



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 12

**Tuesday 31 December 1991**

**Forum on Risks to the Public in Computers and Related Systems**

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

• [Volume 12 Issue 01 \(1 Jul 91\)](#)

- [The Risks of Undelete and the Law \(Ron Dippold\)](#)
- [Patriot missile specifications \(Robert I. Eachus\)](#)
- [Lawsuit Pending over Patriot's Failure to Stop Dharan Scud \(Sean Smith\)](#)
- [Word Perfect file locking poor protection \(John Gilmore and Helen Bergen via Peter Jones\)](#)
- [Statement in Support of Communications Privacy \(John Gilmore\)](#)
- [NIST announces public-key digital signature standard \(John Gilmore\)](#)
- [Re: Videotape of the pilot discussing the crash of UAL 232 \(Robert Dorsett\)](#)

• [Volume 12 Issue 02 \(2 July 1991\)](#)

- [Insecure Superman leads to Superbill \(Paul Leyland\)](#)
- [Too Many Computer Systems Hurt War on Drugs, study says \(PGN\)](#)
- [Colombian Constitution Erased \(Brian Snow\)](#)
- [More phone disruptions \(Fernando Pereira\)](#)
- [Bell Atlantic 26 June Failure \(Robert McClenon\)](#)
- [Re: The Risks of Undelete and the Law \(Al Donaldson\)](#)
- [Searching the RISKS archives via WAIS \(Ephraim Vishniac\)](#)
- ["On the Danger of Simple Answers" \(elnitsky via Rob Slade\)](#)
- [Videotape of the pilot discussing the crash of UAL 232 \(Mary Shafer\)](#)
- [Risk of posting to RISKS \(Jerry Hollombe\)](#)

• [Volume 12 Issue 03 \(8 July 1991\)](#)

- [Alcor/Email suit pays off! \(Henson\)](#)
- [Computer based estimation of mortality \(Richard I. Cook\)](#)
- [On finding a coding bug in the Time Server Daemon \(Martin Minow\)](#)
- [Animated hieroglyphics on telco operators's terminals \(Dan Jacobson\)](#)
- [Dutch Phreaks and Chaos Congress 90 \(Klaus Brunnstein\)](#)
- [Risks Forum and Vulnerability \(Klaus Brunnstein\)](#)
- [Re: Global warming: Not so funny. \(Victor Yodaiken\)](#)
- [Re: "On the Danger of Simple Answers" \(Chuck Karish\)](#)
- [The advantages of posting to RISKS \(Brian Tompsett\)](#)

• [Volume 12 Issue 04 \(9 July 1991\)](#)

- [Clip-Art Confusion Causes City Change \(Christopher Davis\)](#)
- [Hiding a face on television \(Tim Smith\)](#)
- [A RISKy night in Georgia \(Robert E. Van Cleef\)](#)
- [Risks of HR 1400 to modem community \(Jim Thomas\)](#)
- [Dissemination of confidential information \(Hugh Cartwright\)](#)
- [Review of "TERMINATOR 2: Judgment Day" \(R. Mehlman\)](#)
- [Re: Computers and Exporting \(Vadim Antonov\)](#)
- [Re: Formalism vs Experimentation \(Vadim Antonov, Daniel Palumbo\)](#)
- [Disk based crime plan \(Rob Boudrie\)](#)
- [Deleting vs. Shredding \(Brad Templeton\)](#)
- [Re: The Risks of Undelete and the Law \(Steven Tepper, William Ricker\)](#)

• [Volume 12 Issue 05 \(11 July 1991\)](#)

- [TRW Accused of Exploiting Consumers \(PGN\)](#)
- [Dissemination of confidential information \(Adam Curtin\)](#)
- [Phone disruptions \(Ed Andrews\)](#)
- [\(Im\)probability theory \(By Arthur Salm\)](#)
- [Leaking of Gates memo not an IT risk \(Henry J. Cobb\)](#)
- [Coding bug \(Dennis L. Mumaugh\)](#)
- [Re: A RISKy night in Georgia \(Trevor Kirby, Bruce Perens, Paul Smee\)](#)
- [Risk Preferences \[Research effort!\] \(Kevin Crocker\)](#)
- [FINAL CALL, COMPUTING & VALUES CONFERENCE, AUG 12-16 \(Walter Maner\)](#)

• [Volume 12 Issue 06 \(16 July 1991\)](#)

- [Bay-Area Long-Distance Service Disrupted \(again!\)](#)
- [Computer Showers a Briton with Gifts \(Henry Cate III via Mark Brader&rec.humor\)](#)
- [Computer "assistance" in the UK Grand Prix \(Brian Randell\)](#)
- [Re: auto telemetry records \(Erik Nilsson\)](#)
- [Free \[Canadian\] Money? \(Mark Batten\)](#)
- [Nitwit ideas \(Niven and Pournelle\) \(Clive Feather\)](#)
- [Puzzle boxes for critical device interfacing \(Ross Williams\)](#)
- [U.S. Electronic Data Move Challenged on Privacy Issue \(NYT via Jeff Helgesen\)](#)
- [NPTN Infosphere Report \(Sue Anderson\)](#)
- [Re: Risks of Posting to RISKS \(Chuck Dunlop\)](#)

• [Volume 12 Issue 07 \(16 July 1991\)](#)

- [RISKS: US West 10x charges users \(patlo\)](#)
- [Houston City Hall voice-mail prank \(PGN, S. Spenser Aden\)](#)
- [Re: Risks of posting to newsgroups \(Li Gong\)](#)
- [1992 IEEE Symposium on Research in Security and Privacy \(John McLean\)](#)
- [Puzzle Boxes: Reply to comments \(Ross Williams\)](#)

• [Volume 12 Issue 08 \(25 July 1991\)](#)

- [Another false apprehension -- erroneous database information \(PGN\)](#)
- [Human Error Blamed for Soviet N-Plant Problems \(PGN\)](#)
- [Shuttle Atlantis out to launch \(PGN\)](#)
- [Risks of getting used to computers \(Geoff Kuenning\)](#)
- [Index of Known MsDos Malware: 998 viruses/trojans \(Klaus Brunnstein\)](#)
- [Sometimes they even warn you about the pitfalls \(self-trapping\) \(Andrew Koenig\)](#)
- [Smart cockpit with no backup \(Henry Spencer\)](#)

- [Black boxes in autos for accident "facts" \(Mark Seecof\)](#)
- [Re: Artificial Dissemination \(Edward Jung\)](#)
- [Volume 12 Issue 09 \(25 July 1991\)](#)
  - [The limits of simulation \(Henry Spencer\)](#)
  - [RISKS vs. RISKS \(Steve Bellovin\)](#)
  - [Gottschalks rejects check \(Todd Heberlein\)](#)
  - [Proposed law on computer searches \(Chris Hibbert\) \[longish\]](#)
  - [New Jersey "software engineering" registration legislation \(John M. Ritter via Arthur Rubin\) \[longish\]](#)
- [Volume 12 Issue 10 \(29 July 1991\)](#)
  - [Summer slowdown \(PGN\)](#)
  - [Egad, sail-by-wire! \(W. K. \(Bill\) Gorman\)](#)
  - [Third Chicago Airport: Rare Events & Computer Projections \(William E. Mihalo\)](#)
  - [Risks of human error in Soviet nuclear "industry" \(Tom Blinn\)](#)
  - [Re: Smart cockpit with no backup \(Simson Garfinkel\)](#)
  - [Licensing of Software Engineers \(Bill Murray\)](#)
  - [Re: New Jersey "software engineering" registration legislation \(Bob Frankston\)](#)
  - [ACM SIGSOFT '91, SOFTWARE FOR CRITICAL SYSTEMS \(Judith Burgess\)](#)
- [Volume 12 Issue 11 \(30 July 1991\)](#)
  - [DEFSTAN 00/55-56 \(Victoria Stavridou and Andres Ravn\)](#)
  - [Computer problems at BCCI \(David Shepherd\)](#)
  - [Census data in the Land of Oz \(Michael Panosh\)](#)
  - [Soft Eng Cntrl aids during Hydraulic Failure \(Science News\) \(Jeffrey Sorensen\)](#)
  - [Risks of human error in Soviet nuclear "industry" \(Ken Mayer\)](#)
  - [Cardphone Problems in Ireland \(D.P.O'Donoghue\)](#)
  - [Book review: Practical Unix Security \(Clifford Stoll\)](#)
  - [\\*WRONG\\* ftp-adress in Brunnstien: Index of Known Malware \(Eibo Thieme\)](#)
  - [Re: Smart cockpit with no backup \(Henry Spencer\)](#)
  - [Re: The limits of simulation \(Henry Spencer\)](#)
  - [Re: Licensing of Software Engineers \(Henry Spencer\)](#)
  - [Data entry is NOT software engineering.. \(Thomas P. Blinn\)](#)
  - [New Jersey "software engineering" registration legislation \(Arthur Rubin, A. Padgett Peterson, Christopher R Riley, Chris Riley, Joseph Beckenbach\)](#)
  - [Flawed assertion in RISKS-12.08 \(Mark Seecof\)](#)
  - [Re: Risks of Posting to RISKS \(Jerry Hollombe\)](#)
- [Volume 12 Issue 12 \(12 August 1991\)](#)
  - [Teenage Hacker Emulates Hess \(PAJ\)](#)
  - [Future Risks \(Hilarie Kauiolani Orman via Richard Schroepfel\)](#)
  - [Security comes to the Free Software Foundation \(Martin Minow\)](#)
  - [Lotus Marketplace Epilogue \(Marc Rotenberg\)](#)
  - [Computer frustration \(Andrew Goldberg via Les Earnest\)](#)
  - [Yet another threat to telephone privacy \(Jeff Makey\)](#)
  - ["Enemy of the State" -- Story on risk to privacy \(Richard Thomsen\)](#)
  - [Firefighters won't give first aid to AIDS patients \(Sean Eric Fagan\)](#)
  - [Lifestyle discrimination \(Marty Thomas\)](#)
- [Volume 12 Issue 13 \(19 August 1991\)](#)
  - [Junk Mail in Outer Space: Shuttle test mail-bombed \(Peter Scott\)](#)

[ATM mixup in New York \(John Martin\)](#)

- [Computer failure helps Bakthiar murder suspect \(Fernando Pereira\)](#)
- [Deutsche Airbus 2000 \(Martyn Thomas\)](#)
- [Bell V22 Osprey crash \(Martyn Thomas\)](#)
- ["Doctored" radios \(PGN\)](#)
- ["Virus Implants in DoD Weapons" \(David Risler via Jerry Leichter\)](#)
- [Cracker charged in Australia \(Fernando Pereira\)](#)
- [Profitable Drug Wars -- Innocents Presumed Guilty \(mauler via Charles Hoequist\) \[SEE ALSO RISKS-12.13LAW\]](#)
- [Patriot and Dhahran again \(Phil R. Karn\)](#)
- [Re: "Traffic crystal ball" may be in your car's future \(Secty Samuel Skinner, \[editorial\], via Jeff Helgesen\)](#)
- [Risks of Calling Reporters in Ohio: Procter & Gamble \(PGN\)](#)
- [Risk of Power Failures in Computer Controls: 9 Mile Point \(PGN\)](#)

• [Volume 12 Issue 14 \(19 August 1991\)](#)

- [TRW Wrong on Credit Reports for Entire Town \(Scot Drysdale\)](#)
- [Computer Crime Bill - S1322 \(Robert E. Van Cleef\)](#)
- [Bank Shot \(RISKS of automatable documents\) \(Ed Ravin\)](#)
- [Misuse of computerized auto registration info \(Rodney Hoffman\)](#)
- [Risk of licensing programmers -- lost freedom and creativity \(John Gilmore\)](#)
- [A320 revisited \(Robert Dorsett\)](#)
- [Re: Procter&Gamble \(Steve Bellovin\)](#)
- [Re: FSF machine having to clamp down on security \(Paul Mauvais\)](#)
- [Re: "locking" DoD smart weapons \(Guy Sherr\)](#)
- [Re: Rumor regarding Soviet calibers \(Michael Edelman\)](#)
- [More Credit Bureau Risks \(Mike Waters\)](#)
- [RISKS of calling 911 from cellular phones \(E.M. Culver\)](#)
- [Book: "Narcissistic process and corporate decay..." \(Dan Jacobson\)](#)

• [Volume 12 Issue 15 \(22 August 1991\)](#)

- [Electronic mail beams shuttle's message home \(Joe Abernathy, PGN\)](#)
- [The RISKS of a national computerized entertainment ticketing network \(KJPhelan\)](#)
- [Personal data in California \(Phil Agre\)](#)
- [Electronic Library Systems in Airlines \(Robert Dorsett\)](#)
- [Microsoft, IBM demonstrating faults in each other's products \(Jon Jacky\)](#)
- ["Citicorp Creates Controversy With Plan To Sell Data ..." \(Jerry Leichter\)](#)
- [NY Times Letter on Fake Documents \(Sanford Sherizen\)](#)
- [ATM videotapes \(Jyrki Kuoppala\)](#)
- [Re: Bell V22 Osprey crash -- assembly error \(Henry Spencer\)](#)

• [Volume 12 Issue 16 \(26 August 1991\)](#)

- [Pacific Bell "Message Center" failure in San Francisco Area \(David Schachter\)](#)
- [More Risks of Computer Billing -- \\$22,000 water bill \(PGN\)](#)
- [Risk Perception \(Rodney Hoffman\)](#)
- [More on Houston Chronicle spacemail item \(Joe Abernathy\)](#)
- [Internal computer fraud at Pinkerton \(Rodney Hoffman\)](#)
- [P&G phone record search \(Mark Seecof\)](#)
- [RISKS on trusting organizations like CERT \(Jyrki Kuoppala\)](#)
- [TCAS sees ghosts \(IEEE Spectrum article via Jim Horning\)](#)
- [More on the Lauda Air crash \(Brian Acohido via Nancy Leveson\)](#)

• [Volume 12 Issue 17 \(26 August 1991\)](#)

- [Computer-related problems at Cape Canaveral \(Steve Bellovin\)](#)
- [Computer communications and the aborted Soviet coup \(PGN\)](#)
- [Medical records for sale \(Jerry Leichter\)](#)
- [Citicorp selling of credit card data \(Bud Couch\)](#)
- [Automating commodities markets \(Cameron Laird\)](#)
- [Re: Bank Shot \(RISKS of automatable documents\) \(Jerry Hollombe\)](#)
- [Re: Microsoft, IBM demonstrating faults in each other's products \(Flint Pellett\)](#)
- [More about California's Automatic Vehicle Identification spec \(Steve Bagley\)](#)
- [California DMV AVI proposal \(Phil Agre\)](#)
- [Use of ATM for blackmail in UK TV script \(Mark Evans\)](#)
- [Desktop Forgeries \(John Moore\)](#)
- [Re: SSNs \(Brad Templeton\)](#)
- [Sometimes you can only get there using the long way around \(Bob Cunningham\)](#)
- [Re: canopus.stanford.edu goes nova \(Joe Dellinger\)](#)
- [FTCS 22--Symposium on Fault-Tolerant Computing \(Jack Goldberg\)](#)

• [Volume 12 Issue 18 \(27 August 1991\)](#)

- [13 Aug 91 NY Nine Mile Point 2 Nuclear Plant Incident Reassessed \(PGN\)](#)
- [Risks to Computers from Coup Attempt \(Aldis Ozols\)](#)
- [Oil Firm Surveys for Data and a Data Interchange Format \(John F Stoffel\)](#)
- [Ada beats C++ according to the DoD \(John F Stoffel\)](#)
- [Unwarranted equivalence assumptions \(Andrew Koenig\)](#)
- [Study Recommends Earthquake Warning Network \(Fernando Pereira\)](#)
- [Re: Firefighters won't give first aid to AIDS patients \(Tim Oldham\)](#)
- [Re: Cracker charged in Australia \(Richard A. O'Keefe\)](#)
- [FAA seems misled \(Re: TCAS Sees Ghosts\) \(Richard Johnson\)](#)
- [Risks of CDROM publishing \(Donald M. Craig\)](#)
- [The RISKS of a national computerized entertainment ticketing network \(Steve McDowell\)](#)
- [New List: C+HEALTH \(Computers and Health\) \(Judy Smith\)](#)

• [Volume 12 Issue 19 \(28 August 1991\)](#)

- [Phone Fraud \(Ed Andrews summarized by PGN\)](#)
- [\(Assumed\) False Alarm at Nuclear Plant \(Rodney Hoffman\)](#)
- [O, Oh, what a difficult name \(Gene Spafford\)](#)
- [Programs Pester Public Policy People \(Jeffrey Sorensen\)](#)
- [Re: 13 Aug 91 NY Nine Mile Point 2 Nuclear Plant Incident \(Steve Bellovin\)](#)
- [Re: Ada beats C++ according to the DoD \(Brinton Cooper\)](#)
- [Re: Unwarranted equivalence assumptions \(Brinton Cooper\)](#)
- [Re: TCAS sees ghosts \(Steve Jay, Lars-Henrik Eriksson, Keith Hanlan\)](#)
- [pugwash.dcs.ed.ac.uk goes nova too \(John Butler\)](#)
- [NIST High Integrity Lecture Series: talk by Laszlo Belady \(Laura Strigel\)](#)

• [Volume 12 Issue 20 \(30 August 1991\)](#)

- ["Thieves Hit Social Security Numbers" \(Yasmin Anwar via PGN\)](#)
- [Jetliners in near-miss over Cleveland \(PGN\)](#)
- [More T/CAS \(Martyn Thomas, Robert Dorsett\)](#)
- [Overseeing dementia patients by computer \(Urban Fredriksson\)](#)
- [Heisenberg effect for credit data? \(Peter G. Capek\)](#)
- [The story of O \[and Ng\] \(Jerry Leichter, Stuart I Feldman\)](#)
- [A number is no name \(Clifford Johnson\)](#)
- [The need for utilities to deal with non-standard situations \(Tom Lincoln\)](#)
- [Uncle Sam Can't Keep Track of his Trillions \(Bob Frankston\)](#)

• [Volume 12 Issue 21 \(DIGEST 31 August 1991\)](#)

- [`Risk perception' \(Phil Agre\)](#)
- [Flaming makes the mainstream media \(again\) \(Charles Forsythe via Gene Spafford\)](#)
- [Phone Fraud Story a Fraud? \(Michael Barnett\)](#)
- [Re: Phone Fraud -- Langley VA \[anonymous\]](#)
- [+&\\*\\$ \(Bob Frankston\)](#)
- [Banks, Credit Cards, and Short Names \(Bill Biesty\)](#)
- [YASSNS \(Yet Another Social Security Number Story\) \(S. Peter Loshin\)](#)
- [Re: Programs Pester Public Policy People \(Jeffrey Sorensen\)](#)
- [Police tickets & computers in the Netherlands \(Ralph Moonen\)](#)
- [Re: Cracker charged in Australia \(Gene Spafford\)](#)
- [Senseless Actions Invite Trouble \(Charlie Lear\)](#)
- [A Danger Associated with Intelligent Terminals \(Douglas Thomson\)](#)
- [Re: Unwarranted equivalence assumptions \(Andrew Koenig\)](#)
- [Old School Reports of the Famous \(Kernel Mustered via Spaf and Keith Bostic\)](#)

• [Volume 12 Issue 22 \(3 September 1991\)](#)

- [Madison mail mess-up \(Tom Slone\)](#)
- [RISKS of using electronic mail, and universal addressing \(David Parnas\)](#)
- [Re: +&\\*\\$ \(Tom Blinn\)](#)
- [Re: Study Recommends Earthquake Warning Network \(Floyd Ferguson\)](#)
- [Re: Risks of Risk Perception Research \(William P Gardner, Craig Seidel\)](#)
- [Symposium on Reliable Distributed Systems, Advance program \(Lorenzo Strigini\)](#)
- [DIAC-92 CALL FOR PAPERS AND PARTICIPATION \(Douglas Schuler\)](#)

• [Volume 12 Issue 23 \(3 September 1991\)](#)

- [Herb Caen on Computerized Radar \(via Mike Seibel, Brad Templeton, Allan Meers\)](#)
- ["Miser held in record Social Security fraud" \(Barry Jaspan\)](#)
- [Re: "Thieves Hit Social Security Numbers" \(Lars-Henrik Eriksson\)](#)
- [Computer Abuse Amendments Act of 1991 \(Thomas Zmudzinski\)](#)
- [Re: A Danger ... with Intelligent Terminals \(Paul Stachour\)](#)
- [Complain to Journalists \(John E. Mollwitz\)](#)
- [The RISKS of Superiority \(Arthur Clarke \[!\] via Ellen Spertus\)](#)
- [NASA severs connection on electronic mail linkup \(wrapup by Joe Abernathy\)](#)

• [Volume 12 Issue 24 \(4 September 1991\)](#)

- [Radiation therapy machine dose rate doubled by configuration error \(Lawrence W. Berkley and James A. Purdy, summarized by Jon Jacky\)](#)
- [Salomon Brothers -- Database Design \[anonymous\]](#)
- [Airworthiness Directive for 747-400 electrical system \(Robert Dorsett\)](#)
- [`Risk perception' \(Phil Agre\)](#)
- [Re: Risk Assesment High Priesthood \(Robert W. Kerns\)](#)
- [Re: A number is no name \(EKristia...\)](#)
- [Re: Re: +&\\*\\$ \(Bob Frankston\)](#)
- [Re: "Thieves Hit Social Security Numbers" \(Urban Fredriksson\)](#)
- [Re: Risks of a Universal Identifier \(Martin Minow\)](#)

• [Volume 12 Issue 25 \(5 September 1991\)](#)

- [A kludge too far? FAX-to-OCR-to-speech \(Bob Frankston\)](#)
- [LA Times Article on E-mail \(Mike Kimura\)](#)
- [Re: RISKS of using electronic mail \(Brian Clapper, David Parnas\)](#)

- [More on SSN risks \(Glen Osterhout\)](#)
- [Universal Email addresses and SSN \(Jim Anderson\)](#)
- [Re: "Thieves Hit Social Security Numbers" \(Bob Frankston\)](#)
- [Re: National Character variations in ASCII \(Jim Haynes\)](#)
- [Pork barrel software validation \(Paul Eggert\)](#)
- [Multics/UNIX Lessons \(Edward Rice\)](#)
- [Call for Papers, FICS 92, Singapore \(Harold Joseph Highland\)](#)

• [Volume 12 Issue 26 \(6 September 1991\)](#)

- [The Dead Sea Scrolls and Data Security \(Jerry Leichter\)](#)
- [Charging batteries \(Erling Kristiansen\)](#)
- [``Returns for Senders" \(US Postal Service handling of forwardings\) \(Dinah Wisenberg Brin in Common Cause, via PGN\)](#)
- [Re: Portability of E-mail Addresses \(Robert Neff\)](#)
- [DDN Management Bulletin 84 on NIC transfer \(NIC\)](#)
- [Re: +&\\*\\$ \(David J. Fiander, Tom Blinn\)](#)
- [Re: Story of O \(Will Martin\)](#)
- [Re: A number is no name \(Merlyn LeRoy, Bob Frankston\)](#)
- [Re: RISKS of using electronic mail ... \(Brinton Cooper, Bob Frankston\)](#)
- [Re: National Character variations in ASCII \(Bob Frankston\)](#)

• [Volume 12 Issue 27 \(7 September 1991\)](#)

- [Play the lottery via Nintendo \(Mike Cepek\)](#)
- [Re: Salomon Brothers -- Database Design \(Jeff Berkowitz\)](#)
- [The REAL RISKS and REWARDS of E-Mail \(Larry Press via Tom Lincoln\)](#)
- [Re: ``Returns for Senders" \(Willis H. Ware\)](#)
- [Re: +&\\*\\$ \(John Moore, Andy Goldstein\)](#)
- [Re: A number is no name \(RMRichardson, Bob Frankston\)](#)
- [Re: Unusual characters in addresses \(David Lamb\)](#)
- [Re: A permanent EMAIL address \(Mike Van Pelt\)](#)
- [Re: RISKS of using electronic mail" \(David Parnas, John Sloan\)](#)
- [Re: The Dead Sea Scrolls and Data Security \(Chuck Karish\)](#)
- [Re: WHOIS \(David A. Curry, Chuck Karish\)](#)
- [A better model for cracking \(Scott Draves\)](#)
- [Prize for Most Useful Computer Virus \(Cliff Stoll\)](#)
- [15,000 Cuckoo Letters \[Another RISK OF EMAIL?\] \(Cliff Stoll\)](#)

• [Volume 12 Issue 28 \(9 September 1991\)](#)

- [FAA on 755 thrust reversers \(PGN\)](#)
- [Inmate, working for TWA, steals credit card numbers \(Rodney Hoffman\)](#)
- [Re: Salomon Brothers -- Database Design \(William Dye\)](#)
- [Fax machine IDs \(Robert Morris\)](#)
- [Re: Unusual characters in addresses \(Bob Frankston\)](#)
- [Failsafe mode for 3.5" Floppies \(Don Phillips\)](#)
- [Re: The RISKS of Superiority \(John Hobson\)](#)
- [Re: A Danger ... with Intelligent Terminals \(Randolph Bentson\)](#)
- [Risk assessment: a specific experience \(Mark Fulk\)](#)
- [Re: Risk Perception \(Geoff Kuenning, Chuck via Phil Agre, David Chase, Dan Drake, Craig Partridge, William P Gardner, Phil Agre, Fred Heutte\)](#)

• [Volume 12 Issue 29 \(10 September 1991\)](#)

- [CIA dumps on the National Security Archive \(Tom Slone\)](#)

- [CAA grant Cat IIIB autoland clearance for 747/767 \(Martyn Thomas\)](#)
  - [Follow-up on Hobson's M16 story \(Jim Purtilo\)](#)
  - [Risks of Incompatibilities \(Harry Erwin\)](#)
  - [Crackers for hire \(Mark Seecof\)](#)
  - [Re: Salomon Brothers -- Database Design \(Dan Drake\)](#)
  - [Re: Risk assessment: a specific experience \(Peter Wayner\)](#)
  - [Re: The risk of thinking we are in control \(Larry Seiler\)](#)
  - [Re: National characters on car plates \(Torsten Lif\)](#)
  - [Re: Failsafe mode for 3.5" Floppies \(BartMassey, BruceHamilton, AndrewKlossner\)](#)
  - [Re: Number of virus events dropping \(Mark Hittinger\)](#)
  - [Re: Prize for Most Useful Computer Virus \(Raymond Chen, Richard A. Schumacher, Dave Butterfield\)](#)
  - [It is RISKy to believe that Averages are `average' \[!\] \(David Paschall-Zimbel\)](#)
  - [Seventh Annual Conference on Computer Assurance \(James Bret Michael\)](#)
- [Volume 12 Issue 30 \(11 September 1991\)](#)
- [Export controls on workstations \(John Markoff via PGN\)](#)
  - [Re: Multinational Character sets \(Hugh Davies\)](#)
  - [Re: National Character variations in ASCII \(Kim Greer\)](#)
  - [Re: Risks of sloppy terminology \(Geoff Kuenning\)](#)
  - [Re: M16 \(Ty Sarna\)](#)
  - [Re: Failsafe floppies? \(Jordan M. Kossack, Bob Jewett, Doug Krause, David Palmer, Mike Berman\)](#)
  - [Re: Beneficial viruses considered harmful \(Brian Rice\)](#)
  - [Re: Prize for Most Useful Computer Virus \(Joe Dellinger\)](#)
- [Volume 12 Issue 31 \(12 September 1991\)](#)
- [Re: Export controls on workstations \(Neil W. Rickert, Brinton Cooper, Haakon Styri\)](#)
  - ["Checkless society" \(Daniel B. Dobkin\)](#)
  - [Re: Multinational Character sets \(Dik T. Winter, Robert Ullmann, Hugh Davies\)](#)
  - [Re: +&\\*\\$ \(Mike Morris\)](#)
  - [Re: M16 and James Fallows' "Two Weapons" \(Jon Jacky, Tom Faller\)](#)
  - [Junk Mail -- In memoriam, Dave Sharp \(Peter Mellor\)](#)
  - [Risks of assumptions? \(R. Cage\)](#)
  - [The seriousness of statistics mistakes \(Jeremy Grodberg\)](#)
  - [Risk Assessment: a specific experience \(Justine Roberts\)](#)
  - [Re: risk analysis \(Victor Yodaiken\)](#)
  - [Averages and distributions \(Jerry Leichter\)](#)
- [Volume 12 Issue 32 \(12 September 1991\)](#)
- [Security in software distribution \(Joe Morris\)](#)
  - [Re: Crackers for hire \(Joan Eslinger, James Deibele\)](#)
  - [Re: Helpful Viruses? \(Stan Kurzban, Bob Johnson, Chuck Royalty\)](#)
  - [Re: Cheap air tix \(Mark Seecof\)](#)
  - [Re: EMP \(Phil Agre, Tom Faller\)](#)
  - [Re: The seriousness of statistics mistakes ... \(Mark Fulk, Ronald A. Thisted\)](#)
  - [Re: ASCII \(Eric Florack, Mark Seecof\)](#)
- [Volume 12 Issue 33 \(15 September 1991\)](#)
- [British Telecom computer failure cuts off 42000 \(Paul Leyland\)](#)
  - [Security Software Bug Locks Up System \(Sanford Sherizen\)](#)
  - [Companies Steal Information \(Sanford Sherizen\)](#)
  - [Industrial espionage \(Jerry Leichter\)](#)
  - [Re: Junk Mail ... 737 crash \(Steven Philipson\)](#)

- [RSA vs. NIST \(digital security standards\) \(Tom Slone\)](#)
- [Re: Salomon Brothers -- Database Design \(Gary Beckmann\)](#)
- [Secret Computations the basis for Corporate Decisions \(Jeffrey Sorensen\)](#)
- [Re: +&\\*# \(Bob Clements, H. Fuss\)](#)
- [History of Internationalization of ASCII \(Paul Green, Lars Henrik Mathiesen\)](#)
- [Export controls on workstations, or, more mantras \(Jerry Leichter\)](#)
  
- [Volume 12 Issue 34 \(16 September 1991\)](#)
  - [Network Security Lacking at Major Stock Exchanges \(PGN\)](#)
  - ["Planted" data in databases \[anonymous\]](#)
  - [Re: RSA vs. NIST \(Greg Rose, Steve Bellovin, Dan Bernstein, Kevin McCurley\)](#)
  - [Re: Export controls on workstations \(Hank Nussbacher, Lars-Henrik Eriksson, John Mainwaring\)](#)
  - [RISKS of trying to get hard facts \[OS/2\] \(Conrad Bullock via Gideon Yuval\)](#)
  - [RISKS \(yet again\) of not enough data \(Bill Gunshannon\)](#)
  - [Re: +&\\*# \(Dave Roberts\)](#)
  - [Re: Multics/UNIX Lessons \(Dick Karpinski\)](#)
  
- [Volume 12 Issue 35 \(17 September 1991\)](#)
  - [Computer security breach at Rocky Flats nuclear weapons plant \(Fernando Pereira, Allen Miller\)](#)
  - [DSA is weak \(Jim Bidzos\)](#)
  - [The difficulty of RSA \(Jerry Leichter\)](#)
  - [Re: RSA vs. NIST \(digital security standards\) \(Richard A. Schumacher\)](#)
  - [Re: Export controls on workstations, ... \(John R. Levine\)](#)
  - [Virus halted government computers in south China \(PGN\)](#)
  - [Smart Pill Bottles \(Joe Abernathy\) \(from CACM via VOGON\)](#)
  - [Retraction: The seriousness of statistics mistakes \(Jeremy Grodberg\)](#)
  - [The seriousness of statistical mistakes \(Clifford Johnson\)](#)
  
- [Volume 12 Issue 36 \(18 September 1991\)](#)
  - [AT&T Phone Failure \(Ed Andrews\)](#)
  - [Fly-by-wire without leaving the ground \(JCF\)](#)
  - [World Bank virus \(Ted Lee\)](#)
  - [SunOS SPARC Integer Division Vulnerability \(CERT Advisory\)](#)
  - [The risks of a computer-based forum \(Brian Holt Hawthorne\)](#)
  - [Descriptive terms \[false positives and negatives\] \(Jon Krueger\)](#)
  - [Risks of mistreating programmers \(Arun Welch\)](#)
  - [Re: Security Software Bug Locks Up System \(Sanford Sherizen\)](#)
  - [RSA stuff \(John Mount\)](#)
  - [Manipulation of digital images \(Joe Morris\)](#)
  - [Re: +&\\*# \(Richard Ristow, John Wichers, Gary Beckmann, Timothy Freeman, Lynn R Grant, John F. Woods\)](#)
  
- [Volume 12 Issue 37 \(20 September 1991\)](#)
  - [Letter to Congress on NIST's DSS \(Jim Bidzos\)](#)
  
- [Volume 12 Issue 38 \(20 September 1991\)](#)
  - [Midwest Stock Exchange Reaps Millions Due to Accounting Glitch \(Jeff Helgesen\)](#)
  - [Newark NJ high school computer problem \(Martin A. Leisner\)](#)
  - [Technology and the oldest profession \(Henry Cox\)](#)
  - [YATO \(Yet Another Telco Outage\) \(Richard Johnson\)](#)
  - [AT&T switch trouble \(Fernando Pereira\)](#)
  - [English Supermarket Checkout Failure \(Maddock\)](#)

[Samurai Hackers' Cunning Employer Screening Process \(Marco Barbarisi\)](#)

- [Re: Fly-by-wire without leaving the ground \(A. Padgett Peterson\)](#)
- [MSAFP, utilities, and all that \(Mark Fulk\)](#)
- [Computer monitoring of pill bottles \(Jennifer Heymont\)](#)
- [Documentation and lack thereof \(Stanley \(S.T.H.\) Chow\)](#)
- [Just the wrong number \(Jerry Leichter\)](#)
- [Reliability and Redundancy \(Bill Murray\)](#)
- [CPSR Annual Meeting \(Eric Roberts\)](#)

• [Volume 12 Issue 39 \(23 September 1991\)](#)

- [Carpal Tunnel Syndrome strikes \(Peter Mellor\)](#)
- [Risks of technical translation \(Bertrand Meyer\)](#)
- [Patent for Travelmation on Fare-Search System \(Bob Frankston\)](#)
- [Rounding and truncating within multilevel software \(Brenton Hoff\)](#)
- [Re: SunOS SPARC Integer Division Vulnerability \(Dik T. Winter\)](#)
- [Re: Risks of mistreating programmers \(Vesselin Vladimirov Bontchev\)](#)
- [Re: Play the lottery via Nintendo \(Mike Cepek\)](#)
- [Re: documentation and the obsolete parts problem \(Lou\)](#)
- [Ideas made simple \(Bob Frankston\)](#)
- [Book review: Technological Risk, H.W. Lewis \(Jack Goldberg\)](#)

• [Volume 12 Issue 40 \(25 September 1991\)](#)

- [Bell V-22 Osprey - correct sensor outvoted \(John Wodehouse\)](#)
- [Challenger O-ring Problem heads topics at conference on ethics \(George Leach\)](#)
- [People and Public Screens \(Antony Upward, PGN\)](#)
- [Credit bureaus, heisenbugs, and clerical errors \(Peter G. Capek\)](#)
- [Electronic locks at Harvard \(David A. Holland\)](#)
- [Bad error handling in Lamborghini Diablo engine management \(Richard Boylan\)](#)
- [Denver Hacker Hacks NASA \(Andy Hawks\)](#)
- [Re: MSAFP, utilities, and all that \(Eric Eldred\)](#)

• [Volume 12 Issue 41 \(28 September 1991\)](#)

- [Ada Code Formatters pretty dangerous \(Richard G. Hash\)](#)
- [Risks of computerized typesetting \(Simson Garfinkel\)](#)
- [Galileo's Revenge - Junk Science in the Courtroom \(Martin Minow\)](#)
- [Readings in Judgement and Decision Making \(Doug Jensen\)](#)
- [Nintendo Lottery Is For Real \(Jim Huggins\)](#)
- [Radio Shack computerized mailing list problem \(Joseph Poirier\)](#)
- [Re: Security in software distribution \(Kilgallen\)](#)
- [Re: Bell V-22 Osprey \(John Wodehouse, A. Padgett Peterson\)](#)
- [Have you tested your machine lately? \(K. M. Sandberg\)](#)
- [Electronic Locks in Universities \(Martin Ewing, Jim Huggins, Dean Rubine, Kraig Meyer, Mike Carleton\)](#)

• [Volume 12 Issue 42 \(30 September 1991\)](#)

- [Dialup lottery \(PGN\)](#)
- [Space Station Software Hubris \(David Bremner\)](#)
- [Re: V-22 Osprey \(Henry Spencer\)](#)
- [Re: Risks of computerized typesetting \(Lauren Weinstein, Gene Spafford\)](#)
- [Re: Radio Shack computerized mailing list problem \(John R. Levine, et al.\)](#)
- [Re: eelskin wallets and magnetic cards \(Robert Ullmann, et al.\)](#)
- [Re: Have you tested your machine lately? \(Bennet Yee, Henry Spencer\)](#)

• [Volume 12 Issue 43 \(7 October 1991\)](#)

- [Full \(16 rounds\) DES Broken \(Li Gong, Dave Roberts\)](#)
- [AT&T "Deeply Distressed" over Outage \(Mark Seecof, Michael F Eastman\)](#)
- [Fred Cohen's contest and ``good viruses" \(Gene Spafford, John Markoff\)](#)

• [Volume 12 Issue 44 \(8 October 1991\)](#)

- [RISKS of Highway warning signs \(Jim Hofmann\)](#)
- [US Coast Guard's user fiendly software \[sic\] \(Dave Schmidt\)](#)
- [Fiber optics can spontaneously destroy themselves! \(Jeffrey Sorensen\)](#)
- [911 Glitch Delayed Help in Fatal Mt. Prospect Fire \(W.F. Wicks via Mark Brader\)](#)
- [Risks of owning a modem \(Geoff Kuenning\)](#)
- [Emergency phone dialer in Contra Costa county \(Darren Alex Griffiths\)](#)
- [ECC == Error CAUSING Code? Tape drive overcorrects itself... \(John Board\)](#)
- [Re: AT&T "Deeply Distressed" \(Bob Colwell\)](#)
- [Re: Back quotes print wrong \(Dick Karpinski, Simson L. Garfinkel\)](#)
- [Re: Space Station Software Hubris \(Stephen G. Smith\)](#)
- [Schipol Airport \(Peter De Graaf via Mark Kennedy\)](#)
- [Computer Mediated Ethical Discussion: An Invitation \(Peter Danielson\)](#)
- [ACM Computer Security Day \(Beth Olson\)](#)

• [Volume 12 Issue 45 \(9 October 1991\)](#)

