25:18 EDT

In [RISKS-16.79](#), Jeremy Epstein describes a proposed Virginia law requiring that companies notify customers if the software they sell has a self-disabling feature (e.g., after some period of time). The law would apparently not ban such features.

Mr. Epstein then lists two potential risks:

- a) Does informing people that the software is self-disabling encourage them to try to subvert the feature?

I'm actually rather surprised that anyone would consider these to be *\*risks\**. Is it a bad idea to inform people that they are liable for no more than \$50 in charges on their credit cards a bad idea because it encourages them to be careless with their cards? Does telling them their cars have dual-redundant brakes encourage them to experiment with their master cylinders?

There are certainly good arguments for and against banning self-disabling software to begin with. But if it's to be allowed, requiring fair notice to those who receive the software certainly seems very reasonable. If this perhaps makes life a bit tougher for those whose view of doing business is "Well, if the customer doesn't pay up, I'll *\*really\** screw him," isn't that just too bad?

- b) If someone did and that triggered the disable feature, would that come under the law?

It's beyond me what could be in the law that such tampering could possibly "come under". Even if the idea is that people could get themselves into trouble by such tampering, which they would not have been tempted to try without the required disclosure - is there really any reason why the law should try to protect those individuals who are not only dishonest but incompetent to boot?

Mr. Epstein continues: And what if it were used in safety critical systems: "I'm sorry, but the license period on the software in your heart monitor has expired. Please contact the vendor to reenable."

I am at a loss as to what this has to do with the proposed law, vague as the description we have of it might be. Is Mr. Epstein upset because the law doesn't simply ban self-disabling features? It also doesn't ban murder, but so what. A general ban on self-disabling features might require some tough arguing, but a ban on such features for safety-critical systems would be much harder to oppose. In any case, I would think it's hardly necessary: The liability if a deliberate action led to a serious injury or death would be enormous. I should think any lawyer would quite properly have no trouble convincing a jury that the installation of code to disable a heart monitor constituted depraved indifference to human life, among other nasty things - with or without notice.

-- Jerry

## **Self-Disabling Software (Epstein, [RISKS-16.79](#))**

*Bob Brown <bbrown@dkmc.org>*

*Thu, 9 Feb 95 00:01:45 EST*

Jeremy Epstein ([RISKS-16.79](#)) sees a risk in a proposed Virginia law requiring disclosure of self-disabling features in software for sale. Such a law is actually an extremely good idea and a reducer of risks. Many reputable companies, e.g. the SAS Institute, use self-disablers as a way of enforcing their license agreements. Unhappily a small number of disreputable companies have used the same technique to sandbag buyers in the event of a contract dispute. With regard to Mr. Epstein's example of medical monitoring software (ahem) expiring, aren't the RISKS substantially reduced of one knows beforehand that this is going to happen on a given date?

---

## **What "RISKS of Third-Party-Billed Calls"? (Altman, [RISKS-16.80](#))**

*Gary Beckmann <beckmann@world.std.com>*

*Tue, 14 Feb 1995 10:59:07 -0500*

Micah Altman writes about a "risk" of 3rd party calls in [RISKS-16.80](#). However, this has always been SOP as far as I am aware. It was an oft used method of making long distance calls when I was in college. Generally, since I was calling from a listed number, the operator would "take my word for it". My parents would check the phone bill when it came. If they protested a call then the charge would be made to the number I called from. If you call from a pay phone, the operator will verify before charging the number you request.

The only risk is the good ol' risk of not checking you bill when it comes in the mail. At least we have that, the eight years I lived in Austria I never got an itemized bill. You took the Post/Telephone Company's word for it!!! Now, there was a risk!

Gary Beckmann

---

## **Re: What "RISKS of Third-Party-Billed Calls"? (Beckmann, [RISKS-16.81](#))**

*Peter G. Neumann, Moderator <risks@csl.sri.com>*

*Tue, 14 Feb 95 8:53:03 PST*

You are correct that it is not new. But practice a few years ago was NEVER to accept a third-number charge unless it was verified live by the third party. With the new automated servers, that has been abandoned. The savings in fewer operators seems to offset the losses.

---

## **Re: What "RISKS of Third-Party-Billed Calls"? ([RISKS-16.81](#))**

Gary Beckmann <beckmann@world.std.com>

Tue, 14 Feb 1995 15:53:52 -0500

So the question, then, is for whom is the risk? The customer who doesn't read the bill? The telephone carrier who swallows the cost of fraud? The operators who are losing their jobs?

---

**Re: attack scanning (Cohen, [RISKS-16.80](#))**

Stephen Kelley <kelley@vet.vet.purdue.edu>

Mon, 13 Feb 95 15:43:47 -0500

- Management Analytics is offering (in a test mode only) the ability to
- scan sites over the Internet for well-known over-the-wire security holes.

What assurance is there that the results mailed back to the system administrator actually match the result of the test?

Send us the name of a computer you're worried about and we'll try to break in. If we can, we'll tell you about it. Really, we will.

Not my computers, thanks just the same.

Steve Kelley, Purdue University Cytometry Laboratories

---

**Re: attack scanning (Kelley, [RISKS-16.81](#))**

"Dr. Frederick B. Cohen" <fc@all.net>

Mon, 13 Feb 1995 16:11:50 -0500 (EST)

- > What assurance is there that the results mailed back to the
- > system administrator actually match the result of the test?

These are all tests you can perform yourself using public domain software (for the most part). The service is just a convenience for checking against external attack from an external location. But even more importantly, it helps test your detection capability.

- > Send us the name of a computer you're worried about
- > and we'll try to break in. If we can, we'll tell you
- > about it. Really, we will.

Really!

- > Not my computers, thanks just the same.

You are very welcome to use it or not at your discretion.

FC



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 16: Issue 82**

**Friday 17 February 1995**

## Contents

- [New York Parking Meters In Violation of Federal Law](#)  
[A. Padgett Peterson](#)
- [Big Brother in the Big House](#)  
[Peter Wayner](#)
- [Computer aids in predicting death](#)  
[Lauren Wiener](#)
- [Hacker Mitnick arrested](#)  
[Jim Griffith](#)
- [Computer addiction and the 6 O'Clock News](#)  
[Rob Slade](#)
- [New Area Codes & PBX Programs](#)  
[Mich Kabay](#)
- [E-mail risks](#)  
[Vincent Gogan](#)
- [Re: Self-disabling software](#)  
[Bruce Johnson](#)
- [Re: Invisible blue zone](#)  
[David Stodolsky](#)
- [CERT Advisory CA-95:04.NCSA.http.daemon.for.unix.vulnerability](#)
- [Info on RISKS \(comp.risks\)](#)

---

### New York Parking Meters In Violation of Federal Law

*A. Padgett Peterson* <[padgett@tcslr.dnet.mmc.com](mailto:padgett@tcslr.dnet.mmc.com)>  
*Wed, 15 Feb 95 15:32:24 -0500*

Re: Notification on Self-Disabling Software (Jeremy Epstein)

This leads naturally to the following item:

(1998): In a surprise move, federal marshals yesterday seized nearly nine million parking meters in New York City, citing violation of the Software Disability Act of 1996. Consumer advocates praised the move, saying "the meters all stopped working when the time ran out." The Parking Violations

Bureau issued protests that "all motorists in NYC on were issued a notice on 1 April 1975, along with the courtesy windshield cleaning." However, these protests were not accepted, because the majority of motorists ticketed were not old enough to have had licenses at the time.

[I guess April comes early in 1995. PGN]

---

## Big Brother in the Big House

*pcw@access.digex.com <Peter Wayner>  
Wed, 15 Feb 95 21:55:36 PST*

The WSJ has a big article on the prison phone call business on Wednesday, February 15, 1995. The article discusses how the major long-distance companies court prisons because prisoners have nothing better to do than spend heavily on phone calls.

But supplying phone service to prisons is not a risky job, because convicts have a habit of phone and credit card fraud. They'll call an outside phone number at random, con the person who answers into giving out a credit card number, and then use that number to order goodies for themselves.

So, many prisons require the phone-service providers to provide anti-fraud measures, which include tape-recording equipment and voice-print identification. Some prisoners have their access to phones restricted, and they try to use someone else's access codes. The voice print identification can nab these guys. The technology is now being deployed.

All of this avoids the question of just what is prison in a world where the apartments are smaller and telecommuting is more popular. If prisoners can dial out, conduct business, and even access the net, the walls seem filled with virtual loopholes.

[This also gives new meaning to "Reach out and touch someone." PGN]

---

## Computer aids in predicting death

*Lauren Wiener <lauren@reed.edu>  
Thu, 16 Feb 95 21:28:46 -0800*

>From \_The Oregonian\_, 16 Feb 1995, p. D11:

Computer Aids in Predicting Death, by Mike Koller, AP, Philadelphia

[...] Using a new program, researchers say they are able to predict when a terminally ill person will die with more accuracy than doctors using their own judgment. The study could help doctors determine which treatments should be given to terminally ill patients and help decide when life-support efforts should be stopped. "The computer remembers thousands and thousands of cases and keeps the different risk factors in perspective," said Dr. William A. Knaus of George Washington University. Knaus led the study,

published in the Jan. 31 issue of the Annals of Internal Medicine. "And when we included the survival estimate from the patient's own physician in the model, the two together predicted time until death more accurately than either alone," he said. The program was developed from June 1989 to June 1991, using information from 4,301 patients. It was tested from January 1992 to January 1994 on 4,028 patients, Knaus said.

The program, called SUPPORT (Study to Understand Prognoses and Preferences for Outcomes and Risks of Treatments), focused on nine diseases and conditions, such as liver disease, colon or lung cancer, heart or lung disease and multiple organ failure. Knaus said he was confident that Support will prove reliable and eventually be expanded to predict death rates for other diseases. Seriously ill patients with a projected life expectancy of six months were entered in the study when they were hospitalized. [...]

"Most adults say that if they are going to die within a year, they want realistic estimates of their risks, both in the immediate future and during the next few months," Knaus said. "This predictive tool is important for its use for counseling very sick patients and their families."

However, not everyone agrees. Toby Gordon, vice president for planning and marketing at Johns Hopkins Hospital and Health Systems in Baltimore, said the program raises questions. "Any information that helps us learn how to better take care of patients -- in quality of care and quality of life -- makes a contribution," Gordon said. "But whether patients and their families will want to use it is questionable." He also questioned the ramifications of being able to accurately predict death. "In the expansion of computer-assisted technology we will see a proliferation of these techniques, bringing into question ethics and rationing of care," he said.

The authors warned that the project has not been tested outside the strictly controlled settings of teaching hospitals. Its reliability in conventional hospitals settings has not been established, they said.

---

## Hacker Mitnick arrested

*Jim Griffith <griffith@netcom.com>*

*Thu, 16 Feb 1995 23:37:24 -0800*

KCBS Radio (San Francisco) reported tonight that The Well and Netcom combined efforts, resulting in the arrest of 31-year-old hacker Kevin Mitnick in Raleigh North Carolina. Both companies discovered large caches of data being stored on their systems. At the same time, "a well-known San Diego consultant" discovered security breaches in his system. This led to vigorous efforts to track the hacker, and after 24-hour electronic surveillance and at least one cellular phone trace, law enforcement officials arrested Mitnick. Mitnick's early escapades are chronicled in the book *\_CYBERPUNK\_* by Katie Hafner and NY Times reporter John Markoff, and, in fact, Mitnick is accused of breaking into Markoff's computer.

Mitnick, a fugitive from justice, faces up to 30 years in prison for various

crimes, including allegedly breaking into NORAD computers. Law enforcement officials are now wrestling with jurisdictional issues, as Mitnick is wanted for crimes in at least six different jurisdictions.

[See excellent articles by John Markoff in *\*The New York Times\**, 16 Feb (TWO) and 17 Feb 1995. I could not begin to excerpt these three long articles, and of course cannot include them in their entirety. But they are very well done. PGN]

---

## Computer addiction and the 6 O'Clock News

*"Rob Slade, Social Convener to the Net" <roberts@mukluk.decus.ca>  
Thu, 12 Jan 1995 15:09:02 EST {[TIMELY!} Yes, we are backlogged!]*

Hello, my name's Rob, and I'm a ... a ... Netaholic.

They tell me a lot of you have a story like mine. It started out with a committee and someone at the local university offered me an account, just to keep in touch, you know? Then, somebody introduced me to "Computers and Society". I could handle that: it only came every week or so. Then I got into RISKS-FORUM and the IBM-PC Digest. That pretty much guaranteed something every day! I was really smokin', man! I thought I was just King Modem!

In order to feed my habit, I started pushing. I was porting Info-Mac to local bulletin boards for access.time. I started doing unmoderated lists. Then a friend turned me on to Usenet. By this time, I was doing about a half a meg a day.

I was hooked, but I wouldn't admit it. I told myself it was all job-related. I only read VIRUS-L in order to flog my book. But why did I have alt.best-of- usenet in my .newsrsrc? My wife took to asking, "Is that in real time or computer time," when I said I'd be offline in ten minutes.

I didn't recognize the danger signs. I could tell people the first alt.adjective.noun.verb.verb.verb group. My wife left me when I started introducing myself at parties as, "Hi! roberts@decus.ca. What's your group?" I started talking familiarly about people that my friends in Vancouver had never met. I started hoarding accounts. When I found out I could never match Bill Murray's two full columns on a business card, it was a real bad trip. I crashed for a week.

Then, it all fell apart. My access provider started to go flaky. I tried Fidonet, but it just wasn't the same. I ... I ... started reviewing Internet books. It wasn't a pretty sight. Soon, I had two bookshelves completely full. *\*And\** that little pile behind the door where I thought no one could see ...

I finally realized I needed help. As part of the twelve-step process, I'm telling my story in public. And I'm going to bust up my modem ... as soon as I do this one more posting ...

---

Yes, I'm sarcastic. It's an addiction, OK?

Yes, I believe we can all admit that computers can be very addictive. Programming, itself, is as "moreish" as salted peanuts--and often has a similar effect on the waistline. Computers are relatively inexpensive, give results with minimal training, are completely under the control of the user (why else call them "personal" computers?) and don't require any particular considerations. But do they \*cause\* addiction?

Our society seems to be not merely predisposed to, but actually encouraging of, obsessive behaviour. The evidence is not limited to lone psychopaths, the drug culture, cults and tragedies such as anorexia nervosa. Amateur "athletes" who constantly require medical intervention are considered normal. We don't \*really\* believe that a workaholic is a problem. We expect scientists to have no idea of culture and artists to have no idea of technology.

Another newswire report of computer addiction, therefore, adds no new information to the study. We all know computers can be attractive--but we all know that there is a difference between the fellow (usually male, isn't it?) who runs up enormous bills on the Compuserve CB simulator, and those of us whose work or study requires as much online correspondence as we can afford to give. In many cases, the computer is not a cause but merely a means. If it were not the computer, it would be something else. Recently a co-worker happened to drop the comment that he didn't watch much TV--only about five hours a day. If that is OK (or even "not much"!)" can I spend five hours a day with the modem? (Can I add an hour for social utility? As long as I promise not to use Mosaic?)

I am \*not\* saying that computer addiction cannot be a problem. If it is, however, let us give some thought to isolate and identify the difference.

=====

DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733

---

## **New Area Codes & PBX Programs**

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
17 Feb 95 15:11:06 EST*

An AP item on 17 Feb 1995 reported that many businesses in Washington state and Alabama are having trouble receiving phone calls since new area codes were introduced last month. The new area codes, 360 in western Washington and 334 in Alabama, are the first in the country not to use a one or zero as the middle digit. The item reports that PBXs reject area codes that include anything but a 0 or a 1 in the middle position. The problem will worsen when additional area codes are installed in, among other regions, Los Angeles, Denver, and Tampa.

M.E.Kabay,Ph.D., Director of Education, Natl Computer Security Assn  
(Carlisle, PA); Mgmt Consultant, LGS Group Inc. (Montreal, QC)

---

### **E-mail risks (risk of many mail programs)**

*Vincent Gogan <vincent@cs.toronto.edu>*

*Wed, 15 Feb 1995 14:54:36 -0500*

Most mail programs that I have dealt with share a flaw... they don't indicate to whom a message will be actually sent.

This became particularly evident this Valentine's Day when I received a very warm personal note thanking me for some beautiful flowers and indicating how I always knew how to make this women happy. This came as quite a surprise to my wife (and myself)!

... Many a sitcom episode has started with a weaker premise than this. Luckily, my wife would never have fit in with the Three's Company crowd and all is well.

Still, this probably happened because of quite a simple error. This women either typed in an alias/nickname that didn't work or just typed the first name of her suitor instead of his account name. In either case, the mail program should have indicated to whom the message would be sent. For local addresses (as this was), the actual name of the recipient (as opposed to the account name) should be indicated.

Vincent Gogan vincent@cs.toronto.edu

---

### **Re: Self-disabling software (Leichter, [RISKS-16.80](#))**

*"Bruce Johnson" <JOHNSON@tonic.pharm.arizona.edu>*

*Thu, 16 Feb 1995 11:40:28 MST*

If a third party triggers the disable feature, or, even under the right circumstances, the owner of the software (ie: the client has paid, but you disable it anyway) that is a felony in most states, theft by control; ie : embezzling. If you hold the software to ransom through such an act, it's also a felony.

As a side note...this was used as a plot device in the movie "Single White Female" a few years back, as a revenge sub-plot.

Bruce Johnson, University of Arizona, College of Pharmacy  
Information Technology Group

---

### **Re: Invisible blue zone (Jonas, [RISKS-16.81](#))**

*David Stodolsky <david@arch.ping.dk>*

Thu, 16 Feb 95 23:03:51 +0100 (CET)

> The cancelbots then cancel those postings and I'm essentially barred from  
> the internet.

Cancelbots are not normally being used to cancel spams. The articles are typically selectively cancelled, often one copy will be left in a newsgroup in which it is "on-topic". Non-spam posts by the same sender are not affected.

[Also noted by roeber@vxcern.cern.ch (Frederick G.M. Roeber). PGN]

However, there is now a Call for Discussion (CFD) about reorganization of the news hierarchy. This could, among other things, create a moderated newsgroup, news.admin.net-abuse.announce, for the posting of announcements, etc., related to abuse. Opponents fear that a moderated group would give the announcements a stamp of authority that would lead to attacks on the apparent abusers.

Axel Boldt is maintaining an "Internet Advertisers Blacklist" To quote a draft FAQ, "Administration of Cancel Messages": Axel Boldt <boldt@math.ucsb.edu> should be notified about abusive advertisers, so they can be added to his Internet Advertiser's Blacklist. Please use the word "Blacklist" somewhere in the subject line. Make sure to check the last version of the List first, so that he won't get multiple complaints about incidents already covered. The newest version is always available over the WWW at URL: <http://math-www.uni-paderborn.de/~axel/blacklist.html>.

> ... I have no way to know to appeal (let alone to whom) and I must get

Fears of this development have led to the organization of the NetNews Judges (TM) List (this is a reformatted InterNIC resource entry):

=====

Judges-L - NetNews Judges List

Resource Type: Mailing list

Description: The Judges' List distributes messages to a panel of Judges who cancel multiple posts to NetNews immediately. The List is used to help Judges organize themselves, finalize policy, and set procedures to enforce rules. It is primarily directed to those who issue cancels. Secondarily, to those who survey cancels issued, in order to ensure that the cancel facility is not being abused. The protection of the NetNews system from overload by posts to multiple newsgroups is the focus of activity.

Access: Messages go to: Judges-L@UBVM.cc.buffalo.edu.

Subscriptions go to: LISTSERV@UBVM.cc.buffalo.edu.

Services: Dispute Resolution:

Complaints are primarily about spam, multiple off-topic

posts. Posters may also complain about inappropriate cancels. An opinion is reached via a consensus decision-making procedure based upon private deliberations in which all parties may participate.

Preparation of Periodic Posts:

Frequently Asked Question (FAQ) lists are prepared to inform users about appropriate use of cancel messages, how to file complaints, how the List processes complaints, etc.

Keywords: posting software, law, security mechanism, control message, freedom of speech, censorship, due process, advertisement, chain letter, rumor, conflict resolution, forgery, infection, news administration, kill file

David S. Stodolsky, PhD \* Social \* Internet: david@arch.ping.dk  
Tornskadestien 2, st. th. \* Research \* Tel.: + 45 38 33 03 30  
DK-2400 Copenhagen NV, Denmark \* Methods \* Fax: + 45 38 33 88 80

---

## **CERT Advisory CA-95:04.NCSA.http.daemon.for.unix.vulnerability**

*CERT Advisory <cert-advisory@cert.org>  
Fri, 17 Feb 1995 17:36:01 -0500*

[Also, see CA-95:03, February 16, 1995, Telnet Encryption Vulnerability, if you are using Berkeley Telnet with the experimental Telnet encryption option using the Kerberos V4 authentication. PGN]

CA-95:04                      CERT Advisory  
                                February 17, 1995  
                                NCSA HTTP Daemon for UNIX Vulnerability

The CERT Coordination Center has received reports that there is a vulnerability in the NCSA HTTP Daemon V.1.3 for UNIX. Because of this vulnerability, the daemon can be tricked into executing shell commands.

If you have any questions regarding this vulnerability, please send e-mail to Beth Frank at the NCSA, efrank@nca.uiuc.edu.

### I. Description

A vulnerability in the NCSA HTTP Daemon allows it to be tricked into executing shell commands.

### II. Impact

Remote users may gain unauthorized access to the account (uid) under which the httpd process is running.

### III. Solution

The following solution was provided by the HTTPD Team at SDG at NCSA.

#### Step 1:

In the file httpd.h, change the string length definitions from:

```
/* The default string lengths */  
#define MAX_STRING_LEN 256  
#define HUGE_STRING_LEN 8192
```

to:

```
/* The default string lengths */  
#define HUGE_STRING_LEN 8192  
#define MAX_STRING_LEN HUGE_STRING_LEN
```

#### Step 2:

Install the following patch, which performs the functionality of strsubfirst (i.e., copy src followed by dest[start] into dest) without the use of a temporary buffer.

---[Lengthy patch deleted for RISKS. Contact CERT FOLKS. PGN]---

After you apply this patch, recompile httpd, kill the current running process, and restart the new httpd.

[The CERT Coordination Center thanks Steve Weeber, Carlos Varela, and Beth Frank for their support in responding to this problem.]

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in Forum of Incident Response and Security Teams (FIRST).

If you wish to send sensitive incident or vulnerability information to CERT staff by electronic mail, we strongly advise that the e-mail be encrypted. The CERT Coordination Center can support a shared DES key, PGP (public key available via anonymous FTP on info.cert.org), or PEM (contact CERT staff for details).

Internet E-mail: cert@cert.org

Telephone: +1 412-268-7090 (24-hour hotline)

CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4),  
and are on call for emergencies during other hours.

Fax: +1 412-268-6989

Postal address: CERT Coordination Center  
Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213-3890  
USA

CERT advisories and bulletins are posted on the USENET newsgroup

comp.security.announce. If you would like to have future advisories and bulletins mailed to you or to a mail exploder at your site, please send mail to [cert-advisory-request@cert.org](mailto:cert-advisory-request@cert.org).

Past advisories, CERT bulletins, information about FIRST representatives, and other information related to computer security are available for anonymous FTP from [info.cert.org](http://info.cert.org).

CERT is a service mark of Carnegie Mellon University.



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 16: Issue 83**

**Tuesday 21 February 1995**

## Contents

- [Denver's Computerized Baggage System Finally Works](#)  
[NYT via Edupage](#)
- [Cyberbandits in Europe](#)  
[CommunicationsWeek via Edupage](#)
- [Perfect \(?\) Office Bug can cause harm](#)  
[Gary Gillard](#)
- [I can't help but say more about this addiction thing.](#)  
[Peter Ladkin](#)
- [Sparc10 keyboards and resetting the CPU](#)  
[Carlos M. Puchol](#)
- [Married by computer](#)  
[Scott Sterner](#)
- [UPS not quite so uninterruptable after all](#)  
[Mark Frank via Jerry Leichter](#)
- [Risks of generalized designs](#)  
[Jim Griffith](#)
- [Stolen ATM Card nets \\$346,770](#)  
[Rich Wells](#)
- [Re: JUDGES-L](#)  
[Peter da Silva](#)
- ["PGP: Pretty Good Privacy" by Garfinkel](#)  
[Rob Slade](#)
- [The Coming Plague](#)  
[Peter Wayner](#)
- [Scan results](#)  
[Frederick B. Cohen](#)
- [Symposium on medical records](#)  
[Phil Agre](#)
- [NCSA Conference: Security on the I-Way](#)  
[Mich Kabay](#)
- [Info on RISKS \(comp.risks\)](#)

---

**Denver's Computerized Baggage System Finally Works**

*Edupage <info@ivory.educom.edu>*

*Sun, 19 Feb 1995 20:11:21 -0500*

Denver's new high-tech airport appears finally ready for operation later this month, after four false delays caused primarily by a malfunctioning computerized baggage handling system. The system now seems to be working -- but a \$50 million conventional baggage handling has been built as a backup, just in case the computerized systems should fail again. (\_The New York Times\_ 19 Feb 1995, p.12) [From Edupage 19 Feb 1995]

---

## **Cyberbandits in Europe**

*Edupage <info@ivory.educom.edu>*

*Sun, 19 Feb 1995 20:11:21 -0500*

CommunicationsWeek International reports that computer crackers have been giving European network managers a hard time recently. Among their transgressions are stealing \$150,000 worth of international phone calls from five U.K. companies and causing \$400,000 in losses for a Dell Computer subsidiary that had to shut down a free customer service phone line because of fraud. (\_Information Week\_ 20 Feb 1995, p.63) [From Edupage 19 Feb 1995]

---

## **Perfect (?) Office Bug can cause harm**

*<GILLARD@NIMUE.HOOD.EDU>*

*Tue, 21 Feb 1995 14:17:25 -0500 (EST)*

An annoying, and possibly serious, bug has surfaced in the recent release of Novell Perfect Office for Microsoft Windows. Temporary files may be left behind in the directory designated as TEMP in the user's autoexec.bat file. This is usually C:\TEMP or C:\WINDOWS\TEMP. Left unchecked, the files could eventually accumulate to the point where they clog the directory so that Windows applications will not run. The files take the form ~WT123B.TMP (where 123B is a unique identifier generated by the system) and are 5888 bytes long.

Although Novell/WordPerfect installation help is "aware" of the bug and is "working on it," I was told that at present no user-notification program is being planned.

You might think they'd learn from Intel's recent public relations fiasco....

Gary Gillard, Department of Math & Computer Science, Hood College  
Frederick, Maryland 21701 <gillard@nimue.hood.edu>

---

## **I can't help but say more about this addiction thing. (Slade, 16.82)**

*<ladkin@techfak.uni-bielefeld.de>*

*Sat, 18 Feb 1995 20:29:50 +0100*

In [RISKS-16.82](#), Rob Slade perceptively points out that behavior some have called 'computer addiction' is part of wider patterns, and notes by his analogy that there aren't simple criteria.

It may be helpful to distinguish rather than to conflate: firstly, between compulsive behavior and obsession. I would describe compulsive behavior as following an urge to do something, often repetitively, without concomitant reward other than that of appeasing the urge. We won't count the usual bodily functions..... but if you find yourself washing your hands a few hundred times a day, or the citizens of Koenigsberg set their watches by your daily walk to work, you're probably being compulsive. Obsession is when your thoughts, feelings, maybe actions orient narrowly towards one thing for a disproportionate time, whether it's rewarding or not. Sitting there with the same thought about Demi Moore buzzing round your head, you are obsessed, but not compelled (we hope). If getting rid of mother-in-law is your all-consuming hobby, you may try arsenic in the cake, running her over with the lawnmower, spiking her brandy, and rigging the breech of her shotgun. Your wife might leave you for failing at your single purpose in life, but no one would convict you of compulsive behavior.

These descriptions are dependent on social variables. Nevertheless, excessive obsessive/compulsivity is regarded as one of the 15-20 diagnosable personality extremes in the DSM (the Diagnostic and Statistical Manual, Revision IV, of the American Psychiatric Association, is a helpful guide to the current US classification of human behaviors that may lead to social problems for individuals). Most successful academics, writers, musicians, cooks, winemakers, mathematicians, scientists and sportspeople are more obsessive than the general population. The way to be better than others is to do something with more enthusiasm and for longer - and it helps if this concentration jives with your personality.

Addiction is a state of the organism, rather than predominantly a predisposition to certain behavior. A substance addict has highly goal-related behavior. Being drunk or high for these people is a relatively comfortable state of mind and body for *very* short periods of time. But it ruins their health, and causes self and others all sorts of problems. Addiction may be encouraged or even caused by compulsive behavior, but it is not itself a personality trait, according to the APA. If deleting email sends a thrilling tingle through your fingers, and tickles your corpus callosum until you can't let go, you may be addicted.

But the boundaries are blurred. Whether you call heavy use of computers addictive, obsessive/compulsive, or simply morally virtuous may depend on the context, the evident goals of the behavior, and whether you're spouse or employer. So I won't be too surprised when some misguided soul tries to enroll all us academics, writers, musicians, cooks, winemakers, mathematicians, scientists and sportspeople in a twelve-step program.

Peter Ladkin

---

**Sparc10 keyboards and resetting the CPU**

Carlos M. Puchol <cpg@cs.utexas.edu>

19 Feb 1995 19:05:18 -0600

It has happened to me several times now that I inadvertently knock the keyboard cable of the Sun SPARCstation 10 I work on these days. Most of the times, the result is a complete and instantaneous crash of the machine. So I tried and it seems that unplugging and plugging back in the keyboard cable at the base of the keyboard always crashes and reboots the host. This can obviously cause disks and user data to be lost. Other times only the X Window System dies.

Maybe it is just this particular machine, but otherwise I can't think what is so critical about a keyboard's hardware that could cause the machine crash. No doubt a RISK in my book.

-- Carlos Puchol

-- <http://www.cs.utexas.edu/users/cpg>

---

## Married by computer

<ssterner@BBN.COM>

Tue, 21 Feb 95 07:43:06 -0500

A few months ago I moved into a new apartment. I have since received a lot of junk mail for Mary Thompson, the former resident, whom I have never met. (Name changed to protect the innocent.) From conversations I have had with neighbors, I know that she lived alone. About a month ago, I started to receive credit card ads addressed to "Scott Thompson". I wrote this off as just a database entry error (e.g., only overwriting part of the new resident's name), until this past week. A few days ago I received two identical ads, with one addressed to "Scott Thompson" and the other addressed to "Mrs. Mary Thompson".

Yikes! Married to someone I've never met!

If only our names were confused (e.g., "Scott Thompson"), it would not be much of a risk. However, now that at least one database considers us husband and wife, what kinds of problems does this open?

- Do I get a free ride on \*her\* credit card history, or does she get a free ride on \*mine\*? (Stated the opposite way, do I suffer for \*her\* credit card history, or does she suffer for \*mine\*?)
- If I fill out the credit card applications listing my real name, but they issue the cards to me as "Scott Thompson", am I liable for fraud?
- If I never reply to any of these ads, could this "false name" come back to hurt me? (In other words, do I have to \*proactively\* stop this name from circulating, or could it never cause me harm so long as I do not use it?)

Scott Sterner

---

## UPS not quite so uninterruptable after all

*Jerry Leichter <leichter@lrw.com>*

*Mon, 20 Feb 95 08:33:20 EDT*

[Forwarded with permission of the author. Jerry]

From: Mark Frank <frankmrk@u.washington.edu>

Subject: Need UPS smarter than me.

Date: Sat, 18 Feb 1995 09:11:00 -0800 (PST)

To: Info-VAX@Mvb.Saic.Com

I use a UPS on my PC at home. The power switch is on the front. UPS sits on the floor (the way it has to for the AC outlets to face the right way). The other day I bumped the front of the UPS with my foot and hit the power switch, power went off, and I lost my work. Now that really pissed me off... they SAID it was UNINTERRUPTABLE, but one little nudge of the power switch and off it went! Wouldn't honor the warranty, either.

Ok...Ok... so I'm a moron. Moral to the story: If you are considering a UPS for a workstation-sized computer, be sure to get one with appropriate protection (like a hinged door) covering the power switch.

Mark S. Frank, Department of Radiology, University of Washington, 325 9th Ave  
Seattle, WA 98104 frankmrk@u.washington.edu (206) 223-3561

---

## Risks of generalized designs

*Jim Griffith <griffith@netcom.com>*

*Tue, 21 Feb 1995 11:19:15 -0800*

I'm playing in a computer-moderated play-by-mail game with a not-to-be-named company out of Oregon, and I ran into an interesting software logic gap. In the game, players have locations with soldiers defending it. Locations can contain guilds (representing an organization supporting a certain skill or collection of skills). A location's owner may be different from the owners of the guilds within it. In addition to the location's soldiers, guilds' soldiers can be ordered to defend the location against attack if both the location's and guilds' owner agree.

An amusing incident just occurred, when we captured a location from an enemy position. Capturing it required us destroying all of the location's soldiers. However, one of the location's guild owners tried to take the location back from us by putting soldiers in his guild and then trying to launch a "guild coup".

Unfortunately, the guild which attacked the city was also ordered to defend the city against attack. The location's previous owner had set this up with the guild's owner, and the change in ownership from our conquering the location didn't affect the guild defense options. So the guild ended up fighting

itself. Needless to say, it lost.

And in another amusing result, it turned out that the defender's ending values from a battle are written to the database before the attacker's. So since the attacker had no troops left, the guild ended up with no troops left - even though the guild-as-defender had troops survive the battle.

This kind of problem crops up all of the time in software development. At my previous company, I had a problem attempting to deal with real-time data when an application which was both a data consumer and a data producer attempted to request data from itself. The normal protocol would have been to send the request out to the network, have the network manager route the request back to the application, and have the application handle it in course. But the network manager was "smart" and told the consumer "you're requesting from yourself", and refused the request. This protocol forced anyone writing a producing/consuming application to create its own internal method for requesting data from itself, in addition to the normal method of requesting data from the network.

Both cases come down to developers who pictured a very general model, without considering some of the specific exceptions to the model which may very well occur in day-to-day use. In the game company's defense, this flaw has existed for several years, and as far as they know this is the first time players have actually encountered it.

Jim

---

## Stolen ATM Card nets \$346,770

<RichWells@aol.com>

Fri, 17 Feb 1995 22:25:16 -0500

In [RISKS 16.81](#) "Whittle, Jerome SMSgt" <JWhittle@amclg.safb.af.mil> wrote:  
>5. Karen Smith isn't liable for the theft even though she left her card and  
> PIN number unsecured. I believe that she should shoulder some of the  
> blame and loss.

I hope I'm not the only one who will speak out against this "blame the victim" mentality. Granted, the crime could and should have been prevented, but since it did happen, the blame for the crime falls squarely on the shoulders of the reprobates who committed it.

The risk I see here is that if we continue to cut criminals some slack by placing some of the blame on the victim, we're only going to invite more crime of this sort. To me, this is only slightly more palatable than blaming a rape victim because of how she was dressed.

---

## Re: JUDGES-L (Stodolsky, [RISKS-16.82](#))

Peter da Silva <peter@nmti.com>

Mon, 20 Feb 1995 11:17:43 -0600

> Fears of this development have led to the organization of the NetNews  
> Judges (TM) List (this is a reformatted InterNIC resource entry):

Note that the people who actually do the volunteer work that keep Usenet running, as well as most long time Usenet readers that know about it, consider Judges-L to be a crank list. It's a closed list, with rules about the dissemination of messages outside the official membership. It periodically produces informational postings that have no relationship to accepted net behaviour.

Like any other "authority" on Usenet it has no power but what individuals grant it. Unlike "authorities" like David Lawrence, who is accepted by the majority of sites as being the authoritative source of new groups, Judges-L has no followers except for the people who are actually on the list... and even then some of the people on Judges-L are only there to keep an eye on them.

[Also commented on by Kevin Blackburn Kevin@fairbruk.demon.co.uk]

---

### "PGP: Pretty Good Privacy" by Garfinkel

*"Rob Slade, Social Convener to the Net" <roberts@mukluk.decus.ca>  
Sat, 18 Feb 1995 15:54:54 EST*

BKPGPGAR.RVW 950116

"PGP: Pretty Good Privacy", Garfinkel, 1995, 1-56592-098-8  
%A Simson Garfinkel simsong@next.cambridge.ma.us simsong@expert.com  
%C 103 Morris Street, Suite A, Sebastopol, CA 95472  
%D 1995  
%G 1-56592-098-8  
%I O'Reilly & Associates, Inc.  
%O 800-998-9938 707-829-0515 fax: 707-829-0104 info@ora.com or nuts@ora.com  
%P 393  
%T "PGP: Pretty Good Privacy"

Part one of this guide to Phil Zimmermann's "Pretty Good Privacy" (universally known by its initials, PGP) contains two rather disjointed chapters introducing PGP, itself, and cryptography basics. After that rocky start, however, part two is both readable and rivetting. Chapters on the history of cryptography, the history and development of PGP, privacy, and patents gather both the technical and social aspects of PGP together in one place. The conceptual background for public key cryptography is presented both soundly and in a manner accessible for non-experts. The many controversies over PGP are presented in a very detailed manner.

Part three, "Using PGP", has chapters on file encryption, key creation, key management, email encryption, digital signatures (authentication), key distribution and certification, and Internet key servers. The style of the nutshell books give a very "technical" look to the material, and in some cases

the content is very terse in comparison to Stallings' "Protecting Your Privacy" (cf. BKPRTPRV.RVW). In others (such as key management), though, the text here is paradoxically clearer. In any case, the examples are straightforward and easily followed. (Readers may, however, be excused for failing to follow the explanation of Diffie-Hellman on page 356.)

The appendices cover obtaining and installing PGP for MS-DOS, UNIX and Macintosh.

copyright Robert M. Slade, 1995 BKPMPGAR.RVW 950116  
Vancouver Institute for Research into User Security Canada V7K 2G6  
ROBERTS@decus.ca Robert\_Slade@sfu.ca rslade@cue.bc.ca p1@CyberStore.ca

---

## The Coming Plague

*Peter Wayner <pcw@access.digex.com>  
Mon, 20 Feb 1995 09:31:37 -0500*

While RISKS is ostensibly devoted to the foibles of computer generated bugs, readers of the list will probably enjoy *\_The Coming Plague\_* by Laurie Garrett (Farrar Straus & Giroux). The book explores many of the battlefields between humans and microbes and then concludes that it is only a matter of time before the microbes score some dramatic victories. Many of the themes are familiar to RISKS readers: the fix causes more pain than it solves; the bountiful commonweal often comes with a quicksilver lining; and there is no such thing as the last bug.

The bestselling *\_Hot Zone\_* covers a small part of the scope of this book and it is more a movie outline than a book on science. *\_The Coming Plague\_* comes with copious footnotes and is filled with the technical details that scientists love. I've enjoyed it more and I suspect that others who read this list might feel the same. Given that some computer scientists talk of solving NP complete problems with DNA techniques, I guess that the fields are effectively merged and this is entirely appropriate for this list.

---

## Scan results

*"Dr. Frederick B. Cohen" <fc@all.net>  
Sat, 18 Feb 1995 07:24:56 -0500 (EST)*

Since announcing the on-line over-the-wire security scanning service (<http://all.net:8080>) on the risks forum, over 350 sites have performed scans. I am interested in finding out some things about the results of these scans. Any answers would be welcomed:

- 1) Did the service detect anything you did not expect?
- 2) Was the range of tests interesting enough to warrant keeping the service?
- 3) Is the service genuinely helpful or just a waste of time?
- 4) Did your defense detect the attempted attacks/defend against them?

Thank you in advance for your replies (email to fc@all.net). Also, I

would like to note that scans performed over the last few days, only 20 or so failed to be delivered to the tester because of mail failures.

FC

---

## **symposium on medical records**

*Phil Agre <pagre@weber.ucsd.edu>*

*Sat, 18 Feb 1995 18:28:29 -0800*

A symposium is coming up that has tremendous consequences for the privacy of sensitive personal medical records -- Toward an Electronic Patient Record '95, 14-19 March 1995 in Orlando, Florida. The basic idea is to put all of your medical records on-line in a centralized repository, accessible to any medical professional who needs them. This is great when the folks in the emergency room need your records in a hurry, but it's not so great when your records are also available to insurance companies and marketers, not to mention private investigators who are willing to push the law a little bit. Right now the outlook for serious privacy protections on computerized medical records is not so good. As a result, I think it would be excellent if any net citizens were to attend this symposium and report back to the net community.

I would particularly direct your attention to a meeting of the Standards Subcommittee on Access, Privacy and Confidentiality of Medical Records, which is to be held on Sunday March 12th and will be open to the public. It isn't good enough for privacy to be protected by vague principles and guidelines after the systems have been designed. Privacy capabilities such as patients' control over their personal information must be built into the technical standards, and if you can be in Florida in March then you can help out by informing the net community about the progress of those standards.

More generally, the standards for a whole generation of privacy-sensitive systems are being set right now -- Intelligent Transportation Systems are another example -- and I think it's important for the net community to track the standard-setting process, publicizing problems and intervening to make sure that the new generation of standards makes full use of the new generation of privacy technologies -- especially technologies such as digital cash that are based on public-key cryptography. In the case of medical records, some of the people designing the systems actually are aware of the existence of these new privacy technologies. The hard part is making sure that real privacy protection is actually built into the standards despite the probable pressure of various economic interests to the contrary.

The symposium is organized by the Medical Records Institute. MRI is on the Web at <http://www.nfic.com/mri/mri.html> But I particularly recommend the 36-page paper version of the conference announcement since it includes information about the exhibitors -- valuable raw material for research by privacy advocates. MRI's e-mail address is 71431.2030@compuserve.com and their paper address is 567 Walnut Street, PO Box 289, Newton MA 02160 USA.

Phil Agre, UCSD

---

## NCSA Conference: Security on the I-Way

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
19 Feb 95 22:16:52 EST

SECURITY ON THE I-WAY  
NCSA's 1995 Technical Symposium  
April 10-11, 1995  
Stouffer Concourse Hotel  
Arlington, VA

NCSA is pleased to announce Security on the I-WAY '95, a technical symposium addressing two key security issues: Internet/NII Security and Computer Viruses. Our speakers this year include many of the world's leading experts in these two key areas.

For further information or to register for the conference, please send e-mail to 74774.1326@compuserve.com requesting the registration form.

### CONFERENCE PROGRAM:

#### April 10/Monday:

08:30 Keynote Address

NCSA: New Directions

Dr. Peter Tippett, President, NCSA

#### TRACK 1: Computer Viruses

Track Chairman: Charles Rutstein

#### April 10/Monday:

09:00 Real World Anti-Virus Review and Evaluation

Richard Ford, Editor, Virus Bulletin

Sarah Gordon, Command Software

10:30 Virus Metrics

Joe Wells, IBM Watson Research Center

13:00 Viruses and the Internet

Fridrik Skulason, FRISK Software

14:30 Virus Writing: High-tech InfoSecurity Warfare

Frans Veldman, ESaSS

#### April 11/Tuesday:

09:00 Viruses in the 32-bit Operating Environment

Shane Coursen, Symantec

10:30 Viruses and Windows NT

Charles Rutstein, Price Waterhouse

13:00 The Good, the Bad and the Polymorphic

Alan Solomon, S&S International

#### TRACK 2: Internet/Infrastructure Security

Track Chairman: Ted Phillips

April 10/Monday:

09:00 The Electronic Intrusion Risks to the NII

Ted Phillips, Booz-Allen Hamilton

10:30 Public Key Infrastructure Issues

Warwick Ford, Bell Northern Research

13:00 Internet Security Strategies

Jim Litchko, TIS

14:30 Security Applications for Smartcard Technologies

Jim Dray, NIST

April 11/Tuesday:

09:00 Wireless System Security

Robert McKosky, GTE Laboratories

10:30 Broadband Network Security Issues

John Kimmins, Bellcore

13:00 NII Network Reliability Issues

Mel Sobotka, Booz-Allen Hamilton

14:30 Law Enforcement Perspectives on NII Security

Hal Hendershot, FBI

M.E.Kabay, Ph.D., Director of Education, Natl Computer Security Assn  
(Carlisle, PA); Mgmt Consultant, LGS Group Inc. (Montreal, QC)



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 16: Issue 84**

**Fri 24 February 1995**

## Contents

- [Old manuals, new features = security holes](#)  
[Christopher Klaus](#)
- [Software Firm is Victim of Virus](#)  
[Timothy Hunt](#)
- [National Cryptography Policy: Call for Input and Public Meeting](#)  
[Herb Lin](#)
- [CapAccess compromised](#)  
[Mich Kabay](#)
- [Major file corruptions](#)  
[Charles M. Preston](#)
- [Compact fluorescent lights](#)  
[Edward S Suffern](#)
- [EU office distributes Galicia virus](#)  
[Klaus Brunnstein](#)
- [Call for Papers, Risks in End-User Computing, HICSS '86](#)  
[Ray Panko](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Old manuals, new features = security holes

*Christopher Klaus <cklaus@iss.net>*

*Wed, 22 Feb 1995 17:03:38 +1494730 (PST)*

Many vendors' man pages, books, and magazine articles dealing with setting up an anonymous FTP server recommend something that is a possible security vulnerability. The security flaw is a result of old manual pages and new features being added to ftpd. They recommend the following:

~ftp)

Make the home directory owned by ``ftp" and unwritable  
by anyone.

A new feature added to many ftpd servers is "SITE CHMOD" -- which allows you to change the permissions on a directory. If the main directory is owned by

ftp, then an anonymous ftp user can SITE CHMOD the main directory from unwriteable to writeable. Once this has happened, they can add certain files to the main directory that would allow them shell access to the ftp account, thus to further compromise the system.

Many sites keep their incoming directory un-readable so that the administrator has a chance to verify files before allowing others to grab them. An intruder could undo all these permissions and even trojan existing ftp files.

To fix these problems, make sure the home directory is owned by root and that all files and directories are not owned by ftp. Unless you want anonymous ftp to be able to modify what is on your ftp server.

For other security concerns, I have written a Anonymous Security FTP FAQ (Frequently Asked Questions) that is available by sending mail to info@iss.net with "send Index" in the subject or body of the message.

Internet Security Systems, Inc. Computer Security Consulting  
2000 Miller Court West, Norcross, GA 30071

---

### Software Firm is Victim of Virus

*"Timothy Hunt [Assistant Unix Systems Manager]" <timothy@icr.ac.uk>  
Thu, 23 Feb 95 09:41:20 +0000*

[seen in The Guardian, 23rd February 1995, p9]

More than 200 software developers may have had their computers infected by a virus after Microsoft, the world's leading software developer, gave them infected disks at a seminar in London. Microsoft said yesterday the company that copied the disks for it had also been responsible for carrying out virus checks, and had been sacked because it had "cut corners." A spokeswoman said a developer spotted the virus after the seminar. "We immediately telephoned all the developers who attended and warned them," she said. Microsoft had also written to them all and apologised. It is believed only a few disks contained the virus.

Timothy J. Hunt, The Institute of Cancer Research, Royal Marsden NHS Trust,  
Downs Road, Sutton, Surrey, England SM2 5PT +44 (0)181 642 6011 x3312

---

### National Cryptography Policy: Call for Input and Public Meeting

*"CRYPTO" <crypto@nas.edu>  
Thu, 23 Feb 95 13:16:00 EST*

[This is a follow-up from Herb Lin on his message in [RISKS-16.63](#). PGN]

National Policy and Cryptography:  
A Call for Input and Public Meeting

Over the past few years, few topics have provoked as much debate as the appropriate role of government as it relates to cryptography. What is clear is that cryptography is critical to a wide range of important civilian and military applications involving sensitive or classified information that must be protected from unauthorized disclosure and/or alteration. National cryptography policy -- however it is construed -- has important implications for future U.S. economic competitiveness, national security, law enforcement interests, and the protection of the rights of individual U.S. citizens. In an attempt to clarify some of the issues involved, the U.S. Congress asked the National Research Council to undertake a comprehensive study on cryptographic technologies and national cryptography policy. This study began in late 1994.

The study seeks broad input from stakeholders affected by national cryptography policy. Thus, the study committee invites interested parties to answer the following question:

How, if at all, will new telecommunications technology, such as encryption, make it easier to protect and/or compromise the interests of the relevant constituencies? Some of the constituencies might include individual citizens, organizations in national security and law enforcement, high technology businesses, business in general, and non-profit and/or public service enterprises such as health care and education.

Please use as the standard of comparison the ease today of compromising or protecting these interests. We are interested in scenarios involving both individual users and large-scale impact. Please be sure to tell us the interests you believe are at stake. (If your input involves classified or sensitive information, contact us to make appropriate arrangements.)

All responses received by e-mail or U.S. mail prior to June 30, 1995 will be reviewed by the study committee. In addition, the committee will sponsor a public session to receive oral input on Friday, April 14, 1995, 8:30 AM to 12:30 PM, at the Lecture Room of the National Academy of Sciences, 2101 Constitution Avenue NW, Washington, DC 20418. (No public parking is available.) In the interests of hearing the maximum number of people, speakers will be limited to a statement of 6 minutes each. Anyone who wishes to give oral testimony should submit their request along with their response to the above question. (If you plan only to attend, please inform us as well.) Ground rules for oral presentation and/or a more detailed description of the study and its charge is available upon request to [CRYPTO@NAS.EDU](mailto:CRYPTO@NAS.EDU).

This is your opportunity to make your voice heard on this important subject. One way or another, cryptography policy does affect you. This study is expected to help shape Congressional and

Administration views on national cryptography policy, and the operative question to you is the following: Should this study take your views into account? We hope you answer that question in the affirmative.

Cryptography Project  
Computer Science and Telecommunications Board  
National Research Council  
Mail Stop HA-560  
2101 Constitution Avenue, NW  
Washington, DC 20418  
CRYPTO@NAS.EDU

---

## CapAccess compromised

*"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>  
16 Feb 95 08:00:04 EST*

The Washington Post news wire BYTES column for 95.02.13 (via CompuServe's Executive News Service) reports that the Washington, DC Internet provider, CapAccess, has been compromised by criminal hackers.

The 12,000 users are at risk of impersonation because someone installed "software that stole users' IDs and passwords."

The attack was apparently discovered only when CapAccess officials were informed by anonymous e-mail apologizing for the trick.

M.E.Kabay, Ph.D., Director of Education, Natl Computer Security Assn (Carlisle, PA); Mgmt Consultant, LGS Group Inc. (Montreal, QC)

---

## Major file corruptions

*Charles M. Preston <cpreston@alaska.net>  
Thu, 23 Feb 1995 10:24:47 +0900*

I would like to describe a strange case of file corruption on one of the largest on-line service providers that cost me a day's work and a lot of experimentation to chase down.

Several months ago I used a reliable program with error detection and "auto downloaded" several megabytes of programs and text files.

Most of the files were compressed with PKZIP. After getting a warning from PKUNZIP about a file being corrupt, I checked all the rest, about 15, using PKUNZIP -t. All the files but one were corrupt.

I've downloaded many megabytes and thousands of dollars of files from the service, without this problem. Thinking it was my ..serial port..hard drive ..download protocol..modem..virus.. or the particular directory (security associated) that had a lot of corrupt files, I changed all the software

and hardware a piece at a time. Hours of downloads later, there was only one constant, and it was the on-line service.

I determined it wasn't the files as stored on their hard drive, since I could eventually get a good copy of most files. On the corrupt ones, checksums matched over 2,3 or 4 copies downloaded with different computers and error-detection schemes, including Ymodem, xmodem, and Kermit. This service has a checksum command to match an already downloaded file and prevent duplicate downloads, and it matched the files (corrupt) still there with the files (corrupt) already on my hard drive.

I called support, and they admitted they were having a very odd problem with one of their machines, probably the one with my corrupted files on it.

Two days later, no file corruption. Two weeks later, another batch of the same type of corruption problem. None since then.

With some types of files this kind of corruption would not have been obvious for what it was - the 32 bit PKZIP checksum saved the day, and made it easier to determine the real culprit.

What type of problem, other than malicious programming, could cause these symptoms?

Charles Preston Information Integrity cpreston@alaska.net

Charles M. Preston Information Integrity cpreston@alaska.net

---

## Compact fluorescent lights

*Edward S Suffern <Suffern@DOCKMASTER.NCSC.MIL>*

*Thu, 23 Feb 95 17:27 EST*

For the last few months, I have experienced intermittent problems with the infrared remote controls for my TV, VCR, and stereo. The symptoms were difficulty activating the remote buttons, search operations continuing after they should have stopped, and, very occasionally, spontaneous channel changes. More recently, a friend's TV totally locked up as if one of the buttons was stuck in the activated position.

New batteries had no effect. Disassembly of remotes found nothing. I even disassembled the friend's TV found nothing until I noticed it would work fine on the test bench but not in its normal installed location. This lead me to correlate the problem with the recent installation of energy saving compact fluorescent light bulbs. Further testing proved conclusively that all of my infrared remote receivers were adversely affected by these lights.

The lights in question were manufactured by Lights of America (Models 2004 and 2030TP) but I expect other manufacturers may have the same problem. The bulbs advertise a tri-phosphor that produces a soft white light quality. They also have instant on, flicker free characteristics produced by a solid state circuit that replaces the standard fluorescent ballast.

Based on my observations I can only conclude that the tri-phosphor bulbs emit light in the infrared portion of the spectrum and that the electronics modulate the light at frequencies used by infrared remote control devices.

The manufacturer does include disclaimers about the devices causing "interference if placed within 10 feet of sensitive equipment. (T.V.s, radios, etc.)." (I experienced IR interference problems at 15+ feet.) There is also a statement about compliance with part 18 of the FCC Rules indicating that the device may not cause harmful interference. I assumed these references are directed at RF interference as that is what one normally expects and there is no mention of infrared emissions.

The real risk deals with possible consequences of these lights causing interference with existing and evolving applications of infrared technology such as wireless digital communications, automotive collision avoidance systems, etc.

Edward S. Suffern INFOSEC Consultant Suffern@Dockmaster.ncsc.mil

---

## EU office distributes Galicia virus

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.d400.de>  
Sat, 11 Feb 1995 13:19:59 +0100*

In December 1994, European Commission's office for "dissemination of scientific and technical knowledge" distributed a diskette to more than 1,000 European information brokers, patent offices etc containing a CORDIS News (in German) describing its RTD database etc. This diskette contained a system (boot sector/MBR) infector which besides displaying a message (on May 22nd, after noon: ";Galicia contra telefonica!") also overwrites (unrecoverably) part of a diskette's boot library, and which attempts to format a disk's cylinder. Though this formatting will likely abort, due to a programming error, it is possible that formatting may succeed. Indeed, this virus is malicious and not funny. (For details, see appended VTC Malware Catalog entry).

It is even less funny that this EU office when informed about its malicious gift to its customers found it very hard to locate the source of the contamination; they even could not say whether it came from another EU office or from one of their PCs. Only after some time, they claimed to have found 2 potential leaks which their expert said they now have closed. This implies that for some time, EU's information dissemination was a permanent danger for its customers.

Even more ironically: this EU office belongs to EU's Directorate General (DG XIII) "Telecommunications, Information Market and Exploitation of Research", which (with its branch "B.6 Security of Telecommunications and Information Systems") is responsible for EU's IT Security Criteria (ITSEC), which also participates actual in joint US/EU attempts to develop "Common Criteria". When being informed about the malicious distribution by its sister office, the head of DG XIII's SOG-IS (Senior Officials Group - Information Security)

informed the author that they don't share responsibility for maintaining a proper security as this is done by the European Commission's Office of Security (a typical bureaucratic approach :-). Moreover, this very nice expert claims that "I recognize that such incidents will happen from time to time and that the responsibility \*\*\*falls equally on both sender and receiver\*\*\* to ensure that the most 'hygienic' procedures are used to avoid any unnecessary spread of 'infection'" (quoted from a reply of SOG-IS chair; emphasis added by author). Finally, "controlling viruses is primarily a procedural rather than technical problem".

Both an evidently failing AntiVirus policy (if existing) and such expert opinion makes it rather likely that similar incidents will follow. If I were a virus author (being a civil servant, I have NO CRIMINAL energy as I have NO ENERGY at all :-), I would dream of such a large organisation (several 10,000 bureaucrats) with such "awareness". With their intellectual innocence, they'd surely help to distribute my virii if I only succeeded to infect one PC!

Mildly shocked: Klaus Brunnstein (Feb.11,1995)

=====  
Computer Malware Catalog 2.0: Galicia Virus (10-Feb-95) =====

Entry.....: Galicia Virus

Alias(es).....: (Telefonica.D Virus, see Particularities)

Caroname.....: Galicia

Virtype.....: b

Virus Strain.....: ---

Classification.....: System virus: Boot/MBR infector, memory resident,  
partly self-encrypted.

Length of Virus.....: 1 sector

Length of Virus(RAM): 2 kBytes

----- Preconditions -----

Operating System(s): MS-DOS

Version/Release.....: All models

Computer model(s)...: PC's

----- Attributes -----

Easy Identification.: ID word: V1.

Self recognition in memory: 7C B8 (h) at [0:004C]

Self recognition on disk: 56 31 (h) at [01B3h]

Type of infection...: System: Upon booting from an infected diskette  
or disk (MBR), virus makes itself memory  
resident at top of memory/below 640 kBytes,  
and it hooks Int 13h.

Disk: After booting from an infected diskette,  
memory resident virus will infect MBR  
upon trigger condition; original MBR  
is saved.

Diskette: Once virus became memory resident, it  
will infect any uninfected diskette in  
drive A: and B: upon trigger condition;  
original boot sector is saved.

Infection Trigger...: System/Memory: booting from infected disk/diskette

Disk/Diskette: any read (Int 13) access, when  
drive is not actual drive.

Storage media affected: Diskette,Harddisk

Interrupts hooked...: Int 13h/02 (Read)

Damage.....: Transient: At trigger time, virus displays

message: "Galicia contra =>telefonica!".

This text string is encrypted in virus body.

Permanent/Disk: Upon trigger condition, virus attempts to format 1st cylinder (track 0/head 0/sector 6); due to a programming error (un-initialised buffer address), this attempt will very probably abort with an error.

Permanent/Diskette: Upon infecting a diskette, virus overwrites track 0/head 1/ector which contains part of root directory:

- on 5,25" DD: last sector of root dir;
- on 5,25" HD: 3rd sector of root dir;
- on 3,5" DD: 3rd last sector of root dir;
- on 3,5" HD: 2nd sector of root dir.

As virus does not store this sector elsewhere, parts of root directory (e.g. entries 16-32 on 3.5" HD) are lost.

Damage Trigger.....: Transient: IF (May 22) AND (time > 12:00) AND (access to drive which is not to actual drive)

Permanent/Disk: IF (May 22) AND (time > 12:00) AND (access to drive which is not to actual drive)

Permanent/Diskette: upon infection of boot sector

Particularities.....: Findviru calls the virus "Telefonica.d", probably due to the displayed text, though the virus has no relation to the Telefonica family.

Cryptomethods.....: Partly encrypted (XOR with FFFFH from offset 003Ch to 0159h).

Stealth.....: ---

Polymorphism.....: ---

Tunneling.....: ---

----- Agents -----

Countermeasures.....: Good AntiVirus products (detection/cleaning).

Countermeasures successful: Several actual AntiVirus products detect Galicia, essentially under its name; at publication time, only few AV products (e.g., Kaspersky's AVP) properly clean it from media.

Standard means.....: Cleaning diskettes: format infected diskette (MS-DOS >=5.0, DR DOS >=6.0) with /U.

Cleaning hard disk: Use DOS FDISK /MBR command to overwrite the virus.

----- Acknowledgement -----

Location.....: 1) BSI/German Information Security Agency, Bonn

2) Virus Test Center, Univ Hamburg

Classification by...: 1) Hubert Schmitz (GISA V2)

2) Klaus Brunnstein, VTC

Documentation by....: 1) Hubert Schmitz (GISA V2)

2) Klaus Brunnstein, VTC

Date.....: 10-February-1995

Information Source..: CaroBase entry (1) and additional analysis (2), with information from Kaspersky, Skulason etc.

===== End of Galicia Virus =====

---

## Call for Papers, Minitrack on Risks in End-User Computing, HICSS '86

"Ray Panko" <PANKO@busadm.cba.hawaii.edu>

Tue, 21 Feb 1995 08:35:41 -1000

Twenty-Ninth Hawaii International Conference on System Sciences  
January 3-6, 1996, Maui, Hawaii

Dr. Raymond R. Panko, minitrack coordinator  
Panko@dscience.cba.hawaii.edu

Papers are invited for the minitrack on RISKS IN END-USER COMPUTING as part of the Information Systems track at the Hawaii International Conference on System Science (HICSS).

### Risks in End-User Computing

End users are ordinary computer users, such as managers and professionals, rather than computer professionals. End users control a great deal of all computing. There is growing evidence that this dominance of end-user computing creates risks for organizations and perhaps even society.

We are soliciting research papers in such areas as 1) lab and field studies on errors in spreadsheeting, query languages, and schema development in databases, 2) privacy and security issues related to user access to information, 3) and risks when end users use the Internet. This is not meant to be an exhaustive list.

### HICSS

HICSS is one of the oldest conferences in information systems and computer science. The 1996 conference will be the 29th in an unbroken series. Each year, the conference attracts about 500 computer research professionals. The conference is conducted in cooperation with the IEEE Computer Society and the ACM. The Proceedings are published by the IEEE Computer Society Press.

Making HICSS unique is its organization around minitracks. In a minitrack, the minitrack coordinator receives about fifteen to twenty papers and selects six for presentation at the conference. Selection is based on rigorous refereeing, ensuring high quality. All papers to be presented at the conference are published in the Proceedings, which is available at the start of the conference.

The minitrack focus of HICSS turns each minitrack into a mini-workshop. It provides a critical mass of research papers in a target area, providing the cross-fertilization of ideas. In addition, the conference activities are consciously organized to maximize interactions among the participants. Of course, minitrack participants also attend many other sessions in information systems and computer science.

Please note that HICSS is a research conference. It is not a place for publishing the types of articles that would appear in popular magazines. HICSS papers should be potentially publishable in research journals.

Instructions for submitting papers:

1. Submit 6 (six) copies of the full paper, consisting of 20-25 pages double-spaced including title page, abstract, references and diagrams directly to the minitrack coordinator. Longer submissions will be rejected, as will much shorter submissions.
2. Do not submit the paper to more than one minitrack. Paper should contain original material and not be previously published or currently submitted for consideration elsewhere.
3. Each paper must have a title page which includes the title, full name of all authors, and their complete address including affiliation(s), telephone number(s), and e-mail address(es). For purposes of anonymous refereeing, the author(s) name(s) should not appear in the rest of the paper.
4. The first page of the paper should include the title and a 300-word abstract.

DEADLINES:

MARCH 15, 1995: Abstracts MAY be submitted to minitrack coordinators (or track coordinators) for guidance and indication of appropriate content. Authors unfamiliar with HICSS or who with additional guidance are encouraged to contact any coordinator to discuss potential papers. Abstracts are NOT required but are strongly encouraged.

JUNE 1, 1995: Full papers due [...]

AUG. 31, 1995: Notification [...]

OCT. 1, 1995: Accepted manuscripts due camera-ready plus ONE registration.

NOV. 15, 1995: All other registrations [...]

The Risks in End-User Computing minitrack is part of the Information Systems Track. There are two other major tracks in the conference: Software Technology and Digital Documents. The Information Systems Track itself has several minitracks that focus on a variety of research topics in Collaboration Technology, Decision Support and Knowledge-Based Systems, and Organizational Systems and Technology. For more information contact:

Jay F. Nunamaker, Jr.: E-Mail: [nunamaker@bpa.arizona.edu](mailto:nunamaker@bpa.arizona.edu)  
(602) 621-4475  
FAX: (602) 621-2433

Ralph H. Sprague, Jr.: E-Mail: [sprague@uhunix.uhcc.hawaii.edu](mailto:sprague@uhunix.uhcc.hawaii.edu)  
(808) 956-7082  
FAX: (808) 956-9889

For more information on other tracks, please contact:

Software Technology Track:

Hesham El-Rewini: E-Mail: [rewini@unocss.unomaha.edu](mailto:rewini@unocss.unomaha.edu)

Bruce D. Shriver: E-Mail: [b.shriver@genesis2.com](mailto:b.shriver@genesis2.com)

Digital Documents Track:

M. Stuart Lynn: E-Mail: [msynn@cpa.org](mailto:msynn@cpa.org)

For more information on the conference, please contact the  
conference coordinator:

Pamela Harrington: E-Mail: [hiccs@uhunix.uhcc.hawaii.edu](mailto:hiccs@uhunix.uhcc.hawaii.edu)

(808) 956-7396

FAX: (808) 956-3766

Aloha, Ra3y (the 3 is silent)

Prof. Raymond R. Panko      Internet: [Panko@dscience.cba.hawaii.edu](mailto:Panko@dscience.cba.hawaii.edu)

Decision Sciences Department      Office: (808) 956-5049

College of Business Administration      Fax: (808) 956-9889

University of Hawaii      Secretary: (808) 956-7430

2404 Maile Way      Home: (808) 261-2675

Honolulu, HI 96822      Time of Day: (808) 983-3211

USA      Weather: (808) 833-2849



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 16: Issue 85

Friday 24 February 1995

## Contents

- [Another police sting based on a freebie video offer](#)  
[Clive D.W. Feather](#)
- [More Security Problems on the Internet](#)  
[Edupage](#)
- ["E-Mail Security" by Schneier](#)  
[Rob Slade](#)
- [\\*BUGS in Writing: \[...\] Debugging Your Prose\\*](#), by Lyn Dupre  
[Bob Donegan](#)
- [Re: CERT Advisory CA-95:04.NCSA.http\[...\]vulnerability](#)  
[Timothy Hunt](#)
- [Re: Perfect \(?\) Office Bug can cause harm](#)  
[Keith Schengili-Roberts](#)
- [Re: Perfect \(?\) Office Bug can cause harm](#)  
[Jerome Whittle](#)
- [Re: Sparc10 keyboards and resetting the CPU](#)  
[Tarl Neustaedter](#)
- [Re: Major file corruptions](#)  
[George C. Kaplan](#)
- [Re: Major file corruptions](#)  
[George Buckner](#)
- [Re: Major file corruptions](#)  
[Kenneth Albanowski](#)
- [Re: JUDGES-I](#)  
[David Stodolsky](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Another police sting based on a freebie video offer

"Clive D.W. Feather" <[clive@sco.com](mailto:clive@sco.com)>

Wed, 22 Feb 1995 07:33:49 +0000 (GMT)

[Not really RISKS related, but interesting because stings of this type seem to be becoming a common practice. But soon this will be happening on the information superhighway. PGN]

Drawn by invitations in the name of a fictitious market-research company, 31 "elusive criminals" responded in person to a drawing for a year's free use of telly facilities. After filling out questionnaires on their viewing habits, they were then arrested. "Operation Trick or Treat" turned out to be a Trick. (For you anagram freaks, the bogus company name, Mison Giewold, is an anagram of the name of Detective Constable Simon Weigold, the officer who organized the sting.) [Source: "Prize draw proves winner for police" -- by Nigel Bunyan, \*The Electronic Telegraph\*, 22 Feb 1995; inquiries to its editor at <benry@telegraph.co.uk>. Abstracted by PGN.]

---

## More Security Problems on the Internet (Edupage, 23 Feb 1995)

Edupage <info@ivory.educom.edu>  
Thu, 23 Feb 1995 20:35:30 -0500

The Computer Emergency Response Team has issued a public warning on a vulnerability in some 20 commonly used E-mail programs that run on Unix operating systems. The advisory said the latest discovery could allow a hacker to "read any file on the system, overwrite or destroy files." The ultimate solution to these recurrent security problems, says Purdue University professor Eugene Spafford, is for consumers to demand better security features from software manufacturers. In the absence of improved software, "are we going to continue seeing problems? You bet." (Wall Street Journal 2/23/95 B8)

[Spaf really said that's the ULTIMATE, eh?  
That's as good as it can get?  
Wow! We are really in for a bad time. PGN]

---

## "E-Mail Security" by Schneier

"Rob Slade, Social Convener to the Net" <roberts@mukluk.decus.ca>  
Fri, 24 Feb 1995 13:27:32 EST

BKEMLSEC.RVW 950127

"E-Mail Security", Bruce Schneier, 1995, 0-471-05318-X, U\$24.95/C\$32.50  
%A Bruce Schneier schneier@counterpane.com  
%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8  
%D 1995  
%G 0-471-05318-X  
%I John Wiley & Sons, Inc.  
%O U\$24.95/C\$32.50 416-236-4433 fax: 416-236-4448 800-CALL-WILEY  
%O 212-850-6630 Fax: 212-850-6799 Fax: 908-302-2300 jdemarra@jwiley.com  
%P 365  
%T "E-Mail Security"

This is the third work that I have seen on the PGP (Pretty Good Privacy) text encryption and authentication system. (I understand that at least two more are in the works.) It is also the first to truly present the general

concept of email security by covering the only other realistic option--the Internet Privacy Enhanced Mail (PEM) standard and (Mark) Riordan's Internet Privacy Enhanced Mail (RIPEM) implementation. The book divides roughly into quarters discussing background, practical use, the PGP documentation, and the PEM RFCs.

The work is considerably different, in style, to the Stallings (BKPRTPRV.RVW) and Garfinkel (BKPGPGAR.RVW) efforts. Those books, while not obtuse, were still written with a technical audience in mind. Schneier's work, while definitely showing the expertise he demonstrated in "Applied Cryptography" (BKAPCRYP.RVW), is clearly aimed at the general, non-technical reader. (Interestingly, while he *does* tell you where to find the RC4 algorithm posting, he *doesn't* mention the loophole recently pointed out in the Clipper "Skipjack" algorithm.) The straightforward style lulled me into thinking that chapter one was too long. It isn't: Schneier makes the important point that, for it to be *truly* effective, encryption must be used on *all* correspondence, even trivial items. So well crafted is his argument that it would be difficult to reduce the chapter by so much as a paragraph.

Schneier uses this argument to good effect in pointing out some of the major deficiencies in the two systems. PGP is awkward to use, and PEM may use incompatible algorithms. Surprisingly, he does not emphasize (though he does mention) what is probably the major problem with each--the inability to use the same system within and outside of the United States. The PGP fiasco is too involved to get into here (see the Garfinkel work for details) and there is not yet an "international" implementation of PEM (although there may soon be an "authentication only" version available).

This won't help you design your own algorithm, but it is definitely for any user of email, manager of communications systems, or student of privacy and confidentiality.

copyright Robert M. Slade, 1995 BKEMLSEC.RVW 950127  
DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733

---

### **\*BUGS in Writing: A Guide to Debugging Your Prose\*, by Lyn Dupre**

*Bob Donegan <bobd@aw.com>*  
*Wed, 22 Feb 1995 18:01:13 -0500 (EST)*

\*BUGS in Writing: A Guide to Debugging Your Prose\*, by Lyn Dupre  
ISBN: 0-201-60019-6 \$19.95 (price subject to change), 649 pp., paperback

[And WHAT, might you ask, does this have to do with RISKS? Well, can you think of any bugs in computer systems that have resulted from bugs in writing? We've seen quite a few in RISKS. And besides, this is a terrific book. PGN]

\*BUGS in Writing\*, written with verve and wit, may be the first book on writing that people read for sheer fun. Unlike traditional style manuals,

which present huge hierarchical rules bases (and which hardly make for amusing reading), \*BUGS\* presents an alternative, intuitive way of looking at written language that is based on the concept of ear: the ability to hear, without analysis, whether a given word order, sentence, or term is correct. \*BUGS\* explores problems that writers face, and explains how to rid your prose of these bugs.

Designed for easy browsing, \*BUGS\* comprises 150 independent and easily digestible segments, resembling a daily newspaper column and presented with an unusual, appealing, inviting design. Dupre not only tells you about good writing -- she also demonstrates it for you, conveying simple principles for lucid writing by numerous, intriguing, and frequently hilarious examples that are classified with the bugs system: Bad, Ugly, Good, or Splendid.

\*BUGS\* was developed for anyone who writes and who works with computers, including computer and other scientists, students, professors, business people, programmers, and technical writers. Rather than subjecting yourself to the pain and tedium of wading through a reference book on English grammar, you can pick up \*BUGS\*; you will immediately find yourself browsing interesting and amusing material. While you are enjoying yourself, you will be tuning your ear. As a result, you will write lucid prose that communicates your ideas.

---

## Re: CERT Advisory CA-95:04.NCSA.http.daemon.for.unix.vulnerability

*"Timothy Hunt [Assistant Unix Systems Manager]" <timothy@icr.ac.uk>  
Thu, 23 Feb 95 11:20:36 +0000*

This is a warning about poor distribution of fixes for security holes.

In several locations on the 'net I have found the warning about the security hole in NCSA httpd 1.3.

The fix they suggested was only to change the default string lengths, but didn't include the patch to perform the functionality of strsubfirst().

While this will prevent any current attack programs from gaining access, only a minor change would be necessary to attack the slightly modified httpd (I think!).

This means there are probably a good many httpd daemons out there that are still vulnerable, yet the administrators think they are now secure.

Timothy J. Hunt, The Institute of Cancer Research, Royal Marsden NHS Trust,  
Downs Road, Sutton, Surrey, England SM2 5PT +44 (0)181 642 6011 x3312

---

## Re: Perfect (?) Office Bug can cause harm (Gillard, [RISKS-16.83](#))

*Keith Schengili-Roberts <kschengi@interlog.com>  
Wed, 22 Feb 95 15:21 WET*

I read this submission to RISKS with some amusement. This particular problem is not new to the WordPerfect portion of Novell's Perfect Office -- in fact WordPerfect is far from being the only culprit in leaving behind stray ~\*.tmp files. In the course of its operations, Windows and many Windows applications often write files with a ~\*.tmp filename to the \TEMP directory listed in the AUTOEXEC.BAT file via the SET TEMP= command. Windows normally removes these files automatically when you exit Windows. If Windows crashes, or if you turn off your computer before exiting gracefully from Windows, these files get left behind, and are not erased the next time you start Windows. The accumulation of ~\*.tmp files not only will take up hard drive space, but can interfere with the operation of Windows and Windows applications. Many a mysterious General Protection Fault I've run across on other people's computers have been attributed to an accumulation of ~\*.tmp files on their hard drives.

The best thing to do is to erase these ~\*.tmp files from your hard drive as often as possible. Many people throw in a line within their AUTOEXEC.BAT files which automatically go to the directory where ~\*.tmp files are stored, and delete the contents of that directory before launching Windows. This must be done from DOS, rather than from within Windows, as Windows does not take kindly to the attempted erasure of ~\*.tmp files it is currently using. If you are not sure where your ~\*.tmp files are stored, type SET from the DOS prompt, and the SET TEMP= will tell you which directory to check. If no SET TEMP= line appears, the ~\*.tmp files will reside in your \WINDOWS directory.

My only criticism of WordPerfect (going back to version 5.1 for Windows to the current 6.1 release) in this matter is that they consistently leave behind more ~\*.tmp files than most of the other Windows programs I have used. I still prefer WordPerfect over most other wordprocessors however, so I suffer with the problem and just erase the stray ~\*.tmp files it leaves behind.

Keith Schengili-Roberts, The Computer Paper, 99 Atlantic Avenue #408, Toronto, Ontario M6K 3J8 CANADA kschengi@interlog.com <http://www.wimsey.com:80/tcp>

---

### **Re: Perfect (?) Office Bug can cause harm (Gillard, [RISKS-16.83](#))**

*"Whittle, Jerome SMSgt" <JWhittle@amclg.safb.af.mil>  
Wed, 22 Feb 95 08:19:00 cst*

Unless Novell is really bad about it, I don't think Perfect Office is the only guilty party. We use Microsoft Office here and have the same problems. Actually I think that it is a Windows problem.

One of the things I do when I "tune-up" someone's computer is look for temp files. I search using File Manager with a Search For: ~\*.\*. I have literally found megs of temp files clogging up hard drives.

The user is usually to blame. The temp files should be deleted when the user closes the application or shuts down Windows \*properly\*. If they just turn off the power switch while Windows is still on the monitor,

temp files won't be deleted. In other words, tell them not to hit the power switch until they see C:\. (Another problem with not shutting down Windows properly is there will be lost clusters all over the place on the hard drive. Using CHKDSK /F or SCANDISK, I've recovered up to 50 megs of hard drive space!).

If they don't have a SET TEMP=C:\TEMP (or something similar) statement in their AUTOEXEC.BAT, temp files will just dump all over the place. Also, there better be a TEMP (or similar) directory or the same will happen.

Jerry Whittle, Belleville, Illinois, USA [jwhittle@amclg.safb.af.mil](mailto:jwhittle@amclg.safb.af.mil)

---

## Re: Sparc10 keyboards and resetting the CPU (Puchol, [RISKS-16.83](#))

*Tarl Neustaedter <[tarl@tarl.net](mailto:tarl@tarl.net)>*

*Tue, 21 Feb 1995 23:56:08 -0500*

> It has happened to me several times now that I inadvertently knock the  
> keyboard cable of the Sun SPARCstation 10 I work on these days. Most of the  
> times, the result is a complete and instantaneous crash of the machine.

Actually, this is a feature.

I know, it doesn't sound like a feature. And there are more ways to come to grief by this feature than just mentioned - most notable being the well-intentioned conservationist who powers off an ASCII terminal being used as a sun server console. The agonized screams from the users down the hall usually alert the conservationist as to his impending fate. (See also: <http://pond.cso.uiuc.edu/ducky/docs/jimbo/raptor.html>)

It doesn't actually cause a crash. Since time immemorial (long before I started working with sun serial drivers), a BREAK condition on the console line has been an attention signal telling a Sun to jump into its prom. Unplugging a serial (async) line generates a BREAK condition. Usually, you can recover by typing "go" after you plug the cable back in.

The reason it is a feature; Occasionally a user will do something he regrets (certain programs which clobber the keyboard or simply won't exit should not be run on the console), and the user needs some way to regain control of his system. Unlike PCs, UNIX resents being powered off. It wants to be politely shut down first. If you forget often enough, UNIX will take it's revenge on you by eating your file system. Hence this escape into PROM.

On a normal ascii line, the only safe condition to detect is a "BREAK" - everything else having been assigned functions by Gnu EMACS. On a keyboard, where we aren't limited by ASCII, the "STOP-A" combination is normally used. But "BREAK" serves the same purpose, and will sometimes work when STOP-A won't (send me email if you want the grody details). Once you have gotten back into the prom, you can "sync" the filesystems and reboot.

If you really want to disable this functionality, you could find the call to `abort_sequence_enter()` at the end of `zsa_xsint` in `zs_async.c`, and

NoOp it out. This keeps STOP-A/L1-A functionality (called from kbd.c) while disabling the "BREAK" functionality. It helps to be handy with kadb.

But caveat emptor - Murphy's law guarantees that as soon as you disable this functionality, within the next week you will desperately need it.

Tarl Neustaedter tarl@tarl.net [home], tarl@east.sun.com [work]  
Ashland, MA, USA <http://tarl.net/tarl>

[Rather similar comments also from  
nick@cimio.co.uk (Nick Waterman),  
Craig\_Everhart@transarc.com,  
"Rory O'Donnell" <rol@stadt.sp-media.de>,  
Keith Price <price@raycharles.usc.edu>,  
Mark.Kantrowitz@GLINDA.OZ.CS.CMU.EDU,  
Marc Horowitz <marc@MIT.EDU>,  
edward@igate1.HAC.COM (Ed Bruce),  
and maybe others whose SUBJECT: field said only ``Re: [RISKS-16.84](#)" --  
which means there is a chance that I will NEVER look at those messages,  
unless perhaps I happen to do a search on some keyword. Note:  
there is a WARNING to that effect in the INFO message. PGN]

---

### Re: Major file corruptions (Preston, [RISKS-16.84](#))

*George C. Kaplan <gckaplan@sunspot.ssl.berkeley.edu>  
Fri, 24 Feb 1995 12:39:40 +0800*

Charles M. Preston's story of corrupted files (in [RISKS-16.84](#)) sounds like a situation I once saw that was traced to a flaky disk controller. Sometimes one or more bits would be cleared somewhere in the file. Since it was the "0x20" bit, we first noticed it when random scattered letters were capitalized in text files. Sometime later, presumably after buffers had been flushed, the affected files would be back to normal.

The service tech didn't quite believe us, but he replaced the disk controller board, and the problem went away.

George C. Kaplan gckaplan@ssl.berkeley.edu 1-510-643-5651

---

### Re: Major file corruptions

*George Buckner <GRB@NCCIBM1.BITNET>  
Fri, 24 Feb 95 15:45 EST*

I've discovered a tendency for PKUNZIP to report corrupt files when I run it from a DOS shell while Windows is running. This problem goes away if I close Windows first. (No this isn't a fix or an explanation, but my temporary work-around).