- [TACAS -- good news / bad news \(Martin Minow, PGN\)](#)
- [Safer flying through fly-by-wire \(Henry Spencer\)](#)
- [Friendly \(?\) viruses \(Paul Smee\)](#)
- [Computers and missile control \(Walt Thode\)](#)
- [Re: Known plaintext attacks \(Ted Rodriguez-Bell, Clive Feather\)](#)
- [Re: AT&T "Deeply Distressed" \(Steve Bellovin, Bob Colwell\)](#)
- [Re: Schipol Airport \(Henry Spencer\)](#)
- [Re: RISKS of Highway warning signs \(K. M. Sandberg, Joe Morris, Dominic G. Flory, Michael Cook\)](#)
- [Risks of computerized typesetting \(Paul Wallich, Joe Smith\)](#)
- [Re: Ada Code Formatters \(or the dangers of old software\) \(Kent Mitchell\)](#)
- [Re: Computerized typesetting and character sets \(Richard S. D'ippolito\)](#)

• [Volume 12 Issue 46 \(10 October 1991\)](#)

- [Encryption Exportability \(Clark Weissman\) \(from ``Inside Risks"\)](#)
- [Security Criteria, Evaluation and the International Environment \(Steve Lipner\)](#)

• [Volume 12 Issue 47 \(10 October 1991\)](#)

- [Ex-DMV worker admits altering driving records for money \(Vireday\)](#)
- [Software migration at Johnson Space Center \(Joe Bouchard\)](#)
- [European Ideal Embraces Harmonised Pornography \(Brian Randell\)](#)
- [Prison Phone Phraud \(or The RISKS of Spanish\) \(Jim Flanagan\)](#)
- ["Peace Patent" and "Colossus: The Forbin Project" \(Lauren Weinstein\)](#)
- [UCSC to install touch-tone registration \(HELP WANTED\) \(Darrell Long\)](#)
- [Re: Ada Code Formatters \(... old software\) \(David Parnas\)](#)
- [Re: Encryption Exportability, by Clark Weissman \(Carl Ellison\)](#)
- [Re: Fiber optics can spontaneously destroy themselves! \(Paul Leyland\)](#)
- [Re: Safer flying through fly-by-wire \(Randal L. Schwartz\)](#)
- [Re: ``Friendly" \(?\) viruses \(Bertrand Meyer\)](#)
- [Re: AT&T Outages \(Peter G. Rose\)](#)
- [Re: RISKS of Highway warning signs \(Steven Philipson, Arthur Hamlin, Richard Thomsen, Bob Haar, Keith](#)

[Henson\)](#)

• [Volume 12 Issue 48 \(11 October 1991\)](#)

- [Police raid wrong house -- for second time \(David B. Benson\)](#)
- [Crypto Public Policy \(Bill Murray\)](#)
- [Re: Security Criteria, Evaluation and the International Environment \(Henry Spencer, PGN\)](#)
- [Re: "Safer Flying through Fly-By-Wire \(Arnd Wussing, Mary Shafer\)](#)
- [Re: Computers and missile control \(Eric Prebys\)](#)
- [Re: Software migration at Johnson Space Center \(Bob Frankston, Doug Burke, Guy J. Sherr\)](#)
- [Human error: once more, with feeling \(Don Norman\)](#)
- [Re: AT&T outage \(Bob Colwell, Mark Seecof, Bob Niland, Martyn Thomas\)](#)
- [A step towards adopting DefStan 00-55 \(Vicky Stavridou\)](#)
- [Digital Retouching on the Telephone \(Chuck Dunlop\)](#)

• [Volume 12 Issue 49 \(14 October 1991\)](#)

- [Nuclear Computer Safety Fears \(Antony Upward\)](#)
- [Computer Error by Policeman \(Antony Upward\)](#)
- [Thermostat failure mode \(Liudvikas Bukys\)](#)
- [I really like banks -- world wide! \(Boyd Roberts\)](#)
- [I'm sorry, the computer says your credit is bad \(David Bremner\)](#)
- ["Who Flies the Plane?" \(Ken Tindell\)](#)
- [Risks of Enterprise-Wide Phone Systems \(David Fiedler\)](#)
- [AT&T Outage \(Jerry Schwarz\)](#)
- [Re: "AT&T `Deeply Distressed' \(Flint Pellett\)](#)
- [Re: External risks to computer systems \(Peter Mellor\)](#)
- [Re: Keeping people in the loop \(George W. Leach\)](#)
- [Re: ``Friendly" \(?\) viruses \(Brandon S. Allbery, Paul Smee\)](#)
- [Re: buggy software \(James B. Shearer\)](#)
- [Re: Security Criteria, Evaluation ... \(David States\)](#)
- [Re: Software migration at Johnson Space Center \(Richard H. Miller, Tim Parker\)](#)
- [Informatik journal available \(Duane\)](#)

• [Volume 12 Issue 50 \(15 October 1991\)](#)

- [TRW misreports local taxes \(Mark Seecof\)](#)
- [ATM Doesn't Catch Cash Cache Problem \(Ed Miller\)](#)
- [Re: buggy software \(David Parnas\)](#)
- [Risks of genetic engineering? \(Michael Pilling\)](#)
- [Electronic thermostat failures \(Ralph Palmer, Mary Shafer, Bob Wilson\)](#)
- [ACM SIGSOFT'91: SOFTWARE FOR CRITICAL SYSTEMS \[timely reminder\] \(Nancy Leveson\)](#)

• [Volume 12 Issue 51 \(16 October 1991\)](#)

- [Mathematical and scientific foundations for engineering \(Henry Petroski via PGN\)](#)
- [Thermostat failure \(Richard Schroeppel\)](#)
- [Blockbuster `Loses' Returned Video \(Mowgli C Assor\)](#)
- [Credit Card Fraud \(Brian Randell\)](#)
- [New Massachusetts check/credit card ID law \(John R. Levine\)](#)
- [Giving Away Privacy \(Continued\) \(Sanford Sherizen\)](#)
- [Re: buggy software \(Martyn Thomas, Magnus Kempe, Dave Parnas, Bart Massey, Ernesto Pacas-Skewes\)](#)
- [Re: TRW misreports local taxes \(Rob Spray\)](#)

• [Volume 12 Issue 52 \(21 October 1991\)](#)

[The Future is Here \(Amos Shapir\)](#)

- [The\\_RISKS\\_of\\_Geraldo \(Andy Hawks\) \[totally accidental juxtaposition!\]](#)
- [Re: Police raid wrong house -- for second time \(Amos Shapir\)](#)
- [Re: TRW \(Bob Colwell, Anthony DeBoer, Steve Hollasch\)](#)
- [Re: buggy software \(Mark R Cornwell, James B. Shearer, Byron Rakitzis, Richard Hanlon, Stephen G. Smith, Bob Wilson, David Parnas, David Chase\)](#)
- [Licensing Software Engineers \(Christopher E Fulmer\)](#)

• [Volume 12 Issue 53 \(21 October 1991\)](#)

- [Inappropriate ATM error codes \(Sean Eric Fagan\)](#)
- [Blood Donor Cards \(Robert E. Van Cleef\)](#)
- [RISKS of new E911 system \(Paul Robichaux\)](#)
- [Unusual risks of frequent flying \(Rob Aitken\)](#)
- [Review of THE GLASS COCKPIT \(Robert Dorsett\)](#)
- [Yet another journalistic cock-up \(cracker activity\) \(Simon E Spero\)](#)
- [Assurance of High-Integrity Software - Report \(Rick Kuhn\)](#)
- [Video stores losing videos... \(Chris A. Anderson\)](#)
- [Re: Blockbuster \(Brian Boutel, Matt Crawford, Kevin Hughes, Patricia Shanahan\)](#)

• [Volume 12 Issue 54 \(22 October 1991\)](#)

- [Oki Telephone Programming \(Stuart Bell\)](#)
- [Nintendo lottery sidetracked for now](#)
- [Single Point of Failure in L-1011 Intercom \(Craig H. Seidel\)](#)
- [Computer reads water meter \(John Sullivan\)](#)
- [Risks of software controlled safety switch \(Diomidis Spinellis\)](#)
- [Re: Licensing of Software Engineers \(David Parnas\)](#)
- [Law requiring bug fixes \(Mark Seecof\)](#)
- [Re: Yet another journalistic... \(Amos Shapir\)](#)
- [More ATM anecdotes \(Ralph Moonen\)](#)
- [Re: TRW misreports local taxes \(Matt Bishop\)](#)
- [Re: JSC SMS rehost \(David Carlson\)](#)
- [Avis vs. Spaf \(Gene Spafford\)](#)
- [Re: Have you tested your machine lately? \(Boyd Roberts\)](#)

• [Volume 12 Issue 55 \(23 October 1991\)](#)

- [Power outage downs New York Stock Exchange for 24 minutes \(PGN\)](#)
- [Near-sighted or far-sighted fibre-opticians? \(PGN\)](#)
- [MCI Friends & Family & anyone else with a touch-tone phone \(Brian R. Krause\)](#)
- [Risks of double standards \(on PRODIGY\)? \(David HM Spector\)](#)
- [Use of Prodigy on AMC Computers \(Louise R. Silsby via Brinton Cooper\)](#)
- [A note on RISKS contributions \(PGN\)](#)
- [Re: Videos and "Dumbing Down" \(again\) \(Daniel J Yurman\)](#)
- [Re: More ATM anecdotes \(Mark Bartelt\)](#)
- [Re: Oki Telephone Programming \(Randal L. Schwartz\)](#)
- [Re: Computer reads water meter \(Lauren Weinstein, Sam Ho via John Sullivan, Lars Poulsen, Bjorn N. Freeman-Benson\)](#)
- [Re: Have you tested your machine lately? \(Neil Hunt\)](#)
- [Re: Software Migration at the Johnson Space Center \(Joe Bouchard\)](#)

• [Volume 12 Issue 56 \(25 October 1991\)](#)

- [More O'Hare-raising experiences](#)
- [Swedish election results were delayed \(Martin Minow\)](#)

- [Campaign against telco info services \(Mark Seecof\)](#)
- [The computer is always right. \(E. Kristiansen\)](#)
- [1-900 scam \(Torsten Lif\)](#)
- [RISKS of Electronic Credit Card Authorization \(Derek Atkins\)](#)
- [Australian Software Quality Management Standard \(Douglas Thomson\)](#)
- [AT&T/ATC outage revisited \(Alfred H. Scholldorf via PGN\)](#)
- [Re: Single Point of Failure in L-1011 Intercom \(Brinton Cooper\)](#)
- [Re: Law requiring bug fixes \(Geoffrey H. Cooper\)](#)
- [Re: Prodigy \(Jamie Saker, Fred Gilham, Ronald Hale-Evans, Greg Brail\)](#)

• [Volume 12 Issue 57 \(28 October 1991\)](#)

- [DSA/DSS -- Digital Signatures \(Ron Rivest\)](#)
- [Porn-Sabotage in Italian newspaper \(Enrico Musio\)](#)
- [Re: MCI Friends & Family \(Allan Meers\)](#)
- [Do floor vibrations damage disks? \(Magnus Redin\)](#)
- [Re: Software migration at Johnson Space Center \(Doug Burke\)](#)
- [A New Twist on "Speed Controlled by Radar" \(Andrew C. Green\)](#)
- [Call for Papers ESORICS-92 \(Yves Deswarte\)](#)

• [Volume 12 Issue 58 \(29 October 1991\)](#)

- [Would you put your rook and bishop out on knights like this? \(PGN\)](#)
- [Re: DSA/DSS -- Digital Signatures \(James B. Shearer, Ron Rivest\)](#)
- [FDA-HIMA Conference on Regulation of Software \(Rob Horn\)](#)
- [UCI computing survives power outage \[almost\] \(Doug Krause\)](#)
- [Re: Swedish election results were delayed \(Lars-Henrik Eriksson\)](#)
- [Re: Licensing of Software Developers \(John Gilmore\)](#)
- [The risks of "convenient" technology \(Curtis Galloway\)](#)
- [Free Call-Back \(Lars-Henrik Eriksson\)](#)
- [The flip side of the 1-900 scam \(Andrew Koenig\)](#)

• [Volume 12 Issue 59 \(5 November 1991\)](#)

- [New Computer Center for Soviet President \[anonymous\]](#)
- ["Computer rats on students who don't show up in class" \(Steve M. Barr?\)](#)
- [Bank tries to lose 14 billion pounds \(Nigel Cole\)](#)
- [Management Often Bungles Firing Process \(Jeff Helgesen\)](#)
- [Chaos Congress 91 \(Klaus Brunnstein\)](#)
- [Japan's barriers against IT risks \(Tokyo conf.report\) \(Klaus Brunnstein\)](#)
- [DES is better than anyone would have guessed! \(John Sullivan\)](#)
- [DES Watch \(Richard Outerbridge\)](#)
- [Risks of ``record" and ``replay" terminal capabilities \(Bertrand Meyer\)](#)
- [Re: Licensing of Software Developers \(David Parnas\)](#)
- [Re: campaign against telco info services \(Dave Bakken\)](#)
- [Re: Mathematical and scientific foundations \(Leslie J. Somos\)](#)
- [Re: UCI computing survives power outage \(William Walker\)](#)

• [Volume 12 Issue 60 \(6 November 1991\)](#)

- [Driver arrested in computer muddle: Data protection problem \(paj\)](#)
- [Computer Saboteur Pleads Guilty \(Rodney Hoffman\)](#)
- [Blaming the computer \(again\) \(Randal L. Schwartz\)](#)
- [YAHIR \(Yet another human interface risk\) \(Friedrich Knauss\)](#)
- [Certified Voting Program \(Brian A Wichmann\)](#)
- [Electronically controlled bus transmission \(Mark Seecof\)](#)

- [V-22 Tiltrotor Roll Sensors and Triple Redundancy \(Mike Allard\)](#)
  - [Re: FDA-HIMA Conference on Regulation of Software \(Frank Houston\)](#)
  - [RISKS of propagating legendary RISKS \(Paul Karger\)](#)
  - [Software safety, formal methods, standards \(Jonathan Bowen via Jim Horning\)](#)
- [Volume 12 Issue 61 \(7 November 1991\)](#)
- [Cop Charged with Doctoring Computerized Citation Record](#)
  - [Legal status of digital signatures \(Steve Bellovin\)](#)
  - [The dangers of telco competition \(Lauren Weinstein\)](#)
  - [Oven temperature regulator problem \(Jane Beckman\)](#)
  - [No Power backup on Electronic Fuel Injection \(Gareth Howell\)](#)
  - [Another smart card risk \(34AEJ7D\)](#)
  - [UK Phone charge card risk \(Graham Toal\)](#)
  - [Risks of telephones with status displays \(Neil Strauss\)](#)
  - [Don't bank on computer viruses! \(Gene Spafford\) \[WWN strikes again!\]](#)
  - [NSF researchers required to undergo security checks? \(Nancy Leveson\)](#)
  - [Re: Have you tested your machine lately? \(Matt Crawford, Dave W. Hamaker\)](#)
  - [Re: Blaming the computer \(again\) \(George Malits, Paul J Karafiol\)](#)
  - [Re: A new twist on "Speed Controlled by Radar" \(Clive Dawson\)](#)
  - [Re: Electronically controlled bus transmission \(Adam V Reed, Jamie Mason\)](#)
- [Volume 12 Issue 62 \(12 November 1991\)](#)
- [Leaves cause railway signal failure \(Graeme Tozer\)](#)
  - [Computer controlled train is unsafer \(Bob Devine\)](#)
  - [More air scares and phone moans \(PGN\)](#)
  - [RISKS of infrared car door locks \(Andrew Evans\)](#)
  - [Summary of responses on UK phone card risks \(Graham Toal\)](#)
  - [Re: Licensing of Software Developers \(Brinton Cooper, David Parnas\)](#)
  - [Searching a library database \(Matthew Merzbacher\)](#)
  - [Audi Pedal Pushers \(Bob Ayers \[and others\]\)](#)
  - [Religious bias in RISKS posts is counter-productive \(Bill Gray\)](#)
  - [Re: Radar \(Eric Florack\)](#)
  - [Security failure: recycled "unlisted" phone number \(Steven J. Edwards\)](#)
  - [You can help build the National Public Network. \(Gerard Van der Leun\)](#)
  - [Call for Papers: 5th Annual Computer Virus/Security Conference \(Jack Holleran\)](#)
- [Volume 12 Issue 63 \(14 November 1991\)](#)
- [Copy of Letter to NIST in response to proposed DSS \(Martin Hellman\)](#)
  - [Antivirus software vendor creates viruses \(Richard Kulawiec\)](#)
  - [I DEMAND AN APOLOGY FOR THIS LIBEL! \(W. K. Gorman\)](#)
- [Volume 12 Issue 64 \(15 November 1991\)](#)
- [MCI's Response for RISKS \(Sally McCaffrey\)](#)
  - [Computer-assisted trading \(Brendan Kehoe\)](#)
  - [Risks of truncation in the stock market \(Frank G Kienast\)](#)
  - [gray vs gorman \(Fred Gilham\)](#)
  - [ACM SIGSOFT'91: SOFTWARE FOR CRITICAL SYSTEMS \(Peter G. Neumann\)](#)
  - [5th Refinement Workshop: Theory and Practice of Formal Software Development \(Cliff B Jones\)](#)
- [Volume 12 Issue 65 \(26 November 1991\)](#)
- [Phone outages ... tied to typing mistake \(Rudy Bazelmans/Jim Horning\)](#)

[Weather Service Circuit Failure](#)

- [Problems with nuclear plant safety computer in the UK \(Peter Ilieve\)](#)
- [Results of Train Accident Investigations \(Jymmi C. Tseng\)](#)
- [Bank misdeposits money \(David Shepherd\)](#)
- [Mass. Governor wants to sell list of drivers licenses \[Yes and No\] \(Kent Quirk\)](#)
- [CPSR FOIAs U.S. Secret Service \(Craig Neidorf\)](#)
- [The Trojan Horse named 'AIDS'](#)
- [Banning of autodialers? \(John Sullivan\)](#)
- [A new risk for computer folks? Computers and termination policy \(Mark Bartelt\)](#)
- [E911 system brought to it's knees by a prank \(Glenn S. Tenney\)](#)
- [Study on Computer Addiction \(Chris\)](#)

• [Volume 12 Issue 66 \(26 November 1991\)](#)

- [Pentagon computers vulnerable](#)
- [Risks of hardcoded hexadecimal instead of symbolic constants? \(Tom Blinn\)](#)
- [Re: Leaves cause railway signal failure \(Geraint Jones\)](#)
- [Re: Termination \(David Lamb, anonymous\)](#)
- [Proposed Antivirus Certification \(Klaus Brunnstein\)](#)
- [Call for Papers: IFIP World Congress'92/Vulnerability \(Klaus Brunnstein\)](#)

• [Volume 12 Issue 67 \(2 December 1991\)](#)

- [Computer Delays costs Hospital over \pounds 300,000 \(Paul Leyland\)](#)
- [A RISK of dishonestly using a visible password \(Paul Leyland\)](#)
- [Sprint Voice Calling Card uses SS# \(Lauren Weinstein\)](#)
- [Bright AT&T billing sys? \(Thomson Kuhn\)](#)
- ['Contractor queries data security' \(Matthew Farwell\)](#)
- [Proposed traffic congestion charging system, Cambridge UK \(Hugo Tyson\)](#)
- [Mailing lists - a right royal mistake \(Dave Horsfall\)](#)
- [Re: Leaves, trains, and computers \(Peter Mellor\)](#)
- [Re: Proposed Antivirus Certification \(David A. Honig\)](#)
- [Re: Employee Termination \(anonymous, Bill Murray\)](#)
- [Re: Pentagon computers vulnerable \(Brinton Cooper\)](#)
- [Re: Risks of hardcoded hex instead of symbolic constants? \(Bob Frankston, Bennet Yee, Graham Toal, Brandon S. Allbery, Paul S. Miner\)](#)

• [Volume 12 Issue 68 \(13 December 1991\)](#)

- [Hubble Trouble: Space Telescope shuts itself down \(Henry Cox\)](#)
- [Postal worker leaves automated stamper in test configuration \(Palmer Davis, Joe Brownlee\)](#)
- [2 Safeway preferred customers, to go! \(Bear Giles\)](#)
- [Hospital computer solicits the dead \(Adam Gaffin\)](#)
- [Computer records track killer \(Robert Jenkins\)](#)
- [Train crash in UK - is it human error? \(Olivier M.J. Crepin-Leblond\)](#)
- [TRW lawsuit settled with FTC, 19 states \(Phil R. Karn\)](#)
- [National Fingerprint Database specs \(Clifford Johnson\)](#)
- [Bill on computer usage about to become law in Ireland \(Mark Humphrys\)](#)
- [The description is right, only the language is wrong \(Dan Franklin\)](#)
- [Poll tax incompetence \(Robin Fairbairns\)](#)
- [Truth in Antiviral Advertising \(Russell Aminzade\)](#)
- [Re: Pentagon computers vulnerable \(Steve Bellovin\)](#)
- [Post-structuralism and Technology \(Phil Agre\)](#)
- [Chaos Congress 91 Program \(Klaus Brunnstein\)](#)



[Volume 12 Issue 69 \(16 December 1991\)](#)

- [800 telephone outage due to software upgrade \(PGN\)](#)
- [Stock-listings typo: The possibilities are scary. \(James Parry\)](#)
- [More on Lauda crash and computers \(Nancy Leveson\)](#)
- ["Questioning Technology" in WHOLE EARTH REVIEW \(Rodney Hoffman\)](#)
- [Privacy of Email \(James Ting Lui\)](#)
- [More on E911 and representation \(Bob Frankston\)](#)
- [Re: Computer records track killer \(Brinton Cooper\)](#)
- [Re: The description is right, only the language is wrong \(Scott E. Preece\)](#)
- [The EFF Pioneer Awards \(Gerard Van der Leun\)](#)

• [Volume 12 Issue 70 \(18 December 1991\)](#)

- [Life, Death, and Faxes -- Convicted forger released by bogus fax \(PGN\)](#)
- [BT ordered to pay damages for keyboard injuries \(Olivier M.J. Crepin-Leblond\)](#)
- [Re: Privacy of Email \(Eric Florack\)](#)
- [Re: More on E911 and representation \(Erling Kristiansen\)](#)
- [Software safety, formal methods and standards \(Jonathan Bowen\) \[Full text FTPable from RISKS-12.BOWEN\]](#)
- [2nd Conf on Computers, Freedom, and Privacy \(Lance J. Hoffman\)](#)

• [Volume 12 Issue 71 \(24 December 1991\)](#)

- [Illegal sales of confidential data \(Fernando Pereira\)](#)
- [The London Stock Exchange "Taurus" System \(Brian Randell\)](#)
- [Computer Database of Former E. German State Police \(Stasi\) \(Sanford Sherizen\)](#)
- [Remember, computer data is far from sacred. \(Dean Pentcheff\)](#)
- [Outgoing fax numbers and Mercury PIN security \(Nick Rothwell via Werner Uhrig\)](#)

• [Volume 12 Issue 72 \(31 December 1991 \[actually issued 30 December 1991\]\)](#)

- [Airbus Fuel monitoring; tanks shown full when they were not \(John Van Voorhis\)](#)
- [Recent Novell Software Contains a Hidden Virus \(John Markoff\)](#)
- [Has anybody ever been spoofed on the wide network? \(George Michaelson\)](#)
- [Re: Whole Earth Review Questions Technology \(Tom White\)](#)
- [The Whole Earth is greater than the sum of its parts \(Re: Jerry Mander\) \(PGN\)](#)



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 12: Issue 1**

**Monday 1 July 1991**

## Contents

- [The Risks of Undelete and the Law](#)  
[Ron Dippold](#)
- [Patriot missile specifications](#)  
[Robert I. Eachus](#)
- [Lawsuit Pending over Patriot's Failure to Stop Dharan Scud](#)  
[Sean Smith](#)
- [Word Perfect file locking poor protection](#)  
[John Gilmore and Helen Bergen via Peter Jones](#)
- [Statement in Support of Communications Privacy](#)  
[John Gilmore](#)
- [NIST announces public-key digital signature standard](#)  
[John Gilmore](#)
- [Re: Videotape of the pilot discussing the crash of UAL 232](#)  
[Robert Dorsett](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **The Risks of Undelete and the Law**

*Ron Dippold <rdippold@cancun.qualcomm.com>*

*Thu, 20 Jun 91 06:24:27 GMT*

Here's one about a class A dummy... You'd think he'd be a bit more careful on something like this.

Probably the most dramatic instance of recovery of "deleted" file information appears in a recent ruling of the Pennsylvania Supreme Court, *Com. v. Copenhefer*, 587 A.2d 1353. The defendant's death sentence was affirmed on "overwhelming" circumstantial evidence, including "incredibly comprehensive" evidence seized from the defendant's home pursuant to search warrants.

The computer evidence consisted of drafts of texts of phone calls, ransom and hidden notes, and a 22 point plan for the kidnapping scheme, which eventuated in murder of a bank manager's wife. (The defendant was a bookstore owner who had "unproductive transactions" with the bank).

The defendant argued that the computer evidence should have been suppressed because he had deleted the files, thereby creating an "expectation of privacy" under *Katz* and its progeny. The court's opinion contains a readable explanation of how the deletion only affected the directory, and "subsequent usage never displaced the files in question and they remained in the memory of his computer."

The court soundly, and IMO correctly, rejected this claim, analogizing the retrieval of the deleted file data (by an FBI agent who was a computer expert) to deciphering a coded message in a diary, after the diary was obtained under a valid subpoena.

Somehow, I don't think Mr. Copenhefer will be doing any endorsements for PCTools or another defragmenter; "if only I had used Compress with the Clear option, I wouldn't be on death row now." Among other things, the old-fashioned physical evidence was quite overwhelming. But the case is a striking example of the law adjusting to computer technology.

Sort of unbelievable, especially the part about an FBI computer expert (maybe they borrowed someone from the NSA?), but true! So remember, Norton WIPEDISK is your friend.

Ron Dippold

---

### **✂ Patriot missile specifications**

*Robert I. Eachus <eachus@d74sun.mitre.org>*

*Wed, 19 Jun 91 12:29:39 EDT*

There has been some tendency here to treat the Patriot system "failure" to intercept the El Hussein missile in Dharan as a poor system specification or as badly designed software. This is totally wrong. If someone had gone to the Army before the Gulf War and asked, "In this hypothetical situation...how should the system respond?" The answer would have been to do as it did.

The "problems" in the software were bugs only AFTER it was known IN PRACTICE that 1) there were missiles in that speed range that could and should be attacked, 2) the Patriot systems' primary mission would NOT be defending against hostile aircraft, and 3) that "highly motivated" and experienced crews could successfully engage such missiles in "manual" mode using information from other sites. Given those circumstances updating the software and getting it to the field in a matter of days was a heroic effort, even if it arrived one day too late.

The real risk here is in assuming that the "fog of war" is a myth. You don't know how systems will be used in practice until you have actual combat experience. I have seen many "field mods" to hardware incorporated into later production models because the feature was needed to use the system to best effect in combat. This is NOT a failure of design or specification or production, it is often the result of someone trying something because he is dead anyway if it doesn't work. Such successful tactics quickly become the normal way the weapon is used.

A simple example is dive brakes, which were initially installed on P-38s after many crashed from incompressibility problems. In combat, the only advantage that the P-38 had in some situations over its opponent was the ability to dive faster, so pilots took it to the limit and beyond. The dive brake was invented to "fix" a problem which only occurred when a pilot stayed in a steep dive at full power too long. (Actually, there was a "known fix" by the time the brakes were available--fly an outside loop!) If dive brakes had existed when the plane was designed the designers would have been told to leave them off. No reason to add weight to the plane, and no sane pilot would do something like that anyway... Of course, after experience in combat, pilots would carry as much weight as possible, and try to use it to save their lives.

---

### **✂ Lawsuit Pending over Patriot's Failure to Stop Dharan Scud**

<Sean.Smith@THEORY.CS.CMU.EDU>

Wed, 19 Jun 91 12:26:33 EDT

About half the US soldiers killed in the Dharan Scud attack belonged to a unit stationed outside of Pittsburgh. Recently, the local news has been reporting that a Pittsburgh area law firm is recruiting the families of the deceased to participate in a class action lawsuit against Raytheon, manufacturers of the Patriot missile defense system.

Considering that the system was being operated out of spec, to solve a different difficult problem (defense of a city) than the one it was designed for (point defense), this incident suggests that writing software may be RISKier than we thought...

---

### **✂ Word Perfect file locking poor protection**

Peter Jones <MAINT%UQAM@pucc.PRINCETON.EDU>

Tue, 25 Jun 91 19:52:19 EDT

A file on the SIMTEL20 archives, PD:<MSDOS.INFO>UNCRYPT.ZIP, gives information on how to break files that a WP user has "locked" with a password, in WP lingo. Here are some excerpts pertinent to RISKS.

From: gnu@hoptoad.uucp (John Gilmore)  
Newsgroups: comp.os.msdos.apps,sci.crypt  
Subject: Word Perfect "locked document encryption" is trivial to break  
Date: 27 Aug 90 22:58:27 GMT  
Organization: Cygnus Support, Palo Alto

One thing that came up at Crypto '90 was a short paper from Ms. Helen Bergen at Queensland U. in Australia. She noticed the 'locked document' commands in Word Perfect, used by all the secretaries in her dept., and looked to see how strong it was. It turned out that the MSDOS DEBUG command and an envelope for scratch paper are enough for anyone to decode both a document AND the key used for it! Word Perfect Corp. didn't care about her results (letter reproduced below), but

I thought that some Word Perfect losers, I mean users, here on the net might want to know.

You should consider WP locked documents like ROT13: fine to keep the text garbled until you type a command, useless for keeping things private.

John Gilmore

From: <CSZBERGEN@qut.edu.au>  
Date: Mon, 27 Aug 90 10:28 +1000  
To: cygint!gnu

Dear John,

Here is the letter and a copy of the Latex source of my paper. It will be published in CRYPTOLOGIA in the near future. Thanks for your interest,

Regards,  
Helen Bergen

\*\*\*\*\*

Quote from letter received from WordPerfect Pacific:

Thankyou for the copy of your paper entitled "File Security in WordPerfect 5.0". I sent a copy of the paper to WordPerfect Corporation in the USA and recently received a reply from them.

They confirmed that people have written programs to break the password. However, WordPerfect Corporation does not have such a program and therefore has no way of breaking it. They also pointed out that very few users would know how to write such a program.

It is possible that the manual may be amended in a future edition to clarify the protection that a password gives. They recommend that anyone concerned about security may want to take higher precautions than the password protection.

Thank you for your interest in WordPerfect.

\*\*\*\*\*

#### FILE SECURITY IN WORDPERFECT 5.0

H.A. Bergen School of Computing Science  
W.J. Caelli Information Security Research Centre

Faculty of Information Technology  
Queensland University of Technology  
G.P.O. Box 2434, Brisbane, Q 4001, AUSTRALIA

ABSTRACT: Cryptanalysis of files encrypted with the 'locked document' option of the word processing package WordPerfect V5.0, is shown to be remarkably simple. The encryption key and the plaintext are easily recovered in a ciphertext only attack. File security is thus

compromised and is not in accord with the claim by the manufacturer that: "If you forget the password, there is absolutely no way to retrieve the document".

KEYWORDS: Cryptanalysis, WordPerfect.

## INTRODUCTION

WordPerfect is one of the most popular word processing packages in use today. It has a 'locked document' option which aims at protection of a WordPerfect file from unauthorised access. The manual states "You can protect or lock your documents with a password so that no one will be able to retrieve or print the file without knowing the password - not even you". The manual also claims that "If you forget the password, there is absolutely no way to retrieve the document" [1].

[detailed explanation omitted]

In the 4.2 version, the only text encrypted was that contained in the actual document. This is unknown plaintext. In version 5.0, however, the printer information as well as the document text is encrypted. We have identified bytes 16 - 21, 24 - 27, 29 - 41, 43 - 45 as being constant for a particular system (as defined earlier, a particular licenced copy of WordPerfect on a particular PC and printer), and they do not change markedly from one system to another.

So we have the ideal situation of known plaintext for a reasonable number of bytes. This can greatly simplify our attack as it makes it possible to recover the actual key. Then it is trivial to recover the plaintext by using WordPerfect to retrieve the file using the recovered key as the "password". Alternatively, a program could be written to do this as the encryption/decryption algorithm is known. We outline a strategy with the following example from one particular system:

[detailed explanation of finding the key omitted]

- \* Retrieve the plaintext using WordPerfect with the key as the password. This is the easiest way to decrypt the document text.

- \* If no access to WordPerfect is available, then it is straightforward to recover the plaintext with a short C program which implements the decryption algorithm as described previously. This has been done successfully.

## CONCLUSION

The encryption key is easily recovered in an apparent KNOWN CIPHERTEXT ONLY attack, as the system provides enough known plaintext in the printer information regardless of the document plaintext. The analysis, as shown, can literally be done on the back of a (large) envelope.

The analysis may be slightly more difficult where the physical system on which

the files were prepared is completely unknown and vastly different to any system we have encountered, as this may reduce the amount of known plaintext. In these situations, statistical analysis based on the characteristic frequencies of characters in a language is used to decipher text files. This is a standard method which is straightforward although a program may have to be written.

In summary, the cryptanalysis of files encrypted with the 'locked document' option in WordPerfect version 5.0 is remarkably simple. The inclusion of portions of known plaintext in the encrypted file is a fatal flaw in the system, since it provides a mechanism of attack in which the key can be recovered by hand, and document plaintext easily retrieved. All of the key can easily be recovered for keylengths of 1-13 and 15-17, far in excess of commonly used passwords of 8 characters. A high proportion of the key can be deduced for keylengths of 14 and 18-24. The cipher used is too weak, providing little or no protection.

If the attacker has knowledge of any other unencrypted file from the same system, the analysis is made even more simple. We stress that **\*\*both the key and the plaintext can be recovered\*\***, independent of the content of the plaintext.

The worst problem is that it may give a false sense of security. For example, an attacker may decrypt a document, modify it and re-encrypt so that the originator is unaware of the alterations. We conclude that the file security is not consistent with claims made by the manufacturer and is not sufficient to protect sensitive documents from anything but the most naive attack.

#### References

1. WORDPERFECT CORPORATION (1989): WordPerfect for IBM Personal Computers.\\
2. BENNETT, J (1987): Analysis of the encryption algorithm used in the WordPerfect Word Processing Program, Cryptologia, Vol XI. No 4. pp 206-210.\\
3. KONHEIM, A G (1981): *Cryptography, A Primer*, Wiley.\\
4. DENNING, D E (1981): *Cryptography and Data Security*, Addison Wesley.\\
5. CARROLL, J and Robbins, L E (1989): Computer Cryptanalysis of Product Ciphers, Cryptologia, Vol XIII. No 4. pp 303-326.\\

#### Biographical

Helen Bergen is a Lecturer in the School of Computing Science, Faculty of Information Technology, at the Queensland University of Technology. Her research interests within the Information Security Research Centre, Faculty of Information Technology, include cryptology and the application of supercomputers.

Bill Caelli is Director of the Information Security Research Centre within the Faculty of Information Technology at the Queensland University of Technology. He is also Technical Director and Founder of ERACOM Pty. Ltd., a manufacturer of cryptographic equipment. His research interests lie in the development and application of cryptographic systems to enhance security, control and

management of computer and data network systems. -- John Gilmore

{sun,pacbell,uunet,pyramid}!hoptoad!gnu gnu@toad.com

The Gutenberg Bible is printed on hemp (marijuana) paper. So was the July 2, 1776 draft of the Declaration of Independence. Why can't we grow it now?

Peter Jones (514)-987-3542

Internet:Peter Jones <MAINT%UQAM.bitnet@ugw.utoronto.ca>

UUCP: ...psuvax1!uqam.bitnet!maint

---

## ★ Statement in Support of Communications Privacy

<gnu@toad.com>

Tue, 18 Jun 91 22:27:11 -0700

The Electronic Frontier Foundation, Computer Professionals for Social Responsibility, and RSA Data Security Inc. cosponsored a meeting of cryptographers, civil libertarians, business leaders, and people from all over the government who handle cryptography and privacy issues. The following statement was released at the meeting.

### STATEMENT IN SUPPORT OF COMMUNICATIONS PRIVACY

Washington, DC

June 10, 1991

As representatives of leading computer and telecommunications companies, as members of national privacy and civil liberties organizations, as academics and researchers across the country, as computer users, as corporate users of computer networks, and as individuals interested in the protection of privacy and the promotion of liberty, we have joined together for the purpose of recommending that the United States government undertake a new approach to support communications privacy and to promote the availability of privacy-enhancing technologies. We believe that our effort will strengthen economic competitiveness, encourage technological innovation, and ensure that communications privacy will be carried forward into the next decade.

In the past several months we have become aware that the federal government has failed to take advantage of opportunities to promote communications privacy. In some areas, it has considered proposals that would actually be a step backward. The area of cryptography is a prime example.

Cryptography is the process of translating a communication into a code so that it can be understood only by the person who prepares the message and the person who is intended to receive the message. In the communications world, it is the technological equivalent of the seal on an envelope. In the security world, it is like a lock on a door. Cryptography also helps to ensure the authenticity of messages and promotes new forms of business in electronic environments. Cryptography makes possible the secure exchange of information through complex computer networks, and helps to prevent fraud and industrial espionage.

For many years, the United States has sought to restrict the use of encryption technology, expressing concern that such restrictions were necessary

for national security purposes. For the most part, computer systems were used by large organizations and military contractors. Computer policy was largely determined by the Department of Defense. Companies that tried to develop new encryption products confronted export control licensing, funding restrictions, and classification review. Little attention was paid to the importance of communications privacy for the general public.

It is clear that our national needs are changing. Computers are ubiquitous. We also rely on communication networks to exchange messages daily. The national telephone system is in fact a large computer network.

We have opportunities to reconsider and redirect our current policy on cryptography. Regrettably, our government has failed to move thus far in a direction that would make the benefits of cryptography available to a wider public.

In late May, representatives of the State Department met in Europe with the leaders of the Committee for Multilateral Export Controls ("COCOM"). At the urging of the National Security Agency, our delegates blocked efforts to relax restrictions on cryptography and telecommunications technology, despite dramatic changes in Eastern Europe. Instead of focusing on specific national security needs, our delegates continued a blanket opposition to secure network communication technologies.

While the State Department opposed efforts to promote technology overseas, the Department of Justice sought to restrict its use in the United States. A proposal was put forward by the Justice Department that would require telecommunications providers and manufacturers to redesign their services and products with weakened security. In effect, the proposal would have made communications networks less well protected so that the government could obtain access to all telephone communications. A Senate Committee Task Force Report on Privacy and Technology established by Senator Patrick Leahy noted that this proposal could undermine communications privacy.

The public opposition to S. 266 was far-reaching. Many individuals wrote to Senator Biden and expressed their concern that cryptographic equipment and standards should not be designed to include a "trapdoor" to facilitate government eavesdropping. Designing in such trapdoors, they noted, is no more appropriate than giving the government the combination to every safe and a master key to every lock.