George Buckner

---

## Re: Major file corruptions

*Kenneth Albanowski <kjahds@kjahds.com>*

*Fri, 24 Feb 1995 15:49:27 -0500 (EST)*

Charles Preston asks "what type of problem, other than malicious programming, could cause these symptoms?", in regards to an on-line service occasionally serving up damaged files.

The possible reasons for such behaviour are numerous, and it aids no-one to call up the specter of a rouge programmer or "hacker", if such a thing is not known to be true. This is a risk that is now being run by everyone providing an electronic service: an accusation of being "hacked", or of "downloading the users hard disk in secret", or of "damaging files for unknown purposes", (just to name a few,) carries a large weight in the press, and is potentially difficult to fight.

I believe Charles is talking about the CompuServe Information Service, which I have heard some small comments about infrequent damage to downloaded files. The behaviour is supposed to be quite uncommon, and goes away on a repeat of the transfer. Of course, Charles could be talking about any large service that provides files for download. Anything from a damaged disk drive to a fluky controller card to a out-of-tolerance CPU to a buggy program could cause these problems, and I know of no company that is immune to such things.

Lastly, yes, since the file-transfer checksums matched, having a secondary checksum (in this case, actually a CRC provided by PKZIP) would certainly prove useful. That's why PKZIP does it, and why CRCs are in common use. This also points out the risk of not verifying data integrity on all levels. Presumably a CRC check used at some stage in the service's computer would have detected the problem earlier.

Kenneth Albanowski (kjahds@kjahds.com, CIS: 70705,126)

---

## Re: JUDGES-L (da Silva, [RISKS-16.83](#) on Stodolsky, [RISKS-16.82](#))

*David Stodolsky <david@arch.ping.dk>*

*Wed, 22 Feb 95 19:32:08 +0100 (CET)*

Looks like Peter da Silva was confused by the "Cancel Messages: Frequently Asked Questions Part 2" post, a forgery meant as a joke. The List has released a single informational post, a single time. It was developed with contributions from leading Usenet administrators, some of whom have chosen to remain anonymous. When the latest version was approved, via a consensus decision making process, there were about a dozen leading administrators subscribed, and under the rules, anyone of them could have blocked its release, or tried to, thus precipitating a vote. This did not occur. It was a consensus document. (The forgery was, unfortunately, taken seriously by all too many, including the Italian EFF. This perhaps is an indication of the need

for informational posts on this topic.) The authentic document starts with a summary:

Cancel Messages: Frequently Asked Questions (FAQ). Ver. 2.0  
Summary:

You can protect your reputation as a information source by cancelling articles posted under your name as soon as you discover that they are erroneous.

Cancelling other's articles, however, can expose you, your site, and the Net as a whole, to serious threats. The sender should be notified when articles need to be cancelled.

Disputes or doubtful cases can be directed to the Judges' List for resolution.

The List is open to anyone who agrees to follow the rules adopted through the List's consensus decision making process. The List is not confidential, that is, it can be located by a LISTSERV search. It is also open to review by the public. A review command to LISTSERV@UBVM.cc.buffalo.edu will yield the settings and membership of the List. This will show, among other things, that anyone may send mail directly to the List: There is no editor who must approve messages. Since the List now offers confidential dispute resolution, the continued dissemination of messages via mail-to-news gateways, etc. was deemed inappropriate. This question, however, continues to be debated.

Information about the NetNews Judges (TM) List appeared in the \_New Scientist\_ magazine at the end of last year. It is also discussed in the most recent issue of \_Matrix News\_. I was also interviewed recently by a reporter from \_The Chronicle of Higher Education\_ about the List.

David S. Stodolsky, PhD \* Social \* Internet: david@arch.ping.dk  
Tornskadestien 2, st. th. \* Research \* Tel.: + 45 38 33 03 30  
DK-2400 Copenhagen NV, Denmark \* Methods \* Fax: + 45 38 33 88 80



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 16: Issue 86**

**Friday 3 March 1995**

## Contents

- [What Goes Intuit May Not Come Out the Same Taxwise](#)  
[PGN](#)
- [Apple Settles RSI Claim](#)  
[Edupage](#)
- [Apple Settlement Due to Lawyer Error](#)  
[Edupage](#)
- [More Security Problems on the Internet](#)  
[Edupage](#)
- [Encryption Lawsuit Filed in California](#)  
[Edupage](#)
- [Anti-Cyberporn \[Exon\] Bill Introduced](#)  
[Edupage](#)
- [Home Gambling Network](#)  
[Mich Kabay](#)
- [Losing your Marbles and your Barings](#)  
[Peter Wayner](#)
- [UK National Audit Office report on computer misuse in government](#)  
[Brian Randell](#)
- [Re: Perfect \(?\) Office Bug ...](#)  
[Matt Cockerill](#)
- [Blaming the victim for money stolen with lost ATM card](#)  
[Elizabeth Schwartz](#)
- [Sick Medicare Scanner](#)  
[Judith Seeger](#)
- [Interstate Panopticon](#)  
[Phil Agre](#)
- [Risks of living on the left side of the continent](#)  
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

---

## What Goes Intuit May Not Come Out the Same Taxwise

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Fri, 3 Mar 95 07:57:21 PST

Flaws were reported in the PC and Mac versions of TurboTax and MacInTax 1040. These flaws are triggered when transferring tax data to the tax package from other software, such as Quicken. Intuit estimates that the flaws would affect only about 1% of the users. Intuit Chairman Scott Cook apologized that the flaws had been known for a few weeks and had not been publically acknowledged until 1 Mar 1995. He also indicated that new versions can be obtained for free by calling 800-224-0948 (in the US).

[Sources: various news reports 2-3 Mar 1995, including the San Francisco Chronicle]

---

### **Apple Settles RSI Claim (Edupage, 28 Feb 1995)**

*Edupage <info@ivory.educom.edu>*

*Tue, 28 Feb 1995 20:09:58 -0500*

Eight weeks into the first such lawsuit to go to trial, Apple Computer has settled with the plaintiff who claimed her repetitive stress injuries were incurred as a result of Apple's failure to warn about the potential for RSI. One of the requirements in the settlement is that the terms be kept secret. IBM, also named in the suit, has asked the judge to declare a mistrial, saying that news of Apple's settlement was prejudicial. The judge has rejected that motion. IBM says it does not intend to settle. (Tampa Tribune, 28 Feb 1995, B&F1)

---

### **Apple Settlement Due to Lawyer Error (Edupage, 2 Mar 1995)**

*E-D-U-P-A-G-E <info@ivory.educom.edu>*

*Fri, 3 Mar 1995 16:44:13 -0500*

Apple Computer's recent move to settle the repetitive stress injury lawsuit brought by a former high school secretary in Minnesota was prompted by "errors" its law firm, Saperston & Day, made in not turning over some documents before the trial. The judge had threatened to declare a mistrial or impose sanctions because of the oversight. Saperston & Day will pay the settlement. (Wall Street Journal, 28 Feb 1995, B7)

---

### **More Security Problems on the Internet (Edupage, 23 Feb 1995)**

*Edupage <info@ivory.educom.edu>*

*Thu, 23 Feb 1995 20:35:30 -0500*

The Computer Emergency Response Team has issued a public warning on a vulnerability in some 20 commonly used e-mail programs that run on Unix operating systems. The advisory said the latest discovery could allow a hacker to "read any file on the system, overwrite or destroy files." The ultimate solution to these recurrent security problems, says Purdue University professor Eugene Spafford, is for consumers to demand better security features from software manufacturers. In the absence of improved software, "are we going to continue seeing problems? You bet." (Wall

Street Journal, 23 Feb 1995, B8)

---

## Encryption Lawsuit Filed in California (Edupage, 28 Feb 1995)

Edupage <info@ivory.educom.edu>

Tue, 28 Feb 1995 20:09:58 -0500

A graduate student at the University of California at Berkeley has filed a lawsuit against the federal government, charging it with unfairly limiting his ability to discuss his research on encryption software. The plaintiff developed an equation for encrypting information, and wishes to publish a paper on his work, as well as software based on his equation. He would also like to discuss his findings at professional meetings. The federal government's export-control laws restrict the publication of cryptographic software and documentation. The Electronic Frontier Foundation is handling the plaintiff's case. (Chronicle of Higher Education 3/3/95 A19)

---

## Anti-Cyberporn [Exon] Bill Introduced

Edupage <info@ivory.educom.edu>

{[date] lost, on or just after 8 Feb 1985\}

Sen. James Exon (D-Neb.) has introduced legislation calling for two-year prison terms for anyone convicted of sending obscene or harassing e-mail. Commercial providers have protested, noting their service is more like a telephone company, which is not held responsible for the conversations carried over its conduits, but Exon remains unmoved: "If I were against this, if I didn't want to be bothered with it, if I felt it might complicate my ability to make money on the superhighway, that's the argument I would make." Meanwhile the Center for Democracy and Technology is pushing for more sophisticated filters that users could customize to block specific types of messages. "You could have the Pat Robertson rating system, the Motion Picture rating system, the Playboy rating system," says the Center's founder. (\*Wall Street Journal\*, 8 Feb 1995, p. B6)

---

## Home Gambling Network

"Mich Kabay [NCSA Sys\_Op]" <75300.3232@compuserve.com>

25 Feb 95 08:58:45 EST

The Washington Post (95.02.24, p. C1) has an interesting story on virtual gambling:

The Home Gambling Network:

It's Illegal, Maybe Immoral, but Is the Cyberspace Casino  
a Good Bet?

by Richard Leiby

Washington Post Staff Writer

NEW YORK--Surrounded by a sea of techno-suits discussing the future of media convergence in a bidirectional world of system-neutral platforms, the guy with the shaved head and black leather jacket had to smirk. "What's funny to me," John Bates said, "is how tremendously clueless most of these people are."

The author makes for the following key points:

- \* Gambling in the U.S. is a \$400 billion industry.
- \* A hundred people paid U\$595 to attend a one-day conference in NYC entitled, "Interactive Gaming: What's the Payoff?"
- \* Thirty-one year old Bates is "on-line service director" for the Virtual Vegas company, which is proposing "cyberspace casinos where real and computer-generated players interact in 3-D."
- \* US federal law currently makes betting across interstate borders using telecommunications illegal.
- \* In practice, gamblers have been making off-shore bets on U.S. sports events over the phone using their bank credit cards.
- \* The prospect of unlimited access to credit cards for gambling alarms some observers of addicted gamblers: "Give some people a credit-card-reading device with a keypad hooked into their phones or home computers--models of which were exhibited at the conference--and you're bound to have suckers blowing their life savings. And minors will find a way to log on to parental accounts."
- \* In Quebec, an interactive TV show lets people order up to C\$15 (~U\$11) of tickets a week (the limit is spelled out in legislation).
- \* The UBI (Universal Bidirectional Interactive) Consortium based in Montreal is working on a consumer-oriented electronic network which will include gambling services.
- \* Some observers predict "a family-values backlash" against such computer-mediated gambling.

M.E.Kabay,Ph.D., Director of Education, Natl Computer Security Assn (Carlisle, PA); Mgmt Consultant, LGS Group Inc. (Montreal, QC)

---

## **Losing your Marbles and your Barings**

*Peter Wayner <pcw@access.digex.com>  
Wed, 1 Mar 1995 13:08:23 -0500*

The story of the young trader who brought down Barings Bank captivates me as much as it captivates the headline writers at the NY Post. James Glassman

wrote in the Washington Post (March 1, 95), "I don't mean to paint him as a romantic hero, but he has reminded us-- in this age of huge financial institutions guided by high-speed computers-- that one little guy can still move the world." RISKS readers, though, should be intrigued because I suspect that deep below all of this may be an intriguing datapoint on the value of anonymity in the modern, electronic marketplace.

The Osaka Exchange publishes a weekly digest of the position. The Financial Times quoted someone saying, "everyone knew of the trades" and "no one could quite understand what Barings was doing with that sort of position."

This fact leads me to have some fun speculating on what happened. The futures and options markets are quite different from the stock market. Whenever someone loses a dollar, then someone else makes it. Value just doesn't evaporate into smoke like it does on the stock market when everyone decides a stock isn't worth it anymore. So every dollar that Barings lost was gained by someone else.

What does this have to do with anonymity? Everything. There aren't many people playing at these levels in the market so people can gang up on one and other. It's much like games of bridge or hearts where everyone can work together to stiff one player who might be in the lead.

If everyone knew that Barings was so deeply in the hole, they knew that it might not take much to push Barings into bankruptcy. Just a bit more selling in Tokyo and whammo, the firm is theirs at a huge selling price. No need to negotiate payment terms or other factors. If the firm doesn't have enough assets, the futures exchange might make up the difference from an insurance fund.

The strategy that might have been in play was similar to the one that lead to the table stakes rule in poker. The rule limits bets to the smallest pot still in the hand. This prevents the richest player from winning every hand by merely outbidding everyone. Don't play poker against Bill Gates without it. (If you want to see what it could do to a marriage, check out the film "Honeymoon in Vegas.")

There is no such rule in these markets and Barings should have known better than to expose themselves to this risk. I suspect, though, that they might have been much safer if their action was kept anonymous.

Of course this theory is just a theory. As Glassman would like to believe that a little guy can still move the world, I want to believe that large cabals can gang up on the little guy.

---

## **UK National Audit Office report on computer misuse in government**

*Brian Randell <Brian.Randell@newcastle.ac.uk>  
Wed, 1 Mar 1995 11:23:59 +0000*

[Source: COMPUTER HACKING AND THEFT RIFE IN WHITEHALL, by CHRIS BLACKHURST  
Westminster Correspondent, The Independent, 1 Mar 1995.]

Hacking into Whitehall computers soared last year, with a 140 percent rise in the number of reported incidents. An investigation by the National Audit Office, the public finance watchdog, found that Government departments reported 655 hacking incidents last year, of which 111 were successful. Most hackers were internal staff exceeding their authority to obtain unauthorised information to leak to outsiders, and got oral or written warnings. Twelve percent of cases ended in legal action.

The report includes these items:

- Civil servants and outsiders conspired to defraud a Government department of (pounds sterling) 1.5m. Police are investigating and eight arrests have been made.
- A civil servant obtained personal details of colleagues to blackmail them.
- A Government official obtained the private address of a married couple, possibly to assist in the kidnapping of the wife.
- Two staff members were prosecuted and fined (pounds sterling) 3,750 after leaking computer data.

Government computers are also increasingly prone to viruses and programmes designed to harm data and other software. Last year, Government departments and agencies reported a 350 percent rise in virus incidents, to 562. Over half of these cases, NAO points out, were detected by anti-virus scanning software.

Two outbreaks were labelled "significant" by the NAO:

- Thirty-eight viral infections were traced to one PC hard disk, loaded with pirated computer games. Civil servants had been exchanging games by floppy disks or through e-mail. The viruses were the games manufacturer's own anti-bootlegging devices.
- Four PCs in a Government typing pool had been infected with a virus which took two days to eradicate.

If hacking and viruses were not bad enough, theft, reports the NAO, "continues to be a major problem, with portable computers, printers and laptop computers being the main targets."

There were 433 reported incidents of theft of Government computer equipment last year, a rise of 60 percent. In all, equipment costing (pounds sterling) 1.2m was taken. This included two break-ins to the same office within three months and the loss of equipment worth (pounds sterling) 102,000. The thieves, who have not been caught, were thought to have been "stealing to order." Likewise, the culprits behind the theft of 11 PCs and other hardware, worth (pounds sterling) 55,000, have not been found.

In one of the more bizarre incidents, somebody went to the trouble of taking a computer desk from a room and replacing it with an old one. The locked drawers of the desk were broken into, and information, mostly



than the limit. The bank gave her the card and told her it was good for up to \$50 or \$300 or whatever; the bank should be responsible if an error on their part allowed more than this to be taken.

I wonder if any personal theft insurance policies cover losses from ATM cards?

---

## Sick Medicare Scanner

*Judith Seeger <jws@hpl.hp.com>*

*Thu, 2 Mar 95 9:15:10 PST*

San Jose Mercury News' Action Line section, 15 Feb 1995:

SORRY, WRONG NUMBER

Q. In October 1993, I received a statement from Medicare that my wife had medical attention in Healdsburg from a Dr. John Fries. I notified Medicare that this was incorrect. Neither of us had ever been in Healdsburg. Medicare answered, thanking us. The other day we received another letter from Medicare showing that Fries had submitted another claim for treating my wife. It appears someone is using my wife's name and Medicare number to obtain care. Or maybe the doctor is making up these visits. Could you check into it? C.E.F., San Jose

A. No one is using your wife's Medicare number; nor is the claim submitted in a fraudulent manner, says Claudette Ballard, office manager for Fries. The last time this happened and this time, too, Medicare's scanners misread one of Fries' patients' Medicare number and picked up your wife's number. Ballard says the scanner is somehow reading the fifth digit in the number incorrectly and billing the service as if your wife received it. Ballard has contacted Medicare again and was assured steps would be taken so it doesn't happen again. She is writing you a letter to explain the problem in more detail.

---

## Interstate Panopticon

*Phil Agre <pagre@weber.ucsd.edu>*

*Sat, 25 Feb 1995 17:59:07 -0800*

The press is starting to notice some of the serious privacy problems with the rapidly advancing proposals for "Intelligent Transportation Systems" in the United States. Here are a couple of relevant articles:

Richard Simon, Camera gains more exposure as a device for traffic control, Los Angeles Times, 20 February 1995, pages B1 and B3.

This one is about the accelerating use of video cameras on roads in Southern California. In the near term they're mostly to identify the causes of traffic jams. But the Blue Line between Los Angeles and Long Beach will soon have cameras to detect drivers who attempt to circumvent lowered gates to cross the

train tracks. And although the state Office of Traffic Safety is concerned about "a growing problem with commuters eating, reading, changing clothes, brushing their teeth and generally paying less than full attention to the road", it says it has no current plans to check up on these things with its cameras.

The cameras, in case you're wondering, are in bulletproof containers.

Although some of the problems that state traffic officials have identified are genuine, the real difficulty is in their basic philosophy for solving them. Rather than collect information and circulate it in a decentralized fashion that is useful to individual drivers and engineering crews without permitting unlimited accumulation of information that identifies individual drivers, they have set up a general-purpose centralized observation center in downtown Los Angeles.

The slippery slope here is steep: as technologies of surveillance are put in place, new applications will always be available that are only one short step beyond what they've been used for so far. I am generally skeptical about visual metaphors for privacy problems, but this is one case where the Panopticon offers a perfectly simple and straightforward model.

That's not so clear in another, much bigger and more consequential case:

Don Phillips, Big Brother in the back seat?: The advent of the "intelligent highway" spurs a debate over privacy, Washington Post, 23 February 1995, page D10.

This article concerns the "privacy principles" being circulated by the Intelligent Transportation Society of America, which is the industry group coordinating the development of a national architecture for transportation automation systems, including systems that track the locations of vehicles for a range of purposes. Although nobody in the United States is currently proposing that the use of these technologies be made mandatory for drivers, it is very likely that they will become unavoidable as a practical matter, since they will probably be used to implement much more widespread roadway toll-collection. The most recent version of these principles that I have seen is dated December 13th 1994, and they are in fact seriously problematic. For example, they only place very loose restrictions on secondary uses of the information by marketers, and they envision no restrictions on the powers of access to ITS travel information that individual states can confer upon local police. You can retrieve a copy by sending a message that looks like this:

To: rre-request@weber.ucsd.edu  
Subject: archive send its-privacy

Or you can look at them on WWW at:

<http://weber.ucsd.edu/~pagre/its-privacy.html>

I will probably circulate another message about these principles soon. The Phillips article notes that many people are concerned about law enforcement uses of ITS information; ITS America feels that such use is inevitable and

simply wishes the public to be informed of this fact -- they wish to focus on knowing "what the rules are" rather than on actual privacy. The tragedy is that it is completely unnecessary for these systems to collect information that identifies individuals. Profound violations of individual privacy are not the price of progress. Rather, they are the price of using old-fashioned technology, neglecting innovations such as public-key cryptography and digital cash that protect privacy without sacrificing functionality.

Phil Agre, UCSD

---

## Risks of living on the left side of the continent

*"Rob Slade, Social Convener to the Net" <roberts@mukluk.decus.ca>*

*Tue, 28 Feb 1995 12:40:09 EST*

Memoirs of a (coastal) virus researcher

Some people may not be aware that, by disconnecting the modem and attaching a device known as a "telephone", communications circuits may be used for voice communications. Unfortunately, unlike email, "telephone" calls must be synchronous (or, more correctly, bisynchronous) in that both parties must be active on the circuit at the same time. With the rise in modern communications technologies, scenes like the following are becoming more common:

RRING

RRING

RMS : Hello?

DFP: Hi! I'm looking for, ummm, Robert Slade?

RMS: Speaking.

DFP: Oh, good. My name's \_\_\_\_\_ and I'm with the Detroit Free Press. I've got a copy of your book, and I thought we could do a story on this computer virus situation.

RMS: Uh huh.

DFP: I read most of it, and I liked it, but I've got a few ... sa-a-a-y. Isn't Vancouver on the \*West\* Coast?

RMS: Usually.

DFP: Oh, gee, I'm really sorry. See, we're three hours ahead, and ... gee, should I call back later?

RMS: No, that's OK, I had to get up and answer the phone anyway.

DFP (puzzled): Oh, really? Why's that?

RMS: It was ringing.

I love reporters. They always get the straight lines right.

=====

DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733  
Author "Robert Slade's Guide to Computer Viruses" 0-387-94311-0/3-540-94311-0



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 16: Issue 87**

**Tuesday 7 March 1995**

## Contents

- [Authentication: \(1\) Vienna Marathon 1995; \(2\) Lotus Notes](#)  
[Li Gong](#)
- [Sexy photos just computer glitch](#)  
[Louis Todd Heberlein](#)
- [The source of semantic content](#)  
[Erann Gat](#)
- [Government of Singapore](#)  
[Robert Ashcroft](#)
- [Happy Michelangelo's Birthday](#)  
[PGN](#)
- [Microsoft and Lotus spreadsheet errors](#)  
[Timothy Hunt](#)
- [Spreadsheet Errors working paper available](#)  
[Ray Panko](#)
- [6-cent T-shirts](#)  
[Jeremy Stieglitz](#)
- [Risk system comes too late to prevent Barings' collapse](#)  
[Jeremy Stieglitz](#)
- [Securities](#)  
[Bob Frankston](#)
- [Barings: Greenspan quote](#)  
[Frank E. Carey](#)
- [Re: Compact Fluorescent Lights](#)  
[Mike Farringdon](#)
- [Re: Compact Fluorescent Lights](#)  
[Carl Maniscalco](#)
- [Re: Compact Fluorescent Lights](#)  
[Osma Ahvenlampi](#)
- [Info on RISKS \(comp.risks\)](#)

---

**Authentication: (1) Vienna Marathon 1995; (2) Lotus Notes**

*Li Gong* <[gong@cs1.sri.com](mailto:gong@cs1.sri.com)>

*Tue, 7 Mar 95 10:47:47 -0800*

(1) The Manchester Guardian Weekly (week ending March 4, 1995) reported that, in this year's Vienna Marathon, the runners will have to wear specialized computer chips buried inside (or attached to) their shoelaces. The purpose is to ensure that the runners stay on course. Last year, some took short cuts while an Italian rode some distance on the underground (subway). [LG: It is of course easy for one runner to help carry another's shoelaces, but at least collusion is now required.] [Or, put your shoelaces on an accomplice's bicycle, and take public transit? PGN]

(2) On a different matter, Cynthia Dwork of IBM Almaden wrote in ACM SIGACT News 26(1) (March 1995) that the authentication procedure using public-key systems in Lotus Notes, as described in its "Internals online book", has security flaws. Lotus's response is (1) the actual system does not work as described in the manual and (2) how it actually works is proprietary information. [LG: (1) is dangerous by itself, and if (2) is true, then why pretending to describe the procedure in the first place.]

Li GONG Email: gong@csl.sri.com Tel: 415-859-3232 Fax: 415-859-2844  
SRI International, Computer Science Lab, Menlo Park, California 94025, USA

---

### sexy photos just computer glitch

*Louis Todd Heberlein <heberlei@cs.ucdavis.edu>  
Mon, 6 Mar 95 09:00:54 -0800*

>From an Associated Press story entitled  
"Sexy photo just a computer glitch, lab worker says"

A Lawrence Livermore National Laboratory employee was found innocent of misusing lab computers to store sexy photos. Accused of accessing 33 photos of bikini-clad women from an Internet site called "supermodels", the employee said he thought the photos were related to engineering.

The employee has been promoted since the initial charges.

---

### The source of semantic content

*Erann Gat <gat@aig.jpl.nasa.gov>  
Sun, 5 Mar 95 18:50:01 PST*

It's probably old news for RISKS readers, but a very difficult concept for lawmakers, that the semantic content of bit streams is in the eye of the beholder, and that the apparent correspondence between bits and semantics is the result of engineering convention and not an inherent property of the bits. Any attempt to legislate the content of digital communications is therefore doomed to fail because it is trivial to hide the source of semantic content. The following is a simple example of how this can be done; much more sophisticated examples are possible.

Imagine that Senator Exon's bill has passed, and it is now illegal to

transmit pornography on the net.

I take a pornographic image file P and encrypt it with a one-time pad. That is, I generate a string of random bytes the same length as P, and exclusive-or corresponding bytes. The encrypted image I put in a file called F1 and the one-time-pad key I put in a file called F2.

F1 and F2 have some interesting properties. They are both random bit streams, completely devoid of semantic content. In fact, there is no way to tell which file contains the encrypted image and which file contains the key. They are mathematically indistinguishable. All the information in P is now encoded in the \*correspondences\* between the two files. There is really no information in either file. If either file is lost, P is absolutely unrecoverable.

Now suppose that I email F1 to person A and F2 to person B. Then A and B exchange F1 and F2. A and B each can now recover the original image. Has the law been broken? Who broke it? All anyone did in the above scenario was to send a random bit stream to someone else. At no time did anyone send a bit stream with any identifiable semantic content.

One might argue that I broke the law by sending out two files that I knew could be combined to produce a pornographic image. So imagine now that A sends a random bit string F1 to B, who then uses this as a one-time pad to encode P, which B then sends back to A. Has the law been broken? Who broke it?

This scenario has an interesting subtlety. In order to prove that B has transferred information to A and not vice-versa it is necessary to prove that A sent F1 \*before\* B sent F2 (since there is no way to distinguish F1 and F2). So B could never be convicted of violating the law, since he could always claim that he had sent F2 before receiving F1, and that therefore A had transferred P to him rather than vice versa. Even if the government had timestamps to show that F2 was sent after F1, B could claim that this was simply a retransmission.

If A and B exchange P in this way, then they can individually publish F1 and F2, from which anyone can recover P, but both A and B can plausibly deny having done anything but publishing a random bit stream.

The DA might try to prosecute both A and B on a conspiracy charge, but it is not necessary for A and B to have conspired. The mere knowledge that random bit streams can be used in this manner might prompt some people to start sending random bit streams around. Without reliable time stamps there is no way to trace the introduction of semantic content. So as soon as anyone starts to transmit one-time-pads, everyone can publish anything and no one can be prosecuted for it.

The RISK here is that the government will not realize that attempts to legislate content is a hunt for cybersnarks, and that transmitting random bit streams may soon become a crime.

Erann Gat gat@jpl.nasa.gov

[The situation is even more complicated by the availability of programs that mask encrypted messages as graphical image files (.gif), so that irrespective of their REAL content, a message appears to be an innocuous picture. PGN]

---

## Government of Singapore

*Robert Ashcroft <rna@GSB-Pound.Stanford.EDU>*

*Tue, 7 Mar 1995 14:08:14 -0800*

This week's Economist (issue of March 4) has an article about the attitude of the Singapore govt to soc.culture.singapore and the idea of the Internet in general.

The Singapore govt is perhaps not the most liberal in the world, and in particular is highly critical of "western influence". On the one hand it seeks to keep Singapore technologically up to date by wiring the country to the Internet, on the other hand it seeks to maintain control over what its population sees, two obviously incompatible goals. In particular it's concerned about "incorrect" things written in soc.culture.singapore. The information minister, George Yeo, suggests that the youth league of the ruling People's Action Party should set up some sort of truth squad to counteract incorrect posts.

This is a road down which I would just as soon not have a government walk. Could they resist taking the next step, namely forging cancellations and so forth (as for instance, the Church of Scientology seems to have done)?

The Internet \_is a threat to any regime that tries to restrict in anyway what their people see. My own feeling is that any attempt to control it, short of disconnecting it altogether, will be doomed. As The Economist notes, on the Internet, nobody gets the last word. However, I imagine there will be numerous battles before that sinks in. I wonder how many intelligence agencies now have separate Internet sections, studying such things as Internet sabotage methods and the like.

RNA

---

## Happy Michelangelo's Birthday

*<neumann@csl.sri.com>*

*Tue, 7 Mar 95 17:45:03 PST*

Guy Webster, in an \*Arizona Republic\* article, Michelangelo Virus Catches More Businesses This Year reported several strikes this year.

\* Denise Bayless' PC found scrambled data and software on the hard-drive.

\* ``This year has been the worst, without question," said Ken Coleburn, owner of a computer consulting firm in Tempe. His company fielded 140 calls this year, compared with about 30 last year. He suggested this might have

been due to Michelangelo's birthday falling on a workday this year.

\* RG Software Systems in Scottsdale, Ariz., which sells anti-virus software to large companies worldwide, was contacted by three prospective customers in other states Monday. They apparently had lost crucial computer data to Michelangelo, RG Software owner Ray Glath said.

[Several other sources elsewhere -- presumably more careful -- reported no troubles. PGN]

---

## Microsoft and Lotus spreadsheet errors

*"Timothy Hunt [Assistant Unix Systems Manager]" <timothy@icr.ac.uk>  
Mon, 06 Mar 95 14:41:01 +0000*

Suppliers admit to spreadsheet errors [Computing, 2nd March 1995, p.11]

Microsoft and Lotus Development have admitted that their spreadsheet products may produce inaccurate results because of an inherent problem with the design of all computers. Mistakes can occur in precision calculations, of the kind required by engineers and users in the scientific, banking and finance sectors.

Andy Lees, desktop marketing manager at Microsoft UK, said rounding errors may sometimes occur in Excel calculations set to a significant number of decimal places. He said this was due to the conversion of base 10 decimal numbers into base 2 binary digits recognised by computers. Lees played down the problem, saying the margins of error was 'very small' and that few would come across it.

However, users in at least one large merchant bank were last week warned to take extra care over calculations in Excel. Barry Ward, technical support manager at Computacenter, which is providing the bank with PC support services, fears users may be unaware of the problem. He added that the bank stumbled across the error when one of its users manually checked calculations against computer-generated results. 'I've been in the computer business for 19 years and have never come across this problem before. In my opinion, this could throw a spanner in the works for a large multinational company,' he added.

The user was adding and subtracting a simple set of figures: 120, 30.8, 20.5 and -120, -30.8 and -20.5. Instead of zero, the result produced was -1.43 E-15. Ward claimed changing the order of numbers produced different results.

According to Microsoft's Lees: 'There is a limit to the level of accuracy you can get with computers. In Excel a rounding error will sometimes appear on the fourteenth or fifteenth decimal place, but it will be very small. Excel has a high degree of accuracy.'

Lotus Development acknowledged that some users require high levels of precision in calculations, but claimed that rounding errors in its 1-2-3

spreadsheet can be avoided by formatting cells.

[This article reminds me of part of a course during my degree looking at the problem of calculations in the Floating point domain ( $\mathbb{F}$ ). It is often wrongly assumed that  $\mathbb{F}$  and the Real domain ( $\mathbb{R}$ ) are equivalent, but because of limits in the space to store a number, while it is always true that

$a+b-b = a$ ;  $a, b$  member of  $\mathbb{R}$ ,

it is NOT always true that

$a+b-b = a$ ;  $a, b$  member of  $\mathbb{F}$ .

The course also looked into ways of designing algorithms to try and detect and prevent errors of this kind occurring.]

Timothy J. Hunt, The Institute of Cancer Research, Royal Marsden NHS Trust,  
Downs Road, Sutton, Surrey England SM2 5PT +44 (0)181 642 6011 x3312

---

## Spreadsheet Errors working paper available

"Ray Panko" <PANKO@busadm.cba.hawaii.edu>

Tue, 7 Mar 1995 14:13:39 -1000

We have just finished a working paper on spreadsheet errors. The working paper describes our experiment. It also discusses earlier experiments and field audits. The paper also presents a taxonomy of spreadsheet errors.

The good news is that laboratory spreadsheeters only have about the error rate per cell as professional programmers do per program statement. The bad news is that while professional programmers go on to the next step of deep debugging, spreadsheet developers do not do this frequently. Overall, it looks like a significant fraction of the hundreds of millions of spreadsheets produced each year have errors.

The paper is in Word for Windows 2.0 format. You may get it via anonymous ftp from splicer2.cba.hawaii.edu After logging in, go to the Panko directory. Then the SSERRORS directory. The file is SSWPMAR.DOC

I would value any comments and suggestions you might have.

Also, please keep in mind that we will be having a minitrack on risks in end user computing at the January 1996 Hawaii International Conference on System Sciences.

Aloha, Ra3y (the 3 is silent)

Prof. Raymond R. Panko, Decision Sciences, College of Business Admin.,  
University of Hawaii, 2404 Maile Way, Honolulu, HI 96822 (808) 956-5049

---

## 6-cent T-shirts

Jeremy Stieglitz (S&T OnSite) <a-jerems@microsoft.com>

Mon, 6 Mar 95 09:56:00 PST

I recently encountered two RISKS surrounding cash registers. The first occurred while I was on holiday in Arizona. I was caught in a downpour on the golf course and decided to buy an inexpensive t-shirt at the drug store. The shirt was on \*special\* sale, three for ten dollars. When I went to pay for the shirt, the clerk had no problem remembering the price, but an insurmountable problem entering the price into the cash register. No matter what he tried, the register was beeping and chirping everytime he tried to enter 1/3 of \$10.00 as a price. (Perhaps this was simple human error, but there is still a RISK here...) After a rather long line was starting to form in my line, I said to this gentleman, "look, just ring it in as \$3.50." He said he couldn't do that and kept trying to enter the proper price. After what seemed like ten or fifteen tries, he managed to enter something that was accepted by the register, and turned and smiled at me and said, ".06 cents please."

And then, just last week, I needed a shallot for something I was cooking. The grocery store I went to had some very expensive shallots, something like 16\$ a pound! So I took a very small bud and went up to the cash register. The clerk put the bud on the scale, and it came up as 0.0 ounces, which it would not accept. (The scale automatically deducted .1 ounce for the plastic bag.) But I hadn't put a bag on the shallot. Once again, after several tries, and a line forming behind me, I suggested she just tip the scale with her thumb. She wouldn't go for it. She let me have the shallot for free.

The RISKS here seems to be when technological advances do not allow for other alternatives. These automated registers probably do make balancing the books a lot easier at the end of the day, but they don't seem to be very flexible. In the old days, both clerks could have simply entered any price they wanted in their registers. Nowadays, with their complete reliance on these automated registers, balancing the register and not the balance sheet seemed foremost to these clerks. And for lucky consumers like me, sometimes we end up with .06 cent t-shirts and free shallots.

---

## Risk system comes too late to prevent Barings' collapse

*"Timothy Hunt [Assistant Unix Systems Manager]" <timothy@icr.ac.uk>  
Mon, 06 Mar 95 13:48:05 +0000*

[Article in Computing, 2 March 1995, front page]

Risk system comes too late to prevent Barings' collapse

Collapsed merchant bank Barings was only months away from installing a risk management system in its Far East offices which was intended to alert senior executives to gambles being taken with the company's money.

Barings, the UK's oldest investment house, was plunged into financial ruin last weekend when 28-year old Nick Leeson lost more than UKP 750 million of clients' funds on the Singapore derivatives exchange.

In January 1994, the bank began rolling out a communications architecture called BORIS (Barings Order Routing & Information System) to improve the

processing of information about deals. Prior to this, Barings staff had used paper and fax machines to exchange information.

BORIS had gone live in London, Tokyo and New York, with Barings' Far East offices, including Singapore, set to follow by mid-1995. An extension to BORIS, dealing specifically with risk management, went live in London HQ in the last few weeks and was also set to be rolled out in the Far East in the near future.

Dealing in derivatives involves betting on the movement of shares on national stock exchanges and carries substantial risk of losing vast amounts of money.

Frank Ranger, a director of City Consultants, said any system intended to manage that risk needs access to data from every market involved in the transactions. 'There is a clear need to get consolidated information from products in some sort of control function,' he said.

Peter Hynd, Barings' assistant IT director, was unavailable for comment, but sources believe the bank's existing settlement system contributed to the collapse.

The Cash Risk Management system was supposed to flag cash positions, but if settlements were not processed according to the bank's procedures, it could not do so.

Timothy J. Hunt, The Institute of Cancer Research, Royal Marsden NHS Trust, Downs Road, Sutton, Surrey England SM2 5PT +44 (0)181 642 6011 x3312

---

## Securities (as opposed to security?)

<Bob\_Frankston@frankston.com>  
Sun, 5 Mar 1995 18:20 -0500

As the Derivative fiasco continues to unfold I keep thinking about how much it sounds like the typical computer risk though it is an age old financial fiasco. But the resemblance is not just coincidence and it helps in putting the computer risks in perspective. The key characteristic of both is that the effect of an action is out of proportion to the action itself and is not (easily?) predictable. In both cases, hubris is the killer. Fortune had an update on article on the issues (pun?). It is a world populated by those who invest millions or billions on hunches and, even more scary, make bets best of formulas they do not understand. Perhaps no one understands. Sounds like software. (Sounds also like the sophomore effect -- a naive belief in the magic of the new trick one has just learned)

Like software, used with a reasonable understanding and modest goals, derivatives can be effective tools (ironically, to reduce risk). Like software, complexity and a lack of reality checking leads to disaster. And like software, success can breed disaster by encouraging one to plunge deeper and deeper. A billion dollars is a lot to lose, but companies have been brought down by software bugs.

---

## Barings: Greenspan quote

*Frank E. Carey, Bell Labs <f.e.carey@att.com>*

*Mon, 6 Mar 95 09:16:03 EST*

``The one thing the Barings episode illustrates is the productivity for making losses has gone up very significantly in the last 25 years. You couldn't write the execution slips fast enough 25 years ago to lose as much money as was lost by one individual, aided by terrific technology."

Alan Greenspan, chairman of the Federal Reserve, quoted in \*The New York Times\*, 6 March 1995.

---

## Re: Compact Fluorescent Lights ([RISKS-16.84](#))

*<m.g.farringdon@swansea.ac.uk>*

*Wed, 1 Mar 1995 10:14:05 GMT*

We use a light box containing four fluorescent tubes for SAD (Seasonal Affective Disorder) and noticed two weeks ago that the remote controls for TV & VCR wouldn't 'control' when the light box was on. This seems to be the same symptoms that Suffern noticed with compact fluorescent lights.

Incidentally, while we've only been using the light box for three months, it does appear to alleviate SAD symptoms.

Mike Farringdon m.g.farringdon@swansea.ac.uk

---

## Compact fluorescent lights and infrared weirdness

*<HeavyWater@aol.com>*

*Thu, 2 Mar 1995 20:38:13 -0500*

I suppose this isn't really a computer Risk, but someone might find it interesting anyway. Edward S Suffern's report of compact fluorescent lights causing malfunctions in his infrared remote control devices ([RISKS-16.84](#)) reminded me of a related problem that I ran into in my former job as the chief technician for a cable television system.

My installer had reported a problem with a converter that he had just installed (to aid in converter control, installers were issued only enough of set top units to complete their scheduled installations for the day. Any problems encountered were referred to allegedly more trustworthy members of the technical staff.) This converter was equipped with an infra-red remote control device. When I arrived at the subscriber's home, the display on the converter was showing "7" and no matter what channel I attempted to turn it to, the converter always changed back to channel 7. I installed another box, assuming that it would solve the problem--CATV converters are notoriously unreliable despite what your local cable company might tell you. The new converter exhibited exactly the same behavior.

Baffled, I stood next to the TV set scratching my head until I happened to turn towards the viewer's sofa and noticed sunshine glinting off the whirling, chrome-plated blades of an electric fan running by the window--and a lightbulb went on inside my head. Sure enough, when I turned the fan off, the problem went away. Turning the fan back on caused the problem to reappear.