We are pleased that the provision in S. 266 regarding government surveillance was withdrawn. We look forward to Senator Leahy's hearing on cryptography and communications privacy later this year. At the same time, we are aware that proposals like S. 266 may reemerge and that we will need to continue to oppose such efforts. We also hope that the export control issue will be revisited and the State Department will take advantage of the recent changes in East-West relations and relax the restrictions on cryptography and network communications technology.

We believe that the government should promote communications privacy. We therefore recommend that the following steps be taken.

First, proposals regarding cryptography should be moved beyond the

domain of the intelligence and national security community. Today, we are growing increasingly dependent on computer communications. Policies regarding the appropriate use of cryptography should be subject to public review and public debate.

Second, any proposal to facilitate government eavesdropping should be critically reviewed. Asking manufacturers and service providers to make their services less secure will ultimately undermine efforts to strengthen communications privacy across the country. While these proposals may be based on sound concerns, there are less invasive ways to pursue legitimate government goals.

Third, government agencies with appropriate expertise should work free of NSA influence to promote the availability of cryptography so as to ensure communications privacy for the general public. The National Academy of Science has recently completed two important studies on export controls and computer security. The Academy should now undertake a study specifically on the use of cryptography and communications privacy, and should also evaluate current obstacles to the widespread adoption of cryptographic protection.

Fourth, the export control restrictions for computer network technology and cryptography should be substantially relaxed. The cost of export control restrictions are enormous. Moreover, foreign companies are often able to obtain these products from other sources. And one result of export restrictions is that US manufacturers are less likely to develop privacy-protecting products for the domestic market.

As our country becomes increasingly dependent on computer communications for all forms of business and personal communication, the need to ensure the privacy and security of these messages that travel along the networks grows. Cryptography is the most important technological safeguard for ensuring privacy and security. We believe that the general public should be able to make use of this technology free of government restrictions.

There is a great opportunity today for the United States to play a leadership role in promoting communications privacy. We hope to begin this process by this call for a reevaluation of our national interest in cryptography and privacy.

Mitchell Kapor, Electronic Frontier Foundation  
Marc Rotenberg, CPSR  
John Gilmore, EFF  
D. James Bidzos, RSA  
Phil Karn, BellCore  
Ron Rivest, MIT  
Jerry Berman, ACLU  
Whitfield Diffie, Northern Telecom  
David Peyton, ADAPSO  
Ronald Plessner, Information Industry Association  
Dorothy Denning, Georgetown University  
David Kahn, author \*The Codebreakers\*  
Ray Ozzie, IRIS Associates  
Evan D. Hendricks, US Privacy Council

Priscella M. Regan, George Mason University  
Lance J. Hoffman, George Washington University  
David Bellin, Pratt University  
(affiliations are for identification purposes only)

---

## **NIST announces public-key digital signature standard**

<gnu@toad.com>

Thu, 27 Jun 91 11:39:59 -0700

Statement of Raymond G. Kammer, Deputy Director  
National Institute of Standards and Technology  
Before the Subcommittee on Technology and Competitiveness  
of the Committee on Science, Space, and Technology  
On Computer Security Implementation  
House of Representatives, June 27, 1991

### Digital Signature Standard

I know that you are interested in our progress in developing a federal digital signature standard based upon the principles of public-key cryptography. I am pleased to tell you that we are working out the final arrangements on the planned standard, and hope to announce later this summer our selection of a digital signature standard based on a variant of the ElGamal signature technique.

Our efforts in this area have been slow, difficult, and complex. We evaluated a number of alternative digital signature techniques, and considered a variety of factors in this review: the level of security provided, the ease of implementation in both hardware and software, the ease of export from the U.S., the applicability of patents and the level of efficiency in both the signature and verification functions that the technique performs.

In selecting digital signature technique method [sic], we followed the mandate contained in section 2 of the Computer Security Act of 1987 to develop standards and guidelines that ". . . assure the cost-effective security and privacy of sensitive information in Federal systems." We placed primary emphasis on selecting the technology that best assures the appropriate security of Federal information. We were also concerned with selecting the technique with the most desirable operating and use characteristics.

In terms of operating characteristics, the digital signature technique provides for a less computational-intensive signing function than verification function. This matches up well with anticipated Federal uses of the standard. The signing function is expected to be performed in a relatively computationally modest environment such as with smart cards. The verification process, however, is expected to be implemented in a computationally rich environment such as on mainframe systems or super-minicomputers.

With respect to use characteristics, the digital signature technique is expected to be available on a royalty-free basis in the public interest world-wide. This should result in broader use by both government and the

private sector, and bring economic benefits to both sectors.

A few details related to the selection of this technique remain to be worked out. The government is applying to the U.S. Patent Office for a patent, and will also seek foreign protection as appropriate. As I stated, we intend to make the technique available world-wide on a royalty-free basis in the public interest.

A hashing function has not been specified by NIST for use with the digital signature standard. NIST has been reviewing various candidate hashing functions; however, we are not satisfied with any of the functions we have studied thus far. We will provide a hashing function that is complementary to the standard.

I want to speak to two issues that have been raised in the public debate over digital signature techniques. One is the allegation that a "trap door", a method for the surreptitious defeat of the security of this system, has been built into the technique that we are selecting. I state categorically that no trap door has been designed into this standard nor does the U.S. Government know of any which is inherent in the ElGamal signature method that is the foundation of our technique.

Another issue raised is the lack of public key exchange capabilities. I believe that, to avoid capricious activity, Public Key Exchange under control of a certifying authority is required for government applications. The details of such a process will be developed for government/industry use.

#### NIST/NSA Technical Working Group

Aspects of digital signature standard were discussed by the NIST/NSA Technical Working Group, established under the NIST/NSA Memorandum of Understanding. The Working Group also discussed issues involving the applicability of the digital signature algorithm to the classified community, cryptographic key management techniques, and the hashing function to be used in conjunction with the digital signature standard. Progress on these items has taken place; however, as with the digital signature standard, non-technical issues such as patents and exportability require examination, and this can be a lengthy process. We have found that working with NSA is productive. The Technical Working Group provides an essential mechanism by which NIST and NSA can conduct the technical discussions and exchange contemplated by the Computer Security Act and also allows us to address important issues drawing upon NSA's expertise.

---

### **✉ Re: Videotape of the pilot discussing the crash of UAL 232**

*Robert Dorsett <rd@catless.org>  
Sat, 29 Jun 91 00:28:11 CDT*

>There's been a lot of discussion of the safety of fly-by-wire aircraft, so  
>here's the discussion of an accident that very possibly would have been  
>prevented were the DC-10 fly-by-wire rather than hydraulic.

As I'm sure Mary realizes, FBW does not alleviate the necessity for multiple-

redundant hydraulics, and all the plumbing that comes with them. As currently implemented on most aircraft, it simply replaces the means by which the \*hydraulic\* actuators are operated. Instead of cables, there are electrical wires. These leads to one or more computers, which in turn process command inputs from the pilot, leading to the possibility of unconventional control laws. Most of the controversy of FBW occurs at this stage. The severity of the failure involved would have happened whether the DC-10 were FBW or not.

Now, in rebuttal, I'm sure Mary'd point out that the FBW issue would only enter in the form of \*control\* issues subsequent to the accident, introducing unconventional control laws to effectively duplicate (or improve upon) the differential thrust technique Haynes used. And she has a point. But there's always the question of whether the complexity and cost of such software will ever justify its usefulness in the "1:1e-9" catastrophic control failure case. In safety management, there is a point of negative return.

Perhaps a more salient observation would have been: this accident would not have happened if there was full manual reversion on the DC-10, ala the Boeing 707? :-)

Robert Dorsett Internet: rdd@cactus.org UUCP: ...cs.utexas.edu!cactus.org!rdd



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 12: Issue 2**

**Tuesday 2 July 1991**

## Contents

- [Insecure Superman leads to Superbill](#)  
[Paul Leyland](#)
- [Too Many Computer Systems Hurt War on Drugs, study says](#)  
[PGN](#)
- [Colombian Constitution Erased](#)  
[Brian Snow](#)
- [More phone disruptions](#)  
[Fernando Pereira](#)
- [Bell Atlantic 26 June Failure](#)  
[Robert McClenon](#)
- [Re: The Risks of Undelete and the Law](#)  
[Al Donaldson](#)
- [Searching the RISKS archives via WAIS](#)  
[Ephraim Vishniac](#)
- ["On the Danger of Simple Answers"](#)  
[elnitsky via Rob Slade](#)
- [Videotape of the pilot discussing the crash of UAL 232](#)  
[Mary Shafer](#)
- [Risk of posting to RISKS](#)  
[Jerry Hollombe](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***✉* Insecure Superman leads to Superbill.**

*Paul Leyland* <[pcl@convex.oxford.ac.uk](mailto:pcl@convex.oxford.ac.uk)>

*Mon, 1 Jul 91 14:18:30 +0100*

Victim of computer hackers fights BT over \pounds 8,000 bill  
\_The Times\_ (London), 1 July 1991

A director of video films is embroiled in a dispute with British Telecom over an \pounds 8,000 bill after becoming a victim of hackers -- people who steal computer passwords to break into international data bases and use services illegally.

George Snow says the bill will ruin him. Experts say the case highlights increasing concern over one of Britain's most under-reported crimes. For several years, Mr Snow has kept abreast of developments in 3-D computer graphics by using access to an American information service called Compuserve. To cut costs, he became a customer of BT's Dial Plus service, which allows customers to connect their office or home computers to international data bases for the price of a local rather than an international call.

Mr Snow, who has directed programmes for Channel 4 and the Arts Council, and whose pop video credits include Howard Jones, had found the service useful and inexpensive until recently. "My quarterly bill would be around \pounds 30," said the director whose company, WKBC TV, is based in west London. Mr Snow, aged 42, now faces a big unscheduled bill for calls he never made. It appears that hackers illegally obtained Mr Snow's password and BT agrees. The dispute is about who pays the \pounds 5,500 and \pounds 2,500 bills which have been run-up in recent months.

BT says that Mr Snow chose a password that hackers could easily borrow [sic]. He says that the company has a responsibility to ensure its networks are secure. "To clock up \pounds 8,000 worth of bills you have to be talking about someone using the service 24 hours-a-day day in day out," he said.

To break into a data base, hackers will generally first try obvious passwords such as Christian names. They also use programmes that run randomly through words in a dictionary until one opens a data base.

Customers with Dial Plus have to sign a disclaimer stating that they will not use obvious passwords otherwise they might be liable for hackers' bills. A BT spokesman admitted, however, that Mr Snow had joined the service before the agreement came into force.

Mr Snow also says that it was BT which approved Superman, the password stolen by the hackers. The company says that Mr Snow was warned that his account was running up huge bills in early February but that it was sometime later that the password was changed. Mr Snow says that it was changed within days and that by the time BT contacted him the damage had been done with most of the bill having been run up.

He believes that he, and possibly others, are being forced to pay the price for the company's poor security and has called in the Computer Crime Unit at Scotland Yard to investigate.

David Frost, a computer security expert with accountants Price Waterhouse, said yesterday that the amount of hacking taking place in Britain was being seriously underplayed by companies.

BT rejects suggestions that it is cavalier with security. A spokesman said the company would write to Mr Snow this week. He says that he will fight BT in court if it prosecutes him. "\pounds 8,000 is about 10 per cent of my turnover," he said.

[I have a few comments, based solely on the report as printed. I do not know what truly happened. I draw attention to the BT's apparent attitude to

password security. They used the term "borrow", rather than "steal" or "use illegally". They vetted the password, implying that Mr Snow was asked to reveal his password rather than keep it secret. Even so, they gave the OK to a password which is of dubious security. It is generally agreed that proper names, dictionary words, literary characters and the like are easily guessed.

More generally, it is interesting how British newspapers, and *The Times* in particular, are beginning to take an informed interest in the subject of computer security and, indeed, in computer-related risks in general. Apart from some quaint terminology ("programmes", "data bases") they seem reasonably competent at understanding the issues and reporting them clearly to a non-expert audience.

Paul Leyland, pcl@convex.oxford.ac.uk ]

---

### **✂ Too Many Computer Systems Hurt War on Drugs, study says**

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

*Tue, 2 Jul 91 20:08:30 PDT*

The 2 Jul 91 Washington Post noted that the government's war on drugs is being seriously impeded by having to rely on more than 100 different computer systems, according to a report of the General Accounting Office. Many of the computers cannot communicate. Also, "the government has no measures for ensuring that its information is correct and that its systems are protected from outsiders."

---

### **✂ Colombian Constitution 'lost' due to lack of data backup procedures.**

*<BSnow@DOCKMASTER.NCSC.MIL>*

*Sun, 30 Jun 91 10:19 EDT*

Excerpted from The Washington Post, 30 Jun 1991, p.A23:

Computer Glitch 'Kills' Constitution;  
Colombian Charter Appears in Jeopardy  
by Douglas Farah, Special to The Washington Post

BOGOTA, Columbia, June 29 -- The approval of Colombia's new constitution, which modernizes the nation's judicial, political and economic structures, is in jeopardy because a computer apparently ate the text. ...

The committee writing the final version was to turn over the text for final voting Wednesday. However, a technician storing the material in a computer, borrowed from the office of the presidency, erased or lost the final document -- after many of the papers with the drafts of the articles had been thrown away. ... "We literally have people going through trash cans looking for scraps of paper," said one source close to the process. "We do not know how this was allowed to happen, and we have lost an almost vital three days. We cannot debate or vote on a text we do not have in front of us." ...

While there are different versions of how the computer foul-up occurred, sources said a member of the codification committee refused to allow

technicians from the office of the president to have access to the computer, fearing that some of the material could be pirated or changed. Instead, he had a nephew hired to do the computer work.

It turned out that the nephew had only taken a one-year correspondence course in computer programming. ...

[Also noted by Les Earnest, and by "Raleigh F. Romine" <romine@cise.nsf.gov>, who added "It has all the traditional ingredients -- no backups, inexperienced operators, etc. The final quote is the best part." ]

---

## **More phone disruptions**

*Fernando Pereira <pereira@klee.research.att.com>  
Tue, 2 Jul 91 11:17:25 EDT*

Associated Press writer Jim Stader reports today (July 2nd) on another software-induced disruption of phone service affecting over 1 million customers (area code 412 around Pittsburgh) of Pennsylvania Bell for over 6 hours. The problem was probably caused by the same recently installed signalling software that is under suspicion for earlier disruptions in the Washington DC and Los Angeles areas. The bug has not yet been identified, and the possibilities of a virus or other sabotage have not been ruled out. Pennsylvania Bell's president stated that the triggering event might have been different in the various disruptions, but that once the problem is triggered, the symptoms are very similar. In all cases, lines carrying signaling between switches became jammed.

[A subsequent revised version of the AP story summarized above reports on speculation that the cause of the phone disruptions may be sabotage originating in the Middle East. The alleged reason for this is the claim that in most cases the network failures followed the appearance of animated hieroglyphics on operators's terminals.]

Fernando Pereira, 2D-447, AT&T Bell Laboratories  
600 Mountain Ave, Murray Hill, NJ 07974 pereira@research.att.com

[The San Francisco Chronicle front page this morning recorded the Pennsylvania problems, and also noted similar problems in San Francisco, although only for five minutes. It quoted Don Burns, a Bell Atlantic VP: "The fact that we've had, in the short period of a month, several outages causes us to believe that something has been introduced" into the systems. The complexity of highly distributed systems continues to confront us. PGN]

---

## **Bell Atlantic 26 June Failure**

*Robert McClenon <76476.337@compuserve.com>  
01 Jul 91 22:53:08 EDT*

In my opinion, the spreading of the failure of the telephone system on Wednesday (26 June) from Baltimore to Washington and Northern Virginia was an

example of a risk of a high degree of connectedness in a network. In particular, connectedness increases the vulnerability to spreading failures, unless special provisions are made to limit that spread. I think a similar lesson was exhibited (but perhaps not learned) by the failure of the electrical grid connecting the Northeast in 1965 resulting in the New York blackout.

It eventually was necessary to C&P (a subsidiary of Bell Atlantic) to break the links between the four SS7 computers and take each of them down and bring them up separately.

The Washington Post says:

> Bell Atlantic said yesterday that it had probably worsened the scope  
>of the failure inadvertently because it had recently linked all four of  
>the traffic cop computers [Signaling System 7 computers] temporarily...

In other words, connecting the four computers was a two-edged sword, and it cut the wrong way on 26 June 1991. Also, there had obviously been inadequate testing of the software. Something as large as a telephone switching system is not easy to test adequately, and requires a high level of thoroughness in planning the tests.

Robert McClenon

---

## **✉ Re: The Risks of Undelete and the Law (Dippold, [RISKS-12.01](#))**

*Al Donaldson <al@escom.com>*

*Tue, 2 Jul 91 11:33:14 EDT*

In [RISKS-12.01](#), Ron Dippold writes about a case in which a murderer used a computer to plan his crime, and then claimed that when he "deleted" his files he had an "expectation of privacy" regarding the data:

>The court soundly, and IMO correctly, rejected this claim, analogizing the  
>retrieval of the deleted file data (by an FBI agent who was a computer expert)  
>to deciphering a coded message in a diary, after the diary was obtained under a  
>valid subpoena.

I agree that the information was properly used in the trial, but I think the analogy given was incorrect or incomplete. While most people think of computers simply as electronic filing cabinets, there are some weak analogies between writing messages to disk and coding data in a diary (e.g., use of ASCII, way in which bits are written to media). I suspect that these analogies were not appreciated by the court. Instead, they seem to have concluded that "deleting" a file is analogous to encrypting it.

File deletion (actually, removing links to the data) is more analogous to shredding or burning the diary, or tearing out pages and throwing them in the trash (imagine an Apple wastebasket icon.. :-). The defendant did have an expectation of privacy based on his (lack of) knowledge of how file deletion worked, just as someone who sets fire to a stack of papers may expect them to burn completely all the way through and obliterate all of the data written on them. But in the case of burned papers, it may

still be possible to carefully peel them apart and read some information. If you really want to obliterate the \*data\*, you burn the paper completely and then grind the charred paper to small pieces of ash. Similarly, if you want to remove \*data\* from a disk, you overwrite it. If it is really important, like national secrets or murder evidence, then you hacksaw the disk platters into little bitty pieces and throw them into the Potomac. Ask Ollie North.

I agree they should fry Mr. Copenhefer, but I don't like the justification. This will probably establish precedence in future trials, further removing legal practice from physical reality. Wouldn't it have been nice if the court had simply decided to use "un-deleted" data, without any half-baked analogies?

AI

Incidentally, I seem to remember a similar case in Northern Virginia recently in which a Marine was accused of murdering his wife (also a Marine, who disappeared and whose body has not been found). As I remember, investigators found plans on how to carry out a murder and hide the body on a disk belonging to the suspect. His explanation, supported by his mother, was that he was working on a book, a murder mystery, and he has no idea where his wife is. Murder, he wrote?

---

### **✂ Searching the RISKS archives via WAIS (Wollman, [RISKS-11.95](#))**

*Ephraim Vishniac <ephrain@Think.COM>*

*Mon, 1 Jul 91 10:55:48 EDT*

I'm the database maintainer, and I just want to add a few notes.

1. The public WAIS server is down right now. With last week's record heat and some inadequate air-conditioning here, we temporarily killed cmns-vax. It's possible that it will be up sometime tomorrow (July 2nd) after moving to a new machine room, but it might be another day or two.

2. The database is automatically updated. (I should fix the source description.) Issues arriving during the night are saved until we start up in the morning; issues arriving while the system is up are added within ten minutes.

3. A variety of user interfaces for the WAIS system are available by anonymous ftp from think.com, in /public/wais. There's a Macintosh interface in WAISStation-0-62.sit.hqx, and there are gnu emacs and X-Windows interfaces in wais-8-b1.tar.Z. The latter package also includes code for setting up your own servers using whatever Unix host you've got handy. (The public WAIS server uses a Connection Machine. Code for that server is not generally available.)

4. The public WAIS server contains a variety of other databases, including the info-mac digest, Sun-Spots digest, Sun Managers mailing list, King James Version of the Bible, National Institutes of Health Guide to Grants and Programs, and the CIA World Factbook 1990.

Ephraim Vishniac ephraim@think.com ThinkingCorp@applelink.apple.com  
Thinking Machines Corporation / 245 First Street / Cambridge, MA 02142

---

## ✂ "On the Danger of Simple Answers"

Rob Slade <p1@arkham.wimsey.bc.ca>  
Mon, 01 Jul 91 20:26:12 PDT

The following was posted on rec.humor.funny. On the one hand, it shows an appalling naivete. On the other hand, that isn't funny at all:

From: elnitsky@math.lsa.umich.edu  
Subject: global warming  
Date: 30 Jun 91 23:30:04 GMT

"... Perhaps of even greater significance is the continuous and profound distrust of science and technology that the environmental movement displays. The environmental movement maintains that science and technology cannot be relied upon to build a safe atomic power plant, to produce a pesticide that is safe, or even bake a loaf of bread that is safe, if that loaf of bread contains chemical preservatives. When it comes to global warming, however, it turns out that there is one area in which the environmental movement displays the most breathtaking confidence in the reliability of science and technology, an area in which, until recently, no one -- even the staunchest supporters of science and technology -- had ever thought to assert very much confidence at all. The one thing, the environmental movement holds, that science and technology can do so well that we are entitled to have unlimited confidence in them, is FORECAST THE WEATHER! -- for the next one hundred years..."

George Reisman, "The Toxicity of Environmentalism"

This kind of thinking is, unfortunately, all too common, even in the scientific community. If I disagree with it, it must be wrong. If it supports what I believe, it must be right.

True "critical" thinking: that facility which allows us to discriminate between correct and incorrect information and points of view, is too often lacking in our society and world. In addition, all too few people have taken the time to acquire the technical knowledge which allows one to judge scientific pronouncements.

(My subject line is the title of the editorial for the Journal of the American Scientific Affiliation special issue on nuclear power some years back.)

Robert\_Slade@mtsg.sfu.ca Vancouver Institute for Research into User Security  
Canada V7K 2G6

---

## ✂ Videotape of the pilot discussing the crash of UAL 232

Mary Shafer <shafer@skipper.dfrf.nasa.gov>

Mon, 1 Jul 91 14:01:06 PDT

I wrote:

>There's been a lot of discussion of the safety of fly-by-wire aircraft, so  
>here's the discussion of an accident that very possibly would have been  
>prevented were the DC-10 fly-by-wire rather than hydraulic.

And Robert Dorsett comments:

As I'm sure Mary realizes, FBW does not alleviate the necessity for multiple- redundant hydraulics, and all the plumbing that comes with them. As currently implemented on most aircraft, it simply replaces the means by which the \*hydraulic\* actuators are operated. Instead of cables, there are electrical wires. These leads to one or more computers, which in turn process command inputs from the pilot, leading to the possibility of unconventional control laws. Most of the controversy of FBW occurs at this stage. The severity of the failure involved would have happened whether the DC-10 were FBW or not.

No, Robert, it wouldn't have. The loss of two of the hydraulic systems was caused by shrapnel damage to the hydraulic lines. Had this not happened, the airplane would have flown along with two working hydraulic systems and have done just fine. However, the design of the conventional hydraulic system dictates hydraulic runs that were vulnerable to the precise damage caused by this accident.

DC-10s don't use cables, they use nonreversible hydraulic systems. I don't believe that any airliner since the DC-4 or so has had cables.

This has nothing to do with the control laws, nothing to do with redundancy, nothing to do with unconventional systems, it has everything to do with the physical vulnerability of the hydraulic lines and the fact that the wiring is better armored and less vulnerable to shrapnel damage and that other hydraulic runs are better protected from this particular damage.

This is, of course, why battle damage resistance is an important benefit of fly-by-wire and why the military is so fond of it. I worked on the Survivable Flight Conditions Systems F-4 Phantom in the early to mid-70s. The Air Force wasn't interested in fancy control systems or lighter weight, they were interested in surviving battle damage. That's the easiest payoff to FBW.

Now, in rebuttal, I'm sure Mary'd point out that the FBW issue would only enter in the form of \*control\* issues subsequent to the accident, introducing unconventional control laws to effectively duplicate (or improve upon) the differential thrust technique Haynes used. And she has a point. But there's always the question of whether the complexity and cost of such software will ever justify its usefulness in the "1:1e-9" catastrophic control failure case. In safety management, there is a point of negative return.

Nope, I wouldn't point this out because it never even occurred to me until you mentioned it. My only thought was shrapnel damage.

I think you're quite correct about some sort of thrust-only flight path control system. There've only been a very few accidents that resulted in total hydraulic loss with an otherwise flyable airplane. (Two pressure vessel failures--Paris in a DC-10, Japan in a 747--and this one for airliners, the birdstrike to the B-1B out of Dyess.) It doesn't seem to me that there's any reason to develop a system to deal with such a remote possibility. Sometimes you just go ahead and accept the risk, when it's an extremely small risk. Life isn't completely risk-free.

Perhaps a more salient observation would have been: this accident would not have happened if there was full manual reversion on the DC-10, ala the Boeing 707? :-)

This accident wouldn't have happened if the airplane had completely armored hydraulic lines. It happened to a DC-10, it happened to a B-1B, but it's easier to prevent in a fly-by-wire aircraft because you have safer hydraulic runs available and because fly-by-wire wires are more easily armored.

Mary Shafer shafer@skipper.dfrf.nasa.gov ames!skipper.dfrf.nasa.gov!shafer  
NASA Ames Dryden Flight Research Facility, Edwards, CA

---

### **✂ Risk of posting to RISKS**

*The Polymath <hollombe@ttidcb.tti.com>*

*Tue, 2 Jul 91 16:33:19 -0700*

Some years ago, as an apprentice programmer, I learned to craft even my personal, quick-and-dirty utility programs carefully and thoughtfully. The lesson was first driven home as I stood by and watched in horror while one of my uglier personal "tools" was packaged and shipped as part of a product.

Recently, a similar phenomenon caught me again. I received an e-mail query asking permission to include the text of one of my postings to RISKS in a forthcoming book. The request came so long after the fact, I had to ask the publisher to send me a copy of the article in question. I'd long since forgotten it.

The article turned out to be a minor diatribe on the nature of censorship and its relation to Stanford's attempt to ban rec.humor.funny. It was a bit embarrassing to read it again and note its flamish style. All in all, I was mildly surprised our moderator let it through.

I gave my permission for its publication, but requested a footnote be added clarifying my position on the matter. I received a copy of the book in the mail a few days ago, footnote and all. (It also contains RISKS comments on the same subject from Les Earnest and John McCarthy. I'm honored to be found in such company).

The risk? The words we exchange here aren't as ephemeral as they may appear on a VDT screen, so be careful what you say and how you say it. You never know who might decide to package and ship it to a customer. (-:

Oh, yes. The book:

\_Computerization and Controversy: Value Conflicts and Social Choices\_  
Edited by Charles Dunlop and Rob Kling, Academic Press, Inc.  
Harcourt, Brace, Jovanovich, Publishers ISBN 0-12-224356-0

(No, I don't get any royalties).

Jerry Hollombe, Citicorp, 3100 Ocean Park Blvd. Santa Monica, CA 90405  
(213) 450-9111, x2483 {rutgers|pyramid|philabs|psivax}!ttidca!hollombe



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 12: Issue 3**

**Monday 8 July 1991**

## Contents

- [Alcor/Email suit pays off!](#)  
[Henson](#)
- [Computer based estimation of mortality](#)  
[Richard I. Cook](#)
- [On finding a coding bug in the Time Server Daemon](#)  
[Martin Minow](#)
- [Animated hieroglyphics on telco operators's terminals](#)  
[Dan Jacobson](#)
- [Dutch Phreaks and Chaos Congress 90](#)  
[Klaus Brunnstein](#)
- [Risks Forum and Vulnerability](#)  
[Klaus Brunnstein](#)
- [Re: Global warming: Not so funny.](#)  
[Victor Yodaiken](#)
- [Re: "On the Danger of Simple Answers"](#)  
[Chuck Karish](#)
- [The advantages of posting to RISKS](#)  
[Brian Tompsett](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***✉* Alcor/Email suit pays off!**

<[hkhenson@cup.portal.com](mailto:hkhenson@cup.portal.com)>  
Sat, 6 Jul 91 13:23:56 PDT

The long running Alcor/email case against the County and City of Riverside, CA was settled out of court in April of this year. The announcement was delayed until all parties had signed off, and the check had cleared the bank :-).

The Alcor Life Extension Foundation (a non-profit cryonics organization --[alcor@cup.portal.com](mailto:alcor@cup.portal.com)) ran a BBS for members and prospective members from early 1987 through January 12, 1988. On that day, the BBS computer was removed under a warrant to take the computer (but no mention of any contained email) in connection with the investigation into the death of 83-year-old Dora Kent.

(Mrs. Kent was placed into cryonic suspension by Alcor in December of 1987. During and following the investigation, Alcor staff members were publicly accused by county officials of murder, theft, and building code violations. No charges were ever filed and the investigation was officially closed three years later.)

In December of 1988 Keith Henson filed a civil suit to force an investigation of the apparent violations of the Electronic Communication Privacy Act by the FBI, but the case was dismissed by the now convicted Judge Aguilar.

In early 1990, just before the statute of limitations ran out, Henson and 14 others (of the roughly 50 people who had email on the system) filed a civil action against a number of officials and the County and City of Riverside, CA under Section 2707 of the Electronic Communication Privacy Act which forbids inspecting or denying access to email without a warrant.

Some time after the case was filed, the Electronic Frontier Foundation came into existence in response to law enforcement abuses involving a wide spectrum of the online community. EFF considered this case an important one, and helped the plaintiffs in the case by locating pro bono legal help. While the case was being transferred, the County and City offered a settlement which was close to the maximum damages which could have been obtained at trial. Although no precedent was set because the case did not go to trial, considerable legal research has been done, and one judgment issued in response to the Defendants' Motion to Dismiss. The legal filings and the responses they generated from the law firm representing the County/City and officials are available by email from [mnemonic@eff.org](mailto:mnemonic@eff.org) or (with delay) from [hkhenson@cup.portal.com](mailto:hkhenson@cup.portal.com). (They are also posted on Portal.)

The Plaintiffs were represented by Christopher Ashworth of Garfield, Tepper, Ashworth and Epstein in Los Angeles (408-277-1981). The only significant item in the settlement agreement was the \$30k payment to the plaintiffs.

---

## **✂ Computer based estimation of mortality**

*<cook@cse14.eng.ohio-state.edu>*

*Mon, 8 Jul 91 19:52:18 EDT*

The 12 June 1991 issue of JAMA (the Journal of the American Medical Association) contains an important article and editorial.

Article: Blumberg Mark S (1991). Biased Estimates of Expected Acute Myocardial Infarction Mortality Using MedisGroups Admission Severity Groups. JAMA 265 (22): 2965-2970.

Editorial: Iezzoni Lisa I (1991). 'Black Box' Medical Information Systems: A Technology Needing Assessment. JAMA 265 (22): 3006-3007.

Blumberg evaluated the actual mortality in a group of patients and compared those values with the predictions of a standardized computer model which is mandated for use in stratifying Medicare-aged patients with acute myocardial infarction (AMI, i.e. heart attack) in Pennsylvania and (with modifications) in

other states. The stratification of patients is important for evaluating the quality of care. If your hospital sees mostly older patients with multiple chronic diseases, your mortality associated with AMI will be greater than that found in a hospital which treats generally healthier patients. The use of a complex model to adjust for the differences in patient populations between hospitals should, in an abstract sense, leave only those differences which relate to quality of care factors specific to an individual hospital and allow people (mainly health care administration and hospital accreditation bureaus) to rate the hospitals for quality. In these days of increasing health care regulation, attempts to define quality by creating models which normalize mortality (or some other measure) as a means of comparing hospitals (or doctors, surgical procedures, methods of treatment, etc.) are being introduced more and more often.

The system Blumberg tested depends on the evaluation of multiple key clinical factors (KCFs) which are coded by technicians from the medical record and run through a proprietary computer program resulting in assignment of the patient to a risk class. Note that the system is far too complex to permit any individual to assess the correctness of its predictions. In addition, the system is proprietary and so the algorithm and coding scheme is not generally available. [Even if it were, it is doubtful that anyone outside the corporation that developed it would be able to comprehend it.]

Blumberg found that the classification method is statistically biased and concluded that the bias arose from a number of sources (e.g. missing KCFs, KCFs which can vary a great deal in a short time, failure to distinguish missing from normal data, and incorrect weighting). This bias has significant implications for hospitals and physicians and (by extension) for patients. Since the output of the system is used as a measure of quality, some hospitals look better than others for reasons unrelated to the quality of care. There is an incentive to try to improve the 'numbers', i.e. to restructure care to make the quality measure appear more attractive [although doing this is made difficult by the fact that it is hard to determine what controls the evaluation system's output].

In an accompanying editorial, Iezzoni notes that the system is an example of a broad class of health care information product "about which very little is known: the redoubtable 'black box'." She goes on to point out that these systems "typically derive from fields about which users may have little knowledge, such as health services research. Many systems base their determinations on complicated statistical formulas that are dependent on the computational wizardry of today's powerful personal computers. Hence, even if complete technical information is available concerning the system's internal algorithm, it often remains an enigma to those whom it affects... Another factor fostering the black box mystique is the proprietary nature of some of these information products, and the consequent reluctance to reveal 'inner workings' and perceived 'trade secrets'." She then notes that there are no applicable standards which require that these systems be safe and effective (in a manner analogous to the requirements for new drugs) and observes that "[f]ew independent evaluations have been performed, and little is known about their validity for use in new policy initiatives, such as statewide hospital quality assessment. While most developers are at least rhetorically committed to improving the health care provision system, this commitment is not enough, given the tremendous responsibility vested in these systems. Opening the black

box is only the first step. We need to know that the information generated is valid and used in a safe and effective way."

The article and editorial face squarely what has been dealt with in only a peripheral manner before: whatever the \_theoretical\_ potential for producing effective decision support systems using computer models to compare different groups or organizations, the \_practical\_ effect of such systems is likely to be quite problematic. (1) Because the systems represent such a large computation, there is no practical way in which users of the systems can understand their output. These systems are \_oracular\_, that is, their output stands apart from their input in incomprehensible ways (just like the pronouncements from the Oracle at Delphi: there was no conceivable way to know if it they were correct). Some black box systems are comprehensible. We use a number of measuring devices whose internal workings are not easily understood (e.g. the pulse oximeter used to measure oxygen saturation in the operating room) but these are mostly black boxes whose operation is meaningfully connected the observable (and observed) world and whose performance can be understood by individuals. When the black box reaches a certain size or when its performance is determined by lots of data or data over a long period of time, it's output necessarily becomes oracular. The new TCASS aviation collision avoidance system is likely to be a case in point. (2) Because of the great effort to required to generate and integrate these systems (many man years, including massive data collection) it is practically impossible to test them in a meaningful way. Blumberg's effort is one example, but he tested just one medical diagnosis out of many supported by the system; it's hard to think of someone going on to test all the others. (3) The systems depend on information which is easy to acquire (e.g. review of the patient's chart) but may be only remotely related to the issues at hand (e.g. quality of care). The systems have a kind of self qualifying nature: the choice of data and pragmatics of acquisition and processing limit the validity of the conclusions in ways which most of us will agree are unrealistic and misrepresent important features and characteristics of the real underlying process, yet there are no easy ways to improve the data. (4) The systems are always potentially open to successive refinement but their size and complexity makes such refinement unlikely. The makers of such systems will always admit that they are not perfect but that the imperfections could be reduced through improvements or modifications. In reality, however, the system is more likely to remain largely fixed or to track changes in the world only slowly. (5) Paradoxically, these systems may obscure the search for quality by providing an objective, computationally efficient, quantitative metric which is related to quality in only a complicated and remote way. In developing "safety" or "quality assurance" systems, there is a tendency to redefine the goal in terms of the system's output.

What are the implications of this trend in health care (and other domain) information systems for professionals developing decision support systems? When Iezzoni refers to "powerful personal computers" she surely means the computers and those system designers, integrators, programmers, coders, and administrators that make these complex systems possible. What are the responsibilities of designers of such decision support systems? After all, they are well situated to assess the impact of decision support tools on the performance of the large system. Do they perhaps have a responsibility to refrain from creating a large complex information processing system which is likely to have the qualities of the one investigated by Blumberg?

Copyright (c) 1991 by Richard I. Cook

## ✂ On finding a coding bug in the Time Server Daemon

Martin Minow 06-Jul-1991 1428 <minow@ranger.enet.dec.com>

Sat, 6 Jul 91 11:26:50 PDT

While reading through the source code to the Berkeley Time Server (which runs in the background of a group of Unix workstations and keeps their system clocks adjusted to "network average time"), I discovered an interesting code sequence in the networkdelta function. That function takes a set of time delay measurements and computes the network average time change. I.e., it is the core of the time server algorithm:

```
/* this piece of code is critical: DO NOT TOUCH IT */
...
    i++
    if (i = j)
        j++;
...

```

Those of you familiar with C programming will recognize the classic error (I make it frequently) of writing "i = j" (assignment) rather than "i == j" (equality test) in an if statement. Both are legal in this context: "i = j" meaning "assign the value of j to i and then test for inequality to zero."

Some reflections:

- Burying an erroneous statement in a paragraph that says "don't touch" makes matters worse. I only found the bug when I went back to 30 year old "Math 295" tools of pencil and paper and walked through the algorithm one statement at a time to see how it worked.
- The error will only manifest itself if one or more systems is wildly out of agreement with the other systems being served by the time daemon. I.e., it is a classic "normal error" in that it is triggered by some other error and makes matters worse.
- The error results in an incorrect calculation of the network average time, which will be corrected (if anyone notices it) when the entire network is re-synchronized to a standard clock (several dial-up time standard clocks are readily accessible from a dial-up modem).
- If Berkeley (the copyright holder) didn't distribute source code, I wouldn't have found the error. Instead, I'd have written my own procedure which almost certainly have been a poorer algorithm.
- Code reviews -- having your software carefully reviewed by a competent outside consultant -- are useful. (What is the computer engineering equivalent of a pathologist?)
- Beware of language constructions, such as C's "if (i = j)" that are error prone. Having once tried to add a warning for this to a C compiler, I can attest to it being extremely difficult: you want to warn on "if (i = j)" but not on "if ((i = j) != 0)" Ultimately, I decided the cure (heuristics in a the compiler) might be worse than the disease.
- "Beware of language constructions" is a warning to the programmer, and

one that belongs in a "Manual of Programming Style." It is an engineering statement, not one of "Computer Science." I.e., it is at a different level of discourse than "beware of bubble-sorts."

-- My university sent me to a remedial writing course because I couldn't spell or distinguish between "who" and "whom," not to mention "that" and "which" -- should there be remedial programming courses, taught by writing teachers, that concentrated only on style?

It is possible to write quality bug-free software in error-prone languages (just as it is possible to write poor software in languages that would prevent "if (i = j)" errors). However, I am beginning to suspect that this requires the obsessive attention to detail of a contract lawyer, combined with the grace of expression of an essayist.

Martin Minow

---

### **✂ Animated hieroglyphics on telco operators's terminals**

*<Dan\_Jacobson@ATT.COM>*

*Thu, 4 Jul 91 12:40 CDT*

>>>> In [RISKS 12.02](/Risks/12.02.html), 3 Jul 91 03:29:41 GMT, Fernando Pereira said:

F> [A subsequent revised version of the AP story summarized above reports  
F> on speculation that the cause of the phone disruptions may be sabotage  
F> originating in the Middle East. The alleged reason for this is the claim  
F> that in most cases the network failures followed the appearance of  
F> animated hieroglyphics on operators's terminals.]

More likely when the big crash came an ESC ( ) or ESC ( 0 or the like came over the line (along with other accidental garbage characters), common ways of turning on many terminals' "line drawing character set" etc. Good thing the terminals didn't also have a alternative Russian character set, or else there seems a slight RISK that we might be fighting World War III now.

---

### **✂ Dutch Phreaks and Chaos Congress 90**

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de>*

*5 Jul 91 14:08 +0100*

On Chaos Computer Club's last Congress 1990, a Dutch group and few other phreaks reported on some techniques to "travel inexpensively on international networks" (see my report in January 1991). Against their usually detailed description of the content of the respective session, CCCs electronic Congress newspaper describes the reports and discussion only in general terms; no details regarding frequencies and computer programs (which meanwhile replaced the "blue boxes" more flexibly) were given.

According to a report in the ("usually well-informed") German weekly magazine Der SPIEGEL, the Dutch group HAC-TIC now published a detailed report on how to "use" special methods, dial-tunes (with frequencies and sequences of operation) and telephone numbers (in Germany: 0130) in diverse areas of the world to

establish toll-free phone connections via specific programs. As the magazine reports, HAC-TIC aims with its detailed description to counterfeit some people who sell (e.g. on AMIGA) such tune-dialing programs for up to 1,000 DM (about 520\$ currently).

Comment: In discussing with CCC people about their surprisingly careful publication behaviour (enough details to warn before developments, but not sufficient to directly aid in attacking), I found some response to the international discussion on CCC related attacks; against CCCs behaviour in earlier years (e.g. selling the NASA attack protocols for 100 DM), this restrictive policy seemed quite honestly. Now that HAC-TIC has published details of the seminar discussion, another discussion might well come in CCC whether such a restrictive approach was well-advised in CCCs spirit.

Klaus Brunnstein, University of Hamburg, FRG

---

### **Risks Forum and Vulnerability**

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de>*

*5 Jul 91 15:03 +0100*

As an enthusiastic reader of the Risks Forum, I strongly appreciate the information carried and the discussion usually maintained on a high level of competence. Moreover, the diversity and actuality of the topics highly demonstrates that if Risks Forum had not been invented by PGN it must be now. So, RF is a success!

Unfortunately, in discussing critical developments as well as preparing IFIP 1992 World Conference (Madrid, September 7-11, 1992) substream "Diminishing Vulnerability of Information Society", I find it ever more difficult to contribute some essential information which I earlier would have immediately sent. One example: since some time, we experiment how to detect and prevent worm accidents; to this end, we had to analyze minimum requirements of worm mechanisms. Our experiments in NETBIOS and DECNET environment showed clearly that it will be *\*extremely difficult\** to prevent or even detect worms! In this situation, I need start a discussion in a responsive and responsible community how to proceed from here; such a discussion would need more knowledge to assess the threat.

At this point, I learn from several discussion in universities and conferences that Risks Forum is now well-spread and even attracted the interest of scenes such as Chaos Computer Club or diverse BBS read by youngsters. Not that I know yet of a single case where actual discussions in Risks Forum has produced a new threat; but when observing other electronic newsmedia, I find it highly desirable that a discussion of the limit of electronic discussion of risks be undertaken.

My examples are from the anti/virus scene: recently a discussion started (in Virus-L) on how to propagate viruses when invoking commands such as DIR; this technology is well established in MACviruses but virtually unknown in the MsDos arena; what is the impact of such discussion between experts on the virus authors? Another example: When observing recent developments in new threats,

our analysis shows too clearly that their authors know the actual discussion rather well; example: the TEQUILA virus exhibits several aspects of older, less distributed viruses which have been described in detail in Virus-L. Therefore, any constructive discussion in publicly accessible electronic newsmedia must bare in mind the risk to transfer serious information to the wrong parties.

Evidently, insecurity and insafety is an essential message which Risks Forum communicates to the public. This mission is an essential contribution of the ACM committee behind RF (whose chairman Peter is), and as IFIP TC-9 "Computer and Society" chairman, I heavily favour any such discussion. On the other side, responsible behaviour also questions whether reports on computer-induced vulnerability generates, by too much details, new vulnerabilities thus endangering the developments of methods to counterfeit vulnerability. I personally think that a responsible message must be more complex than just arguing: "information technology produces vulnerability; when eliminating IT, you immediately reduce vulnerability": such as simple suggestion is in-historic.

My suggestion for a Code of Discourse Ethics:

- 1) Concerned experts should agree not to enhance the vulnerability by their discussion.
- 2) apart from questions of experiences and basic paradigms, aspects of prevention and countermeasures should even more be discussed.
- 3) For critical technical details, successful electronic media are not well suited, even they are counterproductive.

To avoid any misunderstanding: the guarantee of "free flow of information" is one of the essential values in modern societies, specially IT-based ones. But the "trust" which I assume my communication partners follow may not simply be established via electronic media; trust (defined differently from TCSEC contexts!) is a personal relation to minimize the risk of misinterpretation and the deduction of unwished consequences. By its very nature, trust is hardly to be established via email! The medium therefore limits the responsible use of it. (Example: I personally just received Bill Gates memo on Microsoft's performance and future problems; highly interesting, no doubt: but I assume that Bill Gates will not be glad that I had it. I am highly sure that the community in which I received this information is trustable, and they and I will not uncover any details; but just the fact that I as a non-Microsoft employee got it demonstrates the problem!).

If anybody of the highly respected active participants in this discussion feels this discussion inadequate, I apologize for stimulating it.

Klaus Brunnstein, University of Hamburg, Germany

---

**✉ Re: global warming: Not so funny. (Slade, [RISKS-12.02](#))**

*victor yodaiken <yodaiken%chelm@cs.umass.edu>*

*Wed, 3 Jul 91 15:39:55 -0400*

>This kind of thinking is, unfortunately, all too common, even in the scientific

>community. If I disagree with it, it must be wrong. If it supports what I  
>believe, it must be right.

I'm not sure of the relevance of this note to computing risks, but I am  
offended by the use of a borderline dishonest debating trick in which one  
mis-attributes an obviously absurd opinion to an opponent. Which members of the  
"environmental movement" have have exhibited unlimited confidence in weather  
forecasting? One can certainly be alarmed at the prospect of global warming  
while maintaining a great deal of skepticism about the current state of the art  
in weather prediction. Again, I'm not sure why this material found its way  
into the RISKS digest, but I don't want to leave it unchallenged.

---

**✉ Re: (Slade, [RISKS-12.02](#))**

*Chuck Karish <karish@mindcraft.com>*

*Wed, 3 Jul 91 09:22:08 PDT*

[ To the moderator:

I don't really get the joke here, and I'm not sure the  
reference to the risk of uncritical acceptance of  
simulation results justifies opening this can of worms in  
this forum, but I don't think it would be appropriate to  
let Reisman's trivialization of real problems go unanswered. --crk ]

In [RISKS 12.01](#), Rob Slade quoted a poster at the University of Michigan  
who quoted George Reisman's "The Toxicity of Environmentalism":

>The environmental movement maintains that science and technology cannot be  
>relied upon to build a safe atomic power plant, to produce a pesticide that is  
>safe, or even bake a loaf of bread that is safe, if that loaf of bread contains  
>chemical preservatives.

>

>When it comes to global warming, however, it turns out  
>that there is one area in which the environmental movement displays the most  
>breathhtaking confidence in the reliability of science and technology,  
>[ in the area of very-long-term weather prediction ].

Aside from my reservations about Reisman's rhetorical trick of taking examples  
from the views of extremists to trivialize a broad-based movement with many  
thoughtful adherents, this analysis ignores well-founded concerns. Goods and  
services aren't produced by disinterested scientists in a laboratory. They're  
produced by real-world corporations that have to balance risk against cost. In  
many well-documented instances, the financial stakes have been so high that  
real risks have been covered up and safety improvements have been foregone.

The best example of this is the nuclear power industry, in which it's difficult  
to make any operational regulation more stringent because to do so would be to  
acknowledge that previous regulations had been inadequate and that  
currently-operating plants are less safe than is technically possible. In  
cases like this and like global warming where the perceived hazard is extreme,  
the public is unwilling to accept grandfather clauses and assurances that "this  
subject needs further study; we're not sure what to do yet".

I'll argue that the public concern over global warming is less a result of trust of simulations than of distrust of the technologies that are being blamed for the process. As for the punchline about predicting the weather, I doubt that the current level of concern over global warming would have arisen except that the last decade has shown us (at least in North America) the warmest weather in the past century and a half. The argument that this warm trend is not yet statistically significant as evidence of greenhouse-gas-caused global warming is less persuasive than is personal experience that the weather is warmer than it used to be. --

Chuck Karish karish@mindcraft.com  
Mindcraft, Inc. (415) 323-9000

---

### **✂ The advantages of posting to RISKS**

Brian Tompsett <bct@cs.hull.ac.uk>  
Wed, 3 Jul 91 15:47:35 BST

In [RISKS DIGEST 12.02](#) <hollombe@ttidcb.tti.com> (The Polymath) wrote an anecdote on how an old risks posting had been resurrected for posterity in an upcoming book. It is precisely these activities that make RISKS one of the most valued forms of electronic publication. A RISKS posting can find its way from the electronic media into the paper form (via SIGSOFT notices and CACM) quite rapidly. These items can then be cited by other workers in the field.

It is this phenomenon that makes RISKS almost accepted as a form of refereed publication. It is the efforts of our moderator that makes this so.

[Included in all modesty... Keep the good stuff coming. 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 12: Issue 4**

**Tuesday 9 July 1991**

## Contents

- [Clip-Art Confusion Causes City Change](#)  
[Christopher Davis](#)
- [Hiding a face on television](#)  
[Tim Smith](#)
- [A RISKy night in Georgia](#)  
[Robert E. Van Cleef](#)
- [Risks of HR 1400 to modem community](#)  
[Jim Thomas](#)
- [Dissemination of confidential information](#)  
[Hugh Cartwright](#)
- [Review of "TERMINATOR 2: Judgment Day"](#)  
[R. Mehlman](#)
- [Re: Computers and Exporting](#)  
[Vadim Antonov](#)
- [Re: Formalism vs Experimentation](#)  
[Vadim Antonov](#)  
[Daniel Palumbo](#)
- [Disk based crime plan](#)  
[Rob Boudrie](#)
- [Deleting vs. Shredding](#)  
[Brad Templeton](#)
- [Re: The Risks of Undelete and the Law](#)  
[Steven Tepper](#)  
[William Ricker](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ **Clip-Art Confusion Causes City Change**

*Christopher Davis* <[ckd@eff.org](mailto:ckd@eff.org)>  
Tue, 9 Jul 91 18:53:28 -0400

>From the [\\_Boston Herald\\_](#), July 2, 1991, from "Paul Sullivan's CELEBRITY" page:

"Mayor Dinkins' birthday invites sky-high error"

The Big Apple must @i(really) be turning sour because even an invitation to Mayor @b(David Dinkins') upcoming birthday party features the skyline of @i(Boston) instead of the skyline of New York City.

[... it's for a July 10th fundraising party (my birthday too!) --ckd]

Prominently displayed in the sketch is the famous Citgo sign in Kenmore Square, the old John Hancock Building, the new Hancock Tower and the Prudential Tower.

[...mayor's spokeswoman passes buck to organizing committee]

A committee spokeswoman blamed it on that old standby, computer error. "When you punch in 'skyline,' that's what came out," she said. [phrasing as original; either she's confused about past & present, or the quote got messed up. No [sic] in original --ckd]

>From my reading of that, it appears that there's some sort of "clip art" package involved, probably with titles and/or keywords to select "appropriate" pictures.

Is this a case of the RISKS of using a single-keyword search? More the RISKS of blindly accepting the results, in my opinion. If the photo included with the article is of the card (it's not clear whether it is or not), then someone definitely should have looked twice. (The Mets fans should have at least recognized the Citgo sign from the '86 Series, and the Yankees fans don't need to go that far back. The RISKS of not watching enough baseball?)

Garbage in, Gospel out, once again. This one's just another old story to RISKS readers...

Christopher Davis <ckd@eff.org>, System Manager & Postmaster  
Electronic Frontier Foundation, Cambridge, MA

---

### **✂ Hiding a face on television**

<ts@cup.portal.com>  
Tue, 9 Jul 91 00:40:41 PDT

Being too lazy to change the channel, I'm being subjected to the pseudonews program *\_Hardcopy\_*. As I type this, I'm watching a little boy testify in court about the possible murder of his mother.

To protect the child from being recognized, they are doing something to the video of his face so that it consists of several large squares that change as he moves. This seems to be the standard way to hide things on TV now.

Is this safe? It seems that there should be enough information here to reconstruct the hidden face (or other body parts -- they seem to be using this process to cover up nudity now too).

Tim Smith

---

## **✂ A RISKy night in Georgia**

Robert E. Van Cleef <[vancleef@nas.nasa.gov](mailto:vancleef@nas.nasa.gov)>

Tue, 9 Jul 91 12:32:23 -0700

Computer Crime (Information Weekly, July 8, 1991, page 6)

A Computer Systems Protection Act went into effect last week in Georgia. The Act provides the same punishment for computer thievery as for other types of theft crimes. The bill calls for prison terms of up to 15 years for "computer-assisted theft, trespass, invasion of privacy, and forgery." Under the Act, stealing someone's computer password in Georgia can get you a \$5,000 fine or one year behind bars.

---

## **✂ Risks of HR 1400 to modem community**

<[TKOJUT1@MVS.CSO.NIU.EDU](mailto:TKOJUT1@MVS.CSO.NIU.EDU)>

Wed, 03 Jul 91 21:13 CDT

What are the risks of Bush's proposed crime bill?? There is provision in HR 1400, the House version of the "Comprehensive Violent Crime Control Act of 1991" that should be of concern to those concerned with the potential reduction of Constitutional protections of privacy and association. The current version would also revise 18 USC (sect) 2709 which authorizes the FBI "subscriber information and toll billing records information or electronic communication transactional records" from any "wire or electronic communication service provider."

The subject of the request need not be the person under investigation, but can be made of anybody who is perceived to possess information relevant to an investigation. The language of existing law is sufficiently vague that it seems to include (or could be interpreted by zealous agents to include) any private documents that one may have on a university mainframe that might contain "transactional information" (a broad term with potential for widest possible definition). This could be construed to mean that if somebody on the internet received private e-mail from the target of an FBI investigation, then the first person could be subject to having a variety of private material turned over to the FBI. Current language in HR 1400 also expands the definition of acts subject to investigation by broadening the scope of counter-intelligence.

This is already the current law. The proposed revision adds:

"(c) PENALTY FOR DISCLOSURE.-No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information under this section. A knowing violation of this section is punishable as a class A misdemeanor."

(From HR 1400, Sec. 743. COUNTERINTELLIGENCE ACCESS TO TELEPHONE RECORDS)

Not only is this provision a threat, but there is neither a reasonable length

of time after which such information may be given, nor is there any exception for disclosing the information to another (the information shall not be disclosed to **\*\*ANY PERSON\*\***), including priests or doctors.

When rumors of "national security implications" arose in some of the Secret Service raids last year, it takes little imagination to see the "act first apologize later (if ever)" mentality in action, snooping through records and vague "transactional information." The proposed wording constitutes a threat by adding a level of secrecy to investigative power.

Jim Thomas

---

## **✂ Dissemination of confidential information**

<HCART@vax.oxford.ac.uk>

Tue, 9 JUL 91 09:13:52 BST

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de>  
in [Risks 12.03](#) argues quite reasonably for a Code of "Discourse Ethics".  
and comments on

"... the trust which I assume my communication partners follow..."

While his proposed Code would meet a real need, I am afraid Klaus's own position is weakened when he writes:

> I personally just received Bill Gates memo on Microsoft's  
> performance and future problems; .... I assume  
> that Bill Gates will not be glad that I had it.

Probably not.

> I am highly sure that the  
> community in which I received this information is trustable, and they and I  
> will not uncover any details...

Except that this "trustable community" is already circulating what they know to be confidential information to Klaus, and, presumably, to others.

Doubtless it was inept of Microsoft to allow their e-mail to be intercepted, but if the purpose of those publicising the interception is to expose flaws in the e-mail system, surely the right course is to deal with Microsoft, not to disseminate the information more widely. Those, like Klaus, working in security, have an justifiable interest in security holes uncovered by others. However, circulation of the actual information pulled through these holes in no way helps to seal them. Indeed, it must give rise to serious doubts about the motives of those who retransmit mail to which they have no legitimate access.

Hugh Cartwright. Physical Chemistry, Oxford University, UK.

---

## ✂ Review of "TERMINATOR 2: Judgment Day"

<rmehlman@grumpy.span.nasa.gov>

Sun, 7 Jul 91 22:44:23 PDT

The computers have no BUGS.

[You were expecting, maybe, realism? PGN]

---

## ✂ Re: Computers and Exporting

Vadim Antonov <avg@hq.demos.su>

Sat, 15 Jun 91 17:15:46 +0300 (MSD)

>Take for instance the DES export restriction. Sources for DES have been  
>posted on Usenet.

The source codes and formal descriptions were publically available in USSR long before that posting. I've first seen it being a student and hacking some Unix sources about 1982. Isn't it stupid to continue insisting on export restrictions of the well-known technology?

(I remember our military instructors (military education was mandatory in USSR, sigh) talking about tactical characteristics of Soviet aircrafts referring to the American intelligence sources! Surely, these data were "secret" inside USSR! Familiar scenario, isn't it?)

Vadim Antonov, DEMOS, Moscow, USSR

---

## ✂ Re: Formalism vs Experimentation

Vadim Antonov <avg@hq.demos.su>

Sat, 15 Jun 91 19:34:11 +0300 (MSD)

I tend to agree that formal methods is the useful thing for practical programming; but it's silly to limit CS education by (or to focus it at) formal methods. May be I'm a heretic but there is no such thing as a "programmer". Programming is always a marginal discipline - any real program deals with

a) hardware (I'm worrying why programmers are ignorant in hardware design methods; say the modern buzzword "object-oriented" is nothing more than the sixty-years-old method of modular hardware design. Anyone having experience in digital hardware design have no troubles with parallel programming, etc. Understanding HOW hardware does work is necessary for any good programming.)

b) humans (I dunno why, but programmers often tend to design really anti-human user interfaces. Psychology is the thing most programmers needs to be familiar with. I also think the most programmers should at least have some sense of taste. I got tired looking at the ocean of tastelessness of Messy-Dossy bells and whistles. Good English (or anything else :-)) is not the last part of good documentation.)

c) mathematics (Absolutely necessary in numerous well-investigated fields like numeric computations and syntax analysis AND useful as a mean to improve analytical thinking.)

d) poligraphy (Text-processing is the daily routine of most programmers).  
[Yes, NOT POLYGRAPHY!]

e) business and management (Teamwork, planning and market estimations are necessary things to make something successful - who wants to spend his life creating programs nobody wants to pay for? Still, management often is the second profession of ex-programmers.)

f) specific knowledges in application's domain. (If you're creating a program for robots controlling machine you need to know some mechanics, aren't you.)

\*) after all anybody could note a dozen more things useful in programming.

As you can see the "ideal" programmer should be really universally educated and the modern education is overly concentrated on formal side of programming. Someone noted the Soviet system of education, well... It's really mathematically-based and produces good puzzle-solvers. The "educational" programming suffers from puzzle nature of problems students are used to solve. Real problems are different. Even systems programmers very seldom needs to invent algorithmic tricks. The best solution is the simplest one, not the most tricky and "efficient".

The formalized CS education we have in Soviet Union yields really awful results - for example the quantity of grads capable to write real programs is about 2-3% after the CS Dept. of Moscow U (not the worst one, be sure) - and those students who CAN program all are self-educated hackers and as a rule they had terrible conflicts with educational authorities. Some of the most talented programmers here are still students in their 30s. Thus the practice is against Dijkstra.

Let me state that programming is not the science of coding but the art of finding solutions of non-formalized problems and expressing these solutions in explicit and clear way.

[Paragraph on gender-related matters deleted. PGN]

Vadim Antonov, DEMOS, Moscow, USSR

---

### **✂ Re: Formalism vs. Experimentation**

*Daniel Palumbo <Daniel\_Palumbo.SVMB@air25.larc.nasa.gov>  
28 Jun 91 13:29:45*

Having just concluded an effort to experimentally verify clock synchronization theory, I was drawn to this recent RISKS discussion, However, I found very little substance relating to what I thought was at issue here.

Our group at NASA Langley is concerned with validating/verifying digital flight

control systems on aircraft. One of our battle cries has been that testing (experimentation) is inadequate to demonstrate that a system is 'bet your life' correct. Formal methods (which in the U.S. means proof of correctness) is championed as an alternative.

During the course of my work with clock synchronization theory, I came to believe that experimentation is an absolutely vital part of formal methods. Experimentation can even be considered a formal method if done in a rigorous, scientific method. My more formally oriented co-workers and I have debated this issue with the general consensus (from my perspective) that experimentation is needed any time a design bumps up against the real world. Some have even suggested that experimentation is useful in establishing that a purely logical relationship is not obviously untrue before a proof is attempted.

The question which remains is, "What is the best recipe for mixing formal methods and experimentation to yield the most confidence in a design at the lowest cost?"

[dlp@air12.larc.nasa.gov]

---

### **✂ Disk based crime plan**

*Rob Boudrie <rboudrie@encore.com>*

*Fri, 5 Jul 91 14:01:35 EDT*

There is another "dark side" to this business of using "disk data" of alleged "crime plans" as evidence against a suspect. Unlike typewriting (traceable to a machine); photocopies (also traceable) and handwriting, the digital nature of computer data lends itself to tampering. There is now a virtually detection proof mechanism whereby an overzealous cop can embellish the evidence if the case is weak but (s)he "knows" that the suspect is guilty and wants to prove it. To those who say "they would never do that", I would point out that two Boston police officers were recently convicted of perjury for fabricating an informant to get a search warrant for drugs.

---

### **✂ Deleting vs. Shredding**

*Brad Templeton <brad@looking.on.ca>*

*Wed, 3 Jul 91 15:17:12 EDT*

Is there an expectation of privacy with a shredded document?

After all, it seems to me that a tool to scan in and paste together slices from a single slice shredder (as opposed to the multi-slice ones that just leave little bits of chaff) would not be hard to create. I fully expect that the intelligence types have already built them, although it is unlikely that they would be released to the public.

I wonder how the courts would react to evidence that was a re-combined shredded document?

---

✉ **Re: The Risks of Undelete and the Law ([RISKS-12.02](#))**

Steven Tepper <[greep@speech.sri.com](mailto:greep@speech.sri.com)>  
Wed, 3 Jul 91 12:59:46 PDT

When I worked for the government (a number of years ago) I was told that to dispose of a magnetic tape containing classified information you either had to write over the tape twenty times or burn it. -greep

---

✉ **Re: The Risks of Undelete and the Law**

William Ricker <[wdr@wang.com](mailto:wdr@wang.com)>  
Mon, 8 Jul 91 19:51:43 EDT

In comp.risks Ron Dippold writes: [...]

>The court soundly, and IMO correctly, rejected this claim, analogizing the  
>retrieval of the deleted file data (by an FBI agent who was a computer expert)  
>to deciphering a coded message in a diary, after the diary was obtained under  
>a valid subpoena.

Since you say "IMO" [In My Opinion] not "IMHO" [~ Humble ~], do you mean to imply you are an attorney specializing in Constitutional Appellate matters, or a professor of same?

Do you say "correctly" because

- A\* there was sufficient other evidence to convict, and thus he shouldn't be let free on a technicality?
- B\* the police had specifically listed the computer on the search warrant, and thus the "expectation of privacy" has been breached legally under warrant after due process consideration of probable cause in the warrant hearing.
- C\* the new supreme court would gladly shed some light into the penumbra of the 9th amendment and the right to privacy, anywhere "stare decisis"\*1\* doesn't apply as well as some where it does, and thus this probably won't be overturned on appeal?  
[\*1\* "let the decision (precedent) stand"]
- D\* the \_Katz\_ "expectation of privacy" should be based on what a technically competent expert witness would expect, not what a common user would expect?

This particular case does sound, IMHO, as if "harmless error" could be the finding on the privacy issue, for the first and second reasons (A&B). The allusion to locked/encrypted diaries seized under warrant as precedent makes me suspect B. I would be disheartened if however the finding were that the technical accuracy of the user's expectations were actually material to their coverage by \_Katz\_.

Spurious claims to privacy (e.g. the very recent case of a paper bag of drugs in the car, 89-1690, California v. Acevedo, where accused granted permission to search the car, but claimed no permission to

open the bag was implied and that warrantless search of the bag was a violation of 4th) are to be rejected, IMHO.

However, again IMHO, where even guilty parties really did believe they had privacy, such as the instant Pennsylvania felony kidnap & murder case and Poindexter and North deleting their incriminating ContraGate PROFS messages only to have the IBM mainframe backup tapes read by the House/Senate committees, the 4th/9th penumbra should grant them \*criminal\* evidentiary protection commensurate to their expected privacy. The Senate of course has the right to read government property, and civil/commercial litigation has much looser rules of evidence, where I would expect backups & restorals to be admissible.

(The ContraGate tapes may have been subpoenaed specifically, in which case the Diary Under Warrant might apply, and void the expectation; I would have to read (a) the diary precedent and (b) the subpoena to have any confidence in an opinion.)

I wonder if the appellant convict briefed any surveys on how many users read their manuals or know about UNDELETE utilities?

I wish the convict could appeal this one to the old Warren court; I'd like to know whether Douglas would have found this within his Penumbra, as I think he might have (depending on the facts). The Rehnquist court probably won't even look at it, unless as a vehicle to chip away at the penumbra -- which would be patently abusive, since it can be easily disposed of as a harmless error, since the physical evidence was enough to convict, so original poster tells us.

[Caveat: I'm not an attorney, let alone one specializing in constitutional issues. Hence IM\*H\*O above. But I did take two classes on it in college and have tried to keep up on recent opinions since; opinions.supreme-court from UUNET helps there greatly, especially the \*.S syllabus files.]

/s/ Bill Ricker            wdr@wang.wang.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 12: Issue 5**

**Friday 11 July 1991**

## Contents

- [TRW Accused of Exploiting Consumers](#)  
[PGN](#)
- [Dissemination of confidential information](#)  
[Adam Curtin](#)
- [Phone disruptions](#)  
[Ed Andrews](#)
- [\(Im\)probability theory](#)  
[By Arthur Salm](#)
- [Leaking of Gates memo not an IT risk](#)  
[Henry J. Cobb](#)
- [Coding bug](#)  
[Dennis L. Mumaugh](#)
- [Re: A RISKy night in Georgia](#)  
[Trevor Kirby](#)  
[Bruce Perens](#)  
[Paul Smee](#)
- [Risk Preferences \[Research effort!\]](#)  
[Kevin Crocker](#)
- [FINAL CALL, COMPUTING & VALUES CONFERENCE, AUG 12-16](#)  
[Walter Maner](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***✉* TRW Accused of Exploiting Consumers**

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Thu, 11 Jul 91 15:49:53 PDT

Six states have sued TRW Inc., charging that its credit bureau division secretly grades consumers on their bill-paying ability -- sometimes with inaccurate information -- and sells confidential mail to junk mailers. The NY State suit also charges TRW with providing inaccurate information about consumers to banks and other credit grantors, which often results in denied credit. Texas, Alabama, Idaho, Michigan, and California have filed another suit in State District Court in Dallas TX. (Reuters report in the San

Francisco Chronicle, 10Jul91, p.C1)

---

## ✂ Dissemination of confidential information

Adam Curtin <adam@ste.dyn.bae.co.uk>

Thu, 11 Jul 91 14:07:43 GMT

In [RISKS-12.03](#), Klaus Brunnstein mentions:

- > I personally just received Bill Gates memo on Microsoft's
- > performance and future problems; .... I assume
- > that Bill Gates will not be glad that I had it.

And in [Risks 12.04](#), Hugh Cartwright comments:

- > Doubtless it was inept of Microsoft to allow their e-mail to be intercepted,
- >but if the purpose of those publicising the interception is to expose flaws in
- >the e-mail system, surely the right course is to deal with Microsoft, not to
- >disseminate the information more widely.

Although it doesn't affect the points made by either party on this topic, this does not seem to be a good specific example, for in the "US View" column in the British trade paper "Computing" (4th July 1991), Tom Foremski looks at the recent spate of industry "leaks", and describes Gates' memo as having been "leaked to a Silicon Valley newspaper" and suggests that "[IBM's John Akers' comments and] Gates' memo were deliberately leaked as US computer companies learn from the White House how to manipulate the media." and describes how "... Gates' memo played an important role in defusing overblown investor confidence in Microsoft."

Foremski contrasted this underhand method of reducing stock price with other methods which could lead to panic stock dumping, and described the cost of the defusing: "Microsoft investors dumped stock when they read the newspaper report and the company's share price fell 7% in value in just one day. Gates owns about one-third of Microsoft, a paper loss to him of more than \$320 Million."

Adam

---

## ✂ Software Bugs Blamed for Telephone Outages [Excerpted by PGN]

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

10 Jul 91 10:30:55 U

COMPUTER MAKER SAYS TINY SOFTWARE FLAW CAUSED PHONE DISRUPTIONS  
(EDMUND L. ANDREWS, N.Y. Times, 10 Jul 91)

WASHINGTON A manufacturer of telephone call-routing computers said Tuesday [9Jul91] that a defect in three or four lines of computer code, rather than a hacker or a computer "virus," appeared to be the culprit behind a mysterious spate of breakdowns that disrupted local telephone service for 10 million customers around the country in late June and early this month. In congressional testimony [...], an official of the manufacturer, DSC

Communications of Plano, Texas, said all the problems had been traced to recent upgrades in its software, which had not been thoroughly tested for hidden "bugs."

Although the telephone companies that experienced failures were using slightly different versions of the software, the company said, each version was infected with the flaw. "Our equipment was without question a major contributor to the disruptions," Frank Perpiglia, DSC's vice president for technology and product development, told the House telecommunications subcommittee. "We must be forthright in accepting responsibility for failure." The flaws disclosed Tuesday are a dramatic example of the disastrous consequences that can flow from tiny software glitches buried amid millions of lines of computer code. [...] In making what seemed to be an innocuous change, he said, DSC dropped several algorithms, or processing instructions, that apparently caused the computers to go berserk when they experienced routine malfunctions.

The flawed software was shipped by DSC beginning in March and installed at different times by the phone companies. Officials do not know why the system breakdowns did not begin until June or why they occurred within a short time span.

In response to the breakdowns, the Federal Communications Commission on Tuesday announced it was assembling a special team to investigate issues of network performance. The FCC also said it would meet with representatives from all parts of the communications industry to address issues raised by the recent disruptions, including risks facing the networks and the way technical standards are set.

At the House hearing, officials at Pacific Telesis Group and Bell Atlantic, which own the telephone companies that experienced the trouble, said they were almost certain that the "silver bullet" behind the problems had been identified. "We have found the culprit that caused the serious service disruptions," said Ross Ireland, general manager of network services for Pacific Bell, the telephone subsidiary of Pacific Telesis. Working with DSC, engineers at Pacific Bell were able to duplicate the malfunctions that occurred and successfully tested software containing corrective "patches." But telephone officials cautioned that they may still not have all the answers, and they plan further tests.

Telephone company officials emphasized that all the evidence thus far points away from the likelihood of computer viruses or sabotage by computer "hackers." "To this date, we have found absolutely no evidence of sabotage or a virus," said Fred D'Alessio, vice-president for operations and engineering at Bell Atlantic.

But other troubling questions remain. It is still unclear, for example, whether the highly complex computer systems that run today's telephone networks have been tested rigorously enough.

Officials at DSC admitted that they had not put the software upgrade through a customary 13-week test, because the change entailed only a few lines of new code. "In hindsight, that was a huge mistake," Perpiglia said.

Telephone company officials said they continue to have confidence in Signaling System 7, the basic design of the advanced new network management systems being installed by all the regional Bell companies. But they did not rule out the possibility of more fundamental design flaws.

[One moral of the story is of course that even a one-line change can sink the ship... But there is a more fundamental question for RISKS-motivated folks: can there be adequate assurances that the

system will not have such fault modes? Even the most elaborate testing in the testbeds will not always exhibit the stranger fault modes, particularly those that are dependent on subtle distributed control interactions, timing, load, etc. PGN]

---

## ✂ (Im)probability theory

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

Thu, 11 Jul 91 9:13:16 PDT

INSIDE PEOPLE `Why We Know What Isn't So', By Arthur Salm, Copley News Service

You're about to learn something new, something that has been demonstrated, mathematically, to be true yet probably you won't believe it. Ready?

There's no such thing as a "hot hand" in basketball. Players who seem to be shooting in a hot streak or, for that matter, a cold streak are just hitting and missing at random, playing out the inevitable results of whatever each man's shooting percentage happens to be.

If a player shoots 50 percent, for example, the odds of his hitting any one shot are exactly the same as a coin toss coming up heads. That's easy enough to accept. But if you toss a coin 20 times, there is a 50-50 chance of getting four heads (or, of course, tails) in a row, and a 25 percent chance of getting five in a row. Should you see a basketball player with a 50 percent shooting average take 20 shots in a game and, at one point, hit five in a row, it's almost impossible not to conclude that he's "hot."

The player himself will no doubt say that when he's hot he feels more relaxed, that he just "knows" that the ball is going in. Yet, although analysis of shooting patterns has shown that his chances of hitting a shot after just having hit another are exactly the same as when he has just missed, try to convince him. You're not convinced either, are you?

(Neither is the Boston Celtics' Red Auerbach: "Who is this guy?" he said of the author. "So he makes a study. I couldn't care less.")

This, "The Clustering Illusion," is one of the many psychological phenomena discussed in Thomas Gilovich's "How We Know What Isn't So: The Fallibility of Human Reason in Everyday Life" (The Free Press: 194 pages; \$19.95). "Random distributions seem to us to have too many clusters or streaks of consecutive outcome of the same type," Gilovich writes, "and so we have difficulty accepting their true origins. The term illusion is well-chosen because, like a perceptual illusion, it is not illuminated by repeated examination."

Gilovich says that people do not hold questionable beliefs simply because they aren't supplied with relevant data. Rather, we tend to be unduly influenced by expectation, and to misinterpret the data we have: "It is widely believed that infertile couples who adopt a child are subsequently more likely to conceive than similar couples who do not. Clinical research has shown this to be untrue."

Why do people believe it? Because they expect it to be so. No one notices when an infertile couple adopts and does not subsequently conceive. We tend to count only the hits, and not the misses.

Another good example is that of "precognition."

You'll happen to think of your former roommate, and the next day she calls; you dream of death and two days later Uncle Murray keels over. Amazing! Except that every day hundreds of random thoughts whiz through our heads,

largely ignored and certainly forgotten unless statistically, "until inevitably" one jibes with reality. Then it's, "It was so weird I just had a feeling." Never mind the 2,878 other "feelings" that have come and gone and predicted nothing.

(And what if Uncle Murray had cashed in three days later? Four days? Five weeks? It's so open-ended that you can't lose: Either "you had a feeling about it just recently" a period of time to be determined in retrospect in which case it's determined to be extrasensory perception; or you didn't, making it a non-event signifying nothing.)

Ironically, these misperceptions are the result not of human frailty but of the very abilities that make us human: Pattern recognition and the ability to connect cause and effect.

"Many of the mechanisms that distort our judgment," Gilovich writes, "stem from basic cognitive processes that are usually quite helpful in actually perceiving and understanding the world."

Unfortunately, so powerful is this tendency that we tend to overgeneralize to see patterns where none exists, to insist that an effect be paired with a cause (if no plausible cause is evident, glom onto an implausible one) ... in short, to impose order upon chaos.

The implications of misguided reasoning, Gilovich points out, go beyond the NBA and betting pools among adoptive parents' friends.

Misunderstanding of regression (extreme results, on a second test, tend to deviate toward the norm) can lead dying patients, tragically, to an unshakable reliance on alternative medicines: Since they tend to resort to them when at their worst, they will almost assuredly feel better soon after administering the quack remedies.

Open-endedness also comes into play here: If a patient miraculously recovers, as happens occasionally, the alternative medicines get credit; if the patient dies, he started the new program "too late."

---

### **✂ Leaking of Gates memo not an IT risk.**

*Henry J. Cobb <hcobb@fly2.Berkeley.EDU>  
Wed, 10 Jul 91 00:56:24 PDT*

Mr Gates should have expected a memo he sent to all of his employees to be quickly made public. The only difference being that the e-mail memo would need to be printed by a Microsoft employee before being handed off to the press.

I suspect that Gates himself planned the leak for the publicity value.  
(Perhaps to distinguish himself from the other Gates in the news? :)

Henry J. Cobb hcobb@fly2.berkeley.edu SFB Tyrant  
Ph# (415) 233-7432 6527 Morris Ave. El Cerrito, Ca 94530

---

### **✂ Coding bug (Minow, [RISKS-12.03](#))**

*Dennis L. Mumaugh <dlm@cuuxb.att.com>  
Wed, 10 Jul 91 15:42 CDT*

In [RISKS-12.03](#), Martin Minow writes on finding a coding bug in the Time Server Daemon:

```
/* this piece of code is critical: DO NOT TOUCH IT */
...
i++
if (i = j)
    j++;
...
```

And had some reflections: [...]

I wish to make a couple of comments:

The new ANSI C compiler package provided by AT&T UNIX Systems Laboratories (USL) has added features to lint (C semantic error analyzer) to provide warnings about this and other common coding errors (legal but not wanted). These additions were originally developed by the people supporting the switching machines software (5ESS). C Language tools are available but not used (such as lint) to point out the bad code cited above.

The problem is two-fold: First the UNIX paradigm of separating semantic error analysis into a separate program (e.g. lint) means that the developer must take special action to discover the potential; problems. Second, designing a language to use a minimal number of characters (e.g. C) and overload their meaning, causes potential errors due to mind sets and patterns. Note that C++ is even worse (by design) in overloading and attributing meaning - variables are type converted (e.g. string to integer) without warning.

The RISK is that most programmers never lint their code, much less use the other available tools. The infamous network outage the AT&T had last year might have been found if the code had been checked with a special version of lint.