It seems that the moving blades of the fan were pulse-modulating the sunshine in exactly the right manner to confuse the infra-red receiver in the converter into thinking it was getting the "change to channel 7" command from the remote.

I spent almost another ten years in the industry after that and never ran accross that particular problem again.

Carl Maniscalco (heavywater@aol.com) San Diego, CA

---

### Re: Compact fluorescent lights ([RISKS-16.84](#))

*Osma Ahvenlampi <Osma.Ahvenlampi@hut.fi>*

*Fri, 3 Mar 1995 22:20:45 GMT*

In [RISKS-16.84](#), Edward S Suffern <Suffern@DOCKMASTER.NCSC.MIL> wrote of energy saving fluorescent lights affecting TVs and other remote controlled equipment, suspecting that these type of bulbs emit infra-red enough to confuse remote receivers. This is slightly inaccurate. Energy saving light bulbs actually emit less infra-red radiation than a normal incadescent bulb. However, the light is "strobing" at the 50kHz range, which is about the same as the pulse frequncy of a common remote control. Some receivers (simpler designs) get confused by this, and that's what caused the malfunction.



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 16: Issue 88**

**Weds 8 March 1995**

## Contents

- [Caller ID Ghosts](#)  
[Jim Huggins](#)
  - [Interesting cellular news from Pakistan](#)  
[Abhijit Dutta](#) via [Ben Burch](#)
  - [Re: Microsoft and Lotus spreadsheet errors](#)  
[Barry Margolin](#)
  - [Re: Confused remotes](#)  
[Philip H. Smith III](#)
  - [Re: The source of semantic content](#)  
[Steven Tepper](#)
  - [Re: The source of semantic content](#)  
[A. Padgett Peterson](#)
  - [Re: The source of semantic content](#)  
[Barry Margolin](#)
  - [Re: The source of semantic content](#)  
[Jeremy Epstein](#)
  - [Re: The source of semantic content](#)  
[Jon Krueger](#)
  - [Re: The source of semantic content](#)  
[Tim Kolar](#)
  - [Re: The source of semantic content](#)  
[David Harpe](#)
  - [Re: Sparc10 keyboards and resetting the CPU](#)  
[A. Harry Williams](#)
  - [Re: Sparc10 keyboards and resetting the CPU](#)  
[Simson L. Garfinkel](#)
  - [Re: Sparc10 keyboards and resetting the CPU](#)  
[Ed Bruce](#)
  - [Re: Sparc10 keyboards and resetting the CPU](#)  
[Mark Stalzer](#)
  - [Re: Sparc10 keyboards and resetting the CPU](#)  
[David Honig](#)
  - [Info on RISKS \(comp.risks\)](#)
-

## Caller ID Ghosts

*Jim Huggins <huggins@eecs.umich.edu>*

*Wed, 8 Mar 1995 10:20:31 -0500 (EST)*

News item from the Detroit Free Press, 8 March 1995.

A Detroit area woman last week looked at her Caller ID box (manufactured by CIDCO, Morgan Hills, CA) and was puzzled to notice that it indicated 19 received calls that evening, even though only one person had called. Then she checked the names listed. John F. Kennedy. Thomas Paine. Harry S Truman. John Hancock. Ulysses S. Grant. Samuel Clemens. Ronald Reagan. And many others.

Most of the phone numbers were non-working, but a few were. Ryan Biermann, an English student at the University of Wisconsin-Madison has been plagued with phone calls for Abraham Lincoln recently.

No definitive explanation has been given. Ameritech (the Baby Bell for Detroit and Madison) believes the Caller ID box was probably a pre-programmed demonstration model. Dave Glowacz, a telecommunications consultant in Chicago, suspects the work of a phone hacker.

Depending on the cause, lots of old Risks here (either a faulty demonstration circuit with non-fake data or an insecure data system), but perhaps with a new face to them.

Addendum: accompanying the article is a photo of the Caller ID box listing Abraham Lincoln's name and phone number. I hope Mr. Biermann won't be getting too many more phone calls because of it ...

Jim Huggins (huggins@umich.edu)

---

## Interesting cellular news from Pakistan

*Burch Ben <Ben\_Burch@wes.mot.com>*

*Mon, 6 Mar 1995 17:21:30 GMT*

From misc.news.southasia Sun Mar 5 17:56:49 1995

From: abducta@icaen.uiowa.edu (Abhijit Dutta)

Date: Sun, 5 Mar 1995 00:34:16 GMT

Newsgroups: misc.news.southasia

Subject: Pakistan Forces Motorola To Halt Cellular Services In Karachi

Voice of America, March 04, 1995

By Jennifer Griffin

Islamabad: The Pakistan government has forced the US telecommunications giant, Motorola, to halt mobile telephone service to the country's strife-torn city, Karachi. Pakistani officials are demanding Motorola hand over sophisticated eavesdropping equipment that would allow intelligence agencies to tap into phone calls made on the company's

cellular network. Analysts are saying the government's action is not encouraging to foreign investors. The Pakistan government claims it is trying to crack down on Karachi terrorists using mobile telephones to coordinate attacks and organize violence in the ravaged city.

In a memo to James Beneda, the president of Mobilink -- Motorola's Pakistani joint venture -- the communications ministry demanded equipment needed to tap into all calls made by its subscribers be given to the government.

Without these sophisticated scanners, intelligence agents would not be able to tap into the cellular network. It is the first time the government has admitted such tapping and eavesdropping is commonplace in Pakistan. Mobilink's service to Karachi was cut by the government January fourth.

According to Mobilink's regional manager, Zahid Hussain, two other cellular phone companies presently operating in Karachi have not had their service interrupted because their calls are easily tapped. "The facility the other two cellular companies have, all you do is buy a 200-dollar scanner from Hong Kong or wherever, and you can walk the streets and just keep tuning into different frequencies and listening to people's conversations."

Mr. Hussain says his company will comply with some of the government's demands and will deliver the mobile scanning equipment sometime this month. But, there remain other obstacles to resuming operations. The government has also demanded Mobilink not expand its number of subscribers from the present 3000 -- a request mobilink officials say they cannot possibly honor.

US state department officials and Secretary of Commerce Ron Brown are said to have brought the matter to the attention of Pakistan's Washington Ambassador, Maleeha Lodhi.

The US-based company has invested more than 32-million dollars in establishing its Pakistani operation since last August, and intended to invest nearly 20-million dollars more this year.

The scandal has caused many foreign businessmen to rethink their investment in Pakistan, where they say licensing agreements are easily rewritten and often disregarded. Mr. Hussain says the government's handling of the incident sends a negative signal to foreign investors, particularly on the eve of prime minister Benazir Bhutto's trip next month to the United States.

Ben Burch Motorola Wireless Data Group Ben\_Burch@wes.mot.com

---

**Re: Microsoft and Lotus spreadsheet errors (Hunt, [RISKS-16.87](#))**

<barmar@nic.near.net>

Wed, 8 Mar 95 06:17:33 EST

>Barry Ward, ... `I've been in the computer business for 19 years and  
>have never come across this problem before. ...

I find it difficult to imagine someone who's been in the computer business for two decades and has never heard of floating point round-off errors. This should be part of any computer science curriculum.

Of course, part of the problem is that 20 years ago, virtually all business software was written in COBOL or PL/I, and that's probably Mr. Ward's background. These languages provide fixed-point decimal as a built-in data type, and require that decimal arithmetic be done accurately. There may still be round-off errors (e.g. dividing 100 by 3, or multiplying .01 by .01 and putting the result in a variable with two digits after the decimal point), but the programmer has direct control over the level of precision.

These days, end users use spreadsheets to write "business software", and the spreadsheet designers seemed to have forgotten how business software has traditionally worked. The spreadsheet implementors are simply using the built-in mathematics that C provides, which is not appropriate for this problem domain. Floating point was designed for scientific computing -- it's often not much of a problem that errors are introduced, since there's an inherent imprecision in the input data (since it's translated from the analog real world to the digital cyber world).

Barry Margolin, BBN Internet Services Corp. barmar@near.net

---

## Re: Confused remotes

703) 506-0500 <PHILS@RELAY.RELAY.COM (Philip H. Smith III,>  
Wed, 08 Mar 95 07:59:24 EST

Re: the various appends about lights, etc., fooling remote controllers: I used to have a Jerrold cable box that had a clock in it. When I used my stereo receiver remote, it would sometimes cause the Jerrold clock to jump an hour. What was interesting about this was that this was NOT a function offered by the Jerrold remote! ...phsiii

[This is a clock that goes JERROLD McBoing-Boing when it triggers the alarm? If it change the right <left?> digit, it would become a YEAR-OLD clock. PGN]

---

## Re: The source of semantic content ([RISKS-16.87](#))

Steven Tepper <greep@datatools.com>  
Tue, 7 Mar 95 21:51:17 PST

> [The situation is even more complicated by the availability of  
> programs that mask encrypted messages as graphical image files  
> (.gif), so that irrespective of their REAL content, a message  
> appears to be an innocuous picture. PGN]

What about going in the other direction? If you take an image file or some other data file (say a core dump file) that appears random, apply some simple operations (say XOR with various values) to it and run the output through a program that filters out everything except strings of alphanumeric characters (such as the Unix "strings" program), eventually you're bound to come up with something that contains some obscene words, possibly "misspelled". A zealous prosecutor could use this to "prove" that the original was an encrypted form of obscene text.

---

**Re: The source of semantic content ([RISKS-16.87](#))**

*A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>*

*Wed, 8 Mar 95 10:17:21 -0500*

[The situation is even more complicated by the availability of programs that mask encrypted messages as graphical image files (.gif), so that irrespective of their REAL content, a message appears to be an innocuous picture. PGN]

Let's consider something even easier: Take a digital picture "A" of a politico presenting an award. Using a graphics editor, a miscreant removes certain items and adds a mustache (or something). The two digital files are then XORed so that only the changes remain in file "B".

Again we have a two part solution but now the first part is mixed so that the second becomes a night sky or lost in the 24th bit of the first.

Viewed as sent, it is an innocuous picture, but rearranged...

Can you see the prosecutor trying to explain "yes but if you switch this and change that color and twitch you nose it becomes..."

Kinda like the person (not catching me with that one) complaining of the indecent behaviour next door: "Yes officer, it's horrible. Just climb out here on the roof of the garage, lean against that light pole and with these infrared binoculars you can see it just as plain..."

"Life will find a way". Padgett

---

**Re: The source of semantic content (Gat, [RISKS-16.87](#))**

*<barmar@nic.near.net>*

*Wed, 8 Mar 95 06:17:33 EST*

>If A and B exchange P in this way, then they can individually publish F1 and >F2, from which anyone can recover P, but both A and B can plausibly deny >having done anything but publishing a random bit stream.

Unless they actually didn't know what the purpose of those random bit streams were, they would be perjuring themselves. They would have to

convince a judge (and maybe jury) that they really thought they were just random bit streams, and they were passing them to each other for no reason. Were I on the jury, I would be skeptical.

Barry Margolin, BBN Internet Services Corp. barmar@near.net

---

**Re: The source of semantic content (Gat, [RISKS-16.87](#))**

*Jeremy Epstein -C2 PROJECT <jepstein@cordant.com>*

*Wed, 8 Mar 95 10:11:09 EST*

In [RISKS-16.87](#), gat@aig.jpl.nasa.gov (Erann Gat) had some very clever comments about ways of exchanging bit streams that together make up a picture. I'd propose another scenario: if U1 embeds a pornographic image in the background of a picture, and sends U2 a binary image of the picture, U2 may well be unable to detect it. If U2 forwards the picture to U3, who (if anyone) has violated the proposed Exon law? As was shown in a paper published at the 1993 Computer Security Applications Conference, an amazing amount of data can be embedded in a digital picture without it being visible to a human looking at the picture on a screen or on paper.

Truly amazing how little insight our legislators have into the technology they're trying to legislate.

---

**Re: the source of semantic content**

*"Jon Krueger" <jpk@pet.com>*

*Wed, 08 Mar 1995 01:58:08 PST*

> [encrypt image file F1 with one-time pad F2, email F1 to person A  
> and F2 to person B; A and B then exchange F1 and F2]  
> A and B each can now recover the original image. Has the law been  
> broken? Who broke it? All anyone did in the above scenario was to  
> send a random bit stream to someone else. At no time did anyone send  
> a bit stream with any identifiable semantic content.

An undeveloped photo becomes evidence of crime when it's developed and is deemed porn. A special film requiring its own developing process doesn't change this. Whether a crime was committed wouldn't rest on mechanisms of imaging, therefore, but on the image transmitted. If it's deemed porn, chances are all three of you broke the law (plus conspiracy to commit same, given the way you went about it.) Lectures to judge or jury on the mathematical properties of the tools used will probably seem to them like lectures on thin film chemistry.

> One might argue that I broke the law by sending out two files that I  
> knew could be combined to produce a pornographic image.

That would be the prosecution's argument, yes.

> So imagine now that A sends a random bit string F1 to B, who then uses

> this as a one-time pad to encode P, which B then sends back to A. Has  
> the law been broken? Who broke it?

A has conspired with B to effect the transmission of images deemed  
pornographic from B to A. I wouldn't bet the rent on any judge or  
jury concluding anything else.

> B could never be convicted of violating the law, since he could always  
> claim that he had sent F2 before receiving F1, and that therefore A  
> had transferred P to him rather than vice versa. Even if the  
> government had timestamps to show that F2 was sent after F1, B could  
> claim that this was simply a retransmission.

Oh? We couldn't recover P from A or B's storage?  
Or talk to someone who knew where P came from?  
If we do, we don't need to know anything about F1 or F2.  
We know where P came from and where it went to.

Even without that, if timestamp records conflict with B's claims,  
we simply have to choose which one we believe. B's claims might  
be found credible, and might not. The judge or jury decide.

On either grounds, B's toast under a variety of circumstances.

> If A and B exchange P in this way, then they can individually publish  
> F1 and F2, from which anyone can recover P, but both A and B can  
> plausibly deny having done anything but publishing a random bit stream.

The key word here is "plausibly"; plausible to whom? Judge or jury  
might find it less than plausible that A and B engaged in the generation  
and distribution of random bit streams, which later just happened to  
form images in combination.

> The DA might try to prosecute both A and B on a conspiracy charge,  
> but it is not necessary for A and B to have conspired. The mere  
> knowledge that random bit streams can be used in this manner might  
> prompt some people to start sending random bit streams around.  
> Without reliable time stamps there is no way to trace the introduction  
> of semantic content. So as soon as anyone starts to transmit  
> one-time-pads, everyone can publish anything and no one can be  
> prosecuted for it.

The above discussion should demonstrate why this is a rather  
naive view. However anyone who wants to give it a whirl is  
welcome to; it's your nickel. The danger lies instead in  
an equally naive view:

> Any attempt to legislate the content of digital communications is  
> therefore doomed to fail

And therefore we need do nothing. Wrong. The fact is that clever  
games such as these will not impress the judicial system nor derail  
the legislative process. If the law gets on the books it will work  
its damage. Such schemes as suggested above will be looked on as

what they are, attempts to evade it or confuse its enforcement; little will be gained; it might even be counterproductive. No, if we want to stop Senator Exon's nonsense, we have to do it the old fashioned way: organizing, lobbying, informing, and persuading.

Jon Krueger jpk@pet.com (510) 523-2514

---

**Re: The source of semantic content (Gat, [RISKS-16.87](#))**

*Tim Kolar <tkolar@cisco.com>*

*Wed, 8 Mar 95 10:09:29 PST*

Erann Gat's article on semantics ([RISKS-16.87](#)) provides a nice example of the difficulties of identifying any bit stream with certainty.

Unfortunately it also provides an example of an all too common Risk: Engineers confusing scientific "proof" with that of a legal nature.

Censorship is already enforced on the internet. In particular, allowing transfer of encryption technology out of the U.S. is illegal. This leads to awkward situations for companies who's products include security, but by Gat's arguments they can get around the problem by simply encoding the software and sending it as two "random" bit streams. Anyone who decides to try this, please be sure to let us all know...

Sarcasm aside, I don't think anyone believes that Department of Commerce (or Defense, or whoever enforces that restriction) would even slow down on their way to the courthouse because the information was encrypted. Intent is far more important than encoding, and I don't believe they'd have any trouble with a conviction.

But back to the basic Risk: Engineers forgetting the end users and getting wrapped up in notions of mathematical certainty and "solid" proof. Remember: your firewall supports an overall security policy. Your automated flight system supports a pilot. Your software filters support the legal system.

In all these cases the software is not the end all be all, but an aid to accomplishing some other task. At some point we may feel comfortable replacing humans with software completely for these uses, but RISKS forum itself is a testimony to how far off that actually is.

-Tim Kolar

---

**Re: The source of semantic content (Gat, [RISKS-16.87](#))**

*<David\_Harpe@mm.cobb.ziff.com>*

*Tue, 07 Mar 1995 22:46:57 -0500 (EST)*

>Now suppose that I email F1 to person A and F2 to person B. Then A and B  
>exchange F1 and F2. A and B each can now recover the original image. Has  
>the law been broken? Who broke it? All anyone did in the above scenario

>was to send a random bit stream to someone else. At no time did anyone send  
>a bit stream with any identifiable semantic content.

Unfortunately, our legal system is not advanced enough to recognize the subtle differences described above. The authorities will wait until the two parts are combined. They will then seize every piece of hardware which appears to be associated with the image. Anyone who happens to be in the mail header will be arrested. During the trial, the reconstructed image is all the jury will see, understand or remember. They will fall asleep during the expert witness testimony regarding public key cryptography. This is the RISK of living in a society which is heavily dependent on technology, but whose users are not very well educated.

David Harpe david\_harpe@mm.cobb.ziff.com

---

### Re: Sparc10 keyboards and resetting the CPU (Neustaedter, 16.85)

"A. Harry Williams" <HARRY@VM.MARIST.EDU>  
Fri, 03 Mar 95 18:54:41 EST

>Actually, this is a feature.

I'm sorry, but throwing a user into an unknown state and requiring them to know they have to type "go" and calling it a feature simply because the operating system can't handle losing power without risk of losing the file system is wrong. It's a kludge covering a bug. It never ceases to amaze me the ends to which people will put up with this from vendors. They won't fix the original bug, but they will add on all sorts of backdoor patches and think they've solved the problem. It would be like taking your car in for service for a rattle, and the garage giving you ear plugs so you can't hear it anymore.

To steal a line from the same Risks issue, the ultimate solution to these recurring file system problems is for consumers to demand working file systems from software manufacturers.

/ahw

---

### Re: Sparc10 keyboards and resetting the CPU (Neustaedter, [RISKS-16.85](#))

Simson L. Garfinkel <simsong@acm.org>  
Fri, 24 Feb 1995 21:22:53 -0500

I would like to take issue with Tarl Neustaedter for saying, in effect, that Sun's decision to have its SPARC computers go into the ROM Monitor when you unplug the keyboard is a FEATURE and not a BUG.

Mr. Neustaedter eloquently says, basically, the following:

1. Sometimes you need to be able to interrupt the computer.
2. User software can completely remap the keyboard.

3. Therefore, we need some signal that can't be remapped to get the user into the ROM Monitor.
4. The only thing left is unplugging the keyboard and plugging it back in.

Here are some things to consider:

1. First at fault is the ROM monitor itself, which has one of the most un-user-friendly prompts I have ever seen. The menus are difficult to read; the commands are not neatly formatted; it's just not clear for non-technical people what to do.
2. I am sure that more files have been left by some poor secretary or other non-technical person accidentally unplugging the keyboard and then plugging it back in (and consequently getting trapped at the ROM prompt), then have been saved by UNIX weenies who have known that they could trap into the ROM monitor by playing this game with the keyboard plug.
3. Mr. Neustaedter's note that this functionality can be disabled by hand-editing the function call to `abort_sequence_error()` in the function `zsa_xsint()` in the file `zs_async.c` is the typical UNIX weenie response: if you don't like it, then search through the source-code (or object code) and fix it yourself.

Yes, it is wonderful that UNIX gives its users such flexibility. But it's also clear that UNIX was designed for small research labs where the users want this sort of flexibility, and not for general use. Putting UNIX into general distribution is dangerous: it's dangerous for the users, and dangerous for those who have to give support to the users.

"It helps to be handy with kadb."

Indeed.

Simson L. Garfinkel

Co-Editor, "The UNIX-HATERS Handbook", IDG Programmer's Press, 1994.

---

## Re:Sparc 10 keyboards and resetting the CPU RISKS (DIGEST 16.83)

*Ed Bruce <edward@igate1.HAC.COM>*

*Thu, 23 Feb 1995 09:06:53 -0600*

This has been a feature of Sun Workstations at least since the Sun-2s. I worked on a project in 1985 with six rack mounted Suns each supporting 6 diskless Suns. There was a table beside each rack and on the table was a keyboard. No CRTs of any kind to be seen. I don't know why, but periodically someone would decide that they needed one of these keyboards. With the result that at least six Suns (generally more as NFS mounts to the now hung server would fail) would freeze up until we could get the keyboard back and reboot the server.

Just last year I was stung by this feature. I was to give a demo on a Sparc

10. Some one had connected the mouse off the left side of the keyboard and I decided I needed it on the right. So I immediately unplugged the mouse then proceeded to disconnect the cable on the right side, and the Sparc 10 proceed to crash. After reconnecting the cables I attempted to reboot. Well it failed to reboot and later it was discovered that one key file had been corrupted (I forget which one).

---

## Re: Sparc10 keyboards and resetting the CPU

*Mark Stalzer <mstalzer@etsd.ml.com>*

*Mon, 27 Feb 95 08:38:05 EST*

This is a good topic for a trivia question in the Computer Bowl. I bet SMI borrowed the break behavior from PDP-11s. I'm not sure when it was introduced into the PDP-11 family (certainly by the mid 70's), but holding the break key for a bit on the console caused a "framing error halt". On a PDP-11/03, this dropped you into the microcode monitor. On machines without a monitor, you had to restart it from the front panel with all the funky lights.

Anyways, it served a useful purpose. On the RSX-11 operating system, you could schedule a job with a priority higher than the command line interpreter. If this job went into an infinite loop, it could not be terminated. The solution was to stop the machine with the break key, and poke around in kernel memory to remove the job (there were various ways to do this.) Hopefully, when the machine was restarted, it would be back to normal.

-- Mark Stalzer (mas@acm.org)

---

## Re: Sparc10 keyboards and resetting the CPU (Puchol)

*David Honig <honig@binky.ICS.UCI.EDU>*

*Mon, 27 Feb 1995 17:09:34 -0800*

Disconnecting the keyboard is the same as the L1-A interrupt which throws Suns (since Model 3s) into their monitor program. Typing "c" for continue will let the cpu resume unixing.

This is indeed obscure behavior if you don't know about it :-0 Most computers have arcane stuff like this mentioned (once) in their voluminous manuals.

Computers aren't the only such systems: there are cars you can shut down by kicking in the right place, where you activate a sensor that shuts off the fuel pump, for instance.

The problem with big systems is no one reads (or understands) whatever descriptions of it there might be.



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 16: Issue 89**

**Friday 10 March 1995**

## Contents

- [Celsius-to-Fahrenheit conversion risk](#)  
[Michael Tobis](#)
- [Two on net porn charges](#)  
[Jonathan Bowen](#)
- [Re: 6-cent T-shirts](#)  
[Evelyn C. Leeper](#)
- [Re: Remote-Control Risks](#)  
[Mike Cavanagh](#)
- [Consumer electronic problems](#)  
[Les Hatton](#)
- [Can Pakistan Eavesdrop in America?](#)  
[Peter Wayner](#)
- [Sow's Ear from a Purse](#)  
[Joseph H Presley](#)
- [Resetting BSD/OS is easy as resetting MS-DOS \(Re: Sparc10\)](#)  
[Kenji Rikitake](#)
- [Re: Microsoft and Lotus spreadsheet errors](#)  
[Tony Lauck](#)
- [Loss of one of the X-31 research airplanes](#)  
[Peter Ladkin](#)
- [PGP Moose: moderator authentication and antispamming tools](#)  
[Greg Rose](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Celsius-to-Fahrenheit conversion risk

*Michael Tobis <tobis@skool.ssec.wisc.edu>  
Wed, 8 Mar 95 18:15:15 CST*

I thought the RISKS readership shouldn't miss this gem, posted in sci.geo.meteorology by stevenb@pauli.jhuapl.edu (Steven Babin at Johns Hopkins University Applied Physics Laboratory):

> There seems to be some confusion over the giant iceberg. [...]

> The Reuters news agency reported that the iceberg was 656 feet 2  
> inches thick, implying a tremendous accuracy of measurement. It  
> is actually 200 m thick and the reporter converted this to English  
> units. Reuters also reported that this event was the result of a  
> 36.5 F increase in temperature since the 1940's. It was actually  
> a 2.5 C increase. The reporter apparently converted this to F  
> as a temperature rather than a temperature difference.  
> I don't know whether this speaks more for the educational level of  
> reporters or more for the fact we should all be using SI units.

The risks of the transmission of technical information by people who don't know what they are talking about will be familiar to RISKS readers. Perhaps more striking is the risk that something as simple as a Celsius to Fahrenheit conversion algorithm can be misused by making invalid assumptions about context.

Michael Tobis tobis@skool.ssec.wisc.edu

[And the mention of SI reminds me of Steve Lipner's OLD joke about being an SI, namely a Civil Engineer. (For those of you who don't get it, sivil injinears are not supposed to be able to spell.) PGN]

---

## Two on net porn charges

<Jonathan.Bowen@comlab.oxford.ac.uk>

Fri, 10 Mar 95 13:13:31 GMT

Newspaper: The Times Higher Education Supplement

URL: <http://www.timeshigher.newsint.co.uk/>

Reference: page ii, Multimedia news section, 10 March 1995

Headline: Two on net porn charges

An 11-month investigation by West Midlands police has led to two men being charged with distributing child pornography on the Internet. The charges arise from a raid by police on the metallurgy department at Birmingham University following information on child pornography passed to them by federal authorities in the United States. ... The prosecution is seen as [a] test case on what can be legally transmitted globally across the network from computer hosts.

Jonathan Bowen, Oxford University Computing Laboratory, Programming Research Group, Wolfson Building, Parks Road, Oxford OX1 3QD, England.

---

## Re: 6-cent T-shirts

Evelyn C. Leeper <ecl@mtgp003.mt.att.com>

Thu, 9 Mar 1995 19:50:44 GMT

> we end up with .06 cent t-shirts and free shallots.

XXXXXXXX

This is a pet peeve of my husband's (and by extension, of mine, I suppose). He keeps trying to explain to the clerks why they should sell him that two-liter bottle of Coke for a cent, when the sign says, ".99c" ("c" actually being a cents-sign).

The Risks in this? I suppose it's the risk that if people have turned over all their computing to machines and don't even \*think\* about where the decimal point should go, then we're all in trouble.

Evelyn C. Leeper | +1 908 957 2070 | Evelyn.Leeper@att.com

---

## Re: Remote-Control Risks

*mike <mike@emgee.demon.co.uk>*

*Thu, 9 Mar 1995 02:18:41 +0100 (GMT)*

I was interested to see the examples of optical remote-control systems being upset by other light sources. In my student days I worked as a TV engineer in holidays. A customer complained that his set would randomly switch channels. Several weeks of to-ing and fro-ing to the workshop failed to find a problem. Eventually the cause was found. The customer kept budgies in an aviary outside the window next to the TV. The set had an ultrasonic remote control. The budgies were setting off the remote. If you made the budgies tweet, the set changed its channel.

These risks are still there 20 years later.

Mike Cavanagh

[A new Hallowe'en motto: Click or tweet?  
With the new noise-cancellation techniques,  
the challenge is how to balance the budgies. PGN]

---

## Consumer electronic problems

*Les Hatton <les\_hatton@prqa.co.uk>*

*10 Mar 1995 11:44:38 +0000*

Has anybody heard of consumer electronic stuff being recalled because of software problems yet? The reason I ask is that most such products will have massive amounts of software in them by the end of the decade, (many tens of thousands of lines in such things as televisions, cars, washing machines, electric razors and so on).

As an example:

In August'94 I rented a Vauxhall Omega car for 1 month. This car was brand new and consequently has a number of micro-processor controlled systems.

In the first week, the sun-roof started to oscillate (in the rain!). The sun-roof is a simple rotating switch which you turn to the position you want

the roof and then leave it to move there. Mildly concerned and alternately dampened by this, my eldest son figured out that by pushing the button, the roof reset. On looking through the manual, in tiny writing at the back, this featurette was described, "in case of some circumstances when the sun-roof ...".

One week later, I discovered one morning that the car was completely without power - not even the control panel lights came on. A volt-meter revealed that the battery was perfectly OK. A call to the RAC (Royal Automobile Club, a UK organisation that operates a rescue service like the US. AAA), brought an engineer out who said it was one of two things, one of which he could fix. He moved the drive lever from Park to Drive and back and all the lights came on and the engine would then start. (The drive train is also controlled by a microprocessor in this car). I asked him what was the one he couldn't fix. He said that on this model, the auto immobiliser (the cute little button on the key ring) could in some circumstances at the edge of its range so immobilise the car that only the factory could get it going, (the ultimate theft deterrent!). I suspect that this is also controlled by a microprocessor. In fact on this car, the radio is controlled by two microprocessors !

In terms of reliability growth modelling, one person experiencing two defects and hearing of another in just one month in one car adds up to a shaky reliability record.

Hence my question at the beginning. Maybe its just me, because I'm in the profession.

Les Hatton, Ph.D. C.Eng, Director of Research & Engineering, Programming Research Ltd, England les\_hatton@prqa.co.uk +44 (0) 1 932 888 080

---

## Can Pakistan Eavesdrop in America?

*Peter Wayner <pcw@access.digex.com>*

*Thu, 9 Mar 1995 14:44:35 -0500*

[RISKS-16.88](#) includes a transcript of a Voice of America broadcast describing Pakistan's hardball play to get access to Motorola's best cellular eavesdropping technology. The transcript says that Pakistan shut down Motorola's cellular service until it got the device that would let them eavesdrop on all conversations.

I'm not sure if Motorola complied, but I hope that someone asked these questions:

1) Can this eavesdropping hardware work in the United States? Many speculate that Pakistan wants to be (or is) a member of the nuclear club of nations. When a Princeton undergraduate designed a nuclear bomb for credit, he was visited by someone who seemed to be a Pakistani intelligence operative. The goal? Nuclear information.

2) Can this eavesdropping hardware work against Motorola? Industrial

espionage is a popular way for countries to do "research." Does Pakistan want to build up a local electronics company?

3) Can this eavesdropping hardware be used against US companies angling for business in Pakistan?

4) Will the technology make its way into the hands of the terrorists?

Several days ago, US citizens were killed in an ambush. The dead included at least one intelligence operative. Today's Washington Post says that some witnesses claimed a police car with a submachine gun mounted on the top stood by idling and let the killers get away. The excuse is that they were afraid. The ambush was supposedly retaliation for the US capture of terrorists.

Years ago, we only needed to worry about whether we could trust our immediate neighbors and the other folks in town. Now trust is a global game.

---

### **Sow's Ear from a Purse (Tepper, [RISKS-16.88](#))**

*Joseph H Presley <presley@whserva.wh.att.com>*

*Fri, 10 Mar 95 10:39:21 EST*

A zealous and unscrupulous prosecutor could "prove" that the KJV (King James Bible) is obscene by using a mask of  $A=[KJV \text{ xor } obscene]$ .  $[A \text{ xor } KJV]$  gets you the obscene file. Can you imagine trying to prove that you didn't just erase your encryption mask to a technologically naive jury?

I should also mention that you could transmit  $A$  as your file and your recipient use  $KJV$  as the encryption mask.

Joe Presley

---

### **Resetting BSD/OS is easy as resetting MS-DOS (Re: Sparc10 keyboards)**

*Kenji Rikitake <kenji@reseau.toyonaka.osaka.jp>*

*Fri, 10 Mar 1995 13:17:25 +0900*

The Sparc10 story reminds me of my 486 PC running BSD/OS; it was configured to ask for rebooting if you press CTRL+Alt+Delete as default. I immediately disabled this feature. I even consider this a bug, although you can fix it by recompiling the kernel.

Think about this. Most MS-DOS users know CTRL+Alt+Delete, and many of them just do it if they think they have done something wrong with their PCs. And few of them know the difference between MS-DOS and BSD/OS; what if they start to use BSD/OS? Rebooting everytime they think they've got crashed?

BSD/OS has another design flaw on its X server. You can terminate it anytime by pressing CTRL+Alt+Backspace. This is enabled as default, though you can turn this off by its configuration file. I respect flexibility of UNIX, but it's obviously dangerous to enable emergency-stop features to everybody.

// Kenji Rikitake <kenji@reseau.toyonaka.osaka.jp>

---

## Re: Microsoft and Lotus spreadsheet errors

*Tony Lauck <tlauck@CERF.NET>*

*Thu, 09 Mar 1995 09:46:17 -0500*

Errors in financial calculations are not new. When I worked at Autex, Inc. in the early 70's I wrote a program to calculate bond tables. I was told that my calculations, right or wrong, had to agree with a certain book that all the traders used. Bond prices were given in dollars and cents and I was told that a difference of one cent was unacceptable. A one cent error in a large trade could easily cost more than a Wall Street lunch for two, hence was significant.

The bond table book gave the formula used and indicated the method of rounding. It was very easy to duplicate these calculations, but would they agree using a different processor? By printing out my own version of the book and comparing each entry by hand I found only a single error, in the amount of one cent. In the early 70's fancy desk calculators still ruled. The one I happened to have had a switch that controlled rounding mode (down, up, halfway) so it could do interval arithmetic. Cranking the calculation on this calculator to 15 digits I was able to bound the correct value. It was almost exactly halfway between two pennies, and my rounding was correct. (This didn't surprise me as I had used 64 bit floating point, a large number of guard digits indeed for a four decimal place answer.)

Knowing that I was right and the book wrong was a nice position. I discussed this with my boss and we decided to stick with our value. I secretly hoped there would be a dispute someday between two traders over this entry, figuring that I could somehow turn this into a nice lunch. No such chance.

Do people still use these old tables? How many have errors?

---

## Loss of one of the X-31 research airplanes

*<ladkin@techfak.uni-bielefeld.de>*

*Mon, 6 Mar 1995 00:22:37 +0100*

Flight International, 1-7 February 1995, reports the loss of a Rockwell-Daimler-Benz Aerospace X-31A enhanced fighter-manoeuverability research aircraft on 19 January 1995. 'Investigations [...] are focusing on the air-data system, say sources close to the project.

"There is a possibility that hardware operation of some of the systems may be involved [and] it cannot be excluded that the instruments were giving false readings," says one source, adding that there is no indication that the aircraft's advanced flight control system was involved [...].'

Flight International, 8-14 February 1995, reports that investigations are centred on the pitot-static system (which measures altitude and airspeed by

means of pressure differentials, and that pitot icing is suspected by some. 'The aircraft was [...] in straight-and-level flight, when [the pilot] detected false airspeed readings, followed by pitch oscillations. These increased and were followed by a violent roll before [the pilot] ejected.'

So, investigators suspect that false sensor readings caused by icing-up of the sensors led to inappropriate actions of the flight control system which led to loss of control. Generally, airplanes which may fly in instrument conditions, i.e. clouds, including my Piper Archer, are equipped with pitot heat to avoid similar problems, but if my pitot ices up, all I lose is my airspeed indicator, and not my control. A colleague who is a Chief Engineer at NASA Dryden, where the accident took place, points out that airplanes such as F4s, which are not fly-by-wire airplanes, have also been lost when false sensor readings led to inappropriate actions of the flight control system - but in the case of an F4 it is a mechanico-hydraulic system rather than a computer. She suggests that a distinction be made between the flight control system itself, which implements the control laws, and the system that sends signals to the actuators to wiggle the control surfaces.

While we may not be able to ascribe the 'fault' to a 'computer' in this case, it does raise the continuing issue as to how one ascribes faults. It is always possible in theory to replace a computer control system by wires, pulleys, hydraulics, bells and whistles - but not to fit all this hardware in the same airplane all at the same time. For example, Airbus argues that its computer-controlled airplanes are 'evolutionary', that is, the same control characteristics could be achieved with more traditional control systems - and the only consequence of computer control is weight savings, and therefore extended range or the ability to carry more passengers. This is debatable. The more interconnection between systems contributing to control (possible when most things are software unless extreme care is taken), the more opportunity for an inappropriate sensor reading to send everything haywire. The X-31 would not be able to fly without computer control. It is true that any individual system fault may be replicated by means of wires, pulleys and hydraulics. But I doubt that this knowledge would help anyone to analyse the fault and prevent its reoccurrence. I suspect that techniques developed by computer scientists for dealing with safety-critical computers are more useful. Whereas in the case of my Archer, only plumbers would be involved .....

Peter Ladkin

---

## PGP Moose: moderator authentication and antispamming tools

*Greg ROSE <Greg\_Rose@sibelius.sydney.sterling.com>*

*10 Mar 1995 20:28:33 +1000*

-----BEGIN PGP SIGNED MESSAGE-----

PGP Moose

=====

by Greg Rose <Greg\_Rose@sydney.sterling.com>

The aim of this software is to monitor the contents of consenting moderated newsgroups, and to automatically cancel messages that appear in the newsgroup without having been authorised by the moderator(s) of the group. This has (obviously) been prompted by the recent spammings.

PGP, the crux of the cryptographic software, was written by Phil Zimmermann <prz@acm.org>, who otherwise has nothing to do with this. The cryptographic framework was written by Greg Rose <Greg\_Rose@sydney.sterling.com>. The INN news system hooks are being provided by Chris Lewis <clewis@ferret.ocunix.on.ca>.

#### How Does It Work?

- - - - -

When a moderator wants to protect their group from forged/unapproved postings, they should register their interest with one or more of the sites running PGP Moose, and pick up the submission script. As part of this process, the moderator would specify a PGP public key that is allowed to approve postings.

When a post comes in, and the moderator wishes to approve it, they do whatever they would normally do before actually using inews (or whatever) to post the message. As their last action, they run the PGP Moose Approval program "pmapp". This inserts a special form of Approved: header which looks like this:

```
Approved: PGP Moose V0.9 950310 sci.crypt.research
  iQBVAgUBL1/Kg2zWcw3p062JAQEYIgH/Xyrz6LaGG+fHaSxoexMECovzkloADrQx
  l73IXIUQEIoFI5jnDBBdHVvqTMEPS0118ytYVQZoQrdStuXB9Oc9gQ==
  =azqs
```

In this example you can see that the approval carries a date stamp and the name of the newsgroup in question. These, as well as the From: and Subject: lines, and the non-blank lines of the message itself, are used as input to the PGP program to generate a signature. The PGP signature is inserted into the Approved: header, mostly so that it won't interfere with, or be confused with, any signature in the body of the message.

Anybody can check whether the message has been modified in any significant way, simply by running the PGP Moose Approval Checking program "pmcheck". More importantly, though, the sites running the

PGP Moose Checking Daemon will be doing this automatically for every posting to the registered newsgroups. And, if a posting fails the checks, it will be automatically cancelled and a notification sent to the moderator.

This software is made freely available for just about any purpose, but I've retained copyright so as to keep some semblance of involvement. See the last section of this file.

The Bits:

- -----

PGP Moose consists of a number of Bourne Shell scripts calling standard Unix utilities and PGP. I could have used perl more elegantly, but this stuff is marginally more widely available. If there are Unix version dependencies, they should be considered to be bugs and I'll happily attempt to remove them.

pmapp usage: pmapp newsgroup [file]

This script takes the not-yet-posted article, specified either by filename or from standard input, and creates a signature for it, which is then inserted in the Approved: header. The article, ready for posting, appears on the standard output.