=Dennis L. Mumaugh, ATT Computer Systems, Computer Systems Technical Services, Lisle, IL ...!{att,attmail}!cuuxb!dlm OR dlm@cuuxb.att.com

[For archivalists gathering lint lore, see [RISKS-9.54](#) and 56.]

---

### **re: A RISKy night in Georgia (Robert E. Van Cleef)**

*Trevor Kirby <Trevor.Kirby@newcastle.ac.uk>  
Thu, 11 Jul 91 11:43:22 BST*

In [Risks-12.04](#) Robert E. Van Cleef writes :-

```
>To protect the child from being recognized, they are doing something to the
>video of his face so that it consists of several large squares that change as
>he moves. This seems to be the standard way to hide things on TV now.
>Is this safe? [...]
```

The answer is the human eye can sort it out. Just try squinting at the picture

and it becomes recognisable. It might prevent the film being used as evidence in a court of law but provides minimal protection against people who know you.

TRev

---

### **✂ Re: hiding a face on television**

*pixar!news@ucbvax.berkeley.edu <bruce@pixar.com>*

*Thu, 11 Jul 91 14:29:49 PDT*

The process used to hide a face on television is called "pixellation". An area of the screen is imaged at a reduced resolution. Image processing can allow one to smooth the image, and make it somewhat more recognizable, but does not recover lost information. There IS sometimes a way to recover more information:

If the sampling method used to make the squares is simple point sampling of a single point under the square, one could recover some of the lost information by watching the face MOVE under the squares and tracking the position and value of the sample points. These could then be combined into a still picture. If the value of the square is an average of the pixels under it, this gets harder. If there isn't much movement, or there are too few squares, you won't have enough pixels.

You can also recover the original voice from those voice-distorter boxes. Most of the modern ones use commutation, and I think older ones used a hetrodyne. Both processes can be reversed.

Defeating this kind of thing takes an engineer with the right equipment, and a willingness to put in the time to guide the process manually.

Bruce Perens

---

### **✂ Hiding a face on television**

*Paul Smee <P.Smee@bristol.ac.uk>*

*Thu, 11 Jul 91 15:16:14 BST*

> Is this safe?

Seems to depend on the version of the video processor used. Certainly, with the earlier versions at least, you could get a very clear visual image of what was being hidden by simply squinting while watching the picture. Popular folklore, over here at least, had it that the image you got WAS in fact a reasonable reconstruction of what they were trying to hide, and at least one of the broadcasters paid lip service to this by switching to a different video processor which was said to garble things more efficiently. A good artist (or someone with a PhotoFit identification kit) could of course convert their visual impression to a hardcopy one.

There was always the question of how accurate this visualisation effect

was. The problem being, of course, that the human mind tends to fill in details that it can't see but that it knows should be present. So, is the visualisation really an accurate reconstruction of what they are trying to hide? To my mind, this question is a red herring. If the impression is accurate, then you are (potentially) endangering the person you are trying to protect. If the impression is inaccurate, it is still likely to resemble **SOMEBODY**, so putting them at risk.

(I'd guess that the latter case, inaccurate mental reconstruction, would probably be worse, in fact. I'd suspect that if the image you get is really due to your brain 'filling in' the missing parts, it would be likely that it is using people you know for reference.)

Paul Smee, Computing Service, University of Bristol, Bristol BS8 1UD, UK  
P.Smee@bristol.ac.uk - ..!uunet!ukc!bsmail!p.smee - Tel +44 272 303132

---

### **✂ Risk Preferences [Research effort!]**

*Kevin Crocker <risk@cs.athabascau.ca>  
11 Jul 91 22:43:25 GMT*

Hello everyone! I'm doing some research on Risk Preferences (specifically computer users attitudes towards risks - both endogenous and exogenous) and am seeking some volunteers to complete a survey.

If you are interested in participating in this endeavour you can ftp the files from:

131.232.10.8 (aupair.cs.athabascau.ca) in the directory

/risk/ps for the postscript files  
/risk/txt for the text files, and  
/risk/scr for the screen files.

Please make sure that you take all the files in whichever form you wish. Each directory has several files in it.

Please also e-mail me telling me what you took so that I can keep track of what's what! risk@cs.athabascau.ca

Thanks for your indulgence and assistance.

Kevin Crocker, Assistant Professor, Finance Studies, Athabasca University

[If you cannot FTP, contact Kevin, NOT RISKS! Also, I presume  
KEVIN will share any interesting results with all of us. PGN]

---

### **✂ FINAL CALL, COMPUTING & VALUES CONFERENCE, AUG 12-16**

*Walter Maner <bgsuvax!maner@cis.ohio-state.edu>*

12 Jul 91 03:00:52 GMT

FINAL CALL FOR PARTICIPATION  
N C C V / 91  
THE NATIONAL CONFERENCE ON COMPUTING AND VALUES  
August 12-16 in New Haven, Connecticut USA

o CURRENT STATUS

The workshop structure of N C C V / 91 limits participation to approximately 500 registrants, but space is still available at this time (mid-July). Registration is \$225 for the full conference, \$100 for any of the special one-day workshops. Limited scholarships are available for persons with disabilities. Deeply discounted motel rates (Quality Inn, 203/387-6651) and air fares (USAir Gold File #36470000) remain available.

o MORE THAN 50 DISTINGUISHED SPEAKERS

Ronald E. Anderson, Daniel Appleman, John Perry Barlow, Tzipporah Ben Avraham, Tora Bikson, Timothy Binkley, Della T. Bonnette, Leslie Burkholder, Terrell Ward Bynum, David Carey, Jacques N. Catudal, Gary Chapman, David Chaum, Frank Connolly, Marvin Croy, Peter Danielson, Dorothy Denning, Peter Denning, Charles E. M. Dunlop, Batya Friedman, Ken W. Gatzke, Richard Gordon, Donald Gotterbarn, Michael S. Hart, Barbara Heinisch, Deborah Johnson, Mitch Kapor, Isaac Victor Kerlow, John Ladd, Marianne LaFrance, Ann-Marie Lancaster, Paul Lansky, Doris Lidtke, Walter Maner, David H. Martin, Dianne Martin, Keith Miller, James H. Moor, William Hugh Murray, Barbara Nessim, Peter Neumann, George Nicholson, Helen Nissenbaum, Daniel Ort, Judith Perrolle, Amy Rubin, Lillian F. Schwartz, Sanford Sherizen, John Snapper, Kenneth Snelson, Eugene Spafford, Richard Stallman, T.C. Ting, Willis H. Ware, Sally Webster, Vivian Weil, Joseph Weizenbaum, Terry Winograd, Richard A. Wright, and Bob Zenhausern

o 18 FOUR-DAY WORKSHOPS ON SIX MAJOR THEMES (MAIN TRACKS)

- Computer Privacy & Confidentiality
- Computer Security & Crime
- Ownership of Software & Intellectual Property
- Equity & Access to Computing Resources
- Teaching Computing & Values
- Policy Issues in the Campus Computing Environment

o 7 ADDITIONAL ONE-DAY WORKSHOPS (SHORT TRACKS)

On August 13th

- Short track on philosophical and ethical issues
- Short track on campus computing issues

On August 14th

- Short track on legal and governmental issues
- Short track on business and computer ethics issues
- Short track on ethical issues in city government computing

On August 15th

- Short track on issues of accessibility for persons with disabilities
- Short track on software ownership issues

- o COMPUTER ART BY WORLD-FAMOUS ARTISTS
- o COMPUTER MUSIC BY A NATIONALLY KNOWN COMPOSER
- o FILM FESTIVAL ON COMPUTING AND HUMAN VALUES
- o EXTENSIVE EXHIBITS
  - Books and articles
  - Organizations and resources
  - Hardware and software
  - Adaptive technology

N C C V / 91 is funded in part by the National Science Foundation and hosted by the Research Center on Computing and Society and Southern Connecticut State University.

TO REGISTER IMMEDIATELY and assure yourself of a place at N C C V, please send a check payable to "B G S U" for \$225 (full conference) or \$100 (one-day) to

Professor Walter Maner  
Dept. of Computer Science  
Bowling Green State University  
Bowling Green, OH 43403 USA

FOR ADDITIONAL INFORMATION and literature, contact Professor Maner as follows

BITNet MANER@BGSUOPIE.BITNET  
InterNet maner@andy.bgsu.edu (129.1.1.2)  
Fax (419) 372-8061  
Phone (419) 372-8719 (answering machine)  
Phone (419) 372-2337 (secretary)



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 12: Issue 6**

**Tuesday 16 July 1991**

## Contents

- [Bay-Area Long-Distance Service Disrupted again!](#)
- [Computer Showers a Briton with Gifts](#)  
[Henry Cate III via Mark Brader&rec.humor](#)
- [Computer "assistance" in the UK Grand Prix](#)  
[Brian Randell](#)
- [Re: auto telemetry records](#)  
[Erik Nilsson](#)
- [Free \[Canadian\] Money?](#)  
[Mark Batten](#)
- [Nitwit ideas \(Niven and Pournelle\)](#)  
[Clive Feather](#)
- [Puzzle boxes for critical device interfacing](#)  
[Ross Williams](#)
- [U.S. Electronic Data Move Challenged on Privacy Issue](#)  
[NYT via Jeff Helgesen](#)
- [NPTN Infosphere Report](#)  
[Sue Anderson](#)
- [Re: Risks of Posting to RISKS](#)  
[Chuck Dunlop](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***⚡* Bay-Area Long-Distance Service Disrupted (again!)**

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

*Tue, 16 Jul 91 9:08:41 PDT*

At 9:29am on 15 July, a US Sprint fiber-optic cable was cut by a construction crew working at Tassajara Road near Interstate 580 in the San Francisco/Oakland East-Bay area. Repairs were completed 3.5 hours later. Long distance calls from 415 and 408 area codes were affected. In the interim, some Sprint customers were rerouted through AT&T's long distance network. However, this caused 'congestion problems' [for both AT&T and Sprint!]. This was the third outage in the Bay Area this month. [Source: San Francisco Chronicle article,

16Jul91, by Carl T. Hall]

---

**COMPUTER SHOWERS A BRITON WITH GIFTS (from rec.humor)**

Mark Brader <msb@sq.com>

Tue, 16 Jul 91 05:55 EDT

[NY Times via, at least, Henry Cate III, meo@dixie.com, and Mark Brader, SoftQuad Inc., Toronto, utzoo!sq!msb, msb@sq.com]

According to a posting in rec.humor, the following story appeared in the New York Times in April 1972.

COMPUTER SHOWERS A BRITON WITH GIFTS

Eveashan, England. -- Joseph Begley saved 2,000 cigarette coupons and mailed them in to a British cigarette company in order to get a watch. When the watch didn't arrive he wrote and asked why.

Back came three watches. Mr. Begley only wanted one so he mailed back the other two. The next day 10 parcels arrived from the cigarette company. The following day 18 parcels arrived. The day after that 10 more parcels came.

All were trade-in gifts given by the cigarette company in exchange for coupons Mr. Begley never had. Among the gifts were three tape recorders, a doll, a golf bag, two electric blankets, a cot, saucepans, a pressure cooker, and long-playing records.

Mr. Begley wrote a long, pleading letter to the company asking them to stop. In the return mail came a reply saying: "It was a computer error."

The company gave Mr. Begley 10,000 coupons in compensation for his troubles. With these Mr. Begley ordered some tools and a bedspread.

He received a plant stand and two stepladders.

---

**Computer "assistance" in the UK Grand Prix**

<Brian.Randell@newcastle.ac.uk>

Tue, 16 Jul 91 10:34:11 BST

Today's issue of the Independent (a UK national newspaper) has an article about the British Formula 1 Grand Prix held at Silverstone on Sunday (14/7/91) which was won by Nigel Mansell, with Ayrton Senna running out of fuel within sight of the finishing line. The article contains the following paragraphs:

For the second successive week, Senna was fooled by a computer read-out. In France, he was led to believe that the car was low on fuel. It was not. At Silverstone, he was told it had plenty. It had not. Mansell, meanwhile, was attempting to outwit the gearbox computer which left him stranded on the last lap of the Canadian Grand Prix.

He said: "It was just like Canada. I felt it just the same. But you learn from experience. I was able to identify the problem and knew what to do about it. I kept up the revs and kept it in fifth gear as long as possible.

"I'm increasingly worried about being controlled by computers. The driver is becoming more and more the prisoner of the computer."

[Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, UK  
PHONE = +44 91 222 7923 FAX = +44 91 222 8232]

---

**✂ Re: auto telemetry records (John Moore, [RISKS-11.86](#))**

*Erik Nilsson <erikn@boa.mitron.tek.com>*

*Thu, 20 Jun 91 17:44:13 PDT*

One of our customers makes a part used with air bags. The controls for air bags use accelerometers to determine when an air bag should be deployed. Apparently, the speed of the vehicle is also factored into the deploy decision.

Because the auto companies are afraid of lawsuits over faulty deployment, the airbag control includes a flight-recorder-like telemetry record. It isn't clear how accurate this record is. The advice our customer gave us was, if we were in an accident, find and destroy the black box as soon as possible.

- Erik Nilsson erikn@boa.MITRON.TEK.COM

---

**✂ Free Money?**

*Mark Batten <mark@shl.com>*

*Wed, 10 Jul 91 15:42:05 EDT*

A few weeks ago (June 1991) I saw a news article on Canada's NewsWorld (a 24 hour news channel) which related the following story (paraphrased from memory):

A man decided to use his Royal Bank ATM card to get some money out of his account. He used a Co-op (trust company, I believe) ATM machine. He entered his id number and received the money he requested. He then noticed that there was a problem with the printed receipt. It was missing the balance, a transaction number, and similar items. He checked the ATM card and discovered that he had accidentally used his Bell Calling Card rather than the Royal Bank card he intended. He immediately reported the problem to the Co-op branch. They called in the Royal Bank and Bell to determine what had happened.

It turns out the money he received had not been deducted from his account. It had come out of the Co-op's general fund or something like that. The Co-op spokesperson assured the reporter that the problem had been determined and resolved by the end of the day and that it was unique to Bell Calling Cards and the Co-op's ATM software.  
(It was not clear from the report but I believe this happened in Toronto.)

Does anyone know anything more about this?

Mark Batten mark@shl.com uunet!shl!mark

---

### **✂ Nitwit ideas (Niven and Pournelle)**

*Clive Feather <clive@x.co.uk>*

*Mon, 15 Jul 91 12:07:09 BST*

Re: Patriot missile specifications, Robert I. Eachus, [RISKS-12.01](#), "This is NOT a failure of design or specification or production, it is often the result of someone trying something because he is dead anyway if it doesn't work. Such successful tactics quickly become the normal way the weapon is used."

I am reminded of something from *\_The\_Mote\_in\_God's\_Eye\_* by Niven and Pournelle:

"It's a nitwit idea. Nitwit ideas are for emergencies. The rest of the time you go by the Book, which is mostly a collection of nitwit ideas that worked."

Clive D.W. Feather, IXI Limited, 62-74 Burleigh St. Cambridge CB1 1OJ UK  
clive@x.co.uk Phone: +44 223 462 131

---

### **✂ Puzzle boxes for critical device interfacing**

*Ross Williams <ross@spam.ua.oz.au>*

*21 Jun 91 15:18:49 GMT*

INTRODUCTION: I have had an idea for the reliable interfacing of computer systems with critical hardware that I would like to air in this newsgroup.

IDEA: The idea is to place some kind of "puzzle" between the microprocessor and the critical hardware device such that in order to activate the critical device, the microprocessor must send a complex sequence of signals, the sequence being the solution to a puzzle. I call such a device a "puzzle box".

BENEFIT: The benefit of the puzzle box is that the microprocessor is far less likely to activate the critical device under failure conditions than if a simpler interface were used (e.g. address decoder and one bit latch).

GRAY CODE PUZZLE BOX: In order to avoid interface problems themselves, puzzle boxes must be extremely simple. The simplest, most efficient puzzle box I have invented consists of a row of switches wired in serial (through which the critical signal must pass) controlled by simple logic that requires the microprocessor to transmit a Gray code sequence (a "Gray Code Puzzle Box"). Thus, in order to fire the rocket, the microprocessor has to solve the Towers of Hanoi puzzle!

PROVISIONAL PATENT: I have submitted an Australian Provisional Patent

application for this invention (January 1991, June 1991) and am looking for feedback on its originality and usefulness. I am also looking for people to help manage this patent. A copy of the provisional patent application is available upon request (I can email it to you or snail mail it). The application gives an accessible description of the idea and answers common objections.

Although the idea is simple, I have chosen to patent as I view it as somewhat perverse. Engineers spend a lot of their time trying to make it EASIER for pieces of hardware to talk to each other. The puzzle box goes totally against this principle, but in doing so increases safety.

I look forward to reader responses.

Ross Williams Net: ross@spam.ua.oz.au Fax: +61 8 373-4911  
Home phone: +61 8 379-5020 (South Australian Time)  
Snail Mail: 16 Lerwick Avenue, Hazelwood Park 5066, South Australia, Australia

---

## **✂ U.S. Electronic Data Move Challenged on Privacy Issue (NY Times)**

*Jeff Helgesen <jmh@morgana.pubserv.com>  
Mon, 1 Jul 91 12:52:46 -0500*

U.S. ELECTRONIC DATA MOVE CHALLENGED ON PRIVACY ISSUE  
Fears Rise on Possibility of Scrutiny by Federal Agencies  
NY Times -- 29 June 1991

The government said Thursday that it would introduce a Federal standard for authenticating electronic data later this summer, but the announcement prompted an angry reaction from one of the leading private providers of software that protects computer data. The company, RSA Data Security Inc. of Redwood City, Calif., said the Government had failed to address fears about the possibility of a secret "trapdoor," which would permit intelligence and law-enforcement agencies to look at private data.

The issue of providing special mechanisms to permit Government access to private information has caused a growing public debate recently. Earlier this year an anti-terrorism bill in Congress called on the computer and telecommunication industries to permit Federal agencies to look at private data. But the statement was later dropped from the bill after extensive public opposition.

Government officials said that it would be possible for technical experts to examine the standard when it is released this summer and they could decide for themselves whether there were any shortcomings in the design of the standard. "It will be openly published and people can inspect it to their heart's content," said James H. Burrows, head of the computer systems laboratory at the National Institute of Standards and Technology [NIST].

He added that the new standard was not intended to encrypt computer data, and that the Government would continue to rely on an earlier technology known as the Data Encryption Standard to actually hide information from potential

electronic eavesdroppers. He said there was a project underway to develop a successor to that standard, but that it was years away from completion.

In testimony before the House Subcommittee of the Committee on Science, Space and Technology, Raymond J. Kammer, deputy director of the NIST, said on Thursday that the Government was working on final arrangements for a planned "data signature" standard that would permit electronic authentication of documents and access systems as well as protecting against computer viruses and other forms of electronic tampering.

He added that the new standard did not include capabilities for coding messages so that only one person or a group of people could read them. Mr. Kammer acknowledged that the agency's efforts to develop a standard had been, "slow, difficult, and complex." He said his agency had worked with the National Security Agency to develop the new standard and called the relationship between the two "productive." Dr. Burrows said the standards institute had relied heavily on the intelligence agency for the fundamental work that has led to the new standard.

"A public key standard would help promote communications privacy," said Marc Rotenberg, Washington director of Computer Professionals for Social Responsibility. "The problem today is that there is a legitimate concern about the role the NSA might play in the development of such a standard."

Officials at RSA, and other computer security experts, have challenged the Government standard-setting process saying that it was difficult to have confidence in the software being proposed by the Federal agencies because of security agencies' roles in the process. A number of computer security experts have said the security agency has objected to adopting the RSA standard because the system is too difficult for the intelligence agency to crack.

---

## **NPTN Infosphere Report**

*Sue Anderson <aq941@cleveland.freenet.edu>  
Mon, 24 Jun 91 15:58:16 -0400*

Below is the final version of our "Infosphere" report summary. We have formulated general question areas to which we will attempt to respond using, whenever possible, existing data. We also expect that the report will point to many avenues for further research, particularly in areas where data is simply unobtainable.

Computer networking is often heralded for its capacity to facilitate collaboration among researchers, scholars, scientists, authors, etc. We would like to capitalize on this potential... Therefore, if you have any comments on the summary below, would like to offer assistance (by making suggestions, locating/supplying information, or providing funding), or if you want more information, please feel free to contact us (addresses and phone numbers can be found at the end of the following summary).

-----

## The National Public Telecomputing Network

--

### Infosphere Report

In 1955 an important transition occurred in American society. In that year, for the first time, more than half of our work force became "information workers" -- people whose main activity was producing, processing, or distributing information, and producing information technology.

In the 1980's, with the development of low-cost personal computers and high-powered computerized communications networks, the pace of that transition both quickened and deepened. For the first time rapid exchange of information could occur, over globe-spanning distances, within seconds, at extremely low cost. For the first time also, the average citizen had on their desktops the means to tap into those resources from their homes, schools, and workplaces.

Unfortunately, as with many preceding technologies, access to these resources developed unequally. Some individuals and segments of society were able to take immediate advantage of it; others were not (and still are not). The result is a society which appears to be entering the Information Age the way a child enters an ocean for the first time--partly in, partly out, partly fearful, partly intrigued, and not really quite sure what to do next.

This summer and fall, the National Public Telecomputing Network (NPTN), a nonprofit public computer network headquartered in Cleveland, Ohio, will be working on its first annual "Infosphere Report"--a research project similar to those conducted in areas such as economics, population growth, and the environment--which will attempt to assess the nation's capacity to effectively and equitably utilize telecomputing as a medium for meeting its information and communication needs. We are defining the "infosphere" as:

the technical and organizational environment in which the general public can remotely access computer-mediated communication and information resources.

We expect that over-time a portrait will emerge which will describe this nation's progress, with regard to telecomputing, as it encounters the information age. The report will be cumulative, comparative, and prescriptive. It will show where we have been, where we are now, what we are doing well, and where more emphasis is needed.

In general, we see the infosphere as being composed of three interactive components:

**People:** The individuals who are (or could be) using the technology and resources.

**Technology:** The hardware, software and network connections needed to access the resources (e.g., computers, modems, phone lines, network connections, etc.).

**Resources:** The communication and information facilities that can (or could be) remotely accessed via computer (e.g., databases, archives, electronic mail, computer conferencing).

The Infosphere Report will attempt to gauge our progress with regard to each of these areas. The first chapter will be an introduction describing the scope and limitations of the study. Chapters two through four will address each infosphere component: people, technology, and resources. Questions that will be addressed in these chapters include:

#### People

- Who uses the currently available communication and information resources?
- What are the general public's communication/information needs and desires?
- Do they know what's available?
- How can they find out about it?
- Do they have the knowledge and skills to use it?
- Do they have access to the necessary resources to use it?

#### Technology

- What technology exists for accessing communication and information resources?
- What is its availability and cost to the general public?
- What are its strengths and weaknesses? (e.g., ease of use, reliability)

#### Resources

- What remotely accessible communication and information resources exist?
- What are their availability and cost to the general public?
- What are their strengths and weaknesses? (e.g., quantity, quality, appropriateness)

The final chapter of the report will summarize the findings, draw conclusions, discuss implications, and make recommendations for improving our nation's ability to make use of telecomputing to effectively and equitably utilize computer-mediated communication and information resources.

The principal investigator on the project will be T.M. Grundner, Ed.D. As an assistant professor at Case Western Reserve University, Dr. Grundner was an early pioneer in the development of community-based computerized information services. His "St. Silicon Project" in 1984 provided the first data on the effectiveness of using modem equipped microcomputers to deliver community health information. His Cleveland Free-Net Project in 1986 developed the nation's first free, open-access, community computer system. As a result of the success of the Free-Net, in 1989 he founded the National Public Telecomputing Network to foster the growth of community computer systems and to link them together into a common nationwide communications and information network similar to National Public Radio or PBS on television.

The research coordinator is Sue Anderson, Ed.D. (Cand.). Ms. Anderson is a doctoral candidate at the University of Virginia with extensive background in electronic networking and computer conferencing. She will be supervising a staff of volunteer research associates from around the country in the development and analysis of the data for the report.

Persons who are interested in assisting on this project, those seeking more information in general, and (especially) potential funding sources wishing to participate in continuing support, should contact the project at:

The Infosphere Report  
National Public Telecomputing Network  
Box 1987  
Cleveland, Ohio 44106

Voice: 216-368-2733  
FAX: 216-368-5436

Internet: aq941@cleveland.freenet.edu (Sue Anderson)  
aa001@cleveland.freenet.edu (Tom Grundner)

BITNET: aq941%cleveland.freenet.edu@cunyvm (Sue Anderson)  
aa001%cleveland.freenet.edu@cunyvm (Tom Grundner)

CompuServe: 71550,2602 (Sue Anderson)  
72135,1536 (Tom Grundner)

---

### **✉ Re: Risks of Posting to RISKS**

<Chuck\_Dunlop@ub.cc.umich.edu>  
Thu, 4 Jul 91 11:33:00 EDT

In [RISKS 12.02](#), Jerry Hollombe describes our publication of his 1989 RISKS posting about the "censorship" of rec.humor.funny at Stanford University. Mr. Hollombe's piece was reprinted (with his permission) in Charles Dunlop and Rob Kling (eds), *\_Computerization and Controversy: Value Conflicts and Social Choices\_* (Boston, Academic Press, 1991, ISBN: 0-12-224356-0). (See pp.376-379).

In one section of our book, we published 3 excerpts from RISKS in order to document an important debate about a university's cutting off access to a BBS when some people found postings to be personally offensive (a continuing issue!). Les Earnest and John McCarthy criticized Stanford's censorship while Jerry Hollombe argued that the term "censorship" was inappropriate and that Stanford had a right to cut off access to any BBS. We included this debate as one short selection in an 80 page section that examines controversies about "Social Relationships in Electronic Communities".

Our anthology examines many debates about computerization pertinent to quality of worklife, productivity, system design, privacy, social control, gender bias, system security and risks, ethical codes, and social relationships on networks. However, we did not effectively anticipate this new controversy about computerization: one's ability to fairly reprint RISKS (or any BBS) postings after posters have given explicit permission!

Although Mr. Hollombe now regards his February 1989 RISKS posting as "a bit embarrassing", he acknowledges that he gave us explicit permission to reprint it in *\_Computerization and Controversy\_*, with the stipulation that a footnote

be added detailing his current position on the subject. We appreciated Mr. Hollombe's willingness to allow us to reprint his Feb. 1989 posting since it was a counterpoint to McCarthy and Ernest. Without his posting, we would only have been able to portray one side of the debate and might have dropped these particular RISKS excerpts entirely.

Unfortunately, Mr. Hollombe attributes his problem with the reprinting of his RISKS posting solely to publishers and editors, and he conveniently ignores his control over the publication. In [RISKS 12.02](#) he writes:

>The risk? The words we exchange here aren't as ephemeral as they may  
>appear on a VDT screen, so be careful what you say and how you say it.  
>You never know who might decide to package and ship it to a customer.  
>(-:

This complaint strikes us as unfair. It incorrectly suggests that Mr. Hollombe had no control over the reprinting of his RISKS postings. He knew that we wanted to "package and ship" his Feb 1989 RISKS posting to readers of Computerization & Controversy. And he consented to our doing so.

We can understand that Mr. Hollombe might now regret having given us permission; people sometimes regret all sorts of things they have agreed to under "fair" conditions. But that is very different from having his comments published WITHOUT his permission (a kind of theft or coercion). Furthermore, we printed the additional footnote that he requested (and also sent him a complimentary copy of the book). We believe that in following those procedures we were VERY FAIR to Mr. Hollombe.

At the time when we assembled the articles for Computerization and Controversy (mostly previously published articles), we discussed the copyright status of RISKS postings with Peter Neumann. It seemed then that there was no clear legal ruling regarding rights and ownership of BBS postings. We took a very conservative and respectful position in seeking permission from authors wherever possible. For example, if Mr. Hollombe had denied us permission, we would not have published his RISKS posting.

We also note that our position that editors should seek a poster's permission can have significant practical difficulties. The longer the time that elapses between BBS posting dates and the time when editors assemble materials for publication, the harder it may be to locate posters. If someone writes a book about the changing nature and debates of computer risks between 1980-2000 in the year 2005, it may be hard to locate most posters at the mail addresses in their message headers from 1985-1995 (grin).

This issue may be important to RISKS posters, as well as posters on other boards (e.g., political boards, technical and scientific boards, sex boards, personal discussion boards). In all these venues, many people may post with the expectation that their keystrokes are ephemeral, whereas some readers may see them as contributions to the public domain unless they explicitly say otherwise (e.g., through a copyright notice appended to their messages). Significantly, the heading of each RISKS volume now addresses this issue, at least in a limited context (i.e., the reprinting of postings in ACM SIGSOFT's SOFTWARE ENGINEERING NOTES).

Does anyone know the state of the law on these matters? Or the status of the controversies?

Chuck Dunlop

U of Michigan - Flint

Chuck\_Dunlop@ub.cc.umich.edu

Rob Kling

UC-Irvine

kling@ics.uci.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 12: Issue 7**

**Tuesday 16 July 1991**

## Contents

- [RISKS: US West 10x charges users](#)  
[patlo](#)
- [Houston City Hall voice-mail prank](#)  
[PGN](#)  
[S. Spenser Aden](#)
- [Re: Risks of posting to newsgroups](#)  
[Li Gong](#)
- [1992 IEEE Symposium on Research in Security and Privacy](#)  
[John McLean](#)
- [Puzzle Boxes: Reply to comments](#)  
[Ross Williams](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***RISKS: US West 10x charges users***

<[patlo@microsoft.com](mailto:patlo@microsoft.com)>  
Mon Jul 22 13:26:27 1991

Heard on KIRO radio this morning:

US West has implemented a new computer system to time long distance calls more closely. The new system, according to US West representatives, will "save long distance customers considerably in the long term." For the short term, however, it will cost them extra.

The system breaks calls down to the nearest 6-second period, rather than charging the caller for a full minute when only part was used. However, a programming error caused all bills sent out between July 7th and 10th to be computed at 10 times the normal rate. The error was not discovered until 12 days after the system became active.

US West representatives said that "customers who pay the (incorrect) bill will be credited on their next bill."

---

## ✂ Houston City Hall voice-mail prank

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

Sat, 20 Jul 91 14:42:23 PDT

Houston acquired an AT&T telephone system in 1986 for \$28M, but configured it with no passwords required for accessing voice mail. Thus, it should not surprise any of you to hear that recently a "prankster intercepted and rerouted confidential telephone messages from voice-mail machines in City Hall, prompting officials to pull the plug on the telephone system." Messages were being delivered to nonintended recipients. [Source: San Francisco Chronicle, 20Jul91, p.A5]

[Also noted by Steve Bellovin]

---

## ✂ The voice-mail shuffle at City Hall

<ADEN@vf.jsc.nasa.gov>

Tue, 23 Jul 1991 8:51:05 CDT

... A few stations even played quick snippets from one message, which appeared to be a kind of verbal "love letter" left for someone. Needless to say, the intended recipient was not the actual recipient. The perpetrator evidently would somehow try to simulate a message break tone before each misdirected message by whistling a tone on the recording.

While some of the redirected messages were, in some people's opinion, harmless, others were matters of City and State affairs, and the ramifications of these messages not being received were more than trivial. Needless to say, the service was down the next day for "upgrade modification".

As one newscast put it at the end of their story, "when you leave a message at City Hall, don't leave one you wouldn't want repeated in public."

S. Spenser Aden, Lockheed Engineering and Sciences Co. (713) 483-2028  
NASA -- Johnson Space Center, Houston -- Flight Data and Evaluation Office

---

## ✂ Re: risks of posting to newsgroups

Li Gong <li@cambridge.oracorp.com>

Wed, 17 Jul 91 16:01:27 EDT

I remember seeing a report that someone was surprised to find out that his opinion posted to RISKS, a USENET newsgroup, was quoted in a book. I just got the following message from a mailing list's book review section:

ELECTRONIC MAIL ON CHINA. Vol. 1 (February 18 to June 3, 1989) & Vol. 2 (June 4 to July 4, 1989). Edited by Esbjorn Stahle & Terho Uimonen. Stockholm: Skifter utgivna av Foreningen for Orientaliska Studier, 1989. pp. 394 & 424.

Reviewed by Zhenqin Li

This two-volume publication is very unusual, in the sense that it is perhaps the first ever book almost entirely based on articles of a Usenet newsgroup (soc.culture.china or SCC). It should be of interest to a wide readership on the computer networks ...

[Li Gong, ORA Corporation, 675 Mass Ave, Cambridge, MA]

---

## ✦ 1992 IEEE Symposium on Research in Security and Privacy

<mclean@itd.nrl.navy.mil>

Mon, 22 Jul 91 12:12:48 EDT

### CALL FOR PAPERS

1992 IEEE Symposium on                      May 4-6, 1992  
Research in Security and Privacy              Oakland, California

sponsored by  
IEEE Computer Society  
Technical Committee on Security and Privacy  
in cooperation with  
The International Association for Cryptologic Research (IACR)

The purpose of this symposium is to bring together researchers and developers who work on secure computer systems. The symposium will address advances in the theory, design, implementation, evaluation and application of secure computer systems. Papers, panel session proposals, and position papers are solicited in the following areas:

Secure Systems    Privacy Issues    Information Flow  
Network Security    Formal Models    Viruses and Worms  
Database Security    Access Controls    Security Verification/Validation  
Authentication    Data Integrity    Auditing & Intrusion Detection

### INSTRUCTIONS TO AUTHORS:

Send six copies of your papers, panel session proposals, and position papers to John McLean, Program Co-Chair, at the address given below.

We provide "blind" refereeing. Put names and affiliations of authors on a separate cover page only. Abstracts, electronic submissions, late submissions, and papers that cannot be published in the proceedings will not be accepted. Papers submitted from outside North America should be sent via Federal Express or other overnight courier service.

Papers must be received by November 8, 1991 and must not exceed 7500 words. Authors will be required to certify prior to December 20, 1991 that any and all necessary clearances for publication have been obtained. Authors will be notified of acceptance by January 24, 1992. Camera-ready copies are due not later than February 28, 1992.



posting to comp.risks on my puzzle box idea. I have also received some postings forwarded by Peter Neumann.

Because of the volume of mail, the common themes of several of the comments, and the possibility of keeping interested comp.risks readers up to date, I have decided to reply in a posting. I will quote only from those who posted, as I do not think I should quote from private email. If you send me email on this topic and are happy to have it quoted in comp.risks, please say so.

So far, I have not received any fatal technical arguments. However, some messages quote examples that may constitute prior art.

If prior art does exist, I would be interested to know how much puzzle boxes are actually used in practice in safety-critical device interfacing. Most of the "prior art" messages I received quoted applications in areas such as password protection and operating system page protection. Whether or not the puzzle box idea is original, I believe it to be useful, and would like to see it used in safety-critical systems. Judging from the reactions I have received, it seems likely that the puzzle box idea (if well known) has been underused in practice because of an erroneous perception that the technique is subject to a single-point software failure (see below).

A copy of my puzzle box provisional patent application is available by email upon request (i.e. I can email it to you).

Ross Williams, ross@spam.ua.oz.au, 18-Jul-1991

#### Single Point Software Vulnerability

-----  
Most of the mail I received stated that a system employing puzzle boxes is vulnerable to a single-point software error. Lars-Henrik Eriksson's posting is typical of the messages that raised this objection:

From: Lars-Henrik Eriksson <lhe@sics.se>

Date: Wed, 17 Jul 91 09:58:42 +0200

The microprocessor must have a program to send the proper code sequence. Both hardware and software failures might cause this program to run accidentally. It should be safer than having a single bit activate the hardware device. However, it is not clear to me that having the microprocessor send a very complicated code sequence such as the solution to the Hanoi puzzle is any better than just having it send a very simple sequence such as the three numbers 1, 2, 3. In both cases there must be a program to generate the sequence, and in both cases that program could be entered accidentally.

The essence of the objection (in the above and other messages) is that if a puzzle box is employed, there will have to be a subroutine (specifically, an address) which when executed causes the puzzle box to activate. This code structure introduces a single point vulnerability because all that needs to happen is for the Program Counter (PC) to somehow get to that address.

I thought of this problem soon after having the puzzle box idea. There is a paragraph on the topic in the provisional patent application:

Software Trigger --- A danger arises in systems that use puzzle devices if the controlling computer contains a software procedure whose job is to activate the puzzle device. The existence of such a procedure implies that the system is only as safe as the address in the program counter register of the computer. This may not be acceptable. This problem can be countered by using the results of calculations (performed in the computer) leading up to the decision to activate in the actual puzzle device activation sequence itself.

The essence of the solution is contained in the quote, but I will flesh it out further as this was the most common objection.

As far as I can see, a good way to protect systems from accidentally entering certain "dangerous" states is to engineer a tortuous path from "normal" states to the "dangerous" states. The puzzle box does this in hardware. The same trick can be pulled in software.

All of the readers raising the single point software failure objection assumed that there MUST exist a single subroutine whose execution causes the unconditional activation of the puzzle box. This need not be so.

To provide a "tortuous" software activation path, we need to create some distance in the microprocessor state space between the "normal" and the "dangerous" states. Under the above assumption, the distance is just 16 to 32 bits of highly dynamic PC register! To expand the state space, we can create a memory array called firing\_sequence.

```
firing_sequence : array[0..31] of byte;
```

At regular intervals (e.g. during interrupts (with care!)), this array could be zeroed by a routine called (say) reset\_puzzle\_box. A second routine called fire\_puzzle\_box writes the array firing\_sequence to the puzzle box output port.

In any critical system the decision to "fire" will usually be a complex one requiring a number of checks to be performed. As each successive check is passed, the system moves closer to the firing state. For a system that employs a puzzle box, the process can include writing values into the firing sequence array. Thus the various logical decisions that culminate in the decision to fire each contribute part of the "password".

In fact, under certain conditions, you can build the firing sequence into the decision code itself.

```
procedure pour_tea;
begin pour_tea
  read_io(teapot_temperature);
  read_io(cup_sensor);
  read_io(dormouse_sensor);
  read_io(mad_hatter_robot_arm_health);
  reset_puzzle_box;
  if teapot_temperature
```

---



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 12: Issue 8**

**Thursday 25 July 1991**

## Contents

- [Another false apprehension -- erroneous database information](#)  
[PGN](#)
- [Human Error Blamed for Soviet N-Plant Problems](#)  
[PGN](#)
- [Shuttle Atlantis out to launch](#)  
[PGN](#)
- [Risks of getting used to computers](#)  
[Geoff Kuenning](#)
- [Index of Known MsDos Malware: 998 viruses/trojans](#)  
[Klaus Brunnstein](#)
- [Sometimes they even warn you about the pitfalls \(self-trapping\)](#)  
[Andrew Koenig](#)
- [Smart cockpit with no backup](#)  
[Henry Spencer](#)
- [Black boxes in autos for accident "facts"](#)  
[Mark Seecof](#)
- [Re: Artificial Dissemination](#)  
[Edward Jung](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***✉* Another false apprehension -- erroneous database information**

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

*Thu, 25 Jul 91 9:04:40 PDT*

Herb Caen, the San Francisco Chronicle's chronicler of the chronic and (a)cute, starts off the 25 July 91 column with this ad infin-item:

Dennis Perry, an Oakland truck driver, and his good friend, Yvonne Kendrick -- both are black --- rented a Hertz car to drive to Maryland to visit his family. They took along his 4-yr old dgtr, Danielle, and all went swimmingly until they were stopped in white-bread Williamsburg, Iowa, for no apparent reason. The police ran a check on the car and found it listed by Hertz as stolen. It wasn't, of course, but during the 24 hours it took Hertz

to correct the mistake, Dennis and Yvonne were held in jail and Danielle went to a juvenile home. Atty. Dennis Hecht is handling the inevitable suit."

The next item was on Judge Clarence Thomas not being able to get a cab in DC. After that came another item for our series of computer-addressed mail:

Jayne Valdez of Antioch forwards a copy of PG&E's closing bill addressed to her late father, "Bob A. Speake, Deceased," with this neatly boxed encomium printed on it: "Bob Speake, deceased for the last 12 months, you had an excellent payment record. If you need to establish credit at another utility, you may use this message as a credit reference."

---

### **✦ Human Error Blamed for Soviet N-Plant Problems**

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

*Thu, 25 Jul 91 9:08:21 PDT*

Moscow -- Human error caused 20 of the 59 shutdowns at Soviet nuclear power plants in the first six months of 1991, the Trud newspaper reported yesterday. "It is not the first time that we have to admit the obvious lack of elementary safety culture in running reactors," Anatoly Mazlov, the government's head of nuclear safety, said. Mazlov reported that Soviet nuclear power plants worked at only 67 percent capacity in the first six months of 1991. [San Francisco Chronicle, 24Jul91, p.A8]

---

### **✦ Shuttle Atlantis out to launch**

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

*Wed, 24 Jul 91 9:06:22 PDT*

The 24Jul91 morning launch was scrubbed. An NPR report indicated a "faulty engine computer".

Postscript: The 25Jul91 San Fran Chronicle paper had a picture of Atlantis mission commander John Blaha and mission specialist Shannon Lucid holding their ears while fellow crew members taxied their T-38 trainers. The caption briefly mentioned the computer problem (with no details), but also noted that Blaha and Lucid's T-38 failed to start for a return to Houston! (T-38s require an external jumpstart.)

It is perhaps worth contemplating whether computer failures have now become so commonplace that newspaper folks decided there was no need for coverage of the launch scrub itself!

---

### **✦ Risks of getting used to computers**

*Geoff Kuenning <desint!geoff@uunet.UU.NET>*

*Sun, 21 Jul 91 16:02:12 PDT*

The Sunday, July 21 edition of the Los Angeles Times has a story headlined "LAPD Begins Crackdown on Computer Messages." The story reports that the new program is "aimed partly at finding and punishing" officers who sent offensive personal messages cited in the recent Christopher Commission report (issued in the wake of the Rodney King beating) as evidence of departmental racism and sexism. The program "is also aimed at stopping...even innocuous personal messages."

The story goes on to state that several officers have been assigned to the task of spot-checking daily printouts of messages. "Efforts [will be] made to find out who sent" offending messages. It also reports that "snooping by headquarters has led to a 25% decline in...traffic."

"Creating a context for the messages is...difficult because [of an] inflexible computer program," according to the article. Only chronological printouts are available, making it difficult to extract messages relating to a particular car. Messages from a patrol car are not identified as to which of two officers sent them, although sergeants, who occupy cars alone, can be uniquely identified. "The department is trying to get computer experts to write programs" that will extract messages from one car.

I see two risks here. The first, of course, is to the officers, who became so comfortable with the computer system that they forgot (or perhaps were never aware?) that their messages could be monitored. The second is to the department, which is now unable to extract useful data from their files. (This makes me wonder. Wouldn't it be useful to them in court cases to be able to extract the messages from a particular car over a period of an hour or so?)

I also wonder if the Electronic Communications Privacy Act would apply here. Did the officers have a reasonable expectation of privacy in any of their messages?

Geoff Kuenning geoff@ITcorp.com uunet!desint!geoff

---

## **Index of Known Malware: 998 viruses/trojans**

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de>  
24 Jul 91 12:38 +0100*

After weeks of work and excellent assistance of David Chess, Yisrael Radai, Alan Solomon, Padgett Peterson and some others, I just published the "Index of Known Malicious Software: MsDos systems". It covers most of the viruses and trojans reported in this arena (similar indices for Amiga and Macintosh to follow later this year). When summing up, I was deeply depressed: the index counts:

- 120 virus families ("strains") with 59 more sub-families
- with 744 viruses, variants and clones
- plus 7 trojans,
- and 228 single (non-strain) viruses
- plus 19 trojans
- \*\*\* totalling 998 pieces of malware \*\*\*

Though some people (including Alan Solomon) foresaw 1,000 viruses later this

year, the rise in figures has been underestimated. As this development is likely to continue, antivirus experts should cooperate even more strongly than contemporarily discussed.

At the same time, the July edition of VTCs Computer Virus Catalog describes

- + 8 AMIGA viruses totalling 54 viruses
- +10 Macintosh viruses totalling 20 (out of 28 existing)
- +14 PC viruses/trojans totalling 84

The disparity between "virus known" and "viruses classified" (with the aim to maintain a good quality over quantity of classification) demands other tools and methods for analysis, classification and production of countermeasures. We are working harder to a more actual version of Virus Catalog; I am glad that Mr.Jahn joined VTC (for a doctor workm on secure databanks), and that Vesselin Bonchev will join us next week for a (not yet specified) dissertation. On the Moreover, I appreciate any cooperation with serious antivirus experts.

VTC documents (Index of Known Malicious Software: IMSDOS.791; Index of Virus Catalog: Index.791; all entries classified up to now) are now available from FTP:

```
Our FTP server: ftp.rz.informatik.uni-hamburg.de
Login anonymous
ID as you wish (preferably your name)
dir: directory of available information
cd pub/virus: VTCs documents
```

Hoping that this works, I will be absent (with Auto-Reply on) on a sailing trip (with my schooner "Arethusa" which is a small replica of BLUENOSE but with staysails) until August 18. 1991. Klaus Brunnstein, Hamburg

---

### **⚡ Sometimes they even warn you about the pitfalls (self-trapping alarms)**

<ark@research.att.com>  
Wed, 24 Jul 91 22:11:38 EDT

I have a car with a built-in burglar alarm. The alarm is activated if the last door locked is locked from the outside without a key (by locking it on the INSIDE and then holding onto the door handle while closing the door). That means that it doesn't matter who leaves the car first; the alarm will still be armed at a sensible time.

Once the alarm is armed, any attempt to open a door from the inside (after breaking a window, for example) or to start the car, without first unlocking one of the doors from the outside with a key, will set off the alarm.

Do you see the pitfall? The owner's manual actually warns about it. Suppose you're sitting in the car with a passenger. You have locked the door from the inside. Your passenger gets out, locking the other door from the outside. That has just armed the alarm. It is now impossible for you to get out of the car or start the engine without setting off the alarm. With luck, you noticed this was going to happen when the "alarm" light on the center console started flashing; if you caught it in time you could unlock your door from the inside and stop it from arming. Once it's been armed, though, all you can do is get

out of the car, setting off the alarm, and then turn off the alarm from the outside by unlocking the driver's door with the key. I hope your passenger didn't take the key.

---

### ✂ Smart cockpit with no backup

<henry@zoo.toronto.edu>

Wed, 24 Jul 91 02:12:19 EDT

The May 20 issue of Aviation Week (I'm catching up on old issues) has a short piece on the avionics being planned for the USAF's new fighter, the Lockheed F-22. It's no surprise that flight information will be displayed on computer-driven digital displays. What is a bit surprising is that the usual set of small mechanical backup instruments will not be present. Talk about flight-critical software...

Henry Spencer at U of Toronto Zoology utzoo!henry

---

### ✂ black boxes in autos for accident "facts"

Mark Seecof <marks@capnet.latimes.com>

Wed, 24 Jul 91 12:13:14 -0700

Excerpts from an article in the Los Angeles Times June 13, 1991; page E8. Edited and submitted to RISKS Digest by Mark Seecof <marks@latimes.com> of the L.A. Times Publishing Systems Department.

[elisions and bracketed comments mine --Mark S.]

``A Black Box Tells Just the Facts'' LEGAL VIEW column by Jeffrey S. Klein and Louis M. Brown. Klein is an attorney and president of the Times' San Fernando Valley and Ventura County Editions. Brown is professor of law emeritus at USC and chairman of the board for the National Center for Preventive Law.

Most court cases about auto accidents involve disputes about facts, not the law. That means lawyers argue mostly about how fast a car was going, who didn't stop at the red light, whether a driver crossed over the double yellow line, and similar questions. Less time is spent debating legal niceties, such as jury instructions or rules of evidence.

One innovative idea to reduce the time and expense of re-creating the scene of an auto accident in the courtroom was recently suggested by Harold Weston, a Los Angeles lawyer: a ``black box'' for automobiles, just like those in the cockpits of commercial airplanes. Weston offered his proposal in a legal publication, the Los Angeles Daily Journal. The black box would include a running video camera that would record events just the way the driver sees them.

A black box could also record speed, acceleration, braking, turn signals, and even whether the seat belt was fastened. Perhaps the device that triggers the air bag could tell the black box that an accident has occurred, Weston

noted. "If we are going to have dashboards that look like cockpits, shifters that look like throttles, and turbos that sound like turbines, we might as well add the black boxes to complete the whole image," he wrote.

In fact, there is such a device, invented by Joseph A. Michetti, who lives in Ventura. A patent for it was issued in 1989 and it is now being developed for marketing, including a five-minute video about the device, called a "vero-vedi." It has not only one video camera but two--one directed forward and one directed rearward.

Of course, a video recording of an accident, even if it captures all the relevant details, will not reduce the number of accidents, but it could cut down the work of lawyers and judges--and give juries a much better factual base upon which to make decisions. It could also settle insurance claims that might otherwise wind up in court. If an insurance company can see who was at fault, there is less likely to be a courtroom battle.

Pictures of "facts" can be admissible in the courtroom. We are all accustomed to seeing photographs offered as evidence. And some lawyers now make video recordings of the signing of a will.

A video camera in every car might sound expensive in the short run, but it is also preventive. It could save lots of insurance company, lawyer, and court time.

That's the end of the column. Below are my comments, which of course reflect only my personal opinions and not those of my employer.

There are many unexplored ramifications of implementing such a system. Off the top of my head I think of: self-incrimination problems (especially if police want to review the black boxes from every blue Ford sedan on Oahu after a hit-and-run accident, or what if a tape shows some OTHER crime?), sabotage problems (by guilty drivers), and forgery problems (people buy warranty-voiding replacement PROMS for their car computers to increase performance (with greater smog output as the chief side-effect), so I think a market for black boxes which never record excessive speed or always record seatbelt usage would develop, plus another market for "clean videotapes" to be substituted after an accident).

I read an article in Smithsonian sometime in the last year or two (I've hunted for the issue but I must have discarded it)... about very-long haul trucking in Europe/Asia/Africa. Trucks carry goods from England to the Middle-east across many European countries. The trucks are required to have chart recorders that show speed and distance travelled against time. These are called tachymeters and the charts (recorded in a circular fashion) are called "tacho discs." Police review the tacho discs to catch drivers who speed or break hours-of-work rules. The drivers abominate the tacho system and I for one feel some sympathy for them as the police can use the tacho records as a basis for punishing even trivial violations, or worse, to "detect" violations which may have happened in extenuating circumstances not recorded by the device (e.g., exceeding speed limit to pass a very slow vehicle during a small window of opportunity).

Moreover, I suggest that electronic monitoring devices encourage a unilateral (by enforcement agencies and people with axes to grind) revision of the social

contract on which traffic laws are ultimately based. You see, electronic monitoring helps to enforce the strict numerical or other limits in the laws. But real people tend to expect (a) fuzzy enforcement to match their fuzzy obedience (driving 57 or 58 is "close enough" to 55 for most people), (b) lenient enforcement under "otherwise safe" circumstances to match the general belief that it's not much of a crime to speed a little on a good road in good light when there aren't too many other cars around, and last but perhaps most important: fuzzy, lenient enforcement to allow for the fact that the laws are generally much stricter than the majority of voters really want.

I've read of studies showing that a large majority of drivers think they're "better" or "much better than average" drivers. Obviously this is impossible. I suspect that the same drivers (remember, that's most of 'em... including me!) believe that they're qualified by their skills to exercise more discretion than other folks about bending traffic rules. This self-confidence, coupled with the famous inability of legislators to resist voting for harsh laws (so as to avoid accusations of being "soft on drunk drivers|crime|whatever"), means that the laws on the books are often more restrictive than the consensus on what the "practical" law should be. The public relies on soft enforcement practices to make the system work. Micrometric law enforcement is something for which our culture, not to say our legal system, really isn't prepared.

Indeed, there's reason to believe that "human nature" wants us to set the posted speed limit five or ten MPH below what we want the actual top speeds to remain because that's the amount by which people will routinely exceed the posted limit. If you figure that the posted limit has been pegged 10 MPH low for reasons rooted in human psychology, with the concomitant expectation of fuzzy enforcement, then to introduce strict enforcement would amount to a 10 MPH revision of the "real" speed limit.

I think that police, prosecutors, and insurance adjusters tend to like technical means of detecting and quantifying violations of laws or standards, because these means reduce the amount of discretion exercised by the enforcers of the rules and thus the amount of post-hoc argument over how that discretion was exercised.

However, the laws on the books assume the exercise of discretion. Changing the amount of slop in enforcement decisions without changing the standards seems a dangerous business to me. Because it's easier to add a new method than to revise an old standard ("What? You want to have more children run over by speed maniacs?") we might ratchet ourselves into situation that no one really wants.

The biggest RISK of black-boxes for automobiles is that they'll enable strict enforcement of the wrong set of standards.

Footnote: California has several special rules intended to fuzz traffic enforcement in favor of putative violators. The Highway Patrol (state troopers) mostly don't (can't) use radar. Local cops can use radar only after special formalities to justify the limits they're enforcing. §22351 CVC allows a special defense to charges of breaking a posted speed limit < 55 MPH; which is that the driver's speed was safe even though it was over the limit. Because the limit is presumed on its face to be the safe limit, this defense must be

proven by the defendant. People actually do this now and then; the law serves as a check on local jurisdictions which might use unreasonably low speed limits as fine-generating revenue boosters. Lastly, petty violators (including minor speeding tickets but not including reckless or drunk driving) can often avoid trial, conviction, and punishment by going to a court-ordered "traffic school" which costs about \$50 and eight hours of excruciating boredom but saves a fine, point count, and what amounts to another (huge) fine in the form of giant insurance premium increase. Drivers can only do the "traffic school" bit once every 18 months, but the very existence of the dodge (which has been shown to have no effect on accident rates) is an acknowledgement that the official punishment for minor traffic offenses is too harsh.

---

**✉ Re: Artificial Dissemination (See Curtin, [RISKS-12.05](#))**

<edwardj@microsoft.com>

Fri Jul 19 01:48:33 1991

For the edification of the readers of this newsgroup I will repeat what has been said in the press already about the Bill Gates memo: it was not an email message, but a message sent via paper and routed through inter-office mail.

Any leaking that occurred would have happened from someone copying the memo and sending it to an external source. There was no forwarding of email involved. It is therefore not an example of comp.risks as much as an example of human-resources.risks!

Edward Jung



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 12: Issue 9

Thursday 25 July 1991

## Contents

- [The limits of simulation](#)  
[Henry Spencer](#)
- [RISKS vs. RISKS](#)  
[Steve Bellovin](#)
- [Gottschalks rejects check](#)  
[Todd Heberlein](#)
- [Proposed law on computer searches](#)  
[Chris Hibbert](#)
- [New Jersey "software engineering" registration legislation](#)  
[John M. Ritter via Arthur Rubin](#)
- [Info on RISKS \(comp.risks\)](#)

---

### The limits of simulation

<[henry@zoo.toronto.edu](mailto:henry@zoo.toronto.edu)>  
Thu, 25 Jul 91 21:37:48 EDT

The May 27 Aviation Week, reporting on the April 1 test-stand failure of an upgraded SRB for the Titan 4:

Investigators determined that extensive three-dimensional computer simulations of the [motor's] firing dynamics did not reveal subtle factors that they now believe contributed to motor failure. [Program director] Stirling said the full-scale test was essential precisely because computer analyses cannot accurately predict all nuances of solid rocket motor dynamics. "That's why we test", he said.

For those who don't follow the space news, a few seconds into the test the motor pressure rose rapidly and exceeded the limits of the casing, the result being a large, spectacular explosion that destroyed the motor and much of the Edwards AFB test stand.

Henry Spencer at U of Toronto Zoology utzoo!henry

---

## **✂ RISKS vs. RISKS!**

<smb@ulysses.att.com>

Thu, 25 Jul 91 13:52:26 EDT

In the same issue of [RISKS-12.08](#), we have (from PGN)

> Dennis Perry, an Oakland truck driver, and his good friend, Yvonne ...  
and from Mark Seecof:

> However, the laws on the books assume the exercise of discretion.

The contradiction is, of course, obvious. What isn't clear is what to do about it.

Computers are great at making ``objective'' decisions. Civil service rules and government procurement regulations try to mimic this behavior. The goal is not to achieve the best, but to guard against the worst. But even worse can be ``achieved'' when the regulations aren't drafted carefully enough, letting an unscrupulous official finagle through a particular outcome.

--Steve Bellovin

---

## **✂ Gottschalks rejects check**

Todd <heberlei@iris.eecs.ucdavis.edu>

Thu, 25 Jul 91 12:05:57 -0700

I recently tried to purchase some merchandise at a local Gottschalks with a check. Before accepting my check, the clerk checked Shared Check Authorization Network (SCAN) to see if I have had any returned checks. The clerk then informed me that they could NOT accept my check.

Having never bounced a check, and having more than ample money in my checking account, I was very surprised.

After calling my credit union and SCAN, I was able to sort out the error. Gottschalks entered the account number on my check BUT NOT the bank number. SCAN apparently does a look up on just account numbers (as well as account and bank numbers), and as it turned out, someone with the same account number at a different bank had bounced checks. SCAN then returned FAIL.

The result: I could not use a check because someone else at a different bank bounced a check.

If other places only enter account numbers and not bank numbers, I will probably have to get a new account number from my bank. :-{

Todd

---

## **✂ Proposed law on computer searches**

<xanadu!hibbert@uunet.UU.NET>

Thu, 25 Jul 91 14:53:15 PDT

Don Ingraham was one of the prosecutors who talked at the Conference on Computers Freedom and Privacy in March. At the last session, he said he would write and propose new guidelines for prosecutors to follow that would take into account the concerns that were brought up at the conference. Last month, he gave a talk at the first meeting of the Berkeley SIG on Freedom, Privacy, and Technology (affiliated with BMUG and CPSR-Berkeley). He mentioned at that point that he had a draft, and I later asked him for a copy. When I asked him if I could redistribute it, he not only gave me permission, but encouraged me to do so.

If you have suggestions on how to improve the draft, or if you represent a relevant group (CPSR, EFF, ACLU, and ACM come to mind) and would like to offer Don official support, he'd very much like to hear from you. Don isn't electronically connected, so you'll have to send him fax or paper mail, or call him on the phone. If there is interesting discussion here, I'll tell him about it, but I don't promise to show him every word.

What follows is first Don Ingraham's summary, then the draft bill, and finally his commentary on what it means, and what he'd like to have happen with it. This is an important proposal, and it looks like quite a good law.

Chris

hibbert@xanadu.com

uunet!xanadu!hibbert

=====

PROPOSAL FOR PENAL CODE SECTION 1538.6:  
ELECTRONICALLY STORED MATERIAL.

Revised 11 June 1991

Donald G. Ingraham, Assistant District Attorney, Alameda County,  
1225 Fallon Street, Oakland CA 94612 4292 (415) 272-6232 fax 271-5157

The following is a proposal to add to the existing search warrant provisions of the Penal Code some particular restraints on the issuance of warrants which are required by federal law; it would also establish controls on the examination of electronically stored evidence seized in the course of a criminal investigation, and empower the Attorney General to monitor and regulate compliance with this law.

There are four main aspects:

first, it recognizes the existing restraints of federal law, in particular the Privacy Protection Act (42 USC 2000aa) portion of the Civil Rights Act, and also chapter 212 of the Electronic Communications Privacy Act (18 USC 2700 et seq) dealing with stored electronic communications. The portion of the ECPA which addresses the interception of electronic communications is covered by existing law.

second, it establishes the Attorney General of California in a monitoring and regulatory function, not unlike the function now performed in regard to criminal offender record information. In the following text, references to federal law appear in parentheses.

third, it establishes criteria for the inventory and analysis of electronically stored evidence, and affords the person from whom it was seized and other interested parties standing and information to present their interests and concerns to the issuing magistrate.

fourth, it balances law enforcement's necessary investigative authority with the privacy and personal interests of persons affected by the investigation.

This topic is of such significance that it is suggested there be a specific legislative declaration such as this:

=====

Legislative finding:

The legislature finds that investigation and prosecution of crimes in which computers are involved engenders a risk to other rights, including those to conduct a business, to publish, and to conduct private communications. This section clarifies existing requirements of the federal Electronic Communications Privacy Act and the Privacy Protection Act, and also invests the Attorney General with authority to regulate the analysis and examination of electronic media seized under the authority of this chapter.

Addition to Chapter 3, Search Warrants, Title XII, Special Proceedings of a Criminal Nature, California Penal Code.

Section 1536.5

A search warrant for computer-related material cannot be authorized except in compliance with the following restraints. All electronically stored material seized, under a search warrant or otherwise, shall be retained and analyzed as follows:

[a] if the content is reasonably apparently identifiable as intended for publication, a search warrant may be authorized only if the affidavit to that warrant specifically provides probable cause that the material is contraband or the fruits of a crime or things otherwise criminally possessed, or is property designed or intended for use, or which is or has been used as, the means of committing a criminal offense.

(This is directly from Title 42 USC 2000aa(7).]

[b] if examination of electronically stored communications indicates that any particular file is a communication intended to be private and neither party thereto is named as a subject of the search warrant, and the material has been in such storage for under 180 days, the investigating officer may not continue the analysis nor proceed further without obtaining a search warrant for stored electronic communication, as defined by regulations issued by the Attorney General.

(This is adapted from Title 18 USC 2703: the term 'search warrant for stored electronic communication' appears in that Title as a term of art.]

[c] within five court days of any seizure of stored electronic material, the investigating officer will file a supplement to the inventory required by section 1537 which will list all electronic material with all available specificity, including but not limited to file names then identified, and indicate what procedures for analysis are being taken. A copy of that and any subsequent inventories will be furnished to the subject of the search warrant.

A further supplement will be filed with the issuing magistrate every tenth court day thereafter until all electronic material has been analyzed. A copy of all such inventories will be part of the court record and open to public inspection.

[d] Electronic stored media will be analyzed as expeditiously as possible and in the following order: first, material recognizably necessary to the conduct of legitimate business and private communications; second, material recognizably central to the crime under investigation; third, material reasonably suspected of relating to the crime under investigation. The magistrate shall direct the investigating office or prosecutor to return or copy such material to the owner, providing a receipt for the court record.

[e] After the filing of the initial inventory, any person who has reason to believe that he or she would be unfairly adversely affected in business or communications by the retention or analysis of the seized electronic material may petition the issuing magistrate for a hearing to demonstrate that the proposed retention and/or analysis would result in significant injury to a legitimate purpose.

[This provision expands upon existing Calif PC 1538.5, but is specific to electronic media; there is no known federal counterpart. The provision for return by DA, receipt to Court, regular accounting and standing to others affected is not fantasy: we did as much in our Draper prosecution with mutually beneficial effect.]

[f] The Attorney General shall establish regulations for the seizure, examination, and disposition of electronic material obtained in the process of criminal investigations consistent with the intent of this section that intrusion and disruption be as minimal as the requirements of an investigation permit, and in keeping with federal regulation.

[This section empowers the Attorney General to keep computer related criminal investigations by our law enforcement agencies consistent with federal law, without the need to go to the legislature to accommodate changes in the federal law.]

=====

Comment, primarily intended for prosecutors, but open to all

This is the draft of a bill on search warrants for electronically stored material, which will probably be introduced next session: I need to line up AG and other support for it to fly. To put the idea in context, please be aware that Penal Code 1538.5 covers review of searches and is the basis of our traverse motions. It seemed the logical place to put this, rather than in our Computer Crime section-502- or under privacy.

The idea is to get a legislative purpose statement, and then flag areas of concern and potential federal liability:

(a) flags the First Amendment Privacy Protection Act, 42 USC

2000aa, which addresses : ... any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce.." which I try to boil down by the phrase "intended for publication", adding a prefatory qualification, that it be "reasonably apparently identifiable" as such. The federal act makes no such allowance, although I cannot imagine a court imposing it: as it now reads it is rather like forbidding us to open any cabinet that may contain more than one paper clip, at our peril.

(b) does the same flagging as to Chapter 212, Electronic Communications Privacy Act, 18 USC 2700 et seq, again clarifying that it does not apply if one of the parties is already named in the warrant. This would assume that the possibility of electronically stored communications was anticipated by the warrant, which should always be the case. The legislative history is barren on this, but what standing would an intruder have to object?

(c) through (e) create something new, not in the federal law. This basically is a response to the main complaint about the usual investigation, which is that the gear and files disappear into the maw of the eagle, and are seldom if ever heard from again. Having someone say "we're working on it" every other month is not what I think James Madison had in mind. I think that such limbo should not be imposed, assuming that it ever is, and the best way to keep that from happening would be to require a regular accounting and progress report. This would not only be reasonable, but it would also accomplish two other boons: it would give us a need to keep our investigation going instead of watching our resources get reassigned, and it should forestall more draconian controls if this perception gets any more widespread. We did exactly this when we prosecuted John "Captain Crunch" Draper, and it worked well. I wouldn't try to process evidence any other way.

(f) would empower our Attorney General to establish regulations for the search of electronically stored material much as the AG now sets the policies on confidentiality and privacy of Criminal Offender Record Information/"rap sheets". Going by administrative regulation rather than by way of additional legislation guarantees that we will not stray from federal rules, which should keep civil rights prosecutions of prosecutors per 42 USC 1983 at a minimum.

What is needed to bring this about?

The basic hope is to have it debugged and ready to submit by October: ready to submit means, among other things, that we have some organized support from concerned citizens. The immediate hope is that both law enforcement and civil libertarians will see the wisdom of structuring what is now not as structured and be willing to support it. The idea is to keep it clean and simple; if glitches later develop, we could amend it again, but the essential aspect at this point is to get legislative recognition of the fact that search warrants for electronic material are already different from search warrants for other things. If we do that, and can get the Attorney General to agree, it should fly. My fondest hope is that come October I could represent to the appropriate

legislator that the AG, the CDAA, the ACLU, the CPSR, and the academic and business communities thought this a heck of an idea, and in their view essential.

In summary, and in particular regard to the concerns of prosecutors like me, this proposal would avoid the need to develop an electronic privacy measure in California by adopting the federal law, and giving the Attorney General the responsibility to keep up with its amendments through the California Code of Regulations. Two other states, Utah and Florida, have crafted their own versions of the federal Electronic Communications Privacy Act; that independent course risks inconsistencies and uncertainties as the judicial process construes the ECPA. The enactment of this proposal would avoid that, while at the same time providing all available guidelines to law enforcement and to citizens concerned with the freedom to use computer technology and with electronic privacy, who are, after all, a significant portion of the People in whose behalf we prosecutors are privileged to appear.

---

**✉ New Jersey "software engineering" registration legislation (J.M.Ritter)**

<a\_rubin@dsg4.dse.beckman.com>

Wed, 24 Jul 91 09:27:28 PDT

[Following are large excerpts from articles posted by jmr@motown.allied.com (John M. Ritter) on comp.{os.msdos,sys.ibm.pc,unix}.programmer. ]

New Jersey, that state which has lately proved to be "the toughest in the nation" by trampling on its residents is once again attempting to reach all new lows. Now, what has this got to do with programming...?

A bill has passed in the assembly that would require the licensing of computer programmers -- to protect the public interest, of course. Lord knows the number of times I've been accosted in pizza parlors, late at night, by renegade bands of unlicensed programmers. Well, now we'll be able to control these low-lifes.

If you think I'm kidding, read on. What follows is Assembly Bill A-4414, which has already passed the assembly. AT&T has estimated that it would need to license over 5,000 people in New Jersey alone, and there is nothing in the bill that differentiates home from business use.

So watch out: besides being arrested for legally buying a gun 20 years ago, you could also be arrested for modifying a DOS batch file!

New Jersey and you. Perfect together?

John M. Ritter, Allied-Signal, Inc., Corporate Tax Department  
jmr@motown.Allied.COM {att,bellcore,clyde,princeton,rutgers}!motown!jmr

=====

ASSEMBLY, No. 4414

STATE OF NEW JERSEY

INTRODUCED JANUARY 24, 1991

by Assemblywoman KALIK, Assemblymen CASEY,  
Spadoro and Mazur

AN ACT providing for the licensure of software 1[engineers] \_\_\_\_\_1, amending P.L.1971, c.60, P.L.1974, c.46 and P.L.1978, c.73, and supplementing Title 45 of the Revised Statues.

BE IT ENACTED by the Senate and General Assembly of the State of New Jersey:

1. (New section) This act shall be known and may be cited as the ``Software 1[Engineers'] \_\_\_\_\_1 Licensing Act."
2. (New section) The Legislature finds and declares that the public interest requires the regulation of the practice of software 1[engineering] \_\_\_\_\_1 and the establishment of clear licensure standards for software 1[engineers] \_\_\_\_\_1, and that the welfare of the citizens of this State will be protected by identifying to the public those individuals who are qualified and legally authorized to practice software 1[engineering] \_\_\_\_\_1.

3. (New section) As used in this act:

``Board" means the State Board of Software 1[Engineers] \_\_\_\_\_1 established pursuant to section 4 of this act.

``Licensed software 1[engineer] \_\_\_\_\_1" means any person who practices software 1[engineering] \_\_\_\_\_1 and who represents himself to the public by title or by description of services under any title incorporating such terms as ``software engineer," 1`\_\_\_\_\_, "1 ``chartered engineer," or ``CEng" or any similar title or description of services, who is duly licensed pursuant to this act.

``Software 1[engineering] \_\_\_\_\_1" means the process of creating software systems and applies to techniques that reduce software cost and complexity while increasing reliability and modifiability, which includes, but is not limited to, the elements of requirements 1[engineering] \_\_\_\_\_1, design specification, implementation testing and validation, operation and maintenance and software management.

4. (New section) There is created within the Division of Consumer Affairs in the Department of Law and Public Safety the State Board of Software 1[Engineers] \_\_\_\_\_1. The board shall consist of nine members who are residents of the State who shall be appointed by the Governor. Six members shall be licensed software 1[engineers] \_\_\_\_\_1 who have been actively

\_\_\_\_\_

EXPLANATION--Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted in the law.

Matter underlined \_\_\_\_ is new matter. Matter enclosed in superscript numerals has been adopted as follows:

1 Assembly ACP committee amendments adopted June 13, 1991.

2 Assembly floor amendments adopted June 24, 1991.

engaged in software 1[engineering] \_\_\_\_\_ 1 for at least five years immediately preceding their appointment, except that the members initially appointed shall be licensed pursuant to this act within 18 months of appointment. Of the remaining members, two shall be public members, and one shall be a member of the executive branch, all of whom shall be appointed pursuant to section 2 of P.L.1971, c.60 (C.45:1-2.2).

5. (New section) Each member of the board, except the members first appointed, shall serve for a term of five years and shall hold office until the appointment and qualification of his successor. The initial appointment to the board shall be: two members for terms of two years, two members for terms of three years, two members for terms of four years, and three members for terms of five years. Vacancies shall be filled for the unexpired term only. No member may be appointed for more than two consecutive terms.

6. (New section) Members of the board shall be compensated and reimbursed for expenses and provided with office and meeting facilities pursuant to section 2 of P.L.1977, c.285 (C.45:1-2.5).

7. (New section) The board shall annually elect from among its members a chair, vice-chair and a secretary. The board shall meet twice per year and may hold additional meetings as necessary to discharge its duties.

8. (New section) The board shall:

a. Review the qualifications of applicants for licensure;

b. Insure the proper conduct and standards for examinations;

c. Issue and renew licenses to software 1[engineers] \_\_\_\_\_ 1 pursuant to this act;

d. Refuse to admit to examination, refuse to issue, or suspend, revoke or fail to renew the license of a software 1[engineer] \_\_\_\_\_ 1 pursuant to the provisions of P.L.1978, c.73 (C.45:1-14 et seq.);

e. Maintain a record of every software 1[engineer] \_\_\_\_\_ 1 licensed in the State, their places of business, places of residence and the date and number of their license;

f. Establish fees pursuant to P.L.1974, c.46 (C.45:1-3.1 et seq.);

g. Adopt and promulgate rules and regulations pursuant to the "Administrative Procedure Act," P.L.1968, c.410 (C.52:14B-1 et seq.) necessary to effectuate the purposes of this act.

9. (New section) No person shall practice, or present himself as able to

practice, software 1[engineering] \_\_\_\_\_1 unless he possesses a valid license as a software 1[engineer] \_\_\_\_\_1 in accordance with the provision of this act.

10. (New section) The provisions of this act shall not be construed to prevent the following provided that no word, letter, abbreviation, insignia, sign, card or device is used to convey the impression that the person rendering the service is a licensed software 1[engineer] \_\_\_\_\_1:

a. Any person licensed to practice in this State under any other law from engaging in the practice for which he is licensed;

b. Any person employed as a software 1[engineer] \_\_\_\_\_1 by the federal government, if the person provides software 1[engineering] \_\_\_\_\_1 services solely under the direction or control of his federal employer; or

c. Any person pursuing a course of study leading to a degree or certificate in software 1[engineering] \_\_\_\_\_1 at an accredited or approved educational program if the person is designated by a title which clearly indicates status as a student or trainee.

11. (New section) To be eligible for a licensure as a software 1[engineer] \_\_\_\_\_1, an applicant shall submit to the board satisfactory evidence that he has:

a. 2(1)2 Graduated from a program in software 1[engineering] \_\_\_\_\_1 which has been approved for the education and training of software 1[engineers] \_\_\_\_\_1 by an accrediting agency recognized by the Council on Post-Secondary Accreditation and the United States Department of Education; or

(2) Work experience in a current or previous position of employment utilizing the theory and procedures of software designing for a sufficient period of time as determined by the board; and

b. Successfully completed a written examination administered by the board pursuant to section 14 of this act to determine his competence to practice software 1[engineering] \_\_\_\_\_1.

12. (New section) An applicant for licensure who is a graduate of a foreign school of software 1[engineering] \_\_\_\_\_1 shall furnish evidence satisfactory to the board that he has:

a. Completed a course of study in software 1[engineering] \_\_\_\_\_1 which is substantially equivalent to that provided in an accredited program described in subsection a. of section 11 of this act; and

b. Successfully completed a written examination administered by the board pursuant to section 14 of this act.

13. (New section) A fee shall accompany each application for licensure. Licenses shall expire biennially on January 31 and may be renewed upon submission of a renewal application provided by the board and a payment of

a fee. If the renewal fee is not paid by that date, the license shall automatically expire, but may be renewed within two years of its expiration date upon payment to the board of a sum determined by it for each year or part thereof during which the license was expired and an additional restoration fee. If a license has not been renewed within two years of expiration, the license shall only be renewed by complying with the provisions of section 16 of this act or successfully completing the examination administered pursuant to section 14 of this act.

14. (New section) The written examination required in section 11, 12, or 13 of this act shall test the applicant's knowledge of software 1[engineering] \_\_\_\_\_1 theory and procedures and any other subjects the board may deem useful to test the applicant's fitness to practice software 1[engineering] \_\_\_\_\_1. Examinations shall be held within the State at least once every six months at a time and place to be determined by the board. The board shall give adequate written notice of the examination to applicants for licensure and examination.

If an applicant fails the examination twice, the applicant may take a third examination not less than one year nor more than three years from the date of the applicant's initial examination. Additional examinations shall be in accordance with standards set by the board.

15. (New section) The board shall issue a license to each applicant for licensure as a software 1[engineer] \_\_\_\_\_1 who qualifies pursuant to the provisions of this act and any rules and regulations promulgated by the board.
16. (New section) Upon payment to the board of a fee and the submission of a written application on forms provided by it, the board shall issue without examination a license to a software 1[engineer] \_\_\_\_\_1 who holds a valid license issued by another state or possession of the United States or the District of Columbia which has standards for licensure substantially equivalent to those of this State.
17. (New section) Upon payment to the board of a fee and the submission of a written application on forms provided by it, the board shall issue a temporary license to a person who has applied for licensure pursuant to this act who, in the judgment of the board, is eligible for examination. A temporary license shall be available to an applicant upon initial application for examination. A person holding a temporary license may practice software 1[engineering] designing only under the direct supervision of a licensed software 1[engineer] \_\_\_\_\_1. A temporary license shall expire automatically upon failure of the licensure examination but may be renewed for an additional six-month period, until the date of the next examination at which time it shall automatically expire and be surrendered to the board.



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 12: Issue 10**

**Monday 29 July 1991**

## Contents

- [Summer slowdown](#)  
[PGN](#)
- [Egad, sail-by-wire! \(W. K. Bill\) Gorman](#)
- [Third Chicago Airport: Rare Events & Computer Projections](#)  
[William E. Mihalo](#)
- [Risks of human error in Soviet nuclear "industry"](#)  
[Tom Blinn](#)
- [Re: Smart cockpit with no backup](#)  
[Simson Garfinkel](#)
- [Licensing of Software Engineers](#)  
[Bill Murray](#)
- [Re: New Jersey "software engineering" registration legislation](#)  
[Bob Frankston](#)
- [ACM SIGSOFT '91, SOFTWARE FOR CRITICAL SYSTEMS](#)  
[Judith Burgess](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Summer slowdown**

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Mon, 29 Jul 91 9:56:27 PDT

I'll be off the net more or less for the next three weeks. I hope the world of computer-related activities becomes very peaceful and uneventful, so that we don't miss anything. Please keep sending in your goodies, however, and we'll get to them eventually.