In the configuration section at the top of the script, the moderator may build in the PGP User Id to be used for the signature, and the corresponding password. This is simply for convenience, since spammers are not so likely to go cracking the computer to get the password, and it is a relatively simple matter to generate a new user if it is, indeed, compromised. For the paranoid, like myself, if the password is not configured into the script it is read from the terminal instead.

pmcheck usage: pmcheck [article]

This script takes the article, specified either by filename or from standard input, and checks that the Approved: line is something it considers to be correct and that the article has not been

tampered with. Pmcheck returns successfully if everything checks out. Otherwise it will return failure and issue one of a number of error messages, for example:

```
Usage: $0 [article]
Posting not approved with PGP Moose.
Wrong newsgroup: $6 != $GROUP.
Bad signature (altered or damaged file) on $FILE.
Signature '$SIG' on $FILE invalid for newsgroup $GROUP.
```

Anybody can run pmcheck. It behaves slightly differently depending on the existence of a file called (by default) PGP\_Moose\_accept. This file, if it exists, should contain lines with a newsgroup name, some whitespace, and the PGP User Id approved by the moderator (usually made up specifically for this purpose). For example:

```
sci.crypt.pgpmoose    pgpmoose test <ggr@sydney.sterling.com>
```

If such a file exists, pmcheck is silent if all is well, and issues the last of the error messages above if everything else was all right but the signature was from the wrong person.

Without such a file, if the signature is otherwise valid you will get a message like:

```
Valid signature from '$SIG'.
```

A script is being developed by Chris Lewis (who has more control over news stuff than I do) which will perform the automatic cancellations. Stay tuned. There is plenty of prior art, so this shouldn't take too long.

Soon, when I get back from my trip in two weeks, I will create mail server scripts that allow moderators who are not using Unix to use these facilities. The first allows a moderator to mail a PGP signed copy of the article to be posted. The server will then verify that the moderator sent it, and post it with a (different but corresponding) approval. The second will accept an article and return something that you can check the signature on. Either way, any moderator will still need PGP.

## How Do You Register For The Service?

-----

Ahhh, this is the hard part. After all, it would be pretty undesirable if someone, meaning well, took any old body's word for it that some important moderated group should start working this way, before the moderator was able to start approving postings. A great way to hijack a newsgroup.

Another possibility is that someone, having seen what the valid signature looks like, simply creates a whole new PGP key that happens to have the same PGP User ID. Then they can sign and post stuff too.

The solution to both of these problems is the classical one for public key systems. You need either a certifying authority or the PGP Web of Trust. We're using the Web of Trust. If you don't understand about PGP and the Web of Trust, go away now and come back after you really do understand it.

For each newsgroup that wants to utilise this program, the moderator will have to create a special PGP key pair (preferably 512 bits to keep the Approved: lines short), and sign it. They must then establish a path of trust to someone who is running the PGP Moose server. It will be up to the administrator of that server to make sure that only trusted moderators' keys ever get into the server's keyring.

**THERE CAN BE NO SHORTCUTS TO THIS PROCEDURE.**  
Otherwise we are all back where we started.

## What If You Have Multiple Moderators?

-----

Simple. Create one PGP key pair which can approve posting, and share it among the moderators. You have to exchange it securely, but by definition you have PGP, so that shouldn't be too hard. You can still tell which moderator approved a posting from the Sender: line.

Possible Problems We've Forseen:

-----

If an article is mangled e.g. by truncation, it will fail the authentication and be cancelled. Until it is demonstrated otherwise, this is assumed to be a rare and minor problem. When a cancel is issued, mail is sent to the moderator of the group telling them, and they can tell us if it becomes a problem.

Currently the signature produced is assumed to be a PGP version 2.6 compatible one.

The moderated newsgroup in question must be the first newsgroup on the Newsgroups: line; as a corollary it is not possible at the moment for an approved posting to multiple moderated newsgroups.

Only one PGP User Id can approve postings to a particular group. This means that that PGP User's private key must be shared between all of the moderators, with all of the attendant risks.

Status:

- -----

These scripts are implemented already, or as noted above. They are undergoing testing by Chris Lewis <clewis@ferret.ocunix.on.ca>, and as soon as they have settled (within a week for sure) they will be made available via anonymous FTP and posting to comp.sources.misc and sci.crypt.research.

It Really Wasn't That Hard.

- -----

I wish people (other than me and Chris Lewis) had put as much effort into doing this as they did into clogging the Moderators' mailing list. It wasn't hard.

But you know what was hard? What Phil Zimmermann did creating PGP in the first place. Phil is in serious legal hassles over PGP, and if you think this effort saves you or your company some time or money, I'd like you to consider donating some of it to Phil's legal defence fund. Write to me or Phil's lawyer Phil Dubois <dubois@acm.org> regarding how to donate. You can do it over the net using PGP!

Share and Enjoy!

## License Terms

-----  
This software is copyrighted by Sterling Software, and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

-----BEGIN PGP SIGNATURE-----

Version: 2.6

```
iQCVAgUBL2Ao0aRQkCwJ0+ZNAQEC5QQAzYC388xAkKCG+737mOLH0Bg3vbPnISPO
4epkvW7GD6HyaCUq34mhqYx2h1gCn4ywRG0bTZbjOyEMjU9d78Xyar/abu+jkMGc
umwwbcNHssYfsHMsfbrUR8vVz2C8+5ULUyavN9aNRIIFTpekWGkiYfa+NGtIB84I
Xr9QW8Y2TqY=
=tjMn
```

-----END PGP SIGNATURE-----

Greg Rose, Sterling Software, 28 Rodborough Rd., French's Forest. NSW 2086  
Australia. +61-2-975 4777 (FAX: +61-2-975 2921) greg\_rose@sydney.sterling.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 16: Issue 90**

**Tuesday 14 March 1995**

## Contents

- [E-Mail Apology from Prodigy](#)  
[Edupage](#)
- [Kiosk prototype fails to deliver in trial run](#)  
[Bob Frankston](#)
- [Automatic return fire](#)  
[Michael J Zehr](#)
- [Internet providers raided](#)  
[Kevin Yeung](#)
- [Internet-Finland Privacy](#)  
[Lars Arnkil via Bruce Baker](#)
- [Re: Consumer Electronics Problems](#)  
[Willie Smith](#)
- [Mitnick Stole "SATAN" Security Software](#)  
[Edupage](#)
- [Re: PGP Moose](#)  
[Jerry Leichter](#)
- [Re: Microsoft and Lotus spreadsheet errors](#)  
[Steve Bellovin](#)  
[Ken Tindell](#)
- [The source of semantic content: followup](#)  
[Erann Gat](#)
- [Re: Can Pakistan Eavesdrop in America?](#)  
[Laurence R. Brothers](#)  
[John R. Moore](#)  
[Marc Horowitz](#)  
[P.vanMossel](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **E-Mail Apology from Prodigy (Edupage 12 Mar 1995)**

*Edupage* <[info@ivory.educom.edu](mailto:info@ivory.educom.edu)>  
*Sun, 12 Mar 1995 18:24:47 -0500*

A software glitch caused Prodigy's mail system to send 473 E-mail messages

last Friday to wrong members and to lose 4,901 messages on the Internet. The mail system was shut down for five hours, and Prodigy apologized to its members for the malfunction. (Atlanta Journal-Constitution, 11 Mar 1995, B3)

---

## Kiosk prototype fails to deliver in trial run

<Bob\_Frankston@frankston.com>

Sat, 11 Mar 1995 16:49 -0500

This is a short piece from \*The Boston Globe\*, 11 Mar 1995, by Michael Putzel. Apparently the Post Office is planning to deploy lway kiosks. The prototype appears to be a quick hack, a Silicon Graphics Indy (do I hear, overkill?) with a touch scree and, apparently, a web browser for getting around. The article itself didn't tell which technology was being deployed. This is a basic simple approach which I approve of. One of the problems was a standard touch screen problem of having to position one's finger correctly. More interesting was the attempt to get information from the Social Security computer. "It seems that the agency had changed the name of its computer without telling the Postal Service".

This fits my assumption that it is a web browser. The risk is a standard one of deploying a new technology while it is evolving. Many of the initial web pages are going to fade from the lack of interest in supporting them. This will disappoint those who expect a reliable mature service.

Beyond disappointing, however, it doesn't seem much of a risk and can be handled by setting appropriate expectations. It will be more of an issue if (a standard problem with the regulations limiting the Post Office) the technology is widely deployed.

---

## Automatic return fire

<tada@MIT.EDU>

Tue, 31 Jan 95 18:06:20 -0500

>From CIO (February 1995):

Lawrence Livermore Laboratory is working on a system called Lifeguard to help police (and who knows who else) identify from what direction they are being fired upon. The system was apparently developed in response to school shootings where it isn't always easy to spot the shooter visually. As described in 'Government Technology' the system uses a special sensor that emits "ammunition-identifying" signals and attaches to a rifle like a scope. A computer tracks incoming bullets and locates the source. "Anybody who shoots at you from any direction would be immediately located and subject to return fire," says Thomas Karr, head of the Lab team.

I'll leave to everyone's imaginations the risks of hooking a computer to the trigger of a loaded weapon and using it near civilians.

-michael j zehr

[This Lifeguard is completely different from the noneponymous McIntosh program noted in [RISKS-16.72](#). PGN]

---

## Internet providers raided

*keviny@hk.super.net <Mr.Kevin.Yeung@HK.Super.NET>  
Sun, 12 Mar 1995 13:57:57 +0800*

Seven Internet providers in Hong Kong were raided by the Hong Kong Royal Police, alleged to be operating without required licence and "hacking" other computer systems. All computer equipment was seized, and it was reported that police was able to look at any file on the systems - all people's private email and even commercial documents were at risk. Police may close down and check any Internet provider out again at anytime, and companies' information is at risk if someone in police sells the information secretly.

---

## Internet-Finland Privacy

*<spryhma.samlink.arnkila@elvi.vtkk.fi>  
13 Mar 1995 08:21:19 U*

[Edited and submitted to RISKS by "Bruce Baker" <bruce\_baker@qm.sri.com>, with Lars' permission. PGN]

Funny creature this Internet, and the people associated with it, especially "journalist-researchers", as they call themselves. Adding to the unusual mixture recently here in Scandinavia have been the Scientologists and the Police. It would be funny to follow the intrigues if they were fiction, but these are all too real:

### Case #1

A Swedish journalist-researcher "reveals" that an Anonymous Finnish Internet server has been spreading pedophilic pictures. It sounds like a big Issue, but it is not true.

The addresses within the pedophilic-picture files were in fact forged, and they didn't come via the anonymous Finnish server (owned by Johan Helsingius). This part of the news wasn't much publicized.

It seems that the real pedophilic-picture distributing server was a British one.

### Case #2

Finnish Police receive a request from U.S. law enforcement authorities to confiscate (real) user information from the Finnish Anonymous Server. About the same time, Scientologists claimed that someone had broken into their system and was revealing "highly confidential" information via the Finnish anonymous server. Well, of course, the Finnish Police carried out a house search and seizure to obtain real user information from the anonymous server. Then they promptly gave the information to the Scientologists!!!

Lessons, if any:

- o Negative stories receive more press coverage than positive ones.
  
- o Corrections are rarely seen by the reader, especially readers in other countries.
  
- o People, even Police officers, will act as if "The Party Which Brings Up Some Claim/Issue" has been harmed and must be right. They cannot see, that some issues might be brought up under "legitimate cover" to serve other purposes. This "legitimate" cover should be verified etc...and during this process the Police shouldn't give information to the complainant.

Other thoughts:

Can this affect us? Most definitely. What if the Scientologists had made the same charges against our banking system and had asked the Police to reveal user information in our files? And what if we had asked the police to determine who has tried to break into our systems from this or that address? Should we have a right to obtain this information directly from the Police (similar to your Procter and Gamble case several years ago)?

Lars Arnkil

---

### Re: Consumer Electronics Problems (Hatton, [RISKS-16.89](#))

*Willie Smith <wpns@roadrunner.pictel.com>*

*Sun, 12 Mar 1995 12:09:03 -0500 (EST)*

>Has anybody heard of consumer electronic stuff being recalled because  
>of software problems yet?

Typically they tend not to be acknowledged or recalled, as it would be prohibitively expensive for the manufacturers, and they are used to walking all over the consumers. A couple of examples:

An older Sony 5-disk CD player had a shuffle play with a poor random number generator and no memory of what songs it had played, it merely chose a disk at 'random' and then a track at 'random' from that disk. It would, for instance, play disk 3 track 5, disk 2 track 8, disk 3 track 5, "rinse, lather, repeat". The "solution" was to ignore that function and (5 years later) check carefully that Sony had fixed that bug before buying a new model.

Volkswagen had a bug in their Digifant-II electronic engine management computer for a couple of \_years\_ that caused cold-start problems on hot days. It appeared that the computer was reading the engine temperature sensor as "hot", so it didn't "put on the choke". I actually had the service manager at a VW dealer tell me that I had to keep my foot on the gas of a fuel injected, computer controlled car for a minute or two after starting to keep it from stalling[!]. The first-level fix was, after a year

and a half of so called 'service', replacing the computer. The second-level fix was switching car brands. 8\*|

In both cases, the manufacturer was highly motivated to ignore the problem. I would guess that a fair amount of the development of the CD player was writing the software, and producing new CPUs, recalling the players, and repairing them would have cost Sony more than developing a new player from scratch and giving new ones to folks who complained about the old ones. Volkswagen would have spent a small fortune recalling cars and putting new computers in each, if only in the currency of opportunity cost (what they spent in customer good will isn't really a subject for Risks).

When a software company produces a new product, they test it and run it thru beta testing and such to ensure that it works properly. When a hardware company puts software into their product, they may not understand the software, and take the developers word for it's quality.

Willie Smith wpns@pictel.com N1JBJ@amsat.org

---

### **Mitnick Stole "SATAN" Security Software (Edupage, 12 Mar 1995)**

*Edupage <info@ivory.educom.edu>*

*Sun, 12 Mar 1995 18:24:47 -0500*

SATAN software (an acronym standing for Security Administrator Tool for Analyzing Networks), which was developed by Dan Farmer of Silicon Graphics to scan thousands of host computers on the Internet for security vulnerabilities, was stolen by Kevin Mitnick, the computer cracker who was arrested last month by the FBI and is now under indictment for 23 counts of fraud involving computer use. Mitnick broke into Farmer's account on the WELL, a California Internet service provider. Farmer says he has no way of knowing whether Mitnick shared copies of SATAN over the Internet. (The New York Times, 12 Mar 1995, [City edition?] Sec.3, p.11; 11 Mar 1995, p.30)

---

### **Re: PGP Moose**

*Jerry Leichter <leichter@lrw.com>*

*Fri, 10 Mar 95 15:19:57 EDT*

Given the prevalence of Unix (aka broken) mail forwarders out there that believe any occurrence of "From" at the beginning of a line can be "wedged" as >From (did that arrive at your location as >From? It left here unwedged.), we are likely to soon have a new risk on the net: The risk of automatic cancellation of all messages that happen to have the wrong four characters at the beginning of some line. People forwarding messages complete with headers -- beware! Any "From:" lines you include are likely Moosebait!

Oh, yes, there are also some mail forwarders out there that will change any line consisting only of a single "." to one containing "..". There are no doubt some that will make the reverse substitution. There also appear to be gateways around that will replace empty lines with lines containing a single

space, as well as gateways that do strange and wondrous things with spaces at the end of lines. Finally, there appear to be an increasing number of programs that, under certain unclear conditions, use MIME's BASE64 encoding in the midst of otherwise simple ASCII text - you'll see things like =20 at the end of a line.

I suppose the underlying idea here is fine, but unfortunately an attempt to build such a thing on top of the very chaotic and unpredictable world of today's mail systems is to impose many non-obvious risks on users.

-- Jerry

---

**Re: Microsoft and Lotus spreadsheet errors (Lauck, [RISKS-16.89](#))**

<[smb@research.att.com](mailto:smb@research.att.com)>

Sat, 11 Mar 95 19:09:03 EST

Errors in financial calculations are not new. When I worked at Autex, Inc. in the early 70's I wrote a program to calculate bond tables. I was told that my calculations, right or wrong, had to agree with a certain book that all the traders used.

Such problems are even older. Fred Brooks tells a similar story from the mid-1950's. He was assigned to write a program to do billing for petroleum delivered through a pipeline. Now -- the actual volume occupied by a given mass of petroleum varies with the temperature, and there was a standard book listing the correction factor for each grade and temperature. To comply with various contractual and legal provisions, the program had to produce the same answers. Today, we might use an array; back then, there wasn't enough memory to hold such a large table.

No problem, right -- the expansion had to be a matter of simple physical laws, so they could just calculate it. It turned out to be a simple equation. But whoever had drawn up the table in the first place hadn't rounded consistently -- and the program \*had\* to match.

They ended up doing the calculation, and storing a compressed table giving the difference between the calculated values and the legal ones. Never mind reality -- custom ruled.

---

**Re: Microsoft and Lotus spreadsheet errors (Margolin, [Risks 16.88](#))**

Ken Tindell <[ken@Rabat.DoCS.UU.SE](mailto:ken@Rabat.DoCS.UU.SE)>

Mon, 13 Mar 95 11:39:34 +0100

<>Barry Ward, ... `I've been in the computer business for 19 years and <>have never come across this problem before. ...

>

>I find it difficult to imagine someone who's been in the computer business >for two decades and has never heard of floating point round-off errors.

>This should be part of any computer science curriculum.

It's not difficult to imagine at all: just take a look at Ross Anderson's contribution in [RISKS-15.54](#) ("Card Fraud and Computer Evidence"), where the bank claimed that it's software was 100% correct because it used assembler and the "ABEND" statement! (see also CACM November 1994) Not for nothing is "Banker" cockney rhyming slang...

Ken Tindell, Dept. Computer Systems, Uppsala University, PO Box 325 S-751 05, Uppsala, Sweden +46-18-183172 ken@docs.uu.se <http://www.docs.uu.se/~ken>

---

## The source of semantic content: followup

*Erann Gat <gat@aig.jpl.nasa.gov>*

*Thu, 9 Mar 95 11:57:59 PST*

Some of the replies to my article on the source of semantic content indicate that I have not made myself clear. I did not mean to suggest that we should sit back and do nothing, secure in the knowledge that there are technological tricks that can be played to circumvent the law. I am well aware that once the witch hunt for net.pornographers begins in earnest that logic will provide precious little protection, and the "I only sent random bits" defense probably won't hold up in court. That should scare the pants off you; if it doesn't then you haven't understood what I am trying to say.

At the end of my original article I wrote:

"...transmitting random bit streams may soon become a crime."

I meant this to be taken quite literally. Once there is precedent for convicting someone for transmitting porn using the xor trick, then anyone who sends out a random bit stream for *any* reason can (and probably will) be convicted for transmitting porn. Here's one possible scenario:

Let's say that A sends B a random bit stream F1 for some legitimate reason. (For example, he might be a cryptography researcher sending sample output from his latest cryptanalytically secure random number generator for analysis, or he may be a college student who just wants to thumb his nose at the establishment.) If B wants to transmit a pornographic image P and blame it on A, he uses F1 to encode P into F2, and puts F2 onto his public ftp server. To be extra sure, he changes the last-modified date to a week or so ago. B then calls the authorities (or maybe B *is* the authorities) and says, "I have just discovered that A has used my publicly available random file F2 to encode a pornographic image."

Here's another scenario. Let's say that A uses the xor trick to transmit a legitimate file to B in the form of two files F1 and F2. B encodes P with F1 and replaces the content of the legitimate F2 with the result. He then calls the authorities and says, "A sent me these two files, and when I put them together the result was P."

More complex scenarios are possible by observing that the xor trick is not

limited to two files. An image can be one-time-padded an arbitrary number of times, resulting in an arbitrarily large number of files that must be combined to generate the image. Any combination of these files can be used as a key to encode some other image. If freedom-loving people start to use the xor trick a lot, then there could be a tremendous profusion of random files out there that can be combined in an enormous number of ways to produce an enormous number of images. You might even have pornography on your disk and not even be aware of it. In fact, *\*any\** file is just a one-time-pad encoding away from being a pornographic image. Your copy of Microsoft Word has obscenities in it if you just know how to decode them.

This is not at all the same as an undeveloped image on film. In the case of film it is clear that the information content is in the film and not in the developing process. In the case of an encoded file there is literally no way to tell which is film and which is developer, which is encoded image and which is key. As with many things in the cyberworld, fundamental assumptions about the Way Things Work break down here.

Erann Gat gat@jpl.nasa.gov

---

**Re: Can Pakistan Eavesdrop in America? (Wayner, [RISKS-16.89](#))**

*<quasar@ctt.bellcore.com>*

*Sat, 11 Mar 95 13:52:56 EST*

IMHO:

Anyone with the least knowledge of EE (or a subscription to 2600 or Phrack) ought to be able to eavesdrop on cellular telephone conversations without resorting to industrial espionage. It's not like these conversations are encrypted as a matter of course. I suppose it's possible that the Pakistani cellular network uses some form of encryption that requires Motorola technology to solve, but I doubt it. In any event, *\*our\** cellular phone network sends conversations in the clear unless CPE does something special about it.

Anyone who thinks radio transmissions of any sort are secure (at least those which don't employ reasonable crypto protocols) deserves whatever happens to them....

I assume that US diplomatic and intelligence personnel abroad do use some form of encryption in their transmissions, but I also assume (hope) that they don't rely on it for really sensitive information.

As far as terrorist action goes, unless and until government turns into a 1984-ish police state, terrorists and assassins will always be able to carry out attacks. The freedom of information and action in a democratic society more or less guarantees it.

Laurence R. Brothers ~ quasar@bellcore.com

## Re: Can Pakistan Eavesdrop in America

John R. Moore <[ozone@PrimeNet.Com](mailto:ozone@PrimeNet.Com)>

Sun, 12 Mar 1995 09:55:45 LOCAL

Regarding Pakistan's requirement that Motorola provide cellular eavesdropping technology:

>1) Can this eavesdropping hardware work in the United States?

Probably not. Most likely the system is the new global spread spectrum standard, which the US doesn't use and probably won't. That's the good news.

The bad news is that it isn't needed. Anyone can buy a scanner and modify it, or buy a downconverter for it, and then listen in on any analog cellular system today! This is illegal in the US but unenforceable. Recently it has become illegal to manufacture or import a scanner that is "easily modifiable" for cellular reception. However, there are millions of scanners all ready in circulation that can receive cellular or be easily modified for this purpose. Furthermore, many scanners pick up cellular as an image frequency, which means they can be used for cellular monitoring simply by entering a frequency typically 21.4 MHz below the frequency to be monitored.

Newer US systems will be digital (spread spectrum or TDMA) and encryptable, and thus should be relatively secure against foreign monitoring. However, it is possible that the US Government will force suppliers to make monitoring equipment and encryption keys available to them, but the US Government also wants those crypto keys unavailable to anyone else.

John Moore [ozone@primenet.com](mailto:ozone@primenet.com) <http://www.primenet.com/~ozone/>

---

## Re: Can Pakistan Eavesdrop in America?

Marc Horowitz <[marc@MIT.EDU](mailto:marc@MIT.EDU)>

Sun, 12 Mar 1995 22:48:31 EST

<> 1) Can this eavesdropping hardware work in the United States?

The cellular phone system in the US uses FM modulation very similar to that in your radio. Scanners which could scan cellular frequencies (along with amateur bands, police, fire, etc) were once available at such underground shops as Radio Shack. Scanning cellular was made illegal, so these devices dried up, to be replaced with scanners which could scan all the frequencies above except cellular. These scanners could, with the clip of a wire or the press of a "secret" button combination, begin to scan cellular frequencies, even though this activity is illegal. Early in 1994, equipment which could be "illegally modified" to scan cellular was made illegal (that is, the FCC would no longer license it). Older radios (of which I own two) were grandfathered.

There are two RISKS here. One, the US government is deluded enough to believe that these laws prevent cellular scanning. Two, the public is not

educated enough to know that this sort of scanning is so easy,

Oh, and if all of the above isn't enough, every cellphone I've played with has a diagnostic/repair mode which scans cellular frequencies. There is a story of a demo for congress, where someone (who had to be granted immunity for this demo!) took a brand new cellphone out of a box, plugged it in, pushed a few buttons, and 30 seconds after breaking the shrink wrap, scanned through some calls to show how easy it was.

The third risk: Our government is as scared as Pakistan's about widespread encryption. This issue has been covered in RISKS and Privacy Digest before.

Marc

---

### Drop eavesdropping (Wayner, [RISKS-16.89](#))

<P.vanMossel@telecom.ptt.nl>

Tue, 14 Mar 1995 20:35:12 +0100

In [RISKS-16.89](#) (Can Pakistan Eavesdrop in America?) Peter Wayner complains about Pakistan trying to obtain eavesdropping technology.

Why do you expect Pakistan to act different from the USA? Think of Clipper and USA export restrictions on encryption technology...

Maybe the USA does a better job in covering up and might (or is expected to) be more decent in handling the information.

The risk is to use communication technology that can be eavesdropped. Even if we think it's safe now to trust the current government.

Paul van Mossel.



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 16: Issue 91

Tuesday 14 March 1995

## Contents

- [Re: PGP Moose -- Not just the headers!](#)  
[William Oswald](#)
- [Re: Automatic return fire](#)  
[Joseph Chew](#)
- [Scientology Blackmail Risk](#)  
[John V. Vilkaitis](#)
- [Viral morality](#)  
[Rob Slade](#)

---

### Re: PGP Moose -- Not just the headers! (Leichter, [RISKS-16.90](#))

*William Oswald <siwgo01@sip.unisys.com>*  
*Tue, 14 Mar 95 18:06:18 EST*

>... beware! Any "From:" lines you include are likely Moosebait!

I recently sent to the mailing list [folk\\_music@nysernet.org](mailto:folk_music@nysernet.org) this followup to a thread in which readers were contributing names to a list of recommended female blues guitarists:

>Please add Cindy Cashdollar -- a fantastic blues Dobro player.  
>I saw her backing up Leon Redbone a few years ago in Phila. at one  
>of the Penn's Landing concerts, and I would sure like to hear more.

I was surprised to receive the following bounce:

>Subject: Error Condition Re: Re: Female blues guitarists summary  
>X-Listprocessor-Version: 6.0c -- ListProcessor by Anastasios Kotsikonas  
>X-Comment: Folk Music Mailing List

>We are sorry, but this system sensed the following request which may have  
>been inadvertently sent to this list:

>PLEASE ADD

>If your posting was intentional, please accept our apologies and resend your  
>mail message, making sure you do not include anything that may look like a  
>request in the first line of the body of the actual message. If this was  
>indeed a request please resend it to listserver@nysernet.org

William Oswald -- siwgo01@sip.unisys.com

---

**Re: Automatic return fire ([RISKS-16.90](#))**

*Ad absurdum per aspera* <JTCHW@lbl.gov>

Tue, 14 Mar 1995 14:41:15 -0800

Well... I trust that this is simply a case of a missing thought that seemed obvious to the speaker, namely, that the shooter would be subject to return fire by the human, if there were a clean shot and the situation otherwise justified returning fire.

The description is interesting, though. Makes it sound as though some kind of active millimeter-wave radar or sonar-like device were in use, as opposed to passive triangulation of the sound of gunfire. This presents intriguing technical problems. The bullets of common small arms are roughly... oh, for these back of the envelope purposes let's say they're the size of a pencil eraser. They move anywhere from about 800 feet per second (the .45 automatic pistol) to as much as 3000+ fps (the AR-15). They are almost always, but not necessarily, made of metal.

Now, consider that they are fired at ranges from 7 yards (which the conventional wisdom says is the maximum range of most civilian shootings) to contact. An exception might be a drive-by shooting at several tens of yards, or an urban sniper situation at perhaps a couple of hundred yards. We can probably disregard these because of transmitted power and, in the case of a sonar, timing considerations. So this James Bond gizmo might have as little as .007 seconds in which to do the job. In an urban environment it also has to gate out echoes. And unless it's a slick Doppler job, it has to get two readings. Finally, unless it also catches the sound of the gunshot, it *\*still\** doesn't give you the range, just an idea of where to look, based on what you hope is the trajectory.

Meanwhile, in case solving realtime problems in three dimensions isn't fun enough, the shooter might well have moved and/or hidden his weapon.

This could well be quite a tactical asset to a police team. Maybe even an individual officer, in giving him a clue as to where to look. It certainly isn't a cure-all, and, especially in the case of a lone officer, it's easy to imagine RISKS associated with getting into a "heads-down mode" to run a technological crutch and forgetting the tactical situation.

Joe

---

## Scientology Blackmail Risk

Javilk <javilk@netcom.com>

Tue, 14 Mar 1995 14:32:39 -0800 (PST)

If, as was mentioned in the prior edition, the Finish police handed all the anonymous ID database to the Scientologists, many of the people who have used the anonymizing service may RISK exposure to some form of blackmail attempts. One has only to look at some of the articles posted in the Scientology forum on the Usenet to see what they are often accused of.

A few thoughts from a course I once attended at IBM on industrial espionage:

The typical means of gaining control used by some intelligence services, (including private ones,) and often cults, is to make a series of minor but unethical or illegal requests which, once filled, would place the victim greater and greater conflict with their employers, the law, and/or society if their deeds were to be made public. The goal is to deny the victim access to legal and societal services. (And in the case of cults, outside moral support.) Eventually, the victim has no choice but to comply with even the most hienious of operations, or risk long term incarceration, or worse.

One way to avoid this scenario, is to call the would-be blackmailer's bluff and say "No" at the outset. A better way, would be to seek out and cooperate with an appropriate company security or law enforcement agency, such as the FBI, so as to help them turn the blackmail operation into a sting. The would-be victim is usually given immunity from prosecution. In most cases, the typical minor transgressions spoken of via an anonymizing service user would be laughed at by the police; but the concept of blackmail on an organized scale should be taken quite seriously by an organization such as the FBI.

One should also note, that if the FBI, CIA, etc. are not watching the anonymizing services, they are sadly in remiss of their duties. It does not take much to crack such a service! Thus one may suspect that voluntary cooperation at the outset might be to one's benefit in most cases; and in some cases, being blackmailed by a more nefarious organization may actually turn out to be a relatively oportune event.

If the Scientologists begin to fear that many of their potential victims would turn to the FBI, they may become more reluctant to pursue potential victims. Perhaps we should push this concept a bit on the net and elsewhere.

John V. Vilkaitis, Senior Consultant, Software General Corp. javilk@netcom.com

---

## Viral morality

"Rob Slade, Social Convener to the Net" <roberts@mukluk.decus.ca>

Tue, 14 Mar 1995 18:25:21 EST

VIRETHIC

Viral Morality: A Call for Discussion

"Computer ethics" has been an ongoing study in the technical world. On the one hand is the study of the ethical, moral, or proper use of computers. On the other, is the study of computer crime and vandalism. Lately, I have noted a rather desperate interest in courses or training in computer ethics, as well as an increase in the frequency and depth of discussions regarding the ethics of virus writing. I would like to address this latter topic, specifically.

One problem with current discussions and literature regarding the ethics of virus writing and distribution is the lack of dialogue between two opposing camps. This paper is not intended to present any final answer, nor to add to the literature in the field, but to open the field for comment. My purpose in writing this is to provide an initial overview and to elicit feedback from any and all concerned with the topic.

For those of traditional moral stance, the current situation is discouraging. Peter Denning's "Computers Under Attack" (cf. BKDENING.RVW) has a very thorough survey of the field, but it provides little in the way of answers or hope. Deborah Johnson's work "Computer Ethics" (cf. BKCMPETH.RVW) is pre-eminent in the field, but serves only to clarify the problem. Sarah Gordon's interviews with computer students show responses typical of almost all such studies. The base attitude appears to be, "If I find it interesting, and I can do it, why do you say I shouldn't?"

The proponents of security-breaking activities often question the traditional ethical position by asking, "Where's the harm?" This query is directly relevant to discussions of the morality of virus writing.

I should begin by defining two generally opposed groups in this area. First is the "antivirus", or "AV", research community. Many, though not all, of the members of this group would be involved in producing antiviral software. All would study viral programs with a view to eliminating viral programs in the normal computing environment. They take a rather paranoid, and almost obsessive, position with regard to the sharing and distribution of viral code. (They would rejoin this last by pointing out that it isn't paranoia if someone is *\*really\** out to get you.)

The AV community is not really opposed to the writing of viral programs. It is seen as a trivial, and therefore pointless, exercise; but not necessarily evil, in itself. The communication of viral program code is also a normal professional and academic activity, as long as it is limited, done for a stated purpose, and the recipients are known. It is the unregulated exchange of virus code and source, providing open access to anyone with a computer and a modem, that is upsetting. The opposing group is therefore described as the virus exchange community, or "vx" for short. (This designation was first used by Sarah Gordon.) For the purposes of this paper, therefore, references to "virus writing", "virus exchange" or "vx" will mean the uncontrolled or unregulated exchange or provision of access to virus source and object code.

(This does not necessarily mean deliberate distribution of infected programs by such means as infecting a legitimate program and then posting it, without warning, to a bulletin board system. "Trojanizing" of normal software or malicious invasion of systems is certainly happening in some areas, but it is not needed in the current computing situation. While there is debate over the

relative contribution of "natural spread" and virus exchange to the current virus problem, it is known that code made available only as openly published material does eventually infect machines in the normal computing environment. The term vx does not, therefore, require any imputation of sinister motives or hidden activity for the purposes of this discussion.)

There are some grey areas between these two poles. Some people have both written antiviral software \*and\* contributed to viral spread. Given, however, that one could expect a continuum of opinion, those in the middle are remarkably few. Either you are for virus exchange, or against it.

One other, separate, group should be noted. Viral programs are often cited as an example of "artificial life", and the research community in that field, both professional and amateur, have a legitimate interest in viral programming. Work in the a-life field, however, does not justify unregulated code and source exchange. For one thing, current viral programs "in the wild" (those which are to be found in normal home and business computers, as opposed to those which exist only in a research or laboratory environment) have only the most tenuous claim to artificial life. Common viral programs are simplistic snippets of code without anything like the complexity of the simplest known natural life forms. In addition, those who really do work in the artificial life area will be well aware that it does carry possible dangers, and that research should be subject to controls similar to those imposed on biological and genetic study.

The most common argument for virus-writing tends to boil down to, "You can't stop me." Many promote virus writing on the grounds of freedom of speech, a rather curious position in light of the incoherence of the arguments. (The most vocal of these tend to be Americans, who frequently cite "First Amendment Rights". This refers to the first amendment to the U.S. Constitution, which Americans tend to see as some universal law, rather than an arbitrary political document, however desirable.)

Rights, though, carry with them a weight of responsibility. As is often quoted, your "right" to swing your fist ceases at the end of my nose. You have a "right" to free speech--so long as you are responsible and do not perpetrate fraud. You have a "right" to study whatever you like--so long as you are responsible enough not to carry out experiments in poison with human subjects. No PC is an island--at least, not where viral programs are concerned. Therefore, your "right" to study, write and distribute viral programs carries the responsibility to ensure that your creations do not--ever--run on machines where they are not authorized.

One of the most confusing aspects of the "exchange/no exchange" debate is the concept of the "good" virus. There is nothing inherently evil in the concept of reproduction. (Dangerous, yes.) In fact, the very earliest experiment with self-reproducing programs was the Xerox Worm of Shoch and Hupp. This was designed to spawn "segments" of the central program on other machines in the network, thus bringing the power of many processors to bear on a single problem. Thus, in theory, viral programming could represent the same level of advanced technology in software that parallel processing represents in hardware.

That's the theory. And it is promoted by no less eminent a researcher than Dr.

Fred Cohen, who did seminal work on the security-breaking class of viral programs in a thesis, in 1984, and dissertation, in 1986. Unfortunately, the theory founders on some rather hard facts.

There are three questions to ask of a new, inherently dangerous, technology. Has it a useful application? Can it fulfill that application better than current technologies? And, can the danger, either inherently, or effectively, be controlled?

To date, no one has answered those three questions. While a variety of uses have been proposed for viral programs, there are none which are not effectively being done by other means. No viral programs have, indeed, been seen to be as effective as normal systems. Operating system upgrades could not guarantee universal coverage. Network management tasks could not promise reliable feedback. Automated utilities would confuse novice level users, who never run utilities anyway. The most useful function is still that proposed by Shoch and Hupp--and their programs were not, strictly speaking, viral.

(Vesselin Bontchev's examination of this question is the most detailed to date, and is required reading for all who want to join the debate. His proposals, while demonstrating good ideas for safety and control, are still primarily an advanced automated distribution system. The necessity for viral functions in this regard is still unproven.)

Those in the vx camp will point to two current viral programs which, they say, do have useful functions. One of these programs produces compressed executable files, thus saving disk space, while the other performs encryption on files. However, both of these functions are provided by other programs--from which, indeed, code was stolen for those two "good" virals. Neither of the viral programs are as easy to use or control as the original programs, and both have bugs which must place them firmly in the malware grouping, for nuisance value, if nothing else.

Currently, therefore, the utility of viral programs is very much unproven. This would, though, mean only that they are neutral, were it not for the lack of any demonstrable control. Methods of control have been discussed primarily by Fred Cohen, but even he remains unconvincing. The mechanisms generally are limited to environmental checks which can either fail, or be easily cut out of the program. Some have proposed "hunter" virals, to go after programs which "turn rogue", but a program which is corrupted will behave in unpredictable ways and a hunter program would likely consume a lot of resources, fail, or (most likely) both.

(Cohen frequently cites viral "programs which have been running since 1986 with no ill effects" and speaks of a VCE (viral computing environment). There are two points to be noted here. One is that Cohen has not yet described his viral programs in anything like the detail he put into his earlier work, so there can be no independent assessment of his claims. The second point is that the very term, VCE, implies that a viral computing environment is substantially different, and should be kept separate, from the "normal" computing environment as it is currently known. A VCE may very well be a powerful entity, but it is still an unknown and unproven concept.)

Computer viral programs have an inherent danger: that of reproduction and

spread. If you study explosives, and pass along that knowledge, you also have to pass along the materials before there is any risk of a blast. Even then, the materials do not multiply themselves: when exhausted, another supply must be found. The same is *\*not\** true of viral programs. These entities are *\*designed\** to reproduce. And, unlike the study of dangerous animals, or even germ warfare, viral programs are built to reproduce, multiply and spread without the aid of a skilled, or even aware, operator. If you are careless with a deadly animal or weapon, it is still only a single danger in a localized area. If you are careless with a computer virus, it can spread world-wide.

We do not use computers because they are smart. Computers *\*aren't\** smart. Sometimes we use them because they can do calculations very quickly, but even this is only a special case of the real value of computers. Computers always do the same thing in the same way. They are repeatable. They are, in this manner, reliable. Even a computer error can be useful to us--so long as it always happens the same way.

Consider, then, the computer virus. In order to reproduce without the informed assistance of the user, the virus must be, in the computer sense, transparent. It must operate without alerting the operator, or interfering with the operator's interaction with the computer. If the virus even posts a notice ("Hi! I am infecting object X!"), it has a nuisance value and is, therefore, not good. (Vesselin Bontchev notes that even such a notice, by possibly delaying a process, may have grave consequences far beyond annoyance.)

If, however, the virus does *\*not\** notify the operator, then the operator is not aware of some additional code in the machine. This extra code will have an unknown, and inherently unknowable, effect on the computer. The operations of the computer are, therefore, no longer repeatable. This is a Bad Thing (TM).

Some will protest that I have overblown the danger of both the notification messages and the possibility of conflicts. The point that I am trying to make is that you cannot predict the harm which may arise from interference either with the operator or the programs. Software is digital, and is subject to catastrophic collapse without prior warning. For those without a background in computer risk assessment, an excellent overview for the non-professional is found in Lauren Wiener's "Digital Woes" (cf. BKDGTLWO.RVW). An intriguing compilation of the types of things that can go wrong is to be found in Peter Neumann's "Computer Related Risks" (cf. BKCMRLRS.RVW). At the very least, as Sarah Gordon points out, the virus is an autonomous agent, making decisions and carrying out activities according to its own internal constructs and the intention of its programmer. This is very likely not in correspondence with your own intention, and is therefore an invasion of privacy.

A number of virus writers will object that their creations simply are not harmful. Not only is it impossible to guarantee that your virus will not conflict with existing systems, you also cannot guarantee that a given system will not conflict with your virus. Almost all file infecting viral programs will interfere with applications which have an internal integrity checksum or a non-standard loader, and will cause those applications to fail. (An example of this is that Windows programs infected with DOS viral programs always fail to load.) The "Ohio" virus (a prior version of Den Zuk) was not intended to carry any destructive payload, but an unusual interaction with a certain network

operating system caused fatal disk corruption. Since both Ohio and Den Zuk are examples of the often proposed "virus hunter virus", it should be clear that the concept of using a viral program to hunt down and disinfect other viral programs is not a good one.

Historically, and statistically, virus exchange people have been careless and incompetent programmers. Remember that we are talking vx, here, and those viral programs which have been released into the wild. There may be, carefully hidden in the desk of a virus writer, the "perfect" and harmless virus. If so, we haven't seen it yet. The majority have obvious bugs, sloppy coding and derivative programming. Less than one percent are interesting for *any* reason; only a handful have unique styles of algorithms. And even these last have programming pathologies.

There are two other reasons often given to justify virus exchange. The first is generally described as experimentation and education. The second is described as antiviral research, or, more commonly, assessment of antiviral programs. These arguments *do* have some validity, and should be examined. Ultimately, though, the reality fails to support the claim.

The call for experimentation is somewhat tied to the argument for a "good" virus. Current viral technology may be crude and ridiculous, but how can it be improved if there isn't any work or sharing of results? Quite true. The vx community, however, have obviously not read or noted any programming journals or texts. Discussions of programming and algorithms are supported by well-annotated code fragments. You don't present a whole program to discuss a specific function any more than you send an entire car with a manual on auto repair. You certainly don't use encoded or "DEBUG script" object code: that has no explanatory value at all.

And I have yet to see, in the vx materials, any discussion of legitimate and positive uses for viral technology, any discussion of control technology, or any discussion directed at ensuring that viral programs do not create conflicts.

In regard to education, it is true that a study of viral programs is related to a knowledge of operating system internals, as well as assembly language programming. However, viral study *requires* such knowledge, rather than providing it. Giving someone a virus and expecting them to learn from it is akin to "teaching" a surgeon by handing him a scalpel and pointing at a patient. Even the vx "old guard" are beginning to realize this. Viral programs use normal computer functions. If you understand computers, a virus is trivial. If you don't, well ...

As far as virus exchange tutorials go, well, let me put it this way. I am a teacher. Many of you will also know that I review technical books on a daily basis. Some are great, enough are good, many are bad and some are just plain awful. Only a few are worse, in terms of tutorial effectiveness, than vx "zines" (electronic periodicals).

Recently, someone who makes his living pushing virus source code promoted a collection of viral programs by suggesting you could test antiviral programs with it. This, superficially, sounds like a good idea--if you don't know what *real* software testing is like. What do we know about the quality of this

"zoo" (set of virus samples)? What do we know about the structure, organization, documentation and so forth? How many duplicates are there? Of course, we \*do\* want duplicates in some cases; we want every possible variation on polymorphs. (For Tremor, that works out to almost six billion files.) But then, this collection was on a CD-ROM. What a pity. The most successful viral programs are boot sector infectors, and you need to have real, infected disks to truly test for them. At a minimum, you'd want all seven "common" disk formats, in both system and non-system versions. That's fourteen disks--for \*each\* BSI.

For all the length of this piece, it is still only an overview. And, for all it's length, it probably hasn't convinced anyone. Ethics education (it used to be called "values education"), in whatever form and however presented, has very little to show that it works. There are various theories and models of moral training, the most sophisticated probably being Lawrence Kohlberg's "Moral Development" schema. All, though, basically boil down to sitting around talking about ethical dilemmas. They may develop debating skills and rhetorical sophistry, but there is no evidence to suggest that any of these programs leads to any significant change in behaviour.

While Kohlberg's model of moral development has the most detailed construction, its utility is questionable. His system is not so much one of values education as of values measurement. It is, therefore, a guideline for evaluating other ethical training methods rather than a means of instruction and change. Moral development is a six stage structure, assessing the type of reasoning which goes into ethical choices. The stages range from "fear of punishment" to "internal ethical principles". There is great difficulty, however, in determining the "stage" of a given individual. Most ethical discussions will be judged as having reasoning at all of stages three, four and five. This entire document, for example, could be dismissed as being level one reasoning since it mentions the possibility of the danger of virus distribution and could therefore be seen as a "fear of punishment" (negative consequences) on my part. On the other hand, most of Kohlberg's proponents dismiss level six, since even a psychopath could be said to be acting from internal principles. Kohlberg, himself, has stated that he does not know if anyone consistently acts from stage six reasoning.

Probably the major reason for this is that modern society has no fundamental moral foundation. The most widely cited (and Johnson gives an excellent critique of it) is utilitarianism--"the greatest good for the greatest number". Leaving aside the difficulties of assessing such a measure, utilitarianism, along with all the other modern "humanistic" philosophies, has nothing to support itself. Why is "the greatest good for the greatest number" to be chosen over "what \*I\* want"? An alternative is deontology; ethical principles derived from the concept of duty. (Ironically, this philosophy, while arguably superior to utilitarianism, is limited to Kohlberg's stage four almost by definition.) Again, however, there is no underpinning to the concept of duty, itself.

Ironically, the much maligned "Judeo-Christian Ethic" did have such a foundation for moral standards--God. The theistic universe may yet have the last laugh over the mechanical universe of B. F. Skinner's "Beyond Freedom and Dignity". Maybe Jesus \*is\* the answer--or there may be no answer.

## Bibliography

Bontchev, "Are 'Good' Viruses Still a Bad Idea?", Proceedings of the EICAR '94 Conference, pp.25-47, also

<ftp://ftp.informatik.uni-hamburg.de/pub/virus/texts/viruses/goodvir.zip>

Clarkson, "Windows Hothouse", 1994, 0-201-62669-1, U\$34.95/C\$44.95 - lots of artificial life fun with Visual C++

Cohen, "It's Alive!", 1994, 0-471-00860-5, U\$39.95 - an intriguing, provoking and practical exploration of computer programs as "artificial life", but somewhat narrow

Denning, ed., "Computers Under Attack", 1990, 0-201-53067-8 - collection of essays roughly related to security, also "the net"

Ermann/Williams/Gutierrez, "Computers, ethics and society" - textbook for computer ethics course: not great

Gordon, "Technologically Enabled Crime", 1994

Forester/Morrison, "Computer Ethics", 1994, 0-262-56073-9 - lots of great stories, but short on analytical depth

Johnson, "Computer Ethics", 1994, 0-13-290339-3 - the basic work in the field, thorough coverage and good discussion starter

Levy, "Artificial Life", 1992, 0-679-73489-8, U\$13.00/C\$17.00 - an interesting wander through fields studying artificial life but no strong points

Neumann, "Computer-Related Risks", 1994, 0-201-55805-X, U\$24.75 - exhaustive examples from the RISKS-FORUM Digest of potential technological perils

Slade, "Robert Slade's Guide to Computer Viruses", 1994, 0-387-94311-0/3-540-94311-0, U\$29.95 - chapter seven looks at the computer virus and society

Thro, "Artificial Life Explorer's Kit", 1993, 0-672-30301-9, U\$24.95/C\$31.95 - good fun, but little analysis

Wiener, "Digital Woes", 1993, 0-201-62609-8, U\$22.95/C\$29.95 - excellent introduction to the risks of software

(A fuller bibliography on values education readings is available for those demonstrating a willingness to put some effort into it, since, frankly, it's a really disappointing field. Sarah Gordon's "Generic Virus Writer" paper has significant resources here.)

copyright Robert M. Slade, 1995

Permission is granted to post this file, in full, on any system.

=====

DECUS Canada Communications, Desktop, Education and Security group newsletters

Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733  
Author "Robert Slade's Guide to Computer Viruses" (US contact 1-800-SPRINGER)



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 16: Issue 92**

**Thursday 16 March 1995**

## Contents

- [Health card rips off ATM for \\$100,000](#)  
[Roy Beimuts](#)
- [A340 shenanigans](#)  
[Les Hatton](#)
- [Mistake of platform-specific instructions](#)  
[Stanton McCandlish](#)
- [The Manchurian Printer](#)  
[Simson L. Garfinkel](#)
- [Re: Scientology Blackmail Risk](#)  
[Lance A. Brown](#)  
[Jon Green](#)
- [Re: Internet-Finland Privacy](#)  
[Michael Jennings](#)
- [Jumping to conclusions? \(Lifeguard\)](#)  
[Peter da Silva](#)
- [Re: Microsoft and Lotus spreadsheet errors](#)  
[Bear Giles](#)
- [Society and the Future of Computing](#)  
[Phil Agre](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Health card rips off ATM for \$100,000

"AGR CANADA, Research Station, Melfort, Sask." <SYSTEM@skrsmc.agr.ca>  
15 Mar 1995 12:18:46 -0500 (EST)

>From Saskatoon StarPhoenix, March 14:

"BC man sentenced for ATM scam"

PORT HARDY, B.C. (CP) -- A Vancouver Island man who used his health card to steal \$100,000 from a bank machine has been given a year in jail. Richard Lee Mose, 22, of Port Alice, B.C., was found guilty of theft in Campbell River court. A Bank of Nova Scotia official said a processing

problem allowed Mose to use a non-bank card on an automatic teller. With his health-care card, Mose completed several transactions over several hours and got \$109,000 dollars. But the bank machine recorded the information stored on the health card, and police traced it back to Mose.

Roy Beimuts, Melfort, Saskatchewan [beimutsr@em.agr.ca](mailto:beimutsr@em.agr.ca)

---

## A340 shenanigans

*Les Hatton <[les\\_hatton@prqa.co.uk](mailto:les_hatton@prqa.co.uk)>*

*15 Mar 1995 15:56:26 +0000*

The BBC news at 08.30 reported a slight problem which occurred on the morning of 15 Mar 1995 with the ultra high-tech, packed full of software and therefore utterly wonderful Airbus A340.

Apparently on the final part of its approach to Gatwick, both the pilots screens went blank, to be replaced by a polite little message saying "Please wait ...". Somewhat unnerved, the pilots requested that the plane turn left, but it turned right instead. They then tried to get it to adopt a 3 degree approach to the runway, but it chose a 9 degree plummet instead. At this point, from the report, they appeared to gain manual control and landed safely. It is not clear who will pick up the dry-cleaning bill.

Vis a vis this sort of thing, I was at a talk recently, given by the CAA (UK Civil Aviation Authority), at which it was stated that in the past generation of civil aircraft, most of the software problems were reported in the Flight Management System. Not surprisingly, this was the most complex part of the aircraft software system. Not any more it isn't. During the talk, it was also admitted that the newer generation of aircraft such as the A340, other software systems including active systems were "at least as complicated". So what next ?

I suppose it follows on nicely from the story in the October 1994 Risks whereby a Japanese Air Force T-4 jet trainer ejected one of its pilots. Perhaps it didn't like him. :-)

Les Hatton, Ph.D. C.Eng, Director of Research & Engineering, Programming Research Ltd, England [les\\_hatton@prqa.co.uk](mailto:les_hatton@prqa.co.uk) +44 (0) 1 932 888 080

---

## Mistake of platform-specific instructions

*Stanton McCandlish <[mech@eff.org](mailto:mech@eff.org)>*

*Wed, 15 Mar 1995 17:29:33 -0500 (EST)*

One thing that's bugged the hell out of me for several years is the failure of many people giving instructions on finding net resources to do so in a generic manner. Here's a great example:

1. Get into the WWW.
2. Enter the letter G so you can enter the address for the test site.

3. At the prompt, enter the following:

<http://sunsite.unc.edu/jembin/mb.pl>

This was from an announcement off of the Net Happenings list. Anyone following these instructions will get nowhere unless they are using lynx (unless there's another browser that uses the same keystrokes to specify a URL, which I doubt.) The first item implies that the instructions are generic, for whatever means one uses to browse WWW sites (and, incidentally, indicate a fundamental misunderstanding of the technology, since the WWW is not a "thing" that one "gets into", but is a method, a process, a standard.

All the author had to do was put:

URL:<http://sunsite.unc.edu/jembin/mb.pl>

At any rate, the application-dependent specificity of the instructions, though not a problem for anyone that's been using Internet tools for very long, is potentially very confusing and frustrating to less experienced users. And these users exist in ever greater numbers, as systems like AOL and Delphi become increasingly Internetly. I don't mean to single out AOL for any more maligning, but as a forum sysop there besides my other online services duties, I can say from firsthand experience that the technical skill level of AOL users is, on average, staggerly lower that that of the typical shell account user, or almost anyone else online for that matter.

Typical questions I receive from AOL users are: "What happened?" "How do I read this file?" "If I want to download an ASCII file do I have to use the ASCII protocol, or can I use ZModem?" "What do I join?" "Help!" "What is a 'GIF graphics viewer'?" Those aren't snippets. Those are entire message bodies. Such people, confronted with the site instructions I quoted from Net Happenings, are never going to reach the site in question, will probably pound people like me with more questions like the above example in an effort to figure out what to do, and may eventually give up in disgust (a few might actually RTFM and get a clue, but not everyone is a born geek.)

So, there are two RISKS to keep in mind here:

1) If you use platform-specific instructions, you are doing other readers a disservice, and should at very least note that they are platform-specific (or application-specific, or whatever, as apropos). Better yet, just use generic instructions that anyone can use.

2) If you need help with something, but don't \*include enough information\* for them to actually help you, you're unlikely to get a useful response. Include info such as: what kind of system you have, what it's relevant configuration is, what went wrong in detail, what all the items (files, whatever) are specifically that you are referring to, etc.

<A HREF="<http://www.eff.org/~mech/>"> Stanton McCandlish  
</A><HR><http://www.eff.org/>> Electronic Frontier Foundation

<http://www.eff.org/1.html>"> Online Services Mgr. </A>

---

## The Manchurian Printer

*Simson L. Garfinkel <simsong@pleasant.cambridge.ma.us>*

*Wed, 15 Mar 1995 21:28:37 -0500*

The Manchurian Printer, (C) 1995, Simson L. Garfinkel  
[The Boston Sunday Globe, March 5, 1995, Focus Section, Page 83]

Simson L. Garfinkel

Early this month, Hewlett-Packard announced a recall of 10,000 HP OfficeJet printer fax copiers. The printer's power supplies may have a manufacturing defect that could pose an electrical shock hazard. HP says that it discovered the problem with its printers during routine testing; HP was lucky: printers can be very dangerous devices. A typical laser printer, for example, can draw hundreds of watts of power, generate internal temperatures high enough to burn a wayward human hand, and even, under the right circumstances, start a fire.

Most manufacturers, of course, try to design their printers to minimize such risks. Increasingly, however, there is a chance that companies might intentionally design life-threatening flaws into their products so that the flaws can be exploited at a later time. These fatal flaws might be intentionally built into equipment manufactured overseas, as a kind of "insurance policy" in the event of a war between that foreign country and the United States. The flaws might form the basis for a new kind of corporate warfare. Or the flaws might be hidden by disgruntled employees contemplating extortion or revenge.

Indeed, U.S. military planners are increasingly worried about this sort of possibility, they place under a heading "Information Warfare." Nevertheless, although the threat of Information Warfare is very real, an even bigger danger is that the Department of Defense will use this threat to convince the new Congress to repeal the Computer Security Act of 1987. This would effectively allow the National Security Agency to declare martial law in cyberspace, and could place the civilian computer industry into a tailspin.

To understand what the military is afraid of, imagine the Manchurian Printer: a low-cost, high-quality laser printer, manufactured overseas, with built-in secret self-destruct sequence. For years these printers could lay dormant. But send them a special coded message---perhaps a long sequence of words that would never normally be printed together---and the printer would lock its motors, overheat, and quickly burst into flames. Such an attack might be the first salvo in an out-and-out war between the two countries. Alternatively, an enemy company might simply use printers to start selective fires, damage economic competitors, take out key personnel, and cause mischief.

Unlike the movie the Manchurian Candidate, the technology behind the Manchurian Printer isn't science fiction. Last October, Adobe accidentally

shipped a "time bomb" in Photoshop version 3.0 for the Macintosh. A time bomb is a little piece of code buried inside a computer program that makes the software stop running after a particular date. Adobe put two time bombs into its Photoshop 3.0 program while the application was under development. The purpose behind the time bombs was to force anybody who got an advance, pre-release copy of the program to upgrade to the final shipping version. But when it came time to ship the final version of Photoshop 3.0, Adobe's engineers made a mistake: they only took out one of the bombs.

An engineer inside Adobe learned about the problem soon after the product was shipped, and the company quickly issued a recall and a press release. Adobe called the time bomb a "security code time constraint" and said that "although this is an inconvenience to users, the security constraint neither damages the program or hard drive, nor does it destroy any files."

It only takes a touch of creativity and a bit of paranoia to think up some truly malicious variants on this theme. Imagine that a company wants to make a hit with its new wordprocessor: instead of selling the program, the company gives away free evaluation copies that are good for one month. What's unknown to the users of this program is that while they are typing in their letters, the program is simultaneously sniffing out and booby-trapping every copy of Microsoft Word and WordPerfect that it finds on your system. At the end of the month, all of your wordprocessors stop working: Instead of letting you edit your memos, they print out ransom notes.

Any device that is equipped with a microprocessor can be equipped with such a booby-trap. Radios, cellular telephones, and computers that are connected to networks are particularly vulnerable, since an attacker can send them messages without the knowledge or consent of their owners. Some booby-traps aren't even intentional. What makes them particularly insidious is that it is almost impossible to look at a device and figure out if one is present or not. And there is no practical way to test for them, either. Even if you could try a million different combinations a second, it would take more than 200 years to find a sequence that was just 8 characters long.

\* \* \*

Information Warfare isn't limited just to things that break or go boom. The Department of Defense is also worried about security holes that allow attackers to break into commercial computers sitting on the Internet or take over the telephone system.

"This nation is under IW attack today by a spectrum of adversaries ranging from the teenage hacker to sophisticated, wide-ranging illegal entries into telecommunications networks and computer systems," says a report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield, and issued last October by the Office of the Secretary of Defense.

"Information Warfare could pervade throughout the spectrum of conflict to create unprecedented effects. Further, with the dependence of modern commerce and the military on computer controlled telecommunication networks, data bases, enabling software and computers, the U.S. must protect these assets relating to their vulnerabilities," the report warns.

Information warfare changes the rules of war fighting, the report warns. A single soldier can wreak havoc on an enemy by reprogramming the opposing side's computers. Modern networks can spread computer viruses faster than missiles carrying biological warfare agents, and conceivably do more damage. Worst of all, the tools of the information warrior are readily available to civilians, terrorists and uniformed soldiers alike, and we are all potential targets.

Not surprisingly, the unclassified version of the Pentagon's report barely mentions the offensive possibilities of Information Warfare---capabilities that the Pentagon currently has under development. Nevertheless, these capabilities are alluded to in several of the diagrams, which show a keen interest by the military in OOTW---Operations Other Than War.

"They have things like information influence, perception management, and PSYOPS---psychological operations," says Wayne Madsen, a lead scientist at the Computer Sciences Corporation in northern Virginia, who has studied the summer study report. "Basically, I think that what they are talking about is having the capability to censor and put out propaganda on the networks. That includes global news networks like CNN and BBC, your information services, like CompServe and Prodigy," and communications satellite networks. "When they talk about 'technology blockade,' they want to be able to block data going into or out of a certain region of the world that they may be attacking."

The report also hints at the possibility of lethal information warfare.

"That is screwing up navigation systems so airplanes crash and ships run aground. Pretty dangerous stuff. We could have a lot of Iranian Airbuses crashing if they start screwing that up," Madsen says. Indeed, says Madsen, the army's Signal Warfare center in Warrenton, Virginia, has already invited companies to develop computer viruses for battlefield operations.

Our best defense against Information Warfare is designing computers and communications systems that are fundamentally more secure. Currently, the federal organization with the most experience in the field of computer security is the National Security Agency, the world's foremost spy organization. But right now, NSA's actions are restricted by the 1987 Computer Security Act, which forbids the agency from playing a role in the design of civilian computer systems. As a result, one of the implicit conclusions of the Pentagon's report is to repeal the 1987 law, and untie the NSA's hands. Indeed, the Pentagon is now embarking on a high-level campaign to convince lawmakers that such a repeal would be in the nation's best interests.

This argument confuses security with secrecy. It also ignores the real reasons why the Computer Security Act was passed in the first place.

In the years before the 1987 law was passed, the NSA was on a campaign to expand its power throughout American society by using its expertise in the field of computer security as a lever. NSA tried to create a new category of restricted technical information called "national security related information." They asked Meade Data Corporation and other literature search

systems for lists of their users with foreign-sounding names. And, says David Banisar, a policy analyst with the Washington-based Electronic Privacy Information Center, "they investigated the computers that were used for the tallying of the 1984 presidential election. Just the fact that the military is looking in on how an election is being done is a very chilling thought. After all, that is the hallmark of a banana republic."

The Computer Security Act was designed to nip this in the bud. It said that standards for computer systems should be set in the open by the National Institute of Standards and Technology.

Unfortunately, the Clinton Administration has found a way to get around the Computer Security Act. It's placed an "NSA Liaison Officer" four doors down from the NIST director's office. The two most important civilian computer standards to be designed in recent years---the nation's new Escrowed Encryption Standard (the "Clipper" chip) and the Digital Signature Standard were both designed in secret by the NSA. The NSA has also been an unseen hand behind the efforts on the part of the Clinton Administration to make the nation's telephone system "wiretap friendly."

Many computer scientists have said that the NSA is designing weak standards that it can circumvent, so that the nation's information warfare defenses do not get in the way of the NSA's offensive capability. Unfortunately, there's no way to tell for sure. That's the real problem with designing security standards in secret: there is simply no public accountability.

In this age of exploding laser printers, computer viruses, and information warfare, we will increasingly rely on strong computer security to protect our way of life. And just as importantly, these standards must be accountable to the public. We simply can't take our digital locks and keys from a Pentagon agency that's saying "trust me."

But the biggest danger of all would be for Congress to simply trust the administration's information warriors and grant their wishes without any public debate. That's what happened last October, when Congress passed the FBI's "Communications Assistance for Law Enforcement Act" on an unrecorded voice vote. The law turned the nation's telephone system into a surveillance network for law enforcement agencies, at a cost to the U.S. taxpayer of \$500 million.

=====**WHAT FOLLOWS ARE CAPTIONS FOR THE ART**=====

Photo: Box of Microsoft Word 6.0

Even though it's illegal, a lot of people like to "try out" software by making a copy from a friend before they plunk down hundreds of dollars for their own legal copy. Computer companies say that this is a form of software piracy: many who try never buy. More than 2 billion dollars of software is pirated annually, according to the Business Software Alliance.

One way that companies like Microsoft and Novel could fight back is by booby-trapping their software. Sure, customers wouldn't like it if that stolen copy of Microsoft Word suddenly decided to erase every letter or memo that they've written in the past month, but what legal recourse would they have?

=====

Photo: Cellular Telephone

Is your cellular phone turned on? Then your phone is broadcasting your position every time it sends out its electronic "heartbeat." Some law enforcement agencies now have equipment that lets them home in on any cellular telephone they wish (similar technology was used recently to catch infamous computer criminal Kevin Mitnick). Perhaps that's the reason that the Israeli government recently ordered its soldiers along the boarder to stop using their cellular telephones to order late night pizzas: the telephone's radio signal could be a become a homing beacon for terrorist's missiles.

=====

Photo: Floppy Disk

Beware of disks bearing gifts. In 1989, nearly 7000 subscribers of the British magazine PC Business World and 3500 people from the World Health Organization's database received a disk in the mail labeled "AIDS Information Introductory Diskette Version 2.0". People who inserted the disks into their computers and ran the programs soon found out otherwise: the disks actually contained a so-called trojan horse that disabled the victims' computers and demanded a ransom.

=====

Photo: A computer with a screen from America Online, and a modem

Several years ago, users of Prodigy were shocked to find that copies of documents on their computers had been copied into special "buffers" used by Prodigy's DOS software. Prodigy insisted that the copied data was the result of a software bug, and it wasn't spying on its customers. But fundamentally, if you use a modem to access America Online, Prodigy or Compuserve, there is no way to be sure that your computer isn't spying on you while you surf the information highway.

=====

HP's recall affects only OfficeJet printers with serial numbers that begin US4B1-US4B9, US4C1-US4C9, US4BA-US4BU, or US4CA-US4CK. Worried about your OfficeJet? Call HP at (800) 233-8999.

=====

Simson L. Garfinkel writes about computers and technology from his home in Cambridge, Massachusetts.

---

## Re: Scientology Blackmail Risk (Vilkaitis, [RISKS-16.91](#))

"Lance A. Brown" <lab@biostat.mc.duke.edu>  
Wed, 15 Mar 1995 10:58:37 -0500

Vilkaitis is not correct. Postings on alt.security.pgp stated that Finnish authorities secured a warrant to seize the equipment the Finnish Anonymous Server runs on. The owner of the Server negotiated a deal with the authorities where he released the identity of \_one\_ user of the Server and the authorities didn't seize the equipment.

My understanding of the behind-the-scenes goings on is that the Church of Scientology is bringing copyright charges against one of its former

ministers who is now a vocal critic of the CoS on the Internet. The sequence of events, as I understand it, is that someone used the Finnish Anonymous Server to post allegedly copyright material on USENET. The CoS asked the FBI to talk to Interpol who talked to the Finnish Police about getting the ID information of the anonymous poster. Once this ID information was released by the owner of the Server it was immediately handed over to CoS people.

[Also noted by Kevin.P.Maguire@jpl.nasa.gov (Kevin Maguire) and "Matti E. Aarnio [OH1MQK]" <mea@mea.cc.utu.fi>. PGN]

---

### Re: Scientology Blackmail Risk (Vilkaitis, [RISKS-16.91](#))

Jon Green <jonsg@diss.hyphen.com>  
Wed, 15 Mar 1995 09:40:35 +0000 (GMT)

[... more as noted by Lance Brown deleted ... PGN]

Nonetheless, this does represent a worrying precedent. There are persistent rumours that the entire user base of at least one anonymizing service has been compromised by covert action by a security agency, and that's just the start. As has been pointed out elsewhere, any agency monitoring international communications (NSA in the US and GCHQ in the UK, to name two) should have little trouble matching anon ID with real ID if the message is in plaintext and the server in another country. Matching messages where the first leg is PGP-encoded (and the server decodes before retransmission) would be more difficult, but by no means impossible.

The only sensible conclusion is that anon remailers provide anonymity from your peers, not from the law. If you use them illegally, you may well be identified. Them's the breaks.

jonsg@hyphen.com jon@sundome.demon.co.uk

---

### Re: Internet-Finland Privacy ([RISKS-16.91](#))

Michael Jennings <M.J.Jennings@amtp.cam.ac.uk>  
15 Mar 1995 17:16:33 GMT

>Case #1 ... A Swedish journalist-researcher "reveals" that an Anonymous  
>Case #2 ... Finnish Police receive a request from U.S. law enforcement

There have been suggestions on the net (in alt.privacy.anon-server, I think) that these two events may well have been related: specifically that the Church of Scientology might have been indirectly responsible for the 'This anon server is used by pedophiles: shock, horror' stories in the first place, as an attempt to discredit the anon server in order to make the police more likely to raid it for them/ get it shut down. This is only speculation, but it is consistent with their style. It is their standard policy to attempt to discredit their opponents through character assassination at the same time as they attack them through legal means.

For instance, one of the recent posters of copyright material to alt.religion.scientology was described in passing in a Scientology press release as someone who conducted execution-style killings of his pets in front of his children. Paulette Cooper, who wrote a book entitled *The Scandal of Scientology*, found a circular (supposedly written by 'a concerned neighbor') circulating around her apartment block suggesting her 'removal from our residence, and if possible, have her put under appropriate psychiatric care.' Several critics of scientology have been accused (and sometimes tried) for crimes that they did not commit, after having (apparently) been framed by scientologists.

Many people have used the anon server to post critical articles about Scientology. I suspect the church would like it discredited. (Massive amounts of information about this and the church in general can be found at [http://falcon.cc.ukans.edu/~sloth/sci/sci\\_index.html#diary](http://falcon.cc.ukans.edu/~sloth/sci/sci_index.html#diary))

Michael Jennings, Department of Applied Mathematics and Theoretical Physics  
The University of Cambridge. mjj12@damtp.cambridge.ac.uk

---

### Jumping to conclusions? (Lifeguard)

*Peter da Silva <peter@nmti.com>*  
*Wed, 15 Mar 1995 09:44:33 -0600*

> "Anybody who shoots at you from any direction would be immediately located  
> and subject to return fire," says Thomas Karr, head of the Lab team.

I don't read this as "the weapon would automatically return fire" but "the police officer would be able to return fire".

---

### Re: Microsoft and Lotus spreadsheet errors (Bellovin, [RISKS-16.90](#))

*Bear Giles <bear@tiger.cs.colorado.edu>*  
*Wed, 15 Mar 1995 16:56:25 -0700*

>They ended up doing the calculation, and storing a compressed table giving  
>the difference between the calculated values and the legal ones. Never mind  
>reality -- custom ruled.

I can beat that. I recently ported a mess of old FORTRAN meteorological code to C++, and I extensively expanded the validation suite in the process.

During the process I learned that a number of my newly ported functions were returning values a hair off (typically < 0.5%, when the number of significant digits should have resulted in errors two orders of magnitude smaller). I traced the problem to the fact that I was using the best currently known physical constants, while the standard reference tables were using values from the 1960s. Reasonable, since it was published in 1965, but I had to address the differences in the results.

After consulting with the working meteorologists, I eventually put the 1960-era physical constants back into the software. As a practical matter, the resolution of the available data is still coarse enough that the small differences won't make any difference, and it is easier for them to compare the final results than for FORTRAN programmers to understand scientific C++ classes.

But it still grates. At least I was able to eliminate a number of duplicate functions. Previously, someone had made a token effort to include a validation suite (with typically <10 test cases per function), but they made no effort to identify slow and/or inaccurate functions. A tradeoff of speed for accuracy is often justified, but who would ever want to use a function which is significantly slower and less accurate than another one?

Bear Giles [bear@fsl.noaa.gov](mailto:bear@fsl.noaa.gov)

---

## Society and the Future of Computing

*Phil Agre <[pagre@weber.ucsd.edu](mailto:pagre@weber.ucsd.edu)>*

*Wed, 15 Mar 1995 11:52:07 -0800*

The conference on Society and the Future of Computing (SFC'95) will be held from June 11th to 14th in Durango, Colorado. This conference is an initiative of the US Public Policy Committee of the Association for Computing Machinery (USACM). Its focus is on opportunities for socially beneficial applications of computing technology: visions of what's possible ten years from now and agendas for computer science research that can make those visions come true.

Conference speakers include:

Gary Chapman, University of Texas, Austin  
John Cherniavsky, National Science Foundation  
Peter J. Denning, George Mason University  
Linda Garcia, Office of Technology Assessment  
S. Joy Mountford, Interval Research Corporation  
Don Norman, Apple Computer, Inc.  
Roy Pea, Northwestern University  
Paul Evan Peters, Coalition for Networked Information  
Virginia E. Rezmierski, University of Michigan  
Leslie Sandberg, Institute for Telemedicine  
Paul Young, National Science Foundation

Full information about the conference is available from the conference web pages at:

<http://www.lanl.gov/LANLNews/Conferences/sfc95/sfcHome.html>

or send an e-mail message that looks like this:

To: [rre-request@weber.ucsd.edu](mailto:rre-request@weber.ucsd.edu)  
Subject: archive send sfc-95

Poster sessions will be an important part of the conference. For full information on poster submissions, see the conference web pages or contact Doug Schuler <douglas@scn.org>. The deadline is April 1st.

Student scholarships are available as well; information is available from sfc95-students@lanl.gov.

The basic idea is to gather 250 people in a nice place to work hard and have fun learning how to take social issues into account when setting agendas for computer science research. We hope you can join us.

Phil Agre, UCSD



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 16: Issue 93**

**Monday 20 March 1995**

## Contents

- [About the "Altona Railway software glitch"](#)  
[Klaus Brunnstein](#)
- [Credit-Card Fraud](#)  
[NYT via Edupage](#)
- [Keeping buses on time plus a little eavesdropping](#)  
[Mark Kruse](#)
- [Does Internet threaten civilization?](#)  
[Dick Mills](#)
- [Latent risks of cost-benefit analysis](#)  
[Phil Brown](#)
- [Re: Internet-Finland Privacy](#)  
[Peter Kaiser](#)
- [Risks of doing date arithmetic early in the year without FP](#)  
[Peter Ludemann](#)
- [Phone companies with wrong 555-1212 databases](#)  
[Frederick B. Cohen](#)
- [Re: The Manchurian Printer & Prodigy Spies on Users](#)  
[Frank C. Ferguson](#)
- [Software System Safety Class](#)  
[Nancy Leveson](#)
- [First Bank of Internet \(FBOI\) Opens](#)  
[Vinn Beigh](#)
- [Info on RISKS \(comp.risks\)](#)

---

### About the "Altona Railway software glitch"

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.d400.de>  
Fri, 17 Mar 1995 17:48:54 +0100*

German Railway attempted, Sunday March 12 1995 evening, to replace its long established railway switch tower at Hamburg-Altona station by a fully computerized system manufactured by Siemens branch on railway technology. Altona station is one of Germany's large station, with many national and international lines starting or ending here or passing through. Each day,

about 30,000 travellers arrive or depart here, in addition to more than 100,000 passengers using local rapid (S-Bahn) or regional trains.

With about 250 rail shunts and an equivalent number of signals, the old system consisted of 7 major switch-stands, controlled by roughly 50 experienced switchmen. Siemens and German Railway decided to completely change the topology with now about 18 switch-stands to be controlled by INTEL-486 based Real-Time systems. The different switch computers are coordinated by one central operating and display system (BAR 16, for Bedien- und-Anzeige-Rechner, and 16 standing for 16-Bit connection). PC hardware is redundant (2 processors, modular RAM, no disk) to enhance availability and reliability as requested by the certification authority (Eisenbahn Bundes-Amt, EBA). The new architecture is incompatible with the old one and it cannot run in parallel to the old; one economic advantage is that the new system needs about 40 switchmen less which only control the central BAR site.

Immediately after starting the new systems, the central computer (BAR 16) failed. Siemens' experts could not find the cause for hours, so German Railway decided to close up the whole station, forcing passengers to North and South to start from locations up to 25 kilometers away. Search for the fault was difficult as it were very rare. Only on Tuesday afternoon, experts detected that under certain conditions a stack overflow happened. When looking into the routine which should handle stack overflows, they found that this went into a deadlock due to a programming error. Though sufficient free space was available in principle, the allocation of the stack required to build a new RAM with 4,000 bytes onstead of 3,500 as foreseen (indeed, overflow was only with few bytes, so +500 bytes adds some safety :-). Only on Wednesday morning, the bug (which appeared only 4 times in 2 days) was fixed, and rail traffic began to return to Altona station on Wednesday 1:59 pm. But as the switchmen are not accustomed to the new system, even days later allowed restricted traffic.

In a press conference, the responsible Siemens manager argued that the "hidden" faults were difficult to find, and that Siemens experts had assumed that the routine handling stack overflow would NEVER be used! The related operating system is regarded by Siemens as rather safe RT system :-)

In German media (you know: Hamburg is media capital of Germany :-), a discussion on overreliance on computers started. This was stimulated by statements of Siemens and German Railway that any future computer failure will require to again stop the whole switching system to avoid any safety hazard. This is very bad news as the same system is being installed at another site connecting main railway station (Hauptbahnhof) with Berlin and controlling all goods transport originating and ending in Hamburg harbour (Europes 2nd largest container harbour). [Another reason for discussing overreliance are recent bad news on Airbuses, most of which are finally assembled in Hamburg-Finkenwerder's Airbus factories, with many operational Airbuses being maintained in Lufthansa's Hamburg workshops].

The Altona Railway software glitch is another example where (for purposes of rationalisation) all customers become fully dependent of a computerized system. Moreover, the few remaining switchmen will NOT be able to understand, in critical situations, why the computer system behaves as it

does, and they will ONLY be able to switch off the whole system as NO manual mode is foreseen!

Klaus Brunnstein (Univ Hamburg, 17 March 1995)

---

### **Credit-Card Fraud (NYT via Edupage 19 Mar 1995)**

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

Mon, 20 Mar 95 11:24:48 PST

Security experts are disdainful of the low level of programming talent displayed in the pirate program Credit Master, which generates phony credit card numbers. The program works by mimicking the simple "checksum" algorithm that creates the last four digits of a credit card; the checksum formula was developed merely to prevent data-entry errors and never meant to be high-tech security screening. Four college students were arrested last week in Nassau County, NY, charged with using a program to generate false credit numbers and order thousands of dollars of goods. The students then had the merchandise shipped to addresses staked out by the police -- a mistake almost as bad as using cheap programs. (The New York Times, 19 Mar 1995, p.18)

---

### **Keeping buses on time plus a little eavesdropping**

Mark Kruse <kruse@sector.kodak.com>

Sat, 18 Mar 1995 08:48:33 -0500

Seen in the Washington Post:

As part of a war on traffic congestion, Montgomery County Maryland transit officials plan to use the satellite <GPS - "one of the same satellites the Pentagon used during the Persian Gulf War"> to keep buses on time and increase safety for Ride-On's 58,000 weekday riders. ... When the system is begun countywide later this year, county technicians will be able to change traffic signals to green as a tardy bus approaches an intersection. When people call to ask for bus information, a county transit employee will be able to give them the precise time a buss will arrive instead of when it is scheduled to be there. In an emergency, police will know the bus's exact location and will be able \*\*\*to listen in over a microphone installed in the bus."

I see two risks here:

- If riders become dependent on calling in for information on EXACTLY when a bus will be at a particular location, the transit authority will soon be overloaded with phone calls and thus probably making it more difficult for people calling for other reasons to get through (a relatively minor risk given that this is probably not a critical service phone number?)
- What are the criteria for when the police are allowed to listen in over the microphone installed in the bus? Slowly, but surely, 1984 is approaching

(or is time just flowing backwards :-)

Mark W. Kruse

---

## Does Internet threaten civilization?

*Dick Mills <dj.mills@pti-us.com>*

*Sat, 18 Mar 1995 10:29:11 -0500*

An attribute of the Internet is that it makes one-to-many personal communication more effective and more resistant to censorship than any prior form of communication. Therein lies some risks. I am not sure which are most real. Consider the following.

It seems that everyone from Scientologists, to United States senators, to Swedish journalists, to the National Security Agency, to holocaust survivors, wants to censor or constrain the net in some way. Indeed, nearly everyone on this planet seems to believe that we must, at all costs, censor some other person or group. If net censorship proves to be impossible, then the logical conclusion is that everyone, ourselves included, will come to oppose the net. The continued existence of the net must therefore be at risk; right?

Can it be that the stability of civilization is dependent on the natural barriers to effective one-to-many communication? Without the barriers, criminals, pranksters, demagogues, exploiters, fanatics, the politically incorrect, and the religiously incorrect, will all be able to do their thing more effectively. Society becomes more vulnerable, to hoaxes, scams, spams, diatribes, sensationalism, and manipulation. Many laws may become unenforceable. Is it the net that threatens civilization?

More speculative, but perhaps more likely, is the eventual development of a number of object-oriented virus-like agents able to police the net for us. Call it distributed RoboCop. The risk then will be to prevent it from becoming RoboSoverign. :-/

Dick Mills, Power Technologies, Inc., P.O. Box 1058 Schenectady, NY 12301-1058  
dj.mills@pti-us.com phone +1(518)395-5154 fax +1(518)346-2777

---

## Latent risks of cost-benefit analysis

*Phil Brown <pdbrown@mindspring.com>*

*Fri, 17 Mar 1995 17:25:57 -0600*

Recently there was an article in the Atlanta Journal-Constitution about an association of pediatricians (I forget the group's exact name offhand) that was lobbying for a complete ban on advertising for alcoholic beverages, citing health and economic benefits. What makes this issue pertinent for Risks readers, I believe, is the risk of rampant cost-benefit analysis. The problem is not so much with the technique itself, which I have often used with great success, as it is with the slippery slope people find themselves

on once they try to apply it to social situations and human behavior that have strong intangible elements. Alcohol consumption is a case in point. Even in my surliest moods toward purveyors of political correctness, I would agree that alcohol can carry a heavy social burden. So what? Societies are good at identifying and labelling (and then castigating!) perceived burdens. While not a raving libertarian, I am disturbed by forces that trot "scientific method" out on a leash (e.g. cost-benefit analysis) to determine social "costs" and "benefits" and use the results to try and dictate behavior.

I understand that proponents of the Republican Contract With America want to use cost-benefit analysis as a tool to determine when environmental regulation is appropriate. This is a seductive idea on its face, and speaks to the same general problem of trying to reduce human value judgments to the level of dollars and cents. The yin and yang of individual right versus social responsibility is ancient and irremediable. Where one triumphs the other suffers. Yet the human spirit dwells most often in the wasteland between libertarianism and communitarianism, in my humble opinion. As much as the engineering side of my nature wants to believe we all benefit from being able to analyze social issues in the mathematical realm, mathematics is about probing the edges of problems and not about dwelling in the comfortable middle ground.