Please check out the advance information on SIGSOFT '91, SOFTWARE FOR CRITICAL SYSTEMS, 4-6 December 1991, in New Orleans, included as the last item in this issue. This conference will be of unusually high relevance to the RISKS community. PGN

---

## **✂ Egad, sail-by-wire!**

<34AEJ7D@cmuvm.bitnet>

Fri, 26 Jul 91 11:16:50 EDT

I recently noted that the Japanese are aggressively developing a generation of huge, totally unmanned, computer-guided supertankers intended to embark/debark, as well as transit the oceans, in fully automated mode. The risks, based on fly/drive by wire research, of having these vessels transiting the oceans unmanned seems significant. Any supertankers is a significant hazard to navigation by smaller vessels, which are notorious for not being particularly easy to spot on radar. The risk of possible environmental disasters, e.g. Exxon Valdez, exists for all supertankers. Running unmanned, IMHO, exacerbates the situation. The risk of possible terrorism involving a large, relatively slow-moving, completely exposed, unmanned ship, carrying a potentially hazardous cargo through the strategic shipping lanes of the world probably should not be ignored.

W. K. (Bill) Gorman

---

## **✂ Third Chicago Airport: Rare Events & Computer Projections**

"William E. Mihalo" <calumet!wem@gargoyle.uchicago.edu>

Sat, 27 Jul 1991 13:59:07 cdt

Considerable controversy developed during the past year regarding the site selection for a third airport within the Chicago metropolitan area. Once in place the projected number of planes using the airport would exceed the current traffic at O'Hare Field, one of the world's busiest airports. A number of sites have been proposed: 1) an area on the southeast side of Chicago called the Lake Calumet site; 2) an area on the western side of Gary, Indiana and 3) two other "green grass" sites that are located approximately 35 miles south of Chicago.

Richard M. Daley, the mayor of Chicago, has been promoting the Lake Calumet site for over a year. A number of politicians within Gary, Indiana and downstate Indiana have been promoting the Gary site. Both the Lake Calumet and Gary locations are in open land adjacent to some heavily populated areas. Both the Lake Calumet and Gary sites would require massive condemnation of homes in the southeast side of Chicago and in Gary, Indiana.

How does this relate to RISKS? I see two possible links.

The first is the obvious "rare event." Planes tend to crash near airports. For example in May, 1979 a DC-10 crashed shortly after takeoff killing 275 people. The areas adjacent to the Lake Calumet and Gary sites are heavily populated. Moreover, an oil refinery is within 3 miles of the Lake Calumet site and several steel mills are adjacent to the Gary site. The idea of a DC-10 colliding with an oil refinery is admittedly a rare event. The consultants and politicians promoting the Lake Calumet and Gary sites have dismissed such possibilities with little discussion.

Second, the site location for this third airport is based on a series of computer projections performed by outside consultants hired to provide

information on needed runway size, number of passengers and the overall economic impact of the facility. Northwest Indiana and the southeast side of Chicago underwent substantial deindustrialization starting in the 1960's and accelerating in the 1980's. Computer models have projected a payroll of \$2.7 billion, for the Gary airport and an overall economic benefit of \$5.7 billion by the year 2020. These data are being pushed as "fact" (it must be true, it came from a computer). Also, heavily emphasized are estimates of 150,000 to 300,000 jobs that would be created in conjunction with the airport. Work on the noise contours associated with the runway configuration for these two airport sites have been delayed. Also delayed is the projected out-migration of residents from the area.

The entire site selection process is an example of a consulting firm with a PC running amok with projected statistics and estimates. In some cases the media are directly fed the projections with little questioning. The fact that these data were created by a computer simulation or projection is not taken into account. Nor is there any questioning of the type of mathematical model that is being used to generate this data.

Geographic and cartographic software used to map the proposed airport sites has failed to take into account the topography of the land and the number of businesses affected. Massive wetland drainage would be required for the Lake Calumet site. Also, the consultants failed to take into account the substantial migratory bird population (birds and airplanes don't mix) and weather associated with the Lake Calumet and Gary sites (both sites would start near the shore of Lake Michigan and head south). The chairman of the bistate selection committee for the third airport Frank Luersen (CEO for Inland Steel) was forced to resign after the consultants recommended the closure of Cline Avenue (a major divided highway in northwest Indiana) and the closure of the Inland Steel Research Lab. Somewhat embarrassed, the consultants returned with a new runway configuration that allowed Cline Avenue and Inland Steel to remain, but on land immediately adjacent to the Gary airport site.

William E. Mihalo wem@calumet.uucp

---

### **✂ Risks of human error in Soviet nuclear "industry"**

Tom Blinn <blinn@dr.enet.dec.com>

Fri, 26 Jul 91 12:28:19 PDT

In the [RISKS DIGEST 12.08](#), PGN contributed the article "Human Error Blamed for Soviet N-Plant Problems". In the recently translated and published book on the Chernobyl disaster, the Soviet nuclear engineer/scientist Medvedev reported on the root causes, which were, basically, human error. It should be no surprise that, in spite of Glasnost, the fundamental flaws in the system have not been addressed. (I regret I do not have a better reference for Medvedev's book at hand. It is excellent.)

Thomas P. Blinn, Digital Equipment Corporation, Digital Drive -- MKO2-2/F10,  
Merrimack, New Hampshire 03054 ...!decwrl!dr.enet.dec.com!blinn (603) 884-4865

## ✉ Re: Smart cockpit with no backup

<simsong@nextworld.com>

Fri, 26 Jul 91 12:19:26 PDT

Henry Spencer writes that the Air Force's new F-22 has no mechanical backup instruments --- making the flight software extremely flight-critical.

However, on new "fly-by-wire" aircraft, a computer failure would also deactivate all of the aircraft's control surfaces, since the pilot's stick is really nothing more than a joystick on these planes. In the event of a computer failure, the only good that mechanical backup instruments would do would be to let the pilot watch the altitude ticking off on the way down...

---

## ✉ Licensing of Software Engineers

<WHMurray@DOCKMASTER.NCSC.MIL>

Fri, 26 Jul 91 09:36 EDT

I do not read the text of the NJ legislation posted here as requiring the licensing of programmers. Rather it recognizes the existence of a special class of programmer.

It only requires licensing of those who offer themselves for hire as software ENGINEERS. Hire and engineer are both key words. I am a "once and sometime programmer." I have not been employed in that capacity for years. Since I do not offer myself for hire in that capacity, I would not require a license.

Even if I were to take a job as an entry-level programmer [a job for which I am at one and the same time both over and under qualified] I would not need to be licensed under this legislation, since I do not offer myself for hire as an engineer. I would be a programmer, not an engineer. [Nancy L. is a software engineer. Padgett P. is an engineer. I am a mere software author.] I would be making no special claims about my qualifications. It is the special claim of engineer that would subject me to this legislation, not software alone.

Now, while I suspect that this law may be a little premature, past discussions in this list suggest that mere programmers, such as myself, are making decisions for which we are not qualified. The result is as much to put the public at hazard as if I were to undertake to build a bridge. I did, once program at the Louisiana Department of Highways. Some of the work that I did influenced the construction of roads and bridges, but it was done under the supervision of licensed civil engineers, experienced in building roads and bridges.

Soon we will have "smart" roads and bridges in which computer hardware and software will be active components of the roads and bridges. The ability to write the software for those roads and bridges does not necessarily, include the ability to write the specification. It clearly does not include the ability to decide upon the role of the computer or software in the road. This requires special competence which I am not even qualified to judge [but which I would trust Nancy and Padgett to judge.]

Note that the NJ legislature does not attempt to define these qualifications or to describe them. Rather, it leaves that to those who would so hold themselves. This is similar to what it does with other professions.

It is not clear whether or not programming is a profession or not. It is clear that most of the people who engage in it, even some of those who do it for a living, would not qualify under any reasonable definition of professional. It is equally clear that there is a requirement for a group of professionals, trained in the lore and traditions of engineering, not "computer science" who can make decisions about how software is to be designed, built, and used. I know some of the people who do it; they are professional in a sense that some programmers cannot even understand.

I do not trust the NJ legislature to recognize these people. I concur in the NJ legislatures recognition that they can and should have the discretion to recognize their peers and exclude others. It is in the public interest that they do so.

That programmers, without the qualifications of these few, should feel threatened by this is natural and to be expected. However, I do not believe their fears to be justified.

William Hugh Murray, Executive Consultant, Information System Security  
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840 203 966 4769

---

**✉ Re: New Jersey "software engineering" registration legislation (J.M.Ritter)**

<frankston!Bob\_Frankston@world.std.com>  
26 July 1991 19:37 -0400

One fundamental problem is that we are still learning what software engineering entails. Is a Hypercard programmer a software engineer? A spreadsheet macro writer. What about a VCR programmer? Essentially any control of a system that can remember instructions is programming and thus involves software engineering.

I realize that the model the legislature has in mind is a Civil Engineer or a Licensed Bridgebuilder (it is fun to revisit old examples), and that it looks in horror at amateur mistakes being made in building critical systems. But world is changing from engineering final systems to creating refineable systems and thus propagating the empowerment of programming out to the end user and making us all (Unlicensed) Software Engineers.

I greatly fear any attempt to codify what is not understood.

Note that there has been a certification process available (CDP) for a long time. Does anyone pay attention to it?

Actually, there may be a good side to this. From the proposed act:

9. (New section) No person shall practice, or present himself as able to

practice, software 1[engineering] \_\_\_\_\_1 unless he possesses a valid license as a software 1[engineer] \_\_\_\_\_1 in accordance with the provision of this act.

I guess we won't have to deal with nonprofessionals attempting to program their VCRs.

---

## **ACM SIGSOFT '91, SOFTWARE FOR CRITICAL SYSTEMS, Advance E-mail program**

*Judith Burgess <burgess@csl.sri.com>*

*Fri, 26 Jul 91 16:46:29 -0700*

ACM SIGSOFT: '91 SOFTWARE FOR CRITICAL SYSTEMS  
4-6 December 1991, Fairmont Hotel, New Orleans

### PRELIMINARY PROGRAM

Computer systems are increasingly affecting nearly every aspect of our lives. They control aircraft, shut down nuclear power reactors in emergencies, keep our telephone systems running, monitor hospital patients, and execute financial transactions. Although such systems offer considerable benefits, they also pose serious risks in that we are increasingly vulnerable to flaws and other deficiencies in the software, hardware failures, and effects of accidental and intentional computer misuse.

WEDNESDAY, 4 DECEMBER 1991

Welcome and Introduction: 8:45am - 9:00

Mark Moriconi, SIGSOFT '91 Chair (SRI International)  
Peter G. Neumann, Program Co-chair (SRI International)

Session 1: 9:00 - 10:15, Carl Landwehr, Chair

FORMAL VERIFICATION OF ALGORITHMS FOR CRITICAL SYSTEMS

John Rushby (SRI International), Friedrich von Henke (University of Ulm)

STATE-BASED MODEL CHECKING OF EVENT-DRIVEN SYSTEM REQUIREMENTS,

Joanne M. Atlee and John Gannon (University of Maryland)

Discussion

Session 2: 10:45 - 12:30, Dines Bjørner, Chair

RIGOROUS DEVELOPMENT USING RAISE,

Bent Dandanel (CRI, Birkerød, Denmark)

SPECIFYING AND VERIFYING REQUIREMENTS OF REAL-TIME SYSTEMS

K.M. Jensen, A.P. Ravn, and Hans Rischel (Tech. University of Denmark)

A SYSTEMATIC KERNEL DEVELOPMENT

J.F. Sjøgaard-Andersen, C.O. Rump and H.H. Lovengreen (Tech. Univ. Denmark)

Discussion

Luncheon: 12:30 - 2:00

Session 3: 2:00 - 3:45, Elaine Weyuker, Chair

THE INFEASIBILITY OF EXPERIMENTAL QUANTIFICATION OF LIFE-CRITICAL SOFTWARE RELIABILITY

Ricky Butler and George Finelli (NASA Langley Research Center)

PANEL: ARE THERE ABSOLUTE LIMITS TO SOFTWARE VALIDATION?

Elaine Weyuker (NYU Courant Institute)

Bev Littlewood (City University, London)

David Parnas (McMaster University)

Ricky Butler (NASA Langley Research Center)

John Musa (AT&T Bell Labs, Whippany, NJ) (unconfirmed)

The Butler/Finelli paper argues that ultra-high reliability cannot be validated directly with testing alone, nor by the use of fault-tolerance. What are the implications?

Session 4: 4:15 - 5:30, Martyn Thomas, Chair

PANEL: THE CONFUSED WORLD OF STANDARDS FOR CRITICAL SYSTEM

Martyn Thomas (Praxis, plc)

Robin Bloomfield (ADELARD) (unconfirmed)

Peter Neumann (SRI International)

Mike DeWalt (FAA)

Anticipated topics include British MoD DEFSTAN 00-55/56 and various security criteria (e.g., TCSEC, ITSEC, CTCPEC).

What role should such standards play? What should be mandated regarding requirements, specifications, criteria, methodologies, tools, and certification of developers?

THURSDAY, 5 DECEMBER 1991

Session 5: 9:00am - 10:30, Bill Howden, Chair

COMPARING FAULT DETECTING ABILITY OF TESTING METHODS

P.G. Frankl (Polytechnic University), E.J. Weyuker (NYU Courant Institute)

AN EXCEPTION HANDLING MODEL FOR PARALLEL PROGRAMMING AND ITS VERIFICATION

Valerie Issarny (IRISA/INRIA)

Discussion

Session 6: 11:00 - 12:30, Invitational Talk

HUMAN ERROR IN DESIGN

Henry Petroski (Duke University), author of the books "To Engineer is Human: The Role of Failure in Successful Design," and "Pencil"

Luncheon: 12:30 - 2:00

Session 7: 2:00 - 3:30, Victoria Stavridou, Chair

A REAL-TIME TRANSITION MODEL FOR ANALYZING BEHAVIORAL COMPATIBILITY OF TELECOMMUNICATIONS SERVICES

E.J. Cameron and Y-J Lin (Bellcore)

PROGRAMMING AND VERIFYING CRITICAL SYSTEMS BY MEANS OF THE SYNCHRONOUS DATA-FLOW LANGUAGE LUSTRE

C. Ratel (Merlin-Gerin), N. Halbwachs and P. Raymond (IMAG/LGI)

Discussion

Session 8: 3:45 - 5:30, Mark Moriconi, Chair

Invited Talks on Practical Experiences:

Emphasis is on difficult real-world problems, approaches to critical systems development, and lessons learned with respect to requirements, specification, design evaluation, testing, and other forms of assurance.

VALIDATION OF CRITICAL FLIGHT CONTROLS

Jim McWha (Chief Eng., 777 Flight Controls, Boeing)

TELEPHONE SWITCHING SYSTEMS

Michael Meyers (AT&T Bell Labs)

A CASE STUDY OF THE THERAC 25 ACCIDENTS

Nancy Leveson (U.C. Irvine)

Session 9: 8:00pm - 9:30pm, Evening Poster Session

FRIDAY, 6 DECEMBER 1991

Session 10: 8:30am - 10:30, Hermann Kopetz, Chair

STEPWISE DESIGN OF REAL-TIME SYSTEMS

Reino Kurki-Suonio (University of Technology, Tampere)

ON SATISFYING TIMING CONSTRAINTS IN HARD-REAL-TIME SYSTEMS

Jia Xu (York University), David Parnas (McMaster University)

AUTOMATED ANALYSIS OF BOUNDED RESPONSE TIME FOR TWO NASA EXPERT SYSTEMS

C-K Wang, R-H Wang, D-C Tsou, J.C. Browne, and A.K. Mok (University of Texas, Austin)

Session 11: 11:00 - 12:30, Hermann Kopetz, Chair

Open discussion of Real-time Issues

PANEL: WHERE ARE WE AND WHERE SHOULD WE BE HEADED?

Nancy Leveson, (U.C. Irvine) and others.

What is the state of the art in building critical systems?  
What are the limitations of the various approaches? What is needed?

Adjournment at 12:30

=====

ADVANCE REGISTRATION FORM

SIGSOFT '91 -- Software for Critical Systems  
Fairmont Hotel, New Orleans, Dec. 4 -- 6, 1991

Name \_\_\_\_\_  
Affiliation \_\_\_\_\_  
Address \_\_\_\_\_  
City, State and Zip \_\_\_\_\_  
Phone (and FAX) \_\_\_\_\_  
email address \_\_\_\_\_  
ACM or SIGSOFT Membership No. \_\_\_\_\_

Registration Fees (Circle one)

Category	Before	After
	Nov. 1	Nov. 1
ACM or SIGSOFT Member	\$280	\$330
Non-Member	\$330	\$380
Full-time Student	\$180	\$230

To pay by credit card, circle one: AMEX    VISA    MC  
Name on card \_\_\_\_\_  
Card number \_\_\_\_\_ Exp. date \_\_\_\_\_  
Signature \_\_\_\_\_

Make checks payable to SIGSOFT '91 in U.S. dollars. Requests for refunds must be received by Nov. 15. Fees include 3 continental breakfasts, 2 lunches, and the Proceedings.

Dietary requests: vegetarian \_\_\_\_\_ Kosher \_\_\_\_\_ Other? \_\_\_\_\_

SEND THIS FORM WITH FULL PAYMENT TO:  
Judith Burgess / EL266, SRI International, 333 Ravenswood Ave.,  
Menlo Park, CA 94025, USA

For further information, contact Judith Burgess,  
burgess@csl.sri.com phone: (415) 859-5924, FAX (415) 859-2844

NOTE: REGISTRATION BY EMAIL OR FAX IS ALSO PERMITTED (ONLY WITH CREDIT CARD)a.  
(RISKS FORUM READERS MAY PREFER TO TRANSMIT CREDIT CARD NUMBERS BY PHONE OR FAX  
OR OTHER OUT-OF-BAND MEDIUM IF YOU PREFER NOT TO SEND IT ON-LINE!)

=====

FAIRMONT HOTEL RESERVATION FORM  
SIGSOFT '91 -- Software for Critical Systems

New Orleans, Dec. 4 -- 6, 1991

Name \_\_\_\_\_  
 Affiliation \_\_\_\_\_  
 Address \_\_\_\_\_  
 City, State and Zip \_\_\_\_\_  
 Phone (and FAX) \_\_\_\_\_  
 Date/Time of Arrival \_\_\_\_\_  
 Date/Time of Departure \_\_\_\_\_

Room Rates (subject to taxes):

Circle one:           Single \$99       Double/Twin \$119

RESERVATIONS: 1-800-527-4727 or 1-504-529-7111

To guarantee your reservation by credit card:

Circle one: AMEX   MC   Visa   Carte Blanche   Diners Club

Name on card \_\_\_\_\_  
 Card number \_\_\_\_\_ Exp. date \_\_\_\_\_  
 Signature \_\_\_\_\_

These rates apply from Nov. 29 through Dec. 8, subject to availability.  
 Reservations must be received 30 days in advance. A deposit for the first  
 night must accompany your reservation to guarantee it for arrival after 6:00pm.  
 Cancellations must be made 24 hours in advance.

SEND THIS FORM TO:

The Fairmont Hotel, University Place, New Orleans, LA 70140, USA

=====

For further information on the conference, contact Judith Burgess. The General  
 Chairman is Mark Moriconi, Computer Science Laboratory, SRI International, Room  
 EL-249, 333 Ravenswood Ave., Menlo Park CA 94025-3493 (phone 415-859-5364,  
 Internet moriconi@csl.sri.com). Program CoChairs are Peter G. Neumann at SRI,  
 Room EL-243 (phone 415-859-2375, Internet neumann@csl.sri.com) and Nancy  
 Leveson of the University of California at Irvine (currently on sabbatical at  
 the University of Washington, phone 206-543-1695, Internet  
 leveson@cs.washington.edu). The Program Committee consists of David Barstow  
 (Schlumberger), Dines Bj/orner (Technical University of Denmark), Marie-Claude  
 Gaudel (Universite de Paris - Sud), Jim Horning (DEC Systems Research Center,  
 Palo Alto CA), Bill Howden (University of California, San Diego), Hermann  
 Kopetz (Technical University of Vienna), Carl Landwehr (Naval Research  
 Laboratory), Bev Littlewood (City University, London), Leon Osterweil  
 (University of California, Irvine), David Parnas (McMaster University,  
 Hamilton, Ontario, Canada), Fred Schneider (Cornell University), Vicky  
 Stavridou (University of London), Martyn Thomas (Praxis, Inc.), Walter Tichy  
 (University of Karlsruhe), and Elaine Weyuker (NYU Courant Institute).

Johnette Hassell, Tulane University, is managing Local and Travel Arrangements.

[Judith Burgess is handling just about everything else, and all questions should be directed to her.]



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 12: Issue 11**

**Tuesday 30 July 1991**

## Contents

- [DEFSTAN 00/55-56](#)  
[Victoria Stavridou and Andres Ravn](#)
- [Computer problems at BCCI](#)  
[David Shepherd](#)
- [Census data in the Land of Oz](#)  
[Michael Panosh](#)
- [Soft Eng Cntrl aids during Hydraulic Failure \(Science News\)](#)  
[Jeffrey Sorensen](#)
- [Risks of human error in Soviet nuclear "industry"](#)  
[Ken Mayer](#)
- [Cardphone Problems in Ireland](#)  
[D.P.O'Donoghue](#)
- [Book review: Practical Unix Security](#)  
[Clifford Stoll](#)
- [\\*WRONG\\* ftp-adress in Brunstein: Index of Known Malware](#)  
[Eibo Thieme](#)
- [Re: Smart cockpit with no backup](#)  
[Henry Spencer](#)
- [Re: The limits of simulation](#)  
[Henry Spencer](#)
- [Re: Licensing of Software Engineers](#)  
[Henry Spencer](#)
- [Data entry is NOT software engineering..](#)  
[Thomas P. Blinn](#)
- [New Jersey "software engineering" registration legislation](#)  
[Arthur Rubin](#)  
[A. Padgett Peterson](#)  
[Christopher R Riley](#)  
[Chris Riley](#)  
[Joseph Beckenbach](#)
- [Flawed assertion in RISKS-12.08](#)  
[Mark Seecof](#)
- [Re: Risks of Posting to RISKS](#)  
[Jerry Hollombe](#)
- [Info on RISKS \(comp.risks\)](#)

---

## ✂ DEFSTAN 00/55-56

<Victoria.Stavridou@prg.oxford.ac.uk>

Tue, 30 Jul 91 13:11:43 BST

### A COMMENT ON THE REVISED UK MOD STANDARDS 00-55/56

Victoria Stavridou (RHBNC, Univ of London) and  
Anders Ravn (DTH, Technical Univ of Denmark)

Our overall impression is that both interim standards have been substantially improved as a result of the public review exercise undertaken last year. This is particularly true of 00-55 which has been transformed from a long, confused and heavily prescriptive document to a much more sensible 2-part volume which describes the desired goals (Part 1/1 -- Requirements), suggests techniques for achieving these goals and identifies problems associated with certain practices (Part 2/1 -- Guidance).

We have found that the formal methods content has been fully retained in this 2nd version and has in fact been improved since its interactions with non formal design and development aspects have, in many cases, been identified. For instance, the roles of the formal specification and the English commentary have been properly assigned (1/1 29.1) and appropriate uses are suggested (the requirement for verifying the English commentary has been removed!).

Furthermore, this second version of the standard is far less prescriptive. Instead it identifies the goal and then leaves the designer/programmer free to use whatever techniques he wants so long as an overall requirement is satisfied. For instance, instead of banning dynamic memory allocation, there is now a requirement that the storage bounds during normal operation must be analysed and peak memory utilisation should not exceed 50% (2/1 30.50.2). The effect of these changes is that now ProCoS programs (which is of particular interest to us) would comply with the standard which was not the case for the previous version of 00-55.

We are, however, less happy with the very weak links between 00-55 and 00-56. 1/1 8.2 on safety integrity analysis requires that this is carried out in accordance with 00-56; there is, however, no explicit way of relating the state/event spaces of the hazard analysis stage with that of the specification and/or program. This is a giant leap which assumes perfect physical components such as unfailing actuators and sensors! Current work between RHBNC and DTH is investigating this issue for the ProCoS \$SL\_0\$ and fault tree analysis using a gas boiler as the running example.

As a minor point, 00-56 states (6.8.1 Table 9) that the probability of human failure to act correctly in reasonable time after the onset of a high stress condition is between 0.3 and 1.0. It seems to us that a probability of 1.0 is pretty probable as in this case one knows exactly what the human is going to do! You just take the negation!

---

## ✂ Computer problems at BCCI

David Shepherd <des@inmos.com>

Mon, 29 Jul 91 11:20:42 BST

Recent UK newspaper reports have commented that the receivers who are trying to sort out the fraud at the now closed Bank of Credit and Commerce International (BCCI) are being greatly hindered by the fact that all the data is stored on an "archaic" computer system. They are also concerned that someone tipped BCCI off about the investigation before the bank was closed and that the computer records have been deliberately confused.

david shepherd: des@inmos.co.uk or des@inmos.com tel: 0454-616616 x 379  
inmos ltd, 1000 aztec west, almondsbury, bristol, bs12 4sq

[A strong suspicion is that the records had been deliberately confused all along. PGN]

---

### **✂ Census data in the Land of Oz**

Michael.Panosh, Unix.Education, Australia <MWP.MICHAEL@melpn1.prime.com>

Tue, 30 Jul 1991 12:49:36 +1000

Australia is coming up to another census exercise. Overheard on a breakfast radio news broadcast (paraphrase):

"Confidentiality of data is assured as all the census papers are shredded."

Reassured me no end!!

Michael Panosh, Prime Computer, Australia -- mwp.michael@melpn1.prime.com

---

### **✂ Science News Article: Soft Eng Cntrl aids during Hydraulic Failure**

Jeffrey Sorensen <sorensen@spl.ecse.rpi.edu>

Mon, 29 Jul 91 12:20:05 EDT

[Jeffrey drew PGN's attention to a Science News article, 27 July 1991 (V 140, N 4, p 63), entitled "Software may ensure safer landings". It discusses recent problems with hydraulics (including the 1989 Iowa failure), and discusses a new software system:]

The new software system has been tested on various flight simulators, including ones for the McDonnell Douglas F-15 and the Boeing 720. These simulators showed that with only manual control of the engines, crews could maneuver their planes but would have great difficulty landing. With software-controlled engines, however, pilots repeated simulated safe landings -- even in turbulence and crosswinds.

[For the full article, contact Science Service, Inc., Editorial and Business Offices, 1719 N St. N.W., Washington DC 20036 (202-785-2255)]

## **✂ Risks of human error in Soviet nuclear "industry" (Blinn, [RISKS-12.08](#))**

Ken Mayer <ken@visix.com>

Mon, 29 Jul 91 17:27:44 -0400

Whenever I see the words "human error" I always think "human interface design error." I bristle at the idea of blaming people instead of poor design because the operators are the ones who are least able to defend themselves. The most highly skilled, trained human being will still make mistakes every now and then. It is up to designers to build systems that tolerate mistakes, and provide an unambiguous path to a solution.

---

## **✂ Cardphone Problems in Ireland**

"Parsifal aka D.P.O'Donoghue" <8614903@ul.ie>

Mon, 29 Jul 1991 14:20 GMT

The recent thread about disturbances in phone software brought to mind the disruption earlier on in the year to the Cardphones installed by Telecom E/ireann (Irish State phone co) around this campus.

For some reason -never explained or publicised- for a period of approx 2 weeks users could utilise the Cardphones on Campus free of charge. Somehow someone discovered that by dialing the free number "17" (used to test ringback etc), hanging up and then lifting the receiver when the ringback occurred a dialtone was available. This news spread like wildfire amongst the non-Irish students here who took the opportunity to ring home. A certain amount of discreet observation meant that other people found out the method and rang for nothing.

About two weeks later all the cardphones were out of order with a notice stating that a "network upgrade" was taking place and that was the end of that.

Desmond P.O'Donoghue 8614903@ul.ie

---

## **✂ Book review: Practical Unix Security**

Clifford Stoll <well!cliff@fernwood.UUCP>

Wed, 24 Jul 91 14:11:43 pdt

Practical Unix Security, by Simson Garfinkel & Gene Spafford  
O'Reilly & Associates, Inc. ISBN 0-937175-72-2

Now, here's a book that's long overdue. If you're managing a Unix system, get this book. You'll learn much more than just how to secure your system. Garf and Spaf walk you through networks, file systems, and Unix internals, a tour customized for finding security weakness.

Previous Unix security books were aimed at stand alone systems; this is the first that discusses Unix security in a networked environment. It's a practical book ("Never use

Set-User-Id-Shell Scripts") with an underlying current of "here's how Unix works -- be careful of this wrinkle".

Plenty of good stuff here: A chapter on how to discover a break-in, another on legal issues and privacy. A list of sensitive files in Unix. How to figure out Unix log files. Security implications of X-windows and NFS. Kerberos and Secure RPC. Most important, this is the first book to show you how to secure your computer in a networked environment.

Today, most Unix computers have no system administrator. For others, a single manager handles for dozens of workstations. Old time security -- strict isolation -- just won't work. Instead, security depends on understanding acceptable network interactions. For a harried system manager, this book will pay for itself in aspirin.

A few omissions: secure id cards, intrusion detection expert systems, and the Andrew File System. A few chapters are wasted on obvious things: backup your data, change your passwords, RS/232 pinouts, and the old shopworn arguments about what a hacker is.

It's sad that this book needs 500 pages. Their security checklist is twelve pages long -- nobody will ever go through the entire list. Is this the fault of the authors? Or of Unix? Hard to say, but I sure wish there were an faster path to a tight system.

-reviewed by Cliff Stoll 22 July 1991

---

**\*WRONG\* ftp-adress in Brunstein: Index of Known Malware ([RISKS-12.08](#))**

*Eibo Thieme <eibo@rosun1.informatik.uni-hamburg.de>  
Mon, 29 Jul 91 16:51:00 +0200*

The adress of our ftp-server contained a small error, here is the correct version. But remember that our line is really slow !

VTC documents (Index of Known Malicious Software: IMSDOS.791; Index of Virus Catalog: Index.791; all entries classified up to now) are now available from FTP:

Our FTP server: ftp.informatik.uni-hamburg.de  
^^

Login anonymous  
ID as you wish (preferably your name)  
dir: directory of available information  
cd pub/virus: VTCs documents

---

**\* Re: Smart cockpit with no backup**

*<henry@zoo.toronto.edu>  
Tue, 30 Jul 91 12:54:16 EDT*

>... In the event of a computer failure, the only good that mechanical backup  
>instruments would do would be to let the pilot watch the altitude ticking off...

There is some justice in this; "if the computer fails, you're dead". But...  
"The" computer? \*Which\* computer? "Fails"? Fails \*how\*? It is not at all  
inconceivable to have a failure in which some control remains but sophisticated  
instrument presentations are scrambled or absent. Indeed, one would hope that  
the last-ditch emergency fallback mode of the software would be to provide  
basic control and nothing more.

Henry Spencer at U of Toronto Zoology

---

### **✉ Re: The limits of simulation**

<henry@zoo.toronto.edu>  
Sun, 28 Jul 91 19:58:59 EDT

> simulations of the [motor's] firing dynamics did not reveal subtle factors

Actually, this may not quite be true, it turns out. I'm told, by folks I  
shouldn't identify, that some of the simulation work \*did\* at least hint at  
problems. This was not followed up, possibly as a deliberate decision by  
managers who didn't want to hear bad news.

Henry Spencer

---

### **✉ Licensing of Software Engineers**

<henry@zoo.toronto.edu>  
Tue, 30 Jul 91 13:06:41 EDT

>It only requires licensing of those who offer themselves for hire as software  
>ENGINEERS. Hire and engineer are both key words...

An excellent point. Many of the readers of this list may not be aware that  
it is \*already\* illegal to offer yourself for hire as, say, a "mechanical  
engineer" without being a licensed professional engineer. The NJ law is  
closing a loophole in existing practice, not introducing something new and  
radical. "Engineer" is the crucial word; that term is legally protected  
and cannot be used frivolously... in any other field.

(One exception to this: if you are working for somebody else, \*they\* can call  
you an "engineer" without requiring such qualification. [There may be some  
slight restrictions on this, I'm not up on details.] The more activist  
engineers have been known to agitate for removal of this rather large  
exemption.)

Far too many people call themselves "software engineers", many of them having  
nowhere near the background and demonstrated competence expected of a licensed  
engineer in more traditional fields. While implementing the NJ law is going to  
be, um, a learning experience for all concerned, it's a step in the right  
direction.

Henry Spencer at U of Toronto Zoology

---

## ✂ Data entry is NOT software engineering.

*"Dr. Tom @MKO, CMG S/W Mktg" <blinn@dr.enet.dec.com>  
Tue, 30 Jul 91 09:04:08 PDT*

In [RISKS 12.10](#), Bill Murray and Bob Frankston comment on the NJ legislation requiring the registration of "software engineers".

On the whole, I agree with Bill Murray. In spite of the fact that I program, and have even done a certain amount of "software engineering", I doubt that I could qualify as a "registered professional software engineer", in spite of my formal education (at the doctoral level) in computer and computing science and applied statistics.

I find it amusing that Bob Frankston asks "What about a VCR programmer?" The stories of unusable human interfaces in commercial VCRs abound, but I'd hardly characterize the "data entry" aspect of most home VCR use as "programming". In fact, if "VCR programmers" were really software engineers, they probably would have learned (at least a modicum) of human factors considerations, and the products extant in the marketplace might be more approachable.

Bob assumes the legislature is attempting "to codify what is not understood." Actually, the registration and certification of professional engineers is well understood, and it is the very lack of such that evidences the non-professional status of our business.

Dr. Thomas P. Blinn, Digital Equipment Corporation, Digital Drive -- MKO2-2/F10  
Merrimack, New Hampshire 03054 ...!decwr!dr.enet.dec.com!blinn (603) 884-4865

---

## ✂ New Jersey "software engineering" registration legislation

*<a\_rubin@dsg4.dse.beckman.com>  
Mon, 29 Jul 91 13:18:49 PDT*

.... and risks of not looking at your posting software. The original file uses backspace characters to simulate underlining. Most of the underlined text was "design/designing" replacing "engineer/engineering".

2165888@mcimail.com 70707.453@compuserve.com arthur@pnet01.cts.com (personal)  
a\_rubin@dsg4.dse.beckman.com (work)

---

## ✂ Software Engineering Registration (NJ)

*A. Padgett Peterson <padgett%tccslr.dnet@uvs1.orl.mmc.com>  
Mon, 29 Jul 91 17:06:29 -0400*

The concept of registration for "software engineering" seems novel in that the proposal seems to both go too far and not far enough (thanks Bill).

The concept that all programming be regulated, even all commercial programming, is ludicrous. At the same time certain categories of programming cry out for regulation.

As a licensed Professional Engineer, my primary responsibility is to ensure that certain engineering tasks are done in accordance with regulation and in a safe manner. The state of Florida has decided that I (as a result of experience and testing) am competent to determine this. One of the not-so-evident responsibilities is to not accept work that I am not qualified to perform.

In the past, I have had the opportunity to work on many projects that did not require licensing including digital flight controls for several aircraft and a communications topology for the FAA National AirSpace Plan, two areas that probably should have been covered by such licensing.

Other areas that come to mind are many medical software elements, computer assets used for road and traffic control, and emergency telecommunications networks. Certainly, IMHO in recent months we have seen several examples of what happens when software is developed without evident control.

That complex software is difficult to debug does not seem to be an adequate defense for mistakes yet as more and more software replaces mechanical processes, the potential for danger increases. Certainly the computer in my wife's car is easily overridden since mechanical linkages from the wheel to the steering and from the accelerator to the throttle plate still can override any electrical command. A computerized highway control system is another matter. Consider the implications if a traffic signal were to display green in all directions simultaneously. (Yellow might be worse).

Consequently, as more sophisticated systems come into use, a formal method needs to be established to determine that adequate safeguards are provided. The problem is that often, only the designer or design team has the expert knowledge of a particular system required to determine its safety.

This is the reason that registration of engineers came about in the first place: since every critical design cannot be validated, we have to validate the designer. It is not the perfect answer, merely the best choice from what we have.

The major problem that comes about is in designing a certification process that achieves its goals, not an easy task in any discipline but even more so in software since it is still evolving. In electrical engineering, the processes involved in providing adequate power for a building are well defined and codes have been developed that set out these rules. Nothing similar exists for software.

To make matters more difficult, while electrical quanta are reasonably well defined (Alternating Current usually means either 60 or 400 hertz for most purposes & leads and lags are well defined), good computer software must consider the platform, clock speed, memory speed, bus speed, race conditions, failure conditions and a host of other variables, something many programmers are insulated from.

Consequently, at some point, critical designs must be examined by someone who understands not merely the software, but the compiler, the operating system, the CPU, and the installation as well. I would not feel very safe near a nuclear power facility using a control program designed in Visual BASIC by someone who only understood Windows (trademarks acknowledged) though the approach might be well suited to balancing my checkbook.

I can see a very valid need for a counterpart in software to the same certifications a licensed engineer makes when signing off on an engineering design: (in English)

- 1) I am competent to decide if this design is safe and meets applicable design standards.
- 2) I have examined this design in sufficient detail to make this determination.
- 3) Based on study and in my professional opinion this design is safe & meets all applicable standards.
- 4) By affixing my seal, I personally certify that this design and my study of it meet the above criteria.

While the general public is often only aware of (3), all elements are actually present and failure of any element is grounds for censure/suspension/revocation of a professional license - in fact most of the board actions that I see result from defects in (1) or (2).

It should also be mentioned that in many organizations, often only the Chief Engineer needs to be licensed. I would suspect that a Software Engineering license would be much the same.

In short, I can see a very real need for such a licensing requirement, not globally but for those engaged in approval of critical or safety-related projects. The major problem will come from the certification process itself given the bewildering array of platforms, embedded micro-controllers, and languages. It will not be trivial to implement but is something that needs to be done.

A. Padgett Peterson, P.E.

---

## **✉ Re: Licensing of Software Engineers**

*Christopher R Riley <chris@mtuxo.att.com>*

*Tue, 30 Jul 91 11:52:52 EDT*

I think there is a misunderstanding of who is to be licensed. I have seen copies of the text that says "software 1[engineer] \_\_\_\_\_1" and another that says "software 1[engineer] designer1". The footnote at the bottom of page 1 of my copy says:

EXPLANATION--Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted in the law.

Matter underlined thus is new matter. Matter enclosed in superscript numerals has been adopted as follows:

- 1 Assembly ACP committee amendments adopted June 13, 1991.
- 2 Assembly floor amendments adopted June 24, 1991.

Some people's text does not have the word designers, but just the underlining (probably from backspace-underscore pairs in the text).

I think the bill is intended to license software designers. My question is, does this mean that all people who write any piece of software code is a software designer, and thus must be licensed?

Chris Riley chris@mtuxo.att.com

---

### **✂ Re: New Jersey "software engineering" registration legislation (J.M.Ritter)**

*Joseph Beckenbach {Adapter Software Release Engr} <jerbil@ultra.com>  
Mon, 29 Jul 91 18:48:09 PDT*

The two most relevant points here:

- 1) How does this Act differ from any other Engineering Licensure within NJ?