I guess my real beef with cost-benefit analysis, at least as I have seen it practiced by social policy types, is that it skews in favor of social benefit, given that quantizing individual liberty is at best an ethereal exercise. When confronted with a statistic such as one shouting out that "alcohol consumption costs the US in excess of \$100 billion per year in illness, disability, and lost productivity", is one to assume that otherwise rational individuals are wantonly placing some tremendous burden on society with no commensurate return? That's a statistic racing away from the center of any reasoned debate.

We are shackling ourselves with tautologies, brought on by a desire to remove judgment from public discourse. Oppression flows from within.

Phil Brown, Atlanta, GA [pdbrown@mindspring.com](mailto:pdbrown@mindspring.com) -or- [xstential1@aol.com](mailto:xstential1@aol.com)

---

## **Re: Internet-Finland Privacy (Green, [RISKS-16.92](#))**

*Peter Kaiser 16-Mar-1995 1925 <kaiser@heron.enet.dec.com>  
Thu, 16 Mar 95 19:23:31 MET*

Jon Green says about anon remailers that if "you use them illegally, you may well be identified. Them's the breaks."

Not so fast. A friend of mine, a political activist of the 1960s, says of his political activities, that "I've been jailed several times, always for something I actually did. But none of it was illegal." And he points out that in court all the cases were either dismissed or found in his favor.

So the risk of abuse is clear: you may be identified, and pursued by

authority (or by the Church of Scientology) even if you have done nothing illegal. This has a lot to do with the original point of this thread.

\_\_\_Pete kaiser@acm.org +33 92.95.62.97 FAX +33 92.95.50.50

---

## Risks of doing date arithmetic early in the year without floating point

*Peter Ludemann <ludemann@netcom.netcom.com>*

*Fri, 17 Mar 95 17:44 PST*

The recent discussions of risks-of-dates (RISK-16.74, etc.) and Pentium floating point bugs reminded me ...

Some years ago, I had to write a program to match the accounting records from the database server with those of the batch system. The records were in different formats: the database server used the system clock and the batch system used day-of-year+hmmms.

The database vendor had provided a conversion routine which I happily used, only to discover that there were discrepancies of up to 3 minutes between the two systems' records. Eventually I determined that the database vendor's conversion routine was faulty.

I quickly wrote some code in PL/I using double-precision floating point arithmetic (which gave me 55-bit precision, more than enough) and everything worked fine. My code was only a few lines, compared with the pages of convoluted code that the vendor had provided (it was in assembler, emulating 48-bit integer arithmetic on a 32-bit system).

The only reason I caught this error was that I happened to be writing the program near the end of the year: the conversion routine's error increased from almost nothing in January to about 3 minutes in December. If I had written the code in January, I probably wouldn't have caught the error. But the error probably wouldn't have existed in the first place if the conversion code had been written with floating point instead of integer arithmetic.

- peter ludemann ludemann@netcom.com

---

## Phone companies with wrong 555-1212 databases

*Dr. Frederick B. Cohen <fc@all.net>*

*Fri, 17 Mar 1995 17:53:49 -0500 (EST)*

For the last 6 months, people trying to reach my company have been misdirected to the phone number of some poor woman whose family has had ever-increasing numbers of telephone calls for a company she has never heard of. We finally talked to her today and found out that she has been inundated over the last few weeks as a result of articles in Newsweek and the Wall Street journal mentioning my company's name.

She has been trying to get the phone company information operator to make the change since December of 1994, but they have repeatedly told her that her phone number was that of my company and they they could not change it for her.

Finally, today, a reporter called me, told me of the problem he had in finding me, and started me down the path to track down this problem. Several operators and phone companies later (two phone companies were involved here - and they don't talk to each other) I found out that neither company could change the listing - the other one had it.

I got desperate and called the information operator (who had told me previously that they could not change these things). She told me she would change it right away in both databases.

So I called again a little bit later only to find the number had not been changed and that they could not change it except from the business office. The supervisor (it was now after 5PM) tried to find someone in the business office to authorize the change.

Meanwhile, my wife had convinced the poor woman whose family has been traumatized for the last 4 months to give people the new number by herself - there was a certain telephone company hatred comraderie between them - they both said that they had no problem believing that phone companies could screw up this badly.

It is now the weekend, and I am assured by all parties that if I will only try this whole thing again next week sometime, it will be fixed in a jiffie. I'm getting ready to call my lawyer.

FC

---

## Re: The Manchurian Printer & Prodigy Spies on Users ([RISKS-16.92](#))

*Frank C Ferguson <ferguson@eri.erinet.com>*

*Sat, 18 Mar 1995 17:16:59 -0500 (EST)*

... Prodigy insisted that the copied data was the result of a software bug, and it wasn't spying on its customers. But fundamentally, if you use a modem to access ..., there is no way to be sure that your computer isn't spying on you while you surf the information highway." [Simson Garfinkel]

The above is another example of insufficient research. There was and is no software bug. When you delete a file in DOS, all you are deleting is the location of the file that is stored in the FAT (File Allocation Table). The file itself remains on the disk until it eventually gets written over by new files. Prodigy software reserves a "space" on your disk, the size of which is determined by you when you load their software. They use this "space" to cache data that your computer needs to display information on your screen. Use of this space saves large amounts of time because if the data is already on your disk, then they don't have to waste time transferring it to you from a distant location. Initially when this "space" is first allocated, there will be remnants of your old files in it. Eventually, as more and more data

is "cached" in this "space" all your old file info will be written over and no longer viewable. When people became concerned, Prodigy offered free software that would erase all the users old files from that allocated space. They also allowed an independent software auditor to inspect their software to see if it was being used to upload the users files to Prodigy. The Auditor reported that it was not written to do that. That's not to say that it couldn't be. Of course it could be. But if you don't want to risk loss of privacy, then disconnect your modem, LAN, or any other comm link you may have. Why? Because any service could "sneak a peek", not just the ones you mentioned. You obviously are at risk yourself since your address indicates that you are connected to the internet in some fashion.

Frank C. Ferguson ferguson@erinet.com

---

## Software System Safety Class, Nancy Leveson

Nancy Leveson <leveson@cs.washington.edu>

Thu, 16 Mar 1995 10:24:21 PST

LOCATION AND DATE: Seattle, Washington, July 24-26

TEXT: N.G. Leveson, Safeware: System Safety and Computers, Addison-Wesley, 1995.

DESCRIPTION: This class will focus on the unique problems involved in building safety-critical software and describe some techniques that can be used to enhance the safety of software-controlled systems. Emphasis will be on procedures and techniques that are practical enough to be applied to projects today. Real-project experiences with these techniques in different application areas will be described. The class size will be limited to 30 in order to encourage interaction.

Part 1 (Day 1): Management of Safety-Critical Software Projects:  
including organizational, managerial, and technical risk factors, human error and safety, system and software process and tasks, role of management, setting up a safety organization, setting up a safety information system, cost and resource requirements.

Part 2 (Days 2 and 3): Technical Aspects:  
including formal models of accidents, hazard analysis, software hazard analysis, software requirements completeness and analysis, principles of safe design, safe design of the human-machine interface, safety testing and software fault tree analysis (verification of safety).

The two parts may be taken separately or together.

INSTRUCTOR: Nancy Leveson is Boeing Professor of Computer Science and Engineering at the University of Washington (and Adjunct Professor at the University of British Columbia). Dr. Leveson is a founder of the field of software safety and has been doing research and consulting on this topic since 1980. Before becoming a professor, she was a system engineer for IBM. Dr. Leveson consults widely on safety-critical systems for both

government and industry. She has worked with aerospace, nuclear power, transportation, aircraft, and medical systems.

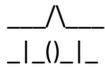
Dr. Leveson is the Editor-in-Chief of IEEE Transactions on Software Engineering, on the editorial board of the Journal of Reliability Engineering and System Safety, an elected member of the Board of Directors of the Computing Research Association, and an appointed member of the NAS/NAE National Research Council Commission on Engineering and Technical Systems. She recently completed a study of the Space Shuttle Flight Software Processes for NASA and the National Research Council and is currently on a National Research Council committee to establish criteria for digital instrumentation and control in nuclear power plants.

For Additional Information Contact Dr. Nancy Leveson, 206-685-1934  
leveson@cs.washington.edu

---

## First Bank of Internet (FBOI) Opens

Vinn Beigh <fboi@netcom.com>  
Sun, 19 Mar 1995 23:03:43 -0800



### A N N O U C E M E N T

For immediate release:                      Contact: fboi@netcom.com  
Monday, March 20, 1995                      Subject of 'info' for details  
Direct questions to Vinn K. Beigh

The First Bank of Internet, FBOI, is announcing the initiation of transaction processing services for Internet electronic commerce. Purchases over the Internet can now be made without exposing personal credit card information. Vendors can now sell products on the Internet without the restrictions imposed by credit card use.

Other Internet purchase procedures require personal credit card information. Those proceedings will be monitored by thousands of people all over the world. Some will attempt to either decode the credit card information or impersonate the customer in future transactions.

The alternative to personal credit cards for electronic commerce is based on an FBOI procured Visa (tm) Automated Teller Machine (ATM) card. The card is prepaid, PIN protected, replaceable, disposable, and good at over 200,000 Visa/PLUS (tm) ATMs in 83 countries.

The safety of FBOI is ensured because access to ATM funds without possession of both the ATM card and the Personal Identification Number (PIN) is not possible. ATM cards are also better than credit cards because their purchase does not require the personal, financial, and employment background of the consumer.

The Visa ATM card is not a credit card. It is cash. The ATM card will be used as a checking account. Using an ATM card allows consumers

to set aside dedicated funds for Internet data purchases. It provides a safe, secure way to transfer cash from consumers to producers. In addition, consumers can reclaim their funds at any time using an ATM.

A check/invoice procedure is used that consumers will find familiar. The consumer first places an order with a vendor. The consumer then sends to the vendor or FBOI an e-mail 'check' for the purchase of the program/file/data product. The vendor sends FBOI an e-mail 'invoice'. FBOI will reconcile the transaction and send e-mail transaction receipts to both the vendor and customer. Cash will be taken from the customer ATM account and credited to the vendor for later payment. FBOI charges a 5% vendor commission per transaction.

Producers of software, information collections, newsletters, graphics, and other data products can use FBOI services for the sale of their products. These vendors can sell their products for prices that would be too low for credit card transactions. Subscription services that charge an up-front fee for one time access to data depositories and services also can participate.

Vendors will benefit from a very large consumer base because this global solution works just as well outside the U.S. as within the U.S.. The Visa ATM network is worldwide. Consumers will benefit from a very large vendor base because software produced in non-North American countries can be offered for sale much easier than now.

The worldwide producers on the Internet can use FBOI services without the expense of owning or renting a dedicated Internet server or a World-Wide Web site. E-mail is the cheapest and simplest of all Internet services. Large Internet commercial services will soon be starting that provide only for the on-line purchase of catalog products. It will not be possible for the individual producer to sell a data product using those services. Those services will collect the consumers credit card information in advance because of Internet security problems.

FBOI transmits no sensitive information over the Internet and prevents forgery and impersonation by using Pretty Good Privacy, PGP (tm), software for all transactions. This freeware provides excellent authentication and anti-alteration security.

In addition to the unsecured nature of the Internet, consumers should be hesitant giving out their credit card information to vendors of unknown credibility. Tracking is much harder on the Internet than magazine direct marketing. Also, it is not the same as mail order merchandise since U.S. Postal Service and Federal Trade Commission mail order laws do not apply to the Internet.

For high volume, low cost, transactions directly between producers and consumers on the Internet contact FBOI.

Further information can be obtained from The First Bank of Internet by sending an e-mail message with the subject "info" to <fboi@netcom.com>.

Visa is a trademark of Visa International Service Association.

PLUS is a trademark of Plus System, Inc.

PGP and Pretty Good Privacy are trademarks of Philip Zimmermann.

The First Bank of Internet (tm) is not a lending institution, and is not chartered.



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 16: Issue 94**

**Tuesday 21 March 1995**

## Contents

- [Deutsche Bahnfires continue](#)  
[Debora Weber-Wulff](#)
- [Canadian Government Almost Spreads Virus](#)  
[Colin Perkel](#)
- [Too high-tech...](#)  
[Bob Wilson](#)
- [Reevaluating Our Trust in Computers](#)  
[Cynthia P. Klumpp](#)
- [Internet: Threat or menace?](#)  
[Eric Raymond](#)
- [Re: Latent risks of cost-benefit analysis](#)  
[Steve Smith](#)  
[David Chase](#)
- [Re: The Prodigious Manchurian](#)  
[Rob Slade](#)  
[Bear Giles](#)
- [Re: First "Bank" of Internet](#)  
[Steve Holzworth](#)  
[Rob Slade](#)  
[Willie Smith](#)
- [Information Security Tutorials](#)  
[Sushil Jajodia](#)
- [AMAST'95 Preliminary Programme available](#)  
[Pippo Scollo](#)
- [Info on RISKS \(comp.risks\)](#)

---

## Deutsche Bahnfires continue

*Debora Weber-Wulff* <[weberwu@cha01.tfh-berlin.de](mailto:weberwu@cha01.tfh-berlin.de)>

*Tue, 21 Mar 1995 12:08:28 +0100*

[This is in response to a query from me to DWW on this subject.

Thanks to Debora for sharing with us what she knows. PGN]

The Deutsche Bahn AG, the German train company, has been working round the clock for a long time to a) electrify the state of Schleswig-Holstein, which is just north of the city-state Hamburg, and b) to install a full computerized train regulation system. The big traintable change is scheduled for next Sunday (March 26), when the daylight time change takes effect, I believe. They went on-line with the regulation system last week and all h\*\*\* broke loose. It was okay for the first few hours, and then suddenly went berserk. I don't have all the details, as I have only listened to radio news the past few days, but they ended up having to route all traffic around this major switching point. The train station in Hamburg Altona, where the diesel locomotives are removed and electric ones put on for continuing trains, or where most people just have to change trains, was put out of service. People had to take the S-Bahn or a bus to the main train station, and ended up missing connections. (And then we have the problem with the local trains being fuller than Indian trains because of a special super-cheap deal on weekends, but that's another and computer-unrelated story.)

I do not know for certain if Siemens is the main manufacturer, but I suspect that it is them together with AEG. They just founded a company together with ABB in Sweden to combine all their rail knowledge. Yes, they subcontract out a lot, some to a little company in Kiel, a bunch to Third-World company (but this is just rumor). How could this pass the testing phase? Well, this is not the first time Siemens has boo-booed (remember the microphone system in the Bundestag? There have been many others). My personal opinion is that Siemens/Sietec does not have control of their Quality Assurance and there are too many programmers there that believe that they can do no wrong, and bosses who believe them, because it costs too much to actually do massive testing. German programmers tend to take it as a personal insult when a fault is detected in code that they have written. Companies like Siemens/Sietec exacerbate the situation. I repeat, this is my personal opinion based on unscientific surveys conducted during drinking and card playing sessions.... so nothing eminently quotable.

There should be an article in Computerwoche (German language) soon about it when the CeBit smoke clears, they enjoy reporting about Siemens/Sietec disasters. I'll keep an eye out for more details.

Debora Weber-Wulff weberwu@tfh-berlin.de

---

## Canadian Government Almost Spreads Virus

*Colin Perkel <colin.perkel@guildnet.org>*

*Tue, 21 Mar 1995 17:46:09 -0500*

The Canadian government's first attempt at electronic distribution of its budget last month could have created havoc -- but not because of the measures it contains. A virus was discovered about an hour before more than 5,000 disks containing budget information were to be sent to the country's major financial institutions. One expert is quoted as saying the situation could have been catastrophic for banks etc.

The RCMP are investigating how the unnamed virus (said to be boot-sector or FAT destructive) had found its way onto the master disk being used to make copies. The master had passed two Revenue Canada virus scans but a last minute check by the company hired to do the copying and distribution turned up the critter.

Given the super secrecy and security surrounding the budget, there are serious questions as to how this could have happened. The RISKS involved in the federal government spreading viruses are obvious!

---

### Too high-tech...

*Bob Wilson <wilson@math.wisc.edu>*

*Tue, 21 Mar 95 09:23:21 CST*

I just heard on the radio an announcement of a new safety project for farmers. Farming is one of the most hazardous occupations, by usual measures, with a significant number of injuries and fatalities happening when farmers get off of a tractor or similar piece of equipment to do a brief task like untangling something, but leave the equipment running. The proposed fix? Use the GPS satellite location system, which will be used by a piece of equipment worn by the farmer and another on the tractor: When they move apart, the tractor gets turned off.

I suspect "the risks are obvious", as well as the availability of MUCH simpler technologies to do the distance sensing if in fact that is a good thing to do....

Bob Wilson wilson@math.wisc.edu

[This sounds almost as far-fetched as the completely computerized SUNDIAL I conjured up for an editorial in the ACM Software Engineering Notes many years ago, as an example of technological overkill. Ultimately, the sundial would have used GPS to provide automatic dynamic seasonal corrections dependent on longitude and latitude, would track its own movement (no pun intended), and would work at night by simulated sunlight. PGN]

---

*<"cklumpp1@vaxa.hofstra.edu"@vaxc.hofstra.edu>*

*Mon, 20 Mar 1995 20:21:24 -0400 (EDT)*

Subject: Reevaluating Our Trust in Computers

Computers have, in most cases, improved the overall quality of life for us. When a computer process goes smoothly we are amazed at the speed and accuracy of the machine. But when something goes wrong, it is human nature to want to place the blame upon someone or something. When the problem is minor we can usually laugh it off or write it off as a "computer error", whether or not this is actually true. But, when the problem has caused severe (life-threatening) consequences we need in depth explanations of

accountability.

Also, the number of people affected by computer errors can range from one person who is directly involved in the use of the computer - to many people who are innocent bystanders. If the operator is the only one inconvenienced by a computer error assuming it created a minor problem, blame can be shrugged off. While at the other extreme, if large numbers of people are affected by the error, blame is sought.

Therefore, there are two determining factors which cause us to want to place blame for the occurrence of computer errors. One factor is the severity of the problem and the other one is the number of people affected.

With the increasing involvement of computers in our daily lives the number of errors occurring is also increasing. Errors seen many times in the past are still occurring while new errors are cropping up with the use of new technology. The dependent relationships between the software, hardware, data input (whether it is by a person or computer generated), procedures, and the communication links [[risks-9.61](#)], create a very complex environment. The blind trust we have in computers and the people who operate or program them may need to be reevaluated. In other words, can and should we always trust a computer operator or a computer with the ever increasing processing of data which affect our lives and then look to blame when failure occurs? Or should we decrease or adjust the trust we place on data input and computers?

While I was doing a search for articles at the library on the periodical database and happen to be short of time one night, the computer froze suddenly for no apparent reason. I had already spent 30 of my precious 90 minutes reading abstracts and marking (to print) the ones I thought were relevant. I had not yet printed the abstracts when the computer stopped responding to keystrokes. I asked the reference librarian if there was anything that could be done. He said "Not usually, but try [Ctrl] Z or [Ctrl] [Enter]." I did - but nothing happened. He shrugged. I shrugged and laughed, then moved over to another machine to start my work all over again...how fitting. I would not have enough time to make copies of the articles I searched for and would have to return another day.

I probably should not have trusted the computer to get me smoothly through my work that night; I left no time for computer error expecting the computer to be 100% reliable.

Cynthia P. Klumpp [cklumpp1@vaxc.hofstra.edu](mailto:cklumpp1@vaxc.hofstra.edu)

---

### **Internet: Threat or menace? (Mills, [RISKS-16.93](#))**

*Eric Raymond <[esr@netaxs.com](mailto:esr@netaxs.com)>*

*21 Mar 1995 15:24:55 GMT*

In a recent comp.risks post, Dick Mills speculates that the stability of civilization up to now may have depended on the ineffectiveness of one-to-many communication, and that the Internet condemns us to drown in

memetic garbage generated by kooks, fanatics, and evangelists.

I suggest Mr. Mills think of it as evolution in action. The people -- and civilizations -- that survive will be those who learn and teach critical reading and thinking skills. This is strictly analogous to the selection effect of biological plagues.

<http://www.thyrsus.com/~esr/home.html>>Eric S. Raymond</a>

---

**Re: Latent risks of cost-benefit analysis (Smith, [RISKS-16.93](#))**

Steve Smith <[sgs@access.digex.net](mailto:sgs@access.digex.net)>

21 Mar 1995 14:32:28 -0500

The risks of cost-benefit analysis that I see are more direct. First, in order to do a cost-benefit analysis, you have to make assumptions about relative values. It is totally impossible to do this in a politically-neutral way. Consider, say, a C-B analysis of a wetland development done by a real-estate developer and and the same analysis done by Greenpeace. No way are they going to be similar.

Second, C-B analyses are trotted out as some kind of Gospel. Somebody comes up with the numbers, lawmakers or bureaucrats make decisions, and the public is stuck with the results. What if the analysis is wildly off? Where is the responsibility?

I would like to see the organizations who do these analyses post a bond. Won't happen, but it's interesting to think about.

Steve Smith                      Agincourt Computing  
[sgs@access.digex.net](mailto:sgs@access.digex.net)              (301) 681 7395

---

**Re: Latent risks of cost-benefit analysis (Smith, [RISKS-16.93](#))**

David Chase <[chase@centerline.com](mailto:chase@centerline.com)>

21 Mar 1995 14:59:46 GMT

[...] Or more generally, cost-benefit analysis skews in favor of what can be "measured" (medical costs, property values, paycheck) at the expense of the "intangible" (freedom, nice-smelling air, peace of mind, a good day fishing, national security, employee loyalty).

Where social benefit is easily measured, it skews towards social benefit. Where social benefit is not easily measured, it skews away. I can well imagine a statistical arms race between the two sides of any costly policy, attempting to assign value to the otherwise intangible costs and benefits of the policy. It's also an entertaining game to see what intangibles are considered so important that they should not have a price tag attached (and by whom).

David Chase CenterLine Software

---

**Re: The Prodigious Manchurian (Garfinkel, [RISKS-16.93](#))**

*"Rob Slade, Social Convener to the Net" <roberts@mukluk.decus.ca>  
Tue, 21 Mar 1995 13:23:45 EST*

In a recent posting, Simson Garfinkel used a reference to Prodigy's former method of handling swap space to point out that certain types of online access systems leave you vulnerable. In today's issue, Frank Ferguson tries to indicate, using details of the MS-DOS FAT and delete function, that such a concern is invalid. They are, or course, both right, but Garfinkel is righter.

While Prodigy never did have any specific function in their software to browse and return information from the user's computer to the company, the software did have provisions to automatically update software. This could (although it wasn't) be used to run other types of software without the user being aware of it. But we don't have to pick on Prodigy. Other commercial systems "take over" your machine when you run the front end software. This is, of course, done to ease the burden of use for the subscriber, but it does mean that the online service can basically do anything they want with your computer. (The same, of course, is true for any software, but commercial online systems have the advantage of being in communication with their own software while it is running on your machine.)

We need not limit the discussion to commercial services. GUI (graphical user interface) systems tend to have a lot of security loopholes and hiding places anyway. The X system has provisions for a remote system to control your workstation. The various World Wide Web browsers, particularly the graphical ones like Mosaic, have the ability to both transfer files and invoke execution of programs. That's all you need for a really nifty virus/worm ...

DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733

---

**Re: The Prodigious Manchurian (Garfinkel, [RISKS-16.93](#))**

*Bear Giles <bear@tiger.cs.colorado.edu>  
Mon, 20 Mar 1995 22:18:44 -0700*

I content that this behavior *\*is\** a bug. The proof is in the public's reaction to finding bits of "their" files in the Prodigy cache area.

To give a human metaphor, imagine a coworker who casually leafs through the papers on your desk while waiting for you to get off the phone. This might be nothing more than a nervous mannerism and he may be totally unaware of what he's doing, but very few people won't be seriously annoyed at him.

To avoid even the appearance of impropriety, most people carefully stare into space (or read a magazine) in this situation.

Prodigy didn't observe this behavior (which in the computer world would have been allocating the space and immediately wiping the current data); it grabbed some disk space and saved a few seconds by not wiping the existing data...

... and found itself tremendously embarrassed because it violated one of the prime rules of our society (regarding privacy). The fact that we're still discussing this years later proves how sensitive of a nerve it hit!

In an era when computers were scarce resources and few people had frequent interactions with one, such behavior could be justified as a valid engineering tradeoff. But computers are now routinely used by a large part of the population, and it is incumbent on the programmer to observe the social conventions even if it proves to be moderately "expensive."

Bear Giles bear@fsl.noaa.gov

---

### Re: First "Bank" of Internet (Beigh, [RISKS-16.93](#))

Steve Holzworth <sch@unx.sas.com>

Tue, 21 Mar 1995 16:23:44 -0500

This "announcement" is so full of holes as to be ludicrous.

- 1) According to the NC Banking Commission, use of the term "bank", with a very few limited exceptions, is illegal for anyone but an organization that is a federally (FDIC) or state chartered, regulated entity. The NC Banking Commission has taken an interest in this announcement, and is forwarding the info to the FDIC...
- 2) "The alternative to personal credit cards for electronic commerce is based on an FBOI procured Visa (tm) Automated Teller Machine (ATM) card. The card is prepaid, PIN protected, replaceable, disposable, and good at over 200,000 Visa/PLUS (tm) ATMs in 83 countries. "

Translation: 'you send us \$x.xx to keep on account (with no interest accrued to you). We deduct purchases from this balance'. What happens if we disagree on the balance and/or dispute transactions? Because this an ATM card as opposed to a credit card, normal fraud liability limitations (\$50.00 US) and disputed charge reversals are not in effect. If someone fraudulently charges against your ATM account, you potentially bear the full loss.

Also, the "vendor" info, sent in response to the specified E-mail request, indicates that the ATM cards are not "rechargeable". When you run your balance down, you must buy a new one. FBOI charges a 5% commission to establish a new card for you (ie - the "setup" fee is 5% of the balance you wish to put on account; when that runs out, you pay another 5% for a new card). Since they charge vendors a 5% commission per transaction, FBOI is keeping 10% of all funds that move through their system.

- 3) "The safety of FBOI is ensured because access to ATM funds without

possession of both the ATM card and the Personal Identification Number (PIN) is not possible. ATM cards are also better than credit cards because their purchase does not require the personal, financial, and employment background of the consumer."

Here is how a transaction is instigated (from FBOI info):

"\*FBOI procedures for creating a vendor E-mail invoice\*

FBOI E-mail invoices are a two line message created by a FBOI vendor. Line one of the message contains the customer Internet E-mail address. Line two contains the transaction amount in US dollars. This message must then be encrypted, signed, in ASCII, and in Text using the PGP command "PGP -seat invoice fboi". The "invoice.asc" is then ready to be E-mailed to fboi@netcom.com with subject "invoice". FBOI will issue an E-mail transaction receipt."

"\*FBOI procedures for creating a customer E-mail check\*

FBOI E-mail checks are a two line message created by a FBOI customer. Line one of the message contains the vendor Internet E-mail address. Line two contains the transaction amount in US dollars. This message must then be encrypted, signed, in ASCII, and in Text using the PGP command "PGP -seat check fboi". The "check.asc" is then ready to be E-mailed to fboi@netcom.com with subject "check". FBOI will issue an E-mail transaction receipt."

FBOI then reconciles the above transactions and sends payment to the vendor (or credits the vendor's ATM card). Note that FBOI recommends product pricing at around ONE US DOLLAR for items! (Almost-Freeware, anyone?)

4) "...In addition, consumers can reclaim their funds at any time using an ATM."

At what service charge per transaction? What limitations on withdrawal amounts (how many transactions will it take to empty my account)? Any yearly fees for this privilege? FBOI info is rather vague in this regard. The only pertinent comment I saw was (pertaining to vendor payment):

"... While the Visa ATM card as a payment method has many advantages (portable, anonymous, and cash in any country of the world), your ATM may not dispense the entire payment due to the exchange rate and possible ATM fees."

5) "...Those services will collect the consumers credit card information in advance because of Internet security problems."

Since those are still credit card transactions, the consumer has much better dispute resolution abilities.

6) "FBOI transmits no sensitive information over the Internet and prevents forgery and impersonation by using Pretty Good Privacy, PGP (tm), software for all transactions. This freeware provides excellent authentication and anti-alteration security."

The description of transactions as in (3) above may or may not be subject

to spoofing. I'm not up enough on crypto to comment.

7) "In addition to the unsecured nature of the Internet, consumers should be hesitant giving out their credit card information to vendors of unknown credibility."

You mean like FBOI?? Based out of a Netcom account (instead of a .com domain)?

8) "...since U.S. Postal Service and Federal Trade Commission mail order laws do not apply to the Internet."

The laws may not apply to the Internet per se, but credit card transactions are still subject to all of the controls of typical "mail order" as is normally practiced via telephone.

9) "The First Bank of Internet (tm) is not a lending institution, and is not chartered."

This says volumes.... (see (1), above).

And finally:

"When FBOI procures a Visa ATM card for vendor customers the card becomes their money. FBOI will be granted access to their funds through the FBOI customer agreement allowing FBOI to possess a duplicate card."

^^^^^^^^^^^^^^^^^^^^^^^^

---

**Re: First "Bank" of Internet (Beigh, [RISKS-16.93](#))**

*"Rob Slade, Social Convener to the Net" <roberts@mukluk.decus.ca>  
Tue, 21 Mar 1995 13:50:53 EST*

The FBOI card does seem to address some of the security concerns for commerce over the net. The replacement of one number by another does not provide any particular safety, but the limit on the card does restrict the damage. However, inquiring minds want to know:

How easy is it, aside from emptying the account, to cancel/change/get a new card? Is there a fee? Is there any recourse if someone empties the account before you do?

Does the encryption apply only to the card number, or to the whole transaction, including time and date stamp?

Does the encryption software come with the card? Is it a smart card? Do you need a card reader of some type? What platforms is the software available on? Is the user responsible for getting/setting up the software?

By using PGP is the FBOI restricting its operations to the US? Is the version of PGP that they are using operating with the RSA algorithm, or another? Is the key size restricted?

If this really does work over E-mail, why do you keep talking about ATM?  
(Does it only work over asynchronous transfer mode networks? :-)

DECUS Canada Communications, Desktop, Education and Security group newsletters  
Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733

---

**Re: First "Bank" of Internet (Beigh, [RISKS-16.93](#))**

*Willie Smith <wpns@roadrunner.pictel.com>  
Tue, 21 Mar 1995 08:15:38 -0500 (EST)*

In [Risks 16.93](#), fboi@netcom.com (Vinn Beigh) writes:

>The card is prepaid [...]

>The safety of FBOI [the non-chartered, non-bank company] is ensured

...by the fact that it's prepaid, and even if FBOI loses all the money  
in the account due to fraudulent transactions, it's your money  
that's gone, not their 5[!!] percent!

>The worldwide producers on the Internet can use FBOI services without the  
>expense of owning or renting a dedicated Internet server or a World-Wide  
>Web site.

Yeah, just get an account on netcom and you're a business! COOL!

>In addition to the unsecured nature of the Internet, consumers should be  
>hesitant giving out their credit card information to vendors of unknown  
>credibility.

Giving cash to some guy with a Netcom account is OK? Maybe I missed  
the smiley, or the original submission was tongue in cheek...

>since U.S. Postal Service and Federal Trade Commission mail order laws  
>do not apply to the Internet.

Another safety net for FBOI. What a gig! Tell you what, I now announce the  
First International Bank Of The Information Supercollider, you send me money  
and I promise not to lose it.

[The money, that is, not the Supercollider. PGN]

Willie Smith wpns@pictel.com N1JBJ@amsat.org

---

**Information Security Tutorials**

*Sushil Jajodia <jajodia@isse.gmu.edu>  
Mon, 20 Mar 95 10:28:42 EST*

INFORMATION SECURITY INSTITUTE  
Sponsored by:

Center for Professional Development  
George Mason University  
Fairfax, VA 22030-4444

Intensive, Short Courses:

- o Information Security Principles and Practice March 27-31, 1995  
Instructors: Marshall Abrams, Daniel Gambel, Sushil Jajodia,  
Harold Podell, Ravi Sandhu
  
- o Recent Developments in Information Security March 27-31, 1995  
Instructors: Marshall Abrams, Daniel Gambel, Sushil Jajodia,  
Harold Podell, Ravi Sandhu
  
- o Practical Security in a Networked Environment April 3-7, 1995  
Instructors: Marshall Abrams, Ravi Ganesan, Sushil Jajodia,  
Brian McKenny, Harold Podell, Ravi Sandhu
  
- o UNIX Security April 3-7, 1995  
Instructors: Marshall Abrams, Ravi Ganesan, Harold Podell, Ravi Sandhu

For further information, visit the Information Security Institute home page through mosaic at <http://www.isse.gmu.edu/~gmuisi>.

---

### **AMAST'95 Preliminary Programme available**

*Pippo Scollo <scollo@cs.utwente.nl>  
Mon, 20 Mar 1995 16:50:49 +0100*

The Preliminary Programme of the AMAST'95 Conference (4th International Conference on Algebraic Methodology And Software Technology, Montreal, Canada, July 3-7, 1995) is available on the WWW at the following URL:

<http://www.cs.utwente.nl/data/amast/amast95/PreliminaryProgramme.txt>

The file includes abstracts of the invited talks, conference schedule, registration information and registration forms, and accommodation and travel information. The deadline for reduced registration fees is:

Monday June 5, 1995

The file is also available by anonymous ftp:

```
host: ftp.cs.utwente.nl
username: anonymous
password: your E-mail address
directory: pub/doc/amast/amast95/
get file: PreliminaryProgramme.txt
```

More information about AMAST'95 is available from the following sources:

1. For bulletins on current status of the conference:

amast95-info@cs.concordia.ca

Tools and Demos: grogono@cs.concordia.ca

Registration: krishnan@cs.concordia.ca

Local Arrangements: missaoui.rokia@uqam.ca

2. For subscribing to AMAST'95 mailing list:

amast95-request@cs.concordia.ca



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 16: Issue 95**

**Weds 22 March 1995**

## Contents

- [UK National Lottery \[scratch as scratch can?\]](#)  
[Pete](#)
- [Re: Too high-tech...](#)  
[Steven Tepper](#)
- [Re: Internet: Threat or menace?](#)  
[Dave Parnas](#)
- [Risks of one-to-many communication](#)  
[Vicki Rosenzweig](#)
- [Latent risks of cost-benefit analysis](#)  
[Ron Ragsdale](#)
- [Re: Risks of doing date arithmetic early in the year...](#)  
[Andrew Marc Greene](#)
- [Re: Prodigy](#)  
[Craig Dickson](#)
- [Re: PGP Moose](#)  
[Jerry Leichter](#)
- [FBOI Apology \(fwd\)](#)  
[FBOI via Willie Smith](#)
- [Re: FBOI](#)  
[Mike Perry](#)  
[Jonathon Tidswell](#)
- [Re: NCSA httpd security hole](#)  
[Timothy Hunt](#)
- [Citizen's Advice on the Internet](#)  
[Phil Overy](#)
- [Re: FBOI and \\*Security Reviews\\*](#)  
[Ross Anderson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### UK National Lottery [scratch as scratch can?]

<[pete@minster.york.ac.uk](mailto:pete@minster.york.ac.uk)>

Wed, 22 Mar 95 15:36:37

Lottery cards are not up to scratch, By Ben Fenton  
>From the Electronic Telegraph

A computer fault forced the National Lottery to suspend its new Instants scratchcard game last night, a few hours after it was launched at a glittering party in Regent's Park, London.

Mr Peter Davis, the director general of the lottery, said that Camelot, which runs it, was "making every effort" to find a solution as quickly as possible. He instructed Camelot to place advertisements in all daily national and key regional newspapers today to reassure customers and said it was vital that players were kept fully informed and their interests protected. He said: "Members of the public who have purchased Instants tickets can be assured that all valid prize claims will be met as soon as possible." Any player who had bought a winning ticket should keep it safe.

The trouble began even before sports and show business personalities and the Red Devils parachute team officially launched the scratchcard scheme in the sunshine at Regent's Park. Thousands of newsagents, service stations and grocers trying to sell the cards found the discouraging message "Function Suppressed" when they attempted to validate them by computer.

Apart from a handful bought around 7am, nobody was able to buy the #1 scratchcards and try for an immediate prize of between #1 and #50,000.

The scratchcards are due to be on sale at 20,000 outlets. To use them, customers rub the card to reveal six cash figures and, if three of them match, they win that amount.

Weekly lottery tickets are not affected by the fault.

---

### **Re: Too high-tech... (Wilson, [RISKS-16.94](#))**

*Steven Tepper <greep@datatools.com>  
Tue, 21 Mar 95 17:13:14 PST*

And what if someone spoofs the farmer's IP address to take control of the tractor? Will the farmer be required to hire a security expert to install a firewall on both systems and make sure the tractor is running the most recent version of sendmail? Will the tractor shut off by mistake because its Pentium CPU had a floating-point error?

Then what about the livestock? Will Bessie's cowbell be replaced with her own GPS system? Will she have to carry a satellite dish on her head? (Will the farmer?)

Come to think of it, GPS would be a good way for Little Bo Peep to keep track of her sheep. This system has definite possibilities.

---

### **Re: Internet: Threat or menace? (Eric Raymond)**

Dave Parnas <parnas@triose.crl.McMaster.CA>

Wed, 22 Mar 95 08:51:19 EST

Eric Raymond, suggests that the same mechanisms that let organisms evolve to be resistant to plagues, evolution, will allow us to evolve to a point where we can manage the changes brought about by technological change. I suggest that he consider the time-constants involved. Evolution in human beings is best measured on a scale of centuries. Evolution in our technology is best measured in terms of months or years.

David Parnas

---

### Risks of one-to-many communication

Vicki Rosenzweig <murphy!acmcr!vr@uunet.uu.net>

Wed, 22 Mar 95 09:53:20 EST

I think Eric Raymond (esr@netaxs.com) is being a bit too sanguine about the risks of memetic garbage, when he suggests that we think of it as evolution in action. First of all, if enough garbage is being transmitted--whether by computer nets or radio hardly matters, for this purpose--it may overwhelm the desired or needed information, for everyone. Second, it may be called "evolution in action" if someone listens to a fanatic preacher and decides to make a suicide attack on something they disapprove of: but to call that "evolution" from the point of view of the victims of that attack does little but allow us not to think too much about what has happened. Third, from a purely evolutionary standpoint, if we are to take one, I would far rather evolve or invent a defense mechanism against such garbage--ideally one that would protect me from other people who take it too seriously--than just dismiss it and hope that I get lucky.

Vicki Rosenzweig vr%acmcr.uucp@murphy.com New York, NY

---

### Latent risks of cost-benefit analysis (Brown, [RISKS-16.93](#))

Ron Ragsdale <rragsdale@oise.on.ca>

Wed, 22 Mar 1995 10:39:54 -0500 (EST)

Phil Brown writes:

>.. was lobbying for a complete ban on advertising for alcoholic beverages,  
>.. citing health and economic benefits.

but his discussion is on the costs and benefits of "alcohol consumption," not "advertising for alcoholic beverages." It is much harder to make a case for the benefits of the endless parade of beer commercials, though they do seem to present a consistently cheerful view of the world.

Professor Emeritus Ron Ragsdale, The Ontario Institute for Studies in Education 252 Bloor Street West Toronto, Ontario, M5S 1V6 CANADA (416) 923-6641 X2252

---

**Re: Risks of doing date arithmetic early in the year without FP**

<Andrew\_Marc\_Greene@frankston.com>

Tue, 21 Mar 1995 10:29 -0500

In [RISKS-16.93](#), Peter Ludemann writes:

> But the error probably wouldn't have existed in the first place if the  
> conversion code had been written with floating point instead of integer  
> arithmetic.

Um, aren't all floating point operations are performed using exclusively integer operations anyway (at least until continuous-voltage real-number ALUs become common)? As Donald Knuth pointed out in the implementation of TeX, if a program does its own floating-point emulation (assume that the programmer gets it right, which was not the case in the example Peter cited) it is more likely to give the same result when it's ported to another system (that may have greater or lesser precision, or may round differently...)

- Andrew Greene

---

**Re: Prodigy (Giles, [RISKS-16.94](#))**

Craig Dickson <cd@crl.com>

Tue, 21 Mar 1995 18:51:56 -0800 (PST)

|I conten[d] that this behavior \*is\* a bug. The proof is in the public's  
|reaction to finding bits of "their" files in the Prodigy cache area.