Answer: I don't know, but someone with a reasonable lawyer in New Jersey could probably find out some information for us. The language seems loose (regulating all practicing "software engineering"), but then we need to compare it to other language being used to regulate, eg, civil engineers.

To my mind, it's a large step in the right direction. Not everyone who's wrapped a bandage needs to be a licensed medical practitioner, just those who intend to make a living of it as a main provider. At least, that's a simplification of my understanding of licensure.

- 2) How does this affect the "common practitioner"?

Answer: Again, I don't know. However, looking at the parallels with other professions, I would venture my layman's interpretation: only those with proper qualifications may legally use the word "Engineer" to refer to themselves professionally.

It does mean that all the job descriptions titled "Software Engineer" will need to turn into "Member of Software Technical Staff".

I'll try to look over it a bit more before adding more humble opinion to the network. Meanwhile, it needs comparison to other Engineering Licensure statutes, such as for civil engineers and architects.

Joseph Beckenbach  
Californian "software-engineer-wannabe"

Test programs not programmers, but license software ENGINEERS!

Joseph Beckenbach jerbil@ultra.com 408-922-0100 x246

---

✂ **Flawed assertion in [RISKS-12.08](#)**

Mark Seecof <marks@capnet.latimes.com>

Fri, 26 Jul 91 11:49:15 -0700

I'm catching some (well-deserved) heat about my assertion that it would "obviously" be impossible for a large majority of drivers to be "(much) better than average." This was poorly expressed, especially if "average" means "arithmetic mean" (of scores in some simple metric).

I should have written out my opinion that an "ability score" versus population plot would reveal a typical "bell-shaped curve," that most drivers would have scores near the middle, that few drivers would score very far above the median, that by definition half of them would score at or below it, and that biases (thank you, Mr. Tanner <mtanner@gmu.edu>) in drivers' perceptions of other drivers on the road would factor into their self-assessment of superiority in such a way as to render it over-optimistic.

[Messages were received from Tim Smith <ts@cup.portal.com>:

"1 1 8 8 8 8 9 9 9 9. Note that the average of these 10 numbers is 7. Note that a large majority of them are above average. This is obviously possible."

... and Jeremy Grodberg <lia!jgro@fernwood.mpk.ca.us>:

"And when it looks like statistics are \*not\* being abused, remember that 97.325% of all statistics are made up." ]

---

✂ **Re: Risks of Posting to RISKS (Dunlop [RISKS-12.06](#))**

The Polymath <hollombe@ttidcb.TTI.COM>

Thu, 18 Jul 91 15:42:44 -0700

There seems to have been an enormous misunderstanding here. That, or lawyers have gotten into the works, somewhere. I hope I can clear things up to everyone's satisfaction.

}In [RISKS 12.02](#), Jerry Hollombe describes our publication of his 1989 RISKS }posting about the "censorship" of rec.humor.funny at Stanford University. Mr. }Hollombe's piece was reprinted (with his permission) in Charles Dunlop and Rob }Kling (eds), *Computerization and Controversy: Value Conflicts and Social }Choices* (Boston, Academic Press, 1991, ISBN: 0-12-224356-0). (See pp.376-379).

[Further details omitted]

Absolutely true. I gave my permission. I had no complaints then and I have none now. In fact, I'm quite proud of having been included in the

book and have been calling my friends' attention to it. Some have expressed interest in obtaining copies for themselves. (I'm reading through it as time permits. So far I've found it interesting and thought provoking).

}... However, we did not effectively anticipate this new controversy }about computerization: one's ability to fairly reprint RISKS (or any BBS) }postings after posters have given explicit permission!

I certainly never intended to raise such an issue. Even if I did have a change of heart (which I didn't) I like to think I'm honorable enough to live with the consequences of my actions. My word, once given, stands. I would not retract it even if I wanted to and could. You had my permission to publish. That stands.

} Unfortunately, Mr. Hollombe attributes his problem with the reprinting of }his RISKS posting solely to publishers and editors, and he conveniently ignores }his control over the publication. In [RISKS 12.02](#) he writes:

}  
>The risk? The words we exchange here aren't as ephemeral as they may }>appear on a VDT screen, so be careful what you say and how you say it.  
>You never know who might decide to package and ship it to a customer.  
>{:-  
> } This complaint strikes us as unfair. ...

This was not intended as a complaint and I'm amazed, and horrified, to see it interpreted as one. As I said in my posting, and have repeated here, I gave my permission for my words to be published. I've had no regrets about that, then or since. Very much the contrary, in fact.

What I was attempting to convey was the idea that many people read, keep copies of and even disseminate what's posted here. It therefore behooves us to write thoughtfully, at least. On a more mundane level, I might have been more reluctant to give permission to use my posting if it had been full of spelling and grammatical errors. I was NOT complaining about the fact of its publication.

}... We believe that ... }we were VERY FAIR to Mr. Hollombe.

I believe you were more than fair. I'd say you were outright generous. I'm not complaining. Tell your lawyers to relax, if that's the problem. I'm not going to sue you. I like being published. Really.

I don't know what more I can say at this point. Please feel free to contact me directly if you have any further questions about the matter. I'll be happy to reconfirm my permission to publish, in writing if that will help.

(Alas, it seems the old risk of being misunderstood in written media is alive and well. That's no one's fault. It's just the nature of the situation).

Jerry Hollombe, Citicorp, 3100 Ocean Park Blvd. Santa Monica, CA 90405

{rutgers|pyramid|philabs|psivax}!ttidca!hollombe (213) 450-9111, x2483



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 12: Issue 12**

**Monday 12 August 1991**

## Contents

- [Teenage Hacker Emulates Hess](#)  
[PAJ](#)
- [Future Risks](#)  
[Hilarie Kauiolani Orman via Richard Schroepel](#)
- [Security comes to the Free Software Foundation](#)  
[Martin Minow](#)
- [Lotus Marketplace Epilogue](#)  
[Marc Rotenberg](#)
- [Computer frustration](#)  
[Andrew Goldberg via Les Earnest](#)
- [Yet another threat to telephone privacy](#)  
[Jeff Makey](#)
- ["Enemy of the State" -- Story on risk to privacy \(Richard Thomsen\)](#)
- [Firefighters won't give first aid to AIDS patients](#)  
[Sean Eric Fagan](#)
- [Lifestyle discrimination](#)  
[Martyn Thomas](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Teenage Hacker Emulates Hess

*paj* <[paj@gec-mrc.co.uk](mailto:paj@gec-mrc.co.uk)>  
9 Aug 1991 11:54:25-BST

Summarised from Computer Weekly, 8th August 1991.

A 16 year old schoolboy named Jamie Moulding has been cautioned by plain-clothed police after hacking into a military computer and trying to sell secrets to the USSR. He claims to have read the Ministry of Defence personnel and payroll files. One computer he entered held details of a British Army tank control system. Moulding first incorporated details of the system into his own simulation package, and then phoned the Soviet Union's London embassy to try to sell the information. Next day two policemen turned up at his home and spoke to his parents.

Moulding's telephone bills were unwittingly paid by his school. He wrote an autodialer program and an automatic hack program which "planted a command which led to a display of passwords".

DEC denied that its systems had been hacked. The police officers were unavailable for comment.

---

## ✂ Future Risks

*Hilarie Kauiolani Orman <ho>  
Sat, 10 Aug 91 02:54:22 PDT*

[Via [fermat!r@la.tis.com](mailto:fermat!r@la.tis.com) (Richard Schroepfel)]

### TINY BUG IN H.S. "GENOME" CAUSES MASSIVE HUMANITY FAILURE

Officials responsible for a spiral galaxy near the middle section of the universe revealed today that a small error in an encoding for the life form "Homo sapiens" was responsible for the near extinction of the partly intelligent species. The change had been introduced during routine maintenance of the life form. Officials explained that the maintenance had been intended to improve the survivability of the species, but inadequate testing had caused it to become susceptible to a new sexually transmitted disease.

Senior universe officials expressed disappointment in the control of the life forms in the galaxy, citing a series of malfunctions, especially near a yellow star at the edge. The H.S. species has required several patches in the field and still seems unstable. The latest change was not tested in alternative universes due to lax controls and lack of funding.

Other officials cited inadequate specification and design review. "How can we guarantee that the species works without a formal definition of what it is?" lamented one senior observer. "These things just look like collections of cells - they just sort of grow. There's no mathematical model that can be used to verify it. I don't see how they ever got it started in the first place."

Insiders feel that the species can be rescued, but expressed doubt about its long-term viability. The estimate of the time needed for a thorough review of the documentation, writing the formal specifications, and verifying the genome encoding, expressibility, and environmental testing, is greater than the lifetime of the universe.

Meanwhile, yet another mutation and alteration of the local laws of physics will be required to back out of this particular upgrade. With funding already stretched, this setback might just spell the end of H.S.

The formally verified Vulcan species, originally slated for production next year, has been delayed due to a series of technical problems and is now scheduled for beta testing after the next big bang.

---

## ✂ Security comes to the Free Software Foundation

Martin Minow 06-Aug-1991 0757 <minow@ranger.enet.dec.com>

Tue, 6 Aug 91 05:12:02 PDT

This is summarized from a front-page article in the Boston Globe, Aug 6, 1991.

The Free Software Foundation (FSF) has been forced to institute security (password) control because "vandals who were able to enter the foundation's system anonymously were not only deleting and trashing files there, but were also entering Internet ... and doing damage in other systems as well." ...

"Michael Bushnell, a programmer at the Free Software Foundation, said the changes are making systems more inconvenient to use and creating an international network that cannot be used without an operator putting himself under surveillance.

""There's not a big sharp impact because, over time, so many networks already created security barriers," Bushnell said. Extension of these restrictions ... "is kind of like when the last critical-of-the-government newspaper is shut down. After it's gone a while, people notice a difference.""

"... An estimated 1,000 to 2,00 persons gained access ... and staff members say they will try to preserve this somehow."

""I feel ashamed not having an open system," says [Richard] Stallman, ... "I feel ashamed having a system that treats everyone as vandals when in fact very few were. ... Every time I think about this I want to cry.""

-----

The above summarizes the first half of a long story. The remainder discusses trust, community, hacking, and access in terms and concepts that will be familiar to Risks readers. About a week ago, Richard Stallman was interviewed on the local NPR morning news (the local portion of Morning Edition) on the closure of the FSF systems.

Personal observation: a few years ago, I had "tourist" access to Internet through an FSF computer and, many years before that, tourist access through MIT-AI. Now, I have (password-protected) access through another MIT system, one of the few that will allow access from "known to be trustworthy" persons.

Martin Minow

minow@ranger.enet.dec.com

[And here is PGN putting out this issue from New Haven, where he will be participating in the National Conference on Computing and Values this week, having expected to be involved in a lively discussion with Richard who might have opposed my position on why security (at least for integrity and availability purposes if not for confidentiality) remains necessary even in an open world... But I am really sorry to see FSF getting cracked. PGN]

---

## **✉ Lotus Marketplace Epilogue**

Marc Rotenberg <Marc\_Rotenberg@washofc.cpsr.org>

Thu, 8 Aug 1991 20:56:02 EDT

Lotus Marketplace Epilogue

CPSR Endorses Equifax Privacy Decision

August 8, 1991

WASHINGTON, DC -- Computer Professionals for Social Responsibility (CPSR) announced today that it supported a decision by Equifax to discontinue the sale of direct marketing lists derived from consumer credit files. CPSR Washington Office Director Marc Rotenberg said, "Equifax did the right thing. Personal financial information should not be fair game for direct marketers. "

The national membership organization of computer professionals had earlier lead a successful campaign to stop the release of "Lotus Marketplace," a series of computer diskettes containing detailed information on 120 million consumers. Name and address information in Marketplace was taken directly from credit files. CPSR has recommended that businesses follow the "Code of Fair Information Practices," which requires that organizations obtain explicit permission before using personal information for secondary purposes, such as direct marketing.

Evan Hendricks, chairman of the United States Privacy Council, said that "This is another victory for the privacy movement in the United States. Equifax continues moving in a positive direction. We will follow this closely to see that their actions match their words. Meanwhile, the focus shifts to TRW and Trans Union who continue to sell mailing lists derived from credit report data."

Marc Rotenberg said that while CPSR was pleased with the recent Equifax decision, there were many other issues that consumers should watch on the credit privacy front, including the indiscriminate use of the Social Security Number, the practice of "pre-screening" credit applicants, and the continued sale of credit information by other credit reporting agencies.

Marc Rotenberg, CPSR Washington Office, 202/544-9240  
rotenberg@washofc.cpsr.org

---

## **✉ Computer frustration**

Andrew Goldberg <ango@jinn.stanford.edu>

Fri, 26 Jul 91 10:50:58 PDT

[Via Les Earnest <les@dec-lite.stanford.edu>]

From the NY Times

The annual Spring Comdex computer show in Atlanta earlier this month meant a booming business for the Bulletstop, an indoor firing range in suburban Marietta where customers can rent firearms and bullets to shoot anything they

please, as long as it is already dead and fits through the doors. The Bulletstop gave Comdex visitors a chance to vent their frustrations by venting PC's, printers, hard disks, monitors and manuals with lead.

Paul LaVista, the owner, said about 10 groups of high-tech types came in during the Comdex show. "I'm not a computer whiz, but one group brought in what looked like a hard disk and blasted it," he said. "Another bunch brought in some kind of technical manual. The thing was enormous, about 2,000 pages. They rented three machine guns -- an Uzi, an M3 grease gun and a Thompson -- and when they were done it looked like confetti."

"It must have been quite a show," LaVista said of Comdex. "Doctors and computer types usually have a lot of pent-up anxiety, but these folks were dragging when they came in. When they left they were really up. The range looked like a computer service center after a tornado."

LaVista said PC's were popular targets year-round. "People are frustrated with them," he said. A year ago seven or eight men carried in a giant old Hewlett-Packard printer. "I ran an extension cord to it, and just as it started to whirr and spit out paper, they blasted it," he said.

---

### **⚡ Yet another threat to telephone privacy**

*Jeff Makey <makey@visicom.com>  
Fri, 2 Aug 91 21:04:04 PDT*

I recently saw an advertisement for a device that lets you plug your telephone into any power outlet in your house, with the claimed benefit that you can use existing wiring rather than spend money wiring every room in your house for phone service. Intercom systems that use this principle have been around for years, with the less-than-obvious risk that a neighbor who is connected to the same power transformer can plug in a similar device in their own home and listen to your conversations. Extended to your telephone, such a neighbor can not only listen to your phone calls (apparently without violating any laws), but can now even make phone calls on your line (surely illegal, regardless of how it is accomplished).

The risks are comparable to those of cordless phones, only skewed a bit. Understandably, the advertisement made no mention of these risks.

:: Jeff Makey                      makey@VisiCom.COM

---

### **⚡ "Enemy of the State" -- Story on risk to privacy**

*Richard Thomsen <rgt@beta.lanl.gov>  
Fri, 2 Aug 91 14:58:02 -0600*

There is a lovely story in the August 1991 issue of Analogue Science Fiction Science Fact by Jack C. Haldeman II called "Enemy of the State" that shows the risks to privacy. It is a series of messages to a consumer. It starts out with a message from FOOD-NET, telling him about starting smoking

again and his pets (according to their records). Then comes a message from his service station, saying his car needs a tune-up and new tires (according to their records). Likewise, he gets messages from NED-CHECK, his dentist, the pet store, etc.

Then he gets a message from the sheriff's office, saying that they would like to discuss some things. For example, he gets his mail at a P.O. box, has an unlisted number, and an answering machine. They say "It is well known that individuals with such equipment are almost always concealing information, especially those with unlisted numbers." They mention deposits to his checking account, by amount and a cash transaction. They mention he is a "substance abuser (beer, nicotine, and caffeine)", the magazines he subscribes to, etc, and also say that "You exhibit wanton disregard for public safety by operating your motor vehicle without the proper maintenance any good citizen would perform as a matter of course."

All in all, an interesting story and quite appropriate to some of the discussions.

Richard Thomsen rgt@lanl.gov

---

### **🚒 Firefighters won't give first aid to AIDS patients**

Sean Eric Fagan <sef@kithrup.com>

Tue, 6 Aug 91 20:32:26 PDT

Arvada, Colo: Volunteer firefighters in this Denver suburb no longer will respond to first-aid calls involving people known to have AIDS or other infectious diseases, city officials said.

[Yes, there is a risk here... read on -- sef]

The fire department's computer system has been programmed to flash a warning to dispatchers if an assistance call comes from someone known to have an infectious disease such as acquired immune deficiency syndrome, said an Arvada official who spoke on condition of anonymity.

[end of excerpt]

Got a grudge against someone? Well, here's a way to cause them lots of problem! (\*extreme\* sarcasm there)

Sean Eric Fagan sef@kithrup.COM

---

### **🚒 Lifestyle discrimination**

Martyn Thomas <mct@praxis.co.uk>

Mon, 12 Aug 91 15:18:53 BST

According to a BBC news programme, there is a growing incidence of discrimination in US employment on the basis of employees' private lives. Examples were given of someone dismissed for smoking cigarettes at home

(detected by urine test), someone refused employment for living with someone to whom they were not married, someone refused employment for a dangerous hobby (hanggliding), someone sacked for being overweight.

If this is a real threat, it provides a compelling reason to shop only with cash, to stay off lifestyle marketing databases. Even a magazine subscription could cost you your job! Point-of-sale terminals could monitor how much alcohol you buy, and how often; how many cigarettes, pregnancy-test kits, junk food ...

Paranoia, anyone?

Martyn Thomas, Praxis plc, 20 Manvers Street,  
Bath BA1 1PX UK. Tel: +44-225-444700. Email: [mct@praxis.co.uk](mailto:mct@praxis.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 12: Issue 13**

**Monday 19 August 1991**

## Contents

- [Junk Mail in Outer Space: Shuttle test mail-bombed](#)  
[Peter Scott](#)
- [ATM mixup in New York](#)  
[John Martin](#)
- [Computer failure helps Bakhtiar murder suspect](#)  
[Fernando Pereira](#)
- [Deutsche Airbus 2000](#)  
[Martyn Thomas](#)
- [Bell V22 Osprey crash](#)  
[Martyn Thomas](#)
- ["Doctored" radios](#)  
[PGN](#)
- ["Virus Implants in DoD Weapons"](#)  
[David Risler via Jerry Leichter](#)
- [Cracker charged in Australia](#)  
[Fernando Pereira](#)
- [Profitable Drug Wars -- Innocents Presumed Guilty](#)  
[mauler via Charles Hoequist](#)
- [Patriot and Dhahran again](#)  
[Phil R. Karn](#)
- [Re: "Traffic crystal ball" may be in your car's future](#)  
[Secty Samuel Skinner](#)  
[\[editorial\]](#)  
[via Jeff Helgesen](#)
- [Risks of Calling Reporters in Ohio: Procter & Gamble](#)  
[PGN](#)
- [Risk of Power Failures in Computer Controls: 9 Mile Point](#)  
[PGN](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Junk Mail in Outer Space: Shuttle test mail-bombed**

*Peter Scott* <[pjs@euclid.JPL.NASA.GOV](mailto:pjs@euclid.JPL.NASA.GOV)>

*Mon, 12 Aug 91 14:22:35 -0700*

From *\_Information Week\_*, August 12 (who got it from *\_Newsday\_*, August 6, p.5):

#### SPACE HACKERS

A test of electronic-mail between earth and laptops aboard the space shuttle Atlantis was intended to lay the groundwork for use of E-mail on space station Freedom. But the test is in jeopardy after 80 E-mail messages were received by the Atlantis crew from unauthorized users. The leak behind the E-mail address remains a mystery. \*Junk Mail In Outer Space\*, Joshua Quittner.

Peter J. Scott, Member of Technical Staff | pjs@euclid.jpl.nasa.gov  
Jet Propulsion Laboratory, NASA/Caltech | SPAN: GROUCH::PJS

---

#### **✂ ATM mixup in New York**

*John Martin <martin@nynexst.com>  
Sun, 18 Aug 91 09:58:27 EDT*

The cover of the August 15th New York Daily News had a 9" x 11" photo of a man using an ATM, and a caption to the effect of "WANTED: This man is using an ATM card that was stolen from a rape victim 40 minutes ago."

The next day, a different man was charged with rape and robbery, and in the August 17th Daily News, the following was printed:

"Earlier this week, police released to the Daily News and other media outlets the photo of another man, saying that he was using a bank card stolen from a rape victim and that they wanted to question him.

"...DeMartino said the initial picture had "a time sequence that differed on the printout from the ATM. The bank said the error was created by the machine downloading.

"The mixup was "a very unfortunate situation," according to Bruce Herman, Apple Bank senior vice president and general counsel.

"There was no malfunction in the ATM system that night," Herman said. "All relevant records and materials with respect to ATM transactions on the night in question were made available to the police at their request for analysis and evaluation."

Unfortunately for the man in the photo, the admission of the mistake did not seem as well publicized as the photo.

John Martin martin@nynexst.com

---

#### **✂ Computer failure helps Bakthiar murder suspect**

*Fernando Pereira <pereira@klee.research.att.com>  
Sat, 17 Aug 91 11:24:20 EDT*

The AP reports from Geneva on 8/16 that one of the suspects in the murder in France of former Iranian prime minister Shapour Bakhtiar spend Monday and Tuesday night at a Geneva hotel, under a false Turkish identity. However, the failure of a police computer used to check hotel registration cards delayed until Wednesday the identification of the suspect, by which time he had already left (This seems to imply that the false identity was known to the Swiss police).

It is interesting how the failure of the computer system is blamed here for something that presumably would have happened anyway if the computer system did not exist. Or is it that the Swiss police have become so dependent on their computer databases that they no longer use slower, more traditional sources and methods (eg. alert hotel staff)?

---

### **✂ Deutsche Airbus 2000**

*Martyn Thomas <mct@praxis.co.uk>  
Mon, 19 Aug 91 13:07:19 BST*

Deutsche Aerospace has proposed a 615-passenger Airbus, according to Flight (3-9 July). DA's executive VP for design and technology says "The tailplane itself would be smaller, because the fly-by-wire flight control system would allow greater inherent instability ...."

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.  
Tel: +44-225-444700. Email: mct@praxis.co.uk

---

### **✂ Bell V22 Osprey crash**

*Martyn Thomas <mct@praxis.co.uk>  
Mon, 19 Aug 91 13:10:30 BST*

The Editor of Aerospace (the Asian monthly magazine) tells me that there was a recent crash of a Boeing Bell V22 Osprey "which tipped on its side due to an admitted 'glitch' in the lateral control system."

Does anyone have further information?

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.  
Tel: +44-225-444700. Email: mct@praxis.co.uk

---

### **✂ "Doctored" radios**

*"Peter G. Neumann" <neumann@csl.sri.com>  
Mon, 19 Aug 91 9:16:29 PDT*

Doctored radios revealed Iraqi moves during Gulf war: report

LONDON, Aug 18 (AFP) - Radio equipment sold to Iraq before the

Gulf war was fixed so that Britain could monitor transmissions giving the allies a crucial advantage during the conflict, the Sunday Telegraph reported here on Sunday.

The British manufacturers did not know that their export equipment had been tampered with "so that the messages sent by the Iraqis could be picked up by Britain's GCHQ intelligence nerve centre" at Cheltenham in western England, the weekly said, quoting senior parliamentary sources".

"Exchanges between Iraqi commanders were picked up and then passed on to the U.S. National Security Agency," the Telegraph quoted sources close to the government sources as saying.

The decision to fix the equipment had been taken well before war broke out, but "at a time when the intentions of the Saddam regime were of deep concern to Western strategists following the execution of journalist Farzad Bazoft and the uproar over the supergun affair."

---

### ✂ "Virus Implants in DoD Weapons"

*Jerry Leichter <leichter@lrw.com>*

*Tue, 13 Aug 91 07:23:52 EDT*

The following message appeared recently on VIRUS-L:

Date: 07 Aug 91 20:28:57 +0000  
From: dar@reef.cis.ufl.edu (David Risler)  
Subject: Virus Implants in DoD Weapons

From the August 1991 "Armed Forces Journal International"

"A draft Pentagon directive that called for implanting a computer "virus" or software disabling mechanism in every major new US weapon system - one that could be remotely triggered if the weapon fell into enemy hands - was under consideration last December at a high DoD level, a knowledgeable source told AFJI recently...If that is the case, the device is more likely to function as a variable duration "enabler"...rather than a disabler that could be remotely activated to prevent a weapon from being used. In all likelihood, no decision regarding implanting either kind of device in advanced weapons will come before the DARPA provides an assessment to Congress of how best to handle the issue. That report is expected on Capitol Hill by August."

The article goes on to say that this would be great for weapons exports and that EEPROMS could carry such "Trojan Horses" that could be activated using electrical signals. Hmmmmmm. Comments?

My comments: First off, I wish people would stop applying the word "virus" and "Trojan horse" to every new kind of software they come across. Such software would not spread, so it's not a virus; and there's little reason to hide the fact that it exists (though of course the details would be secret), so it's not a Trojan horse. "Software disabling mechanism" is about right, of

a bit wordy. Really, it's a lock, just like the lock on your car. It happens to be a "normally unlocked" lock, while most locks we deal with are "normally locked". The difference is understandable, given the circumstances under which the protected devices are used.

In many ways, there is nothing new here. All high-tech weapons already have, in effect, a "variable duration enabler": Their spare-parts supply. This isn't a particularly EFFECTIVE lock, since even in the best of circumstances it can take quite some time for a spare-parts store to be exhausted, and maintainers of military equipment usually prove to be very resourceful at stretching their supply. Besides, there's an active black market.

On a more prosaic level, it's been Soviet practice for years to build guns with a caliber just marginally smaller than that of their expected opponents. Soviet rifles can use NATO bullets, but NATO rifles can't use Soviet bullets - a very effective time-independent "lock".

There have already been jokes about soldiers forgetting the password needed to boot their tank. I'm sure this proposal will lead to all sorts of fears about similar problems. However, especially if implemented with an "enabler" rather than an external disabling signal, I see little problem from a technical point of view - and it strikes me as a very nice safeguard to have. Imagine if all of Iraq's weapons had shut themselves down after 6 months.

Now, from a POLITICAL point of view, it's another question. Would Iraq (or any other country) be willing to purchase weapons so solidly under the control of a potential enemy? Certainly they'd try very hard not to. The history of attempts to control international weapons sales hardly leads one to be optimistic that there won't be countries willing to sell unprotected weapons - not to mention "lock removal" agents (though with computer-controlled weapons their work can be made very, very difficult).

-- Jerry

---

## **Cracker charged in Australia**

*Fernando Pereira <pereira@klee.research.att.com>*

*Wed, 14 Aug 91 09:16:38 EDT*

The AP (8/13/91) reports from Melbourne that Nahshon Even-Chaim, a 20-year old computer science student, is being charged in Melbourne's Magistrates' Court on charges of gaining unauthorized access to one of CSIRO's (Australia's government research institute) computers, and 47 counts of misusing Australia's Telecom phone system for unauthorized access to computers at various US institutions, including universities, NASA, Lawrence Livermore Labs, and Execucom Systems Corp. of Austin, Texas, where it is alleged he destroyed important files, including the only inventory of the company's assets. The prosecution says that the police recorded phone conversations in which Even-Chaim described some of his activities. No plea has been entered yet in the ongoing pre-trial proceedings.

---

## ✂ Profitable Drug Wars -- Innocents Presumed Guilty

Charles (C.A.) Hoequist <HOEQUIST@BNR.CA>

Wed, 14 Aug 1991 17:39:00 -0400

The following was posted to several Usenet groups on 14 August.

Date: 12 Aug 91 13:02:36 GMT

From: mauler@kuhub.cc.ukans.edu

Newsgroups: talk.bizarre,talk.politics.drugs,talk.politics.misc

Subject: "War On Drugs" Atrocities: The Forfeiture Laws

[...]

### P R E S U M E D   G U I L T Y

The Law's Victims in the War on Drugs

The Pittsburgh Press, Sunday, August 11, 1991, p.1

It's a strange twist of justice in the land of freedom. A law designed to give cops the right to confiscate and keep the luxurious possessions of major drug dealers mostly ensnares the modest homes, cars and cash of ordinary, law-abiding people. They step off a plane or answer their front door and suddenly lose everything they've worked for. They are not arrested or tried for any crime. But there is punishment, and it's severe.

This six-day series chronicles a frightening turn in the war on drugs. Ten months of research across the country reveals that seizure and forfeiture, the legal weapons meant to eradicate the enemy, have done enormous collateral damage to the innocent. The reporters reviewed 25,000 seizures made by the Drug Enforcement Administration. They interviewed 1,600 prosecutors, defense lawyers, cops, federal agents, and victims. They examined court documents from 510 cases. What they found defines a new standard of justice in America: You are presumed guilty.

[The articles included some real horror tales. Part One is in [RISKS-12.13LAW](#) in the RISKS archive directory on CRVAX.SRI.COM. PGN]

---

## ✂ Patriot and Dhahran again [and Karn is up late again?]

Phil R. Karn <karn@thumper.bellcore.com>

Thu, 15 Aug 91 02:42:59 EDT

Army Records Say Computer Shutdown Might Have Averted Scud Disaster

By ROBERT BURNS, Associated Press Writer

[A few excerpts by PGN from a lengthy AP item presumably from 15 Aug 91]

Army investigators concluded that the exact reason for Patriot's failure to shoot at the Scud will never be known for sure. But they said the most likely explanation was a previously unknown glitch in Patriot computer software. Army technicians had determined as much as two weeks prior to the attack that the Patriot computer was vulnerable to losing track of incoming Scuds when the computer was kept running for long periods, according to internal Army reports



providing a safer and smoother trip for all drivers. Actually, IVHS technologies already are in use. Features such as cruise control and anti-lock brakes provide "smart car" capabilities to today's drivers. In the not-too-distant future, crash avoidance devices will detect the presence of an obstacle or other vehicle and alert the driver to a possible collision.

The "smart highway" is also a reality in many areas. For example, computers already are used to automatically change traffic signal timing and control the flow of traffic onto freeways to help reduce congestion. The ADVANCE IVHS project goes a step further by providing individual drivers with route guidance information to make their trips safer and faster.

If the U.S. is to stay competitive into the 21st Century, we must invest in innovative ways to move goods and people more safely and efficiently. Being on the cutting edge of technology means taking risks, and frankly, some IVHS technologies may not work. However, there are strong indications that many will. Even today, one Japanese firm claims that they are selling 2,000 navigation devices per month in Japan. If projects like ADVANCE are a success, consumers will be buying these products from American companies and not their European and Japanese competitors.

The long-term benefits from ADVANCE and other IVHS projects will not be known for many years. It is also impossible to predict consumer acceptance of advanced technologies in automobiles or elsewhere. One can only wonder what the early reaction was to those car radios the Mr. Zorn urges us to use. In 1926, Lee de Forest, the man who invented the cathode ray tube said, "While theoretically TV may be feasible, commercially and financially, I consider it an impossibility..."

Only time will tell the full measure of success for ADVANCE and other IVHS technologies. But if we never start, we will never know.

Meanwhile, we at the Department of Transportation will continue working on innovative solutions to assure America's transportation future. For as the Tribune's own editorial put it so well, "...if we have learned anything this century, it is that the future is limitless and its way paved with new notions." Clearly, the Congress shares this view, as both the Senate and House versions of the Surface Transportation Bill now being crafted include substantial increases in spending for research, development and deployment of IVHS technologies.

Samuel K. Skinner U.S., Secretary of Transportation

---

## **✂ Risks of Calling Reporters in Ohio**

*"Peter G. Neumann" <neumann@csl.sri.com>  
16 Aug 91 09:30:23 U*

SEARCH FOR NEWS LEAKS SPURS OHIO PHONE SWEEP  
By RANDALL ROTHENBERG, c.1991 New York Times News Service

Law-enforcement officials in Ohio have searched the records of every telephone user in southwestern Ohio to determine who, if anyone, called a Wall

Street Journal reporter to provide information that Procter & Gamble said was confidential and protected by state law. The investigation goes far beyond examining the telephone records of current and former employees of the giant consumer products company, an inquiry the Hamilton County prosecutor's office confirmed on Monday. The Journal reported the scope of the investigation Thursday.

The prosecutor, Arthur Ney Jr., acting on a complaint by Procter & Gamble, ordered Cincinnati Bell to turn over all the telephone numbers from which people called the home or office of the reporter, Alecia Swasy, from March 1 to June 15.

The situation began sometime before June 17 when Procter & Gamble, which makes Tide detergent, Crest toothpaste and other familiar supermarket products, asked the Cincinnati police to determine whether current or former employees were leaking confidential corporate information to The Wall Street Journal.

On Monday the newspaper reported that the company had been bothered by two news articles published on June 10 and June 11 written by Ms. Swasy, a reporter based in Pittsburgh who covers Procter & Gamble. The articles cited unidentified sources saying that a senior executive was under pressure to resign from the company, and that it might sell some unprofitable divisions. But a spokeswoman for Procter and Gamble, Sydney McHugh, said Thursday that the company "had been observing a disturbing pattern of leaks" since the beginning of the year. She refused to elaborate, but said the decision to pursue legal action was reviewed at several levels in the company and was made by Jim Jessee, a corporate security officer.

Two Ohio statutes protect the unauthorized disclosure of trade secrets. One makes it a felony to transmit formulas, customer lists or other tangible pieces of information that would be valuable to a company and its competitors. But another, broader law makes it a misdemeanor to disclose "any confidential matter or information" without the company's consent.

The Cincinnati police approached the Hamilton County prosecutor's office, which sought and received from a grand jury a subpoena for telephone records.

A copy of the subpoena, dated June 17, was given to The New York Times by someone involved in the case who insisted on anonymity. The subpoena ordered Cincinnati Bell to "identify all (513) area code numbers that have dialed" Ms. Swasy's home or office telephones in Pittsburgh during an eight-week period that started on March 1.

Cincinnati Bell serves 655,297 telephone numbers in the 513 area code, in an area covering 1,156 square miles, said Cyndy Cantoni, a spokeswoman for the company. In the company's entire jurisdiction, which also covers parts of Kentucky and Pennsylvania, about 13 million toll calls are placed in an average month, she said.

Ms. Cantoni said she could not comment on what Cincinnati Bell turned over to the authorities, but said the company routinely complied with subpoenas. Under normal procedure, the company's computers would have automatically searched its customer list and printed out only the originating numbers, and not the names or addresses, of calls to Ms. Swasy's numbers, Ms. Cantoni said.

The Wall Street Journal, which is published by Dow Jones & Co., reported on Monday that neither Ms. Swasy nor executives at the Journal were informed of the subpoena by the authorities.

Neither Terry Gaines, a first assistant prosecutor, nor Ed Ammann, a police department colonel involved with the investigation, returned repeated calls to their offices.

Alan F. Westin of Columbia University, an authority on technology and privacy issues, said the legality of the Ohio authorities' search for the

Procter & Gamble whistleblower may depend on how the investigation was pursued. If Procter & Gamble turned over the names and phone numbers of present and former employees to the police and the police matched that list against the numbers they were given by the telephone company, the rights of other, uninvolved parties may not have been violated, Westin said. But if the police learned the names of people unaffiliated with Procter & Gamble who called the Journal's reporter, he said, or if they turned over a list of numbers to Procter & Gamble for research, some Ohio residents' Fourth Amendment protections may have been sullied. "When technology allows you to run millions of calls involving 650,000 telephone subscribers through a computer in order to identify who called a person, potentially to find out whether a crime was committed, you raise the question of whether technological capacity has gone over the line in terms of what is a reasonable search and seizure," Westin said.

---

### **✦ Risk of Power Failures in Computer Controls**

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

*15 Aug 91 09:19:19 U*

POWER SURGE CAUSES FAILURE OF SYSTEMS IN NEW YORK NUCLEAR PLANT  
By KEITH SCHNEIDER, c.1991 N.Y. Times News Service

WASHINGTON A power surge at dawn Tuesday knocked out instruments that operators used to control the reactor at a nuclear power plant in upstate New York and caused the failure of a succession of systems that monitored the plant's operations.

Workers at the Nine Mile Point Nuclear Station, on Lake Ontario about 6 miles from Oswego, were never in danger from a release of radiation, said Niagara Mohawk Power Corp., the plant's operator and co-owner. But the problems at the Unit 2 reactor, the newest of the plant's two reactors, caused Niagara Mohawk to shut down the plant and declare the second-highest level of alert possible under federal rules. And the Nuclear Regulatory Commission said the plant could not reopen until an investigation into the events, which began Tuesday, was completed.

Niagara Mohawk lifted the alert at 7:45 p.m. Tuesday. It is only the third time that such an alert, known as a site area emergency, has occurred at an American nuclear power plant, the NRC said.

Parts of the monitoring systems were unaffected by the loss of power, enabling the operators to oversee the safe shutdown of the reactor.

According to the NRC, the operating record of Nine Mile Point's two nuclear reactors since the late 1980's has ranked among the worst of the 111 licensed nuclear reactors in the United States. For three years until its status was changed in June, Nine Mile Point was on the agency's list of problem plants.

The emergency was declared after one of three transformers at Unit 2 failed at 6 a.m. The failure caused a powerful surge of electricity to rush back into the plant, tripping the circuit breakers in the main turbine and five of the plant's internal power systems. The turbine shutdown caused the nuclear reactor to automatically begin to shut itself down, plant engineers said. Manual shutdown procedures also were started, they said.

Four of the internal power systems that failed provided electricity to critical gauges, safety monitors, the plant's main computer, and monitoring

equipment in the main control room.

Some of the most important gauges operators use to control the reactor were knocked out, including the one showing the position of control rods in the reactor and another that measured the power of the reaction.

Another system of emergency indicators that failed were annunciators, a series of playing-card-sized windows at the top of the control panel that flash and sound an alarm when equipment or processes are functioning improperly.

Their function is similar to that of red warning lights on an automobile's dashboard, serving as a first line of warning that can be verified by a gauge.

The failure of many primary gauges, the main computer and annunciators meant that if the reactor were an automobile, operators would have been driving with a sheet across the windshield.

Niagara Mohawk and the NRC said they considered the incident to be serious because the power systems had been designed so they would not fail. Each had backup batteries.

In the event of a main electrical failure, circuits were supposed to automatically shift the systems to battery power. The plant's engineers determined Tuesday that the power surge destabilized the circuits that needed to be stable for 4 milliseconds to work properly, said Gary Grant, a senior reactor operator.

"Nobody anticipated this transformer failure and all this happening at the same time," said Grant.

Nine Mile Point is one of 37 nuclear plants in the county manufactured by General Electric Co.

Lynn Wallis, a spokesman for GE in San Jose, Calif, said Tuesday:

"The NRC has evaluated our design. They are licensed and they are safe. That's all I can provide. You ought to talk to the utility and the NRC."

The Nine Mile Point Nuclear Station generates 1,705 megawatts of electricity for upstate New York residents from two boiling-water nuclear reactors.

Unit