No, I don't think so. There is at least a nomenclatural difference between a "bug" -- software that fails to perform as designed -- and a "design flaw" -- software that doesn't do what it perhaps ought to, but does do what it was intended to do. If you want to argue that Prodigy's coders should have realized that not wiping their pre-allocated disk space was a Bad Thing, well, maybe. But it's not a bug, because they probably did it that way on purpose.

You see, it is a perfectly normal thing in MS-DOS application coding to create a large file without initializing its contents when the program knows how big a file it needs before it knows exactly what it will put in it. Prodigy's MS-DOS client software is far from the only well-known program to use this technique. Because they are an on-line service, though, when someone noticed some "deleted" data in a Prodigy file, there was an immediate assumption on the part of ill-informed users that Prodigy's software was spying on them.

One point that has never been quite clear to me about this case -- I've heard both positive and negative answers, and therefore remain confused -- is whether this uninitialized file was ever transmitted to Prodigy. If not, then this whole controversy is utterly nonsensical, since no "violation of

privacy" can possibly occur. If it is transmitted, however, then I would definitely agree that Prodigy should have wiped the file when they created it. It is one thing to have "deleted" data that you ignore sitting in a sector that just happens to be allocated to your file; that's a perfectly normal thing to have happen, and it happens to nearly ALL files, since there is usually some slack space between the logical end of a file and the end of the final disk cluster allocated to that file. It is quite another thing, though, to transmit that data to another system without the user's knowledge and consent.

| Prodigy [...] grabbed some disk space and saved a few seconds by not wiping  
| the existing |data...

Depending on the size of the file and the year in which the software was originally written, we may be talking about much more than "a few seconds". PC hard disks are pretty fast these days, but they weren't always.

---

## Re: PGP Moose

*Jerry Leichter <leichter@lrw.com>  
Sun, 19 Mar 95 11:47:45 EDT*

>Given the prevalence of Unix (aka broken) mail forwarders out there  
>that believe any occurrence of "From" at the beginning of a line can  
>be "wedged" as

That's the way things are \*supposed\* to work. However, it's a fact that many messages have their From's wedged in transit. In fact, it happened with the sample "From" in my RISKS posting as it arrived here.

One cause I have been able to track down is the use of final delivery agents as forwarding agents. It's apparently a fairly common trick to allow "final delivery" to go to an address that really feeds into a pipe to a program that forwards the message onward. Alternatively, some systems implement store-and-forward mailers by using a standard local delivery agent to place stuff into a file that is then later read and forwarded.

In both of these cases, a properly written forwarding agent to unwedge the Froms (though since the convention says nothing about lines that start with ">From " to begin with, it could not do so with 100% reliability). It's a fact that many don't. To give one specific example: PSI, one of the largest commercial Internet providers in the US, wedges Froms on mail it forwards to a subscriber (me). By experimentation, I've determined that some of their nodes do wedge Froms, while others don't. At one time, I tried to get PSI to fix the problem. I got nowhere; they denied any problem existed. See the Unix Hater's Handbook for a copy of their final response to me. (The editors of the UHH decided to leave out PSI's name. I see no reason to do so.)

>headers -- beware! Any "From:" lines you include are likely  
>Moosebait!

Most Unix mail delivery agents escape "From ", but not "From:".

You same "most". Have you counted? Besides, the issue is whether you can rely on the mail system not to do this. You can't.

>Oh, yes, there are also some mail forwarders out there that will  
>change any line consisting only of a single "." to one containing  
>"..". There are no doubt some that will make the reverse  
>substitution. There also appear to be

This is used by mail and news forwarders. In particular SMTP as used by me to submit this message and NNTP as used by me to receive it the first place. There is some broken SMTP and NNTP software, but all that that I have seen is MS-DOS and Windows. Unless you are on a UUCP site and only take news and mail from UUCP sites through pure UUCP paths, it is almost certain that the double dot encoding has been done on it.

What's your point? Do you think that a message containing a line with a single dot on it can legally be delivered with two dots? The RFC's specify how to do dot-encoding, and if you implement it correctly, it's a transparent encoding that exists only while the message is in transit between two systems.

The fact is, there are sites out there that implement it incorrectly. I'll again point to PSI. By experimentation, I was able to determine that some of their inter-machine links double dots and don't undouble them.

>gateways around that will replace empty lines with lines containing a  
>single space, as well as gateways that do strange and wondrous things  
>with spaces at the end of lines. Finally, there appear to be an  
>increasing number of

This does exist as a problem, although not generally with Unix, but with less common operating systems.

Agreed; this seems mainly to be IBM gateways.

>programs that, under certain unclear conditions, use MIME's BASE64  
>encoding

You mean quoted-printable.

Yes.

>in the midst of otherwise simple ASCII text - you'll see things like  
>=20 at the end of a line.

One reason for doing this is to get round software which truncates trailing spaces - that's why trailing spaces get encoded, but the trigger for doing this is normally a single non-ASCII character, or a mail client which falsely declares everything to be 8 bit ISO 8859-1. Generally I would always suspect client software before transport software.

I have no idea what software is doing this. All I can see is the messages as

they arrive here. I know what software I'm running, and I know what it does to the bodies of messages (nothing at all). In some cases, I've tracked down who out there is damaging messages; in other cases, I haven't bothered to spend the time on a thankless task.

- >I suppose the underlying idea here is fine, but unfortunately an
- >attempt to build such a thing on top of the very chaotic and
- >unpredictable world of today's mail systems is to impose many
- >non-obvious risks on users.

Read the MIME RFCs for discussion on transparency issues.

Why should I care what the MIME RFC's have to say? I'm neither sending nor receiving MIME mail; most people on the net are neither sending nor receiving MIME mail; and the original posting proposed to cancel *\*all\** messages that failed a signature test, not just those that were MIME-encoded. (A good thing, since MIME-encoded messages are a small minority.)

The original RFC's are, in fact, decently written and provide for proper transparent transport of 7-bit ASCII (8-bit ASCII was a rarity at the time and wasn't considered). For that matter, the UUCP specs (such as they are) do, too. The fact of the matter is that there seem to be more incorrect implementations of the RFC's out there than correct ones.

The Unix community has been particularly egregious in its attitude that if the specs disagree with widely-distributed Unix programs, then it's the specs that are wrong. In some cases - sendmail is the famous one - it's not even that the Unix programs are wrong, it's that they are so complex to configure that most complete *\*systems\** using them are set up to violate the RFC's, even if in principle they could have been set up correctly.

What programs could, in principle, do is of no importance: The mail system infrastructure is built of what the systems out there actually do, not what they could potentially do - and what they actually do is a mess.

-- Jerry

---

## **FBOI Apology (fwd)**

*Willie Smith <wpns@roadrunner.pictel.com>  
Wed, 22 Mar 1995 10:21:37 -0500 (EST)*

I got this from the FBOI folk(s?):

- >We apologize for sending you our unsolicited [sic] press release. We
- >carefully screened who received our information. Only members of
- >the press and a select group of moderators were to receive our
- >information. We could not, however, determine proper parties in all cases.

>

>Moderators selected from:

- > garbo.uwasa.fi:/pc/doc-net/newsgrps.zip

>

>NO unmoderated group or list was intended to see this information.  
>A moderator best knows the interests of the group.  
>  
>It was NOT intended for Risk. Please let the members know it was an  
>error. Just have them delete it.  
>  
>Please understand our desire to inform the users of the Internet of  
>our services.

So it's a sorta-spam that got away from him. I think it's only too appropriate for Risks! The sad part is, that unless the investigation into his doings noted in the last Risks digest proceeds quickly enough, PT Barnum's motto will guarantee he gets at least some money from some clueless newbies. Not bad for a (guess) \$30 investment in an Netcom account!

Willie

---

## Re: FBOI

*<mikep@trantor.europe.dg.com>*

*Wed, 22 Mar 1995 16:28:35 GMT*

We don't KNOW if FBOI has bad intentions, and we should be careful of assuming so, with no evidence, for there IS a legitimate need for services such as these, and, if they can get away with charges totalling 10%, then clearly there is legitimate money to be made. But we should be mindful of the risks.

We shouldn't consider the use of netcom by a startup business to be any more suspect than we would consider a 'physical' startup not investing immediately in business premises with office furniture, equipment and secretaries - how many of us today work for, or with equipment made by, companies that started out in someones garage? But we should be mindful of the risks.

We don't know to what extent FBOI have considered, and dealt with, the security issues. But we should be mindful of the risks.

As RISKS readers we should all be aware of these risks, and should act accordingly.

But what of the readers of rec.obscurehobby.keentospend? (I'm assuming here that their newsgroups were also posted by FBOI). They may not necessarily be so {skeptical|mistrusting|risk-aware}.

Someone (our esteemed moderator maybe?) would be doing these folks a service by posting (at least to the moderated groups) a summary of the concerns expressed by the RISKS readership.

Mike Perry Data General Ltd +44 (0)181 758 6000 fax: +44 (0)181 758 6758

---

**Re: FBOI**

*Jonathon Tidswell <t-jont@microsoft.com>*

*Wed, 22 Mar 95 14:22:37 TZ*

Steve Holzworth and Rob Slade pointed out the disproportionately high security for FBOI in relation to the security they offered their clients. Rob Slade also raised questions about the cryptographic software, although freely available outside the US, it had (has ?) a non-commercial use clause.

The FBOI operation appears to be opportunistic, but I expect other more serious Internet banking operations will emerge in the very near future. Indeed I have thought (dreamed :-)) about it, but I haven't the time/money to make a serious attempt.

I think the more interesting risks are long term.

Steve Holzworth wrote:

| 1) According to the NC Banking Commission, use of the term "bank", with a  
| very few limited exceptions, is illegal for anyone but an organization  
| that is a federally (FDIC) or state chartered, regulated entity. The NC  
| Banking Commission has taken an interest in this announcement, and is  
| forwarding the info to the FDIC...

[ from the original FBOI posting. ]

| 8) "...since U.S. Postal Service and Federal Trade Commission mail  
order laws

| do not apply to the Internet."  
|

| The laws may not apply to the Internet per se, but credit card transactions  
| are still subject to all of the controls of typical "mail order" as is  
| normally practiced via telephone.

This is fine since the posting came from a US email address, it does not necessarily follow that FBOI is US based.

Consider the case of a real bank in some small tax haven coming on line. What are the implications for local banking laws and taxing systems ?

Consider further the advent of a money changing operation, which buys and sells its own currency the "NetCredit", according to some published pricing which puts 1 NetCredit at about 50c US, and the appropriate prices for other currencies. With the advent of untraceable electronic cash this becomes a perfect money laundering operation. E.g., Buy 1 million NetCredits in New York and sell them for swiss francs in Geneva.

When this becomes available to the ordinary public, no single transaction ever needs fo through a local bank, which is a basic requirement for a black market.

What happens to national tax systems ?

- Jon Tidswell

---

**re: NCSA httpd security hole (RISKS 16:82)**

*"Timothy Hunt [Assistant Unix Systems Manager]" <timothy@icr.ac.uk>  
Wed, 22 Mar 95 10:04:20 +0000*

The following is an update to the information published in RISKS 16:82 that I received in response to a query on the

----- Forwarded message

CA-95:04.README

Issue date: February 17, 1995

Date of last revision: March 15, 1995

This file is a supplement to the CERT advisory CA-95:04, "NCSA HTTP Daemon for UNIX Vulnerability," distributed on February 17, 1995. We update the file when additional information becomes available.

////////////////////

Added: March 15, 1995

Since the advisory was issued, NCSA has provided updated information (please see below) that supersedes information provided in Step 1 of the Solution section of this advisory.

This information can be obtained from:

[http://hoohoo.ncsa.uiuc.edu/docs/patch\\_desc.html](http://hoohoo.ncsa.uiuc.edu/docs/patch_desc.html)

If you have any questions about this vulnerability, please contact NCSA (Elizabeth Frank, efrank@ncsa.uiuc.edu).

Beginning of Text Provided by NCSA

=====

NCSA httpd Patch for Buffer Overflow

A vulnerability was recently discovered in the NCSA httpd. A program which will break into an HP system running the precompiled httpd has been published, along with step by step instructions. The program overflows a buffer into program space which then gets executed.

If you are running a precompiled NCSA httpd, please ftp a new copy of the binary. If you have compiled your own source code, we recommend applying the following Patch to fix the vulnerability in the NCSA HTTP Daemon V.1.3 for UNIX. It modifies the strsubfirst subroutine in util.c.

We believe that earlier versions of the server are vulnerable to a similar attack, and strsubfirst should be modified for all releases of the server.

Cert Advisory CA-95:04 describes the problem and includes two suggested steps. We do not recommend taking step 1, which increases MAX\_STRING\_LEN to

8192. There are 154 occurrences of variables using MAX\_STRING\_LEN and changing them from 256 to 8192 bytes is going to expand the memory needed to run httpd tremendously! On top of that, httpd forks a new process (a complete copy of the parent) for each connection, which if your site gets hit a lot will use unnecessarily large amounts of memory. We have already had reports from admins who have made the change saying they are experiencing performance degradation due to swapping. Step 2, applying the patch to util.c, should be sufficient to fix the problem. There is significantly less forking in Release 1.4 of the NCSA HTTP Daemon which will be released soon.

#### Detecting a Break-in

If the access log contains control characters, there is a chance that someone has tried to break into your system. If your server has died recently, they failed at least one attempt. And, if your server has not crashed and there are control characters in the access log you should assume your system has been compromised.

In this case, servers which currently use the User Directive to run the server as "nobody", have limited the potential damage of an intruder to those commands which "nobody" may execute.

#### Control Characters in the Access Log

You've discovered control characters in your access log. How do you tell if was an intruder?

If the beginning of the line containing the control characters begins sensibly (eg. machine name, and date (the GET periodically gets clobbered)) and ends with a series of control characters, it is a break-in attempt. If the beginning of the line starts with control characters (often nulls), this is a symptom of a collision problem that occurs when two children try to write to the access log simultaneously. This problem has only been seen with moderately to heavily loaded servers. (We are working to fix this in Release 1.4.)

#### Other ways to Make Your Server More Secure

A tutorial about running a secure server is available. We also recommend that the User Directive be used to run the server as "nobody".

#### Patched Source and Binaries

The patched source and precompiled binaries are available. We will also be correcting the source for previous releases, but we will NOT be generating binaries for previous releases.

Elizabeth Frank efrank@ncsa.uiuc.edu [End of Text Provided by NCSA]

---

### Citizen's Advice on the Internet

*phil overy <PJO@ib.rl.ac.uk>*

*Wed, 22 Mar 95 09:21:19 GMT*

The critique of the First Bank of the Internet is the germ of a good idea - why not review new businesses? (more or less as people referee scientific journal articles - then potential investors can weed out the con-merchants BEFORE they create another notorious scam).

I think the Internet will need such a service soon, to cancel out all the gee-whizz proposals flying around which intend to make money out of doing exactly the reverse - keeping people UNinformed. I suppose you could describe it as a CERT at the application rather than the network layer.

The RISK? - you only need to see how the previous Internet authorities were lambasted as they became more bureaucratic to realise that anyone employed in refereeing will be attacked as More Fascist Than Adolf Hitler and of course in breach of The Spirit Of The Free Market and The American Way Of Life. I have already used information from a Usenet news group on Multi-Level Marketing (which is NOT pyramid selling.. honest) to inform someone who was being pushed into representing AmWay - I don't know how much use it was, but he couldn't pretend he was not informed of the cost of doing it.

Phil Overy Rutherford-Appleton lab

---

### **Re: FBOI ([RISKS-16.93](#)) and \*Security Reviews\***

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

*Wed, 22 Mar 1995 12:32:12 GMT*

Can't let the FBOI advert go unchallenged!  
Also, we have made a lot of `Security Reviews' back numbers available,

>Date: Wed 22 Mar 1995

>From: rja14@cl.cam.ac.uk

>Subject: First Bank of Internet

In [RISKS-16.93](#), an advert for the `First Bank of Internet' said, of its VISA ATM card:

> The card is prepaid, PIN protected, replaceable, disposable, and good

> at over 200,000 Visa/PLUS (tm) ATMs in 83 countries.

>

> The safety of FBOI is ensured because access to ATM funds without

> possession of both the ATM card and the Personal Identification Number

> (PIN) is not possible.

ATM security breaks down in many ways - see for example `Why Cryptosystems Fail' at <ftp://ftp.cl.cam.ac.uk/users/rja14/wcf.ps.Z>, which documents a number of incidents. Many of these have been reported in comp.risks over the last few years.

A bank which shows itself to be unaware of risks which are well known to readers of this column does not serve itself well by advertising here,

Ross

\* \* \* \* \*

>Date: Wed 22 Mar 1995

>From: rja14@cl.cam.ac.uk

>Subject: Computer and Communications Security Reviews

Risks readers might be interested to know that the first six issues of 'Computer and Communications Security Reviews' can be downloaded for free from <ftp://cl.cam.ac.uk/users/rja14> (see the ReadMe file there for details).

'Computer and Communications Security Reviews' provides abstracts of current research in computer security, cryptography and related topics.



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 16: Issue 96**

**Weds 22 March 1995**

## Contents

- [Dan Farmer, SATAN and SGI](#)  
[PGN](#)
- [Triggerfish Cellular Phone Tap](#)  
[John R Henry](#)
- [RISKS of non-standard interfaces](#)  
[Ry Jones](#)
- [Pilot not informed of plane's intended destination](#)  
[Mike Crawford](#)
- [Snake Oil and Grantsmanship](#)  
[Douglas W. Jones](#)
- [Profiting from misdialed numbers](#)  
[Matt Weatherford](#)
- [Re: A340 incident at Heathrow](#)  
[Peter Ladkin](#)  
[John Rushby](#)
- [Re: FBOI](#)  
[Mike Crawford](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Dan Farmer, SATAN and SGI

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

*Wed, 22 Mar 95 12:02:12 PST*

An article, Dismissal of Security Expert Adds Fuel to Internet Debate, by John Markoff in The New York Times, 22 Mar 1995, discusses last Monday's departure of Dan Farmer from Silicon Graphics. [RISKS-16.90](#) noted that Dan and Wietse Venema have developed SATAN, a Security Administrator Tool for Analyzing Networks, which Dan plans to release openly to the world on 5 Apr 1995.

RISKS has frequently seen discussions of the pros and cons of making such tools available. If the knowledge of vulnerabilities is not promulgated, the system flaws and configuration weaknesses do not seem to get fixed, and

that knowledge seems to permeate the malicious-hacker community anyway. If the knowledge is promulgated, then the likelihood of exploitations tends to increase -- although it certainly provides an added incentive to clean things up in a greater hurry.

Dan is at the center of this renewed controversy. Markoff's article includes this statement:

In the Internet community, Farmer's case is seen as symbolizing the conflict between a time-honored ideal the free flow of information in cyberspace and the harsh new reality that corporations and government agencies must protect their computer systems against intruders and vandals armed with increasingly sophisticated break-in software.

---

### Triggerfish Cellular Phone Tap

*John R Henry <76655.2677@compuserve.com>  
20 Mar 95 20:05:51 EST*

There has been some discussion in recent issues of cellular phone monitoring in Pakistan. Nobody has mentioned that this technology is currently available off the shelf in the US from Harris Communications (Melbourne FL, address on request).

The Harris "Triggerfish", from a photo in an ad, looks like a laptop computer with an extra box alongside. "Everything you need fits into a a suitcase" in the words of the ad.

It will allow collecting and analysis of dialed number statistics, identifying the telephone number when it is registered under another persons name or an alias, and developing usage patterns.

"Wiretap applications..... provide audio minimization, on/off hook logging, multiple tape recorder outputs and necessary intercept documentation. A headphone jack with volume control and alarm speaker allows the monitoring agent to intercept each and every communication." (From Harris brochure)

The brochure goes on for several pages but I think you get the idea. This is a wiretap in a suitcase. As it is listening to radio waves, there is no way of anyone, including the gov't, knowing when it is being used.

The Triggerfish is sold only to law enforcement agencies and is \*supposed\* to be used only with a court order permitting a wiretap. The risk is, who is to know if and how it is being used?

The brochure was reproduced in a newsletter that I used to get. I don't know how old it is but at least 1, possibly 2 years. I found an undated copy in my desk drawer when I was cleaning house the other day.

So what's the fuss with Pakistan and Motorola? Perhaps somebody should give them Harris' phone number.

76655.2677@compuserve.com (John Henry)

---

## **RISKS of non-standard interfaces**

*Ry Jones <ry.jones@mccaw.com>*

*Wed, 22 Mar 95 12:28:50 -0800*

We have debated and called to attention the troubles involved with non-standard interfaces, such as the power switch on the keyboard of the Mac and the like.

Here's a new one I heard on the radio last night.

According to a study released yesterday (sorry, I didn't write down the name of the study), the post-admittance treatment lag for heart attack patients in hospitals could be reduced from an average of 70 minutes to 30 minutes if the interfaces on the equipment used to treat these patients were standard. This was based on (so the announcer said, I have not seen the study) a hospital where every unit of equipment of type "x" (say, a defibrillator) was purchased with a standard interface. The treatment time went down because the personnel didn't waste time looking for the CHARGE button, instead they knew where it was.

This is a truly amazing claim. If it is true, I would think the business case for purchasing standard equipment in a hospital would be quite strong, even if it was built only on liability reduction. Never mind the fact that 2 patients can be treated in the same window on time that one could before, or that your ROI for each unit of equipment would be higher due to the higher use.

On a related tangent, I was recently in the hospital. The nurse hooked me to an IV, but the flow rate was too low; she went to get a pump. She hooked me into the pump, but couldn't get it started. When she did get it started, the rate was too low and the alarms were going off. She couldn't figure out the interface. I turned the IV pump to face me, and read the large amount of fine print on the side relating to the pump's operation. It turned out she needed to input the size of needle she was using to adjust the flow rate; she was using a small butterfly needle instead of the default needle, which is larger.

---

## **Pilot not informed of plane's intended destination**

*Mike Crawford <crawford@scruznet.com>*

*Wed, 22 Mar 1995 12:07:59 -0800*

I heard on the radio news this morning (KGO 810 AM, about 11 AM) that a planeload of Taiwanese passengers thought their plane had been hijacked when it landed on a small island instead of at the capital Taipei during a domestic flight.

The destination had been changed, and all the passengers knew it, but no one

told the pilot.

I would speculate that the scheduling system held the correct information, so that the displays in the airport directed all the passengers which plane to get onto, but that there is no direct computer link to the airplane, and either no one realized that the pilot needed to be told "manually", or the person responsible flaked.

Mike Crawford

---

## Snake Oil and Grantsmanship

*Douglas W. Jones <jones@pyrite.cs.uiowa.edu>*

*22 Mar 1995 22:37:08 GMT*

I just got a grant announcement from ARPA, discarded it in disgust, and then read Cliff Stoll's newest book, "Silicon Snake Oil". That led me to dredge the announcement out of the wastebasket, because it's such a perfect example of how much snake oil and snake-oil salesmen have come to permeate our field!

DARPA SOL BAA95-21 DUE 052495 POC states that "Proposed research should investigate innovative approaches and techniques that lead to or enable revolutionary advances in the state-of-the-art. Specifically excluded is research which primarily results in evolutionary improvement to the existing state of practice ..."

It seems to me that this wording is a specific invitation to snake oil salesmen and that it explicitly and openly promises to discriminate against an honest proposal that makes a realistic projection of the likely outcome of the proposed research.

In general, my experience leads me to believe that research projects that actually produce revolutionary results rarely anticipate them, and research projects that promise revolutions rarely deliver! I don't deny that the projects funded on the promise of revolution haven't occasionally delivered interesting results, but I greatly detest a system that demands such empty promises as a condition of obtaining funding.

In any case, "Silicon Snake Oil" is a book worth reading. Computer professionals will find it alternately infuriating, when it attacks our specialties, and rewarding, when it attacks all that hocus everyone else in the field has been pushing.

Doug Jones jones@cs.uiowa.edu

---

## Profiting from misdialed numbers

*Matt Weatherford <mattw@atl.com>*

*Wed, 22 Mar 95 12:48:30 PST*

Some time ago, RISKS ran an article about a long distance company offering an 800-operator service for discounted Collect calls. A competitor soon realized that \*many\* folks were dialing 800-operatEr. The competitor soon chartered this number for their own, strikingly similar (some would say indistinguishable to the naked ear) service and raked in the stray dialers.

National Public Radio ran a piece last week telling of another similar incident. A small mom-and-pop company called "The wooden Boat store" was getting thousands of misdialed calls per month for an MCI 800 service. The small business contacted MCI about the problem and when MCI didn't offer any help, the Wooden boat store approached AT&T. Within 1 week, AT&T had set up a "voice mail" message that said something like "Welcome to the wooden boat store. Press 1 for AT&T Operator assistance, or press 4 for the Wooden Boat Store" Note that AT&T did not offer to connect to the intended, originally misdialed MCI service!

Matt Weatherford Atlantis Diagnostics Int'l (206) 487-7826 mattw@atl.com

---

**Re: A340 incident at Heathrow (Hatton, [RISKS-16.92](#))**

*<ladkin@techfak.uni-bielefeld.de>  
Wed, 22 Mar 1995 19:50:56 +0100*

Les Hatton reports in [RISKS-16.92](#) on an incident involving an Airbus A340 on a trip from Japan to London Heathrow. The aircraft is one of the A320/330/340 (also A319/321) family of Airbuses, some of whose primary flight control systems are computer-controlled (that is, the pilots control-stick movements are input to a computer that guides the control systems). The A340 is a very long-haul aircraft, capable of flying the very longest routes without refueling (it holds the world record for length of route flown without refuelling, for normally-equipped civil transport aircraft). The incident is of greatest significance for RISKS readers because it is the first time that an accident report on an A320/330/340 series aircraft specifically cites software and hardware reliability as the main problem.

The incident concerned a Virgin A340 at Heathrow on 19 September 1994 (cf. the incorrect info reported by Hatton). A short article by Christian Wolmar appeared in The Independent newspaper, one of Britain's major dailies, on Wednesday March 15, 1995. After talking to Christian, I obtained a copy of AAIB (Britain's Air Accident Investigation Board) Bulletin No. 3/95, the report on the incident.

I'll spoil the tale for everyone by giving the punchlines first: the description of the problem areas identified during the incident, and the report's conclusion, the 'Safety Recommendation 95-1'. [during quotes, my editorial comments and elisions are contained within square parentheses such as these. PBL.]

[begin quote]

Problem Areas

The AAIB identified and investigated the following problem areas: RTF [radio communication] phraseology; ATC [air traffic control] vectors and ILS [instrument landing system] performance; fuel quantity indications; double Flight Management Guidance System (FMGS) failure and aircraft type certification.

[end quote]

The radio phraseology can be ignored by RISKS readers. ATC vector problems had to do with capturing the 'glideslope', the radio beam angled up into the sky from the end of the runway, down which an aircraft flies in order to land, under instrument conditions. The aircraft at one point encountered a 'false glideslope' at about 9\deg at 5 miles from touchdown and 4,800ft altitude caused by a 'shallow sidelobe' of the ILS. Such problems are known (glideslope is assured for between 1.35\deg and 5.25\deg in the UK) and the airplane wouldn't have got there had it not been vectored there by ATC - but one hastens to add that normally this is not a problem. Just in this case...see below. All the other problems concern the on-board computers, and the AAIB has written to the JAA (Joint Aviation Authority, which does for Europe what the FAA does for the USA) to determine if the JAA was "aware of some of the more significant shortcomings of the A340's fuel and flight management systems before the type certificate was granted".

[begin quote]

Safety Recommendation.

It is recommended that the reliability of the Airbus A340 FMGS and the fuel management system should be reviewed to ensure that modified software and hardware required to achieve a significant improvement in reliability should be introduced as quickly as possible and the subsequent system performance closely monitored.

[end quote]

Here is why they made this recommendation:

[begin quote]

Autopilot and Flight Director heading performance

The reason for the wrong response of the autopilot and one flight director to the left turn demand was a software error [...] [This error] was known to Airbus Industrie and corrective measures for this and several other software deficiencies were contained in [...] standard L-5 that has been issued and incorporated in most A340s on the UK register.

Fuel Quantity indications

In July 1994 Airbus Industrie issued an Operations Engineering Bulletin on the subject of fuel quantity indication. [The bulletin gives detailed descriptions of anomalies, when they occur, and how to take them into account.] Action pending by Airbus Industrie to correct fuel quantity

errors involves the installation of five additional fuel probes in each inner tank and software standard 6.0. Action to correct CG control errors [the center of gravity is adjusted in cruise by moving fuel around, to give efficient cruise performance] is contained in a software only upgrade to standard 6.1. [...]

#### FMGS double failures

After landing the aircraft's Central Maintenance System had logged a fault in No 2 FMGEC. This was removed and sent to France for data extraction and fault analysis. No fault was found within the hardware and a comparable software fault could not be reproduced on the test bench. Nevertheless, the BITE data dump showed that at 1435 hours the No 2 FMGEC had detected a CLASS 1 HARD failure within itself and a simultaneous fault within FMGEC No 1. The investigation was complicated by the involvement of several sub-contractors in the manufacture of the FMGEC and its database.

[...]

Airbus Industrie were aware of the double FMGS failure mode that had first emerged on the A320 series aircraft. On A320/330/340 aircraft, each FMGEC is linked to its own set of peripherals and inertial reference system. Both FMGECs achieve their own computations and exchange data through a cross talk bus. One FMGEC is declared as master and the other as slave; the master FMGEC is related to the engaged autopilot. Some data in the slave FMGEC is synchronised to the master but all data inserted on any MCDU is transferred to both FMGECs and to all peripherals.

According to Airbus Industrie, there are several ways in which the exchange of data and/or a problem in one computer can affect the other computer. Often the computers reset themselves after a few seconds but occasionally a fault results in repetitive resets or attempts to resynchronise. The fifth reset relatches the computer, which will not recover without a power interrupt. Reset breakers for manual power interrupts are on the flight deck overhead panel. Dual resets occur when both FMGECs encounter failures at the same time. They generally occur after a pilot entry that involves use of the navigation database or to an event synchronised between both flight management systems. Latched double failures usually occur if pilots successively perform three inputs that cause a reset, or if an 'impossible' computation of predictions occurs.

Airbus Industrie have succeeded in radically reducing the frequency of double FMGS failures on the A320 series aircraft; they are also addressing the problem on the A330 and A340 series. [...]

[end quote]

I point out that so-called Byzantine failure modes and algorithms for avoiding them in distributed systems were first identified and studied in the 70s by my former SRI colleagues Lamport, Shostak and Pease under the auspices of the SIFT project, and since then by many, many others. As for other such topics in computer science, this was regarded as 'theory' for a few years. I could hazard a guess that many aerospace engineers still have

not heard about this area. The account above of the problems with the A320/330/340 master/slave FMGECs may give RISKS readers reason to inform themselves about the `theory' of how all this anomalous and possibly dangerous behavior can be avoided in the first place. Many papers in the January 1994 issue of the Proceedings of the IEEE speak about the current state of the art.

Finally, the story.

On the ground in Tokyo before departure, one FCMC indicated numerous faults. It is accepted procedure to depart with only one FCMC operative - they did so, and followed the appropriate procedures for calculating fuel with only one FCMC. Early in cruise, the map symbology on the commander's EFIS (Electronic Flight Instrument System) disappeared and his MDCU (Multifunction Control and Display Unit) ceased calculating. They slaved both off the copilot's DMC (Display Management Computer). The EFIS is the pretty screen in front of the pilot that tells him/her which way is up, which way is forward, and which way, as well as how fast (in three dimensions), and where he/she is. The MDCU displays flight plan info, and a bunch of other things. About an hour later, they found that the commander's EFIS had restored. Logical indications from the No.2 FCMC were also restored later by `resetting the computer'.

Now come a few things which one should really think about hard.

Getting close to home (Heathrow), the copilot tuned in the Lambourne VOR (a radio beacon) manually, to ensure that the EFIS displays were still accurate. They were cleared to fly direct to the beacon, but a few miles east, "the commander's EFIS map display symbology froze and lost all computed data [..]. His MDCU displayed the message `PLEASE WAIT' together with a page normally seen only when loading in data before flight. He was unable to obtain any other display. At [roughly the same time], the [copilot's] EFIS and MDCU exhibited identical behavior."

Notice that not all flight control info was lost from the EFIS - they could still fly the airplane. They `dialed in' the ILS using a "back-up method", and while doing so received an ECAM warning of low fuel state and instructions to open crossfeeds (airplanes like this have many tanks and fuel is pumped around between them). The warning reoccurred and readings indicated they had some 2 tonnes (2000kgs) of fuel less than expected. They discussed traffic density with ATC, and eventually declared an emergency in order to get priority for landing.

They had the autopilot automatically capture the ILS, which is when they hit the sidelobe. `The glidepath bar moved rapidly down the ILS display before moving rapidly up once again; the autopilot's attempt to follow the glidepath resulting in unusually high pitch rates and so the autopilot was disconnected.' The commander informed the tower they were having problems with the glideslope and requested an SRA (Surveillance Radar Approach). In an SRA, the controller talks the airplane down localiser and glideslope continuously, by giving an uninterrupted stream of position information relative to the glideslope/localiser pair. It's very impressive.

Aircraft are on `final approach' when they're lined up with the runway

centerline and heading down the glideslope to land. (This should not be confused with when the flight attendant says 'final approach' to the passengers, which is usually when the aircraft is even before \*initial\* approach phase.) The approach was for Runway 09 Right at LHR (the '09' means that it's pointing roughly 90\deg to North). The crew were on the SRA, being vectored (given magnetic headings to fly) to intercept the final approach course. They were flying a heading of 180\deg and were commanded to change to 130\deg. When they turned the heading selector knob on the autopilot, both commander's and copilot's heading 'bugs' moved correctly (that's an indication on the directional gyroscope of which heading you want the autopilot to fly to and hold - I had a lower-tech version on my Piper Archer), but the flight director bars went in opposite directions and the airplane followed the false movement of the copilot's bar, and turned right instead of left. At this stage, the copilot disconnected autopilot and flight directors and flew the plane 'manually' (see first paragraph for why this is not quite an accurate expression for these aircraft).

They landed without further incident; after taxiing in and shutting down, the fuel indications recovered; and thankfully everyone lived happily ever after.

Peter Ladkin

---

**Re: A340 incident at Heathrow (Ladkin, [RISKS-16.96](#))**

*John Rushby <RUSHBY@csli.sri.com>*

*Wed 22 Mar 95 14:06:55-PST*

I'm not sure you need to invoke Byzantine failures to explain the problems reported with the double FMGS failures in the Airbus A340 and its relatives, though Byzantine-fault-tolerant architectures are simpler and more regular than others -- and might therefore be less prone to bugs.

A Byzantine failure is usually interpreted as a hardware fault that causes the errant device (e.g., a sensor) to provide conflicting information to the systems that interrogate it. These faults can be masked by suitable Byzantine-fault-tolerant algorithms (invented, as Peter correctly points out, by Pease, Shostak and Lamport during the SIFT project at SRI. Incidentally, you can retrieve a picture of SIFT, and of Pease, Shostak, and Lamport via WWW at URL <http://www.csli.sri.com/ft-history.html> ).

However, Byzantine hardware faults don't seem to be the problem with the A340 FMGS--rather, it seems to have been a plain bug in the redundancy management. And from the description, it seems that the reason there are bugs is that the design of the system is not amenable to comprehensive analysis and thorough comprehension. The great contribution of Lamport et al. was the "state-machine" approach to fault-tolerant system design (tutorial reference at bottom). The advantage of this approach is that it provides a relatively simple architecture that can provably tolerate ANY KIND of fault, up to some number. In contrast, the type of architecture used in most aircraft systems is based on FMEA, where you explicitly try to anticipate and counter each specific kind of fault. This leads to

complexity, and thence to bugs, and also to the possibility of overlooked fault modes (and, more likely, overlooked COMBINATIONS of faults). The disadvantage of the state-machine approach is that it requires a lot of redundancy (3n+1 channels to withstand n simultaneous faults). This is overcome, to some extent, by the "hybrid" fault-models introduced by the people at Allied Signal who developed the MAFT architecture. (There's a paper by them in the issue of the IEEE proceedings that Peter mentions). MAFT is the only architecture for primary flight control developed by a manufacturer of these things that uses the state-machine approach. It was proposed for the 7J7 and 767X, but Allied dropped out of the bidding after Boeing cancelled these and then invited new proposals for the 777.

Systems above the PFC (primary flight control/computer) level usually seem to use dual, or dual-dual redundancy rather than the quad-and-above found in PFCs. The state-machine approach may not be appropriate here, but I'd hope that ideas from modern fault-tolerant design, and from formal state-exploration and verification could add something.

As an aside, the mechanisms of fault tolerance, distributed coordination, concurrency management, etc. employed in aircraft systems owe little to those studied by academic researchers. For example,

Not far from there (CNRS-LAAS a research center concerned with fault-tolerance), Airbus Industries builds the Airbus A320s. These are the first commercial aircraft controlled solely by a fault-tolerant, diverse computing system. Strangely enough this development owes little to academia. (IEEE Micro, April 1989, p.6)

Of course, there is little reason to suppose that academic researchers know more about fault-tolerant architectures for avionics systems than those who actually develop them, but it does mean that the architectures and mechanisms used in aircraft systems cannot draw on the extensive analyses and (in some cases mechanically checked) proofs that have been published and subjected to peer review in computer science journals.

John

Introduction to the state-machine approach:

```
@article{Schneider:state,
  AUTHOR = {Fred B. Schneider},
  TITLE = {Implementing Fault-Tolerant Services Using the State
    Machine Approach: A Tutorial},
  JOURNAL = {ACM Computing Surveys},
  YEAR = 1990,
  VOLUME = 22,
  NUMBER = 4,
  PAGES = {299--319},
  MONTH = Dec
}
```

We've done lots of work applying formal methods to algorithms for state-machine replication under hybrid fault models.

[You can get the redundancy down to about  $n > 3a + 2s + m$  where a, s, and m are

the numbers of arbitrary (Byzantine), symmetric (wrong but consistent), and manifest (obvious, or crash) faults to be tolerated simultaneously.]

Examples, if you're interested:

<http://www.csl.sri.com/podc94.html>

<http://www.csl.sri.com/tse93.html>

<http://www.csl.sri.com/compass94.html>

<http://www.csl.sri.com/cav93-hybrid.html>

<http://www.csl.sri.com/ftcs93.html>

<http://www.csl.sri.com/fttrft92-jmr.html>

<http://www.csl.sri.com/fttrft92-ns.html>

overview: <http://www.csl.sri.com/tse95.html>

See also NASA's overall program and their own work in this area:

<http://shemesh.larc.nasa.gov/fm-top.html>

John Rushby                      Email: [Rushby@csl.sri.com](mailto:Rushby@csl.sri.com)  
Computer Science Laboratory   Tel: (415) 859-5456 (hit #0 to escape voice-mail)  
SRI International                Fax: (415) 859-2844  
333 Ravenswood Avenue        WWW: <http://www.csl.sri.com/rushby/rushby.html>  
Menlo Park, CA 94025, USA    ftp: <ftp://ftp.csl.sri.com/pub/{reports|pvs}>

---

## Re: FBOI

*Mike Crawford <[crawford@scruznet.com](mailto:crawford@scruznet.com)>*

*Wed, 22 Mar 1995 12:45:33 -0800*

Regarding FBOI having an account on Netcom...

While I can understand a startup company "renting cheap office space", one would think that a new financial institution wouldn't keep its valuables in the electronic equivalent of a public square. There are many, many ways to break Unix security - at the very least, any netcom sysadmin could read and alter FBOI's files, and very likely there are many hackers who know about holes in netcom's system.

If the PGP decryption is to take place on netcom's computers, rather than a private CPU within FBOI's "offices", then the cleartext passphrase will exist in memory where it can be accessed by anyone who can acquire root privileges. In addition, the encrypted secret key would have to be stored online, so it can be copied by an intruder, and one can use a program (trace? I don't recall) that displays all the system calls that a program makes in order to monitor the keystrokes that FBOI's operators make while entering the passphrase to decrypt the secret key.

I consider it the height of irresponsibility to operate a financial service on a public access Unix system. Netcom might consider whether they would be liable in the event of a security breach.

If you could make \$100,000 by hacking an OS known to be as impregnable as swiss cheese, and you didn't have the ethical sense to stop you, wouldn't you put some effort into making off with the goods?

Mike Crawford

---



Search RISKS using [swish-e](#)

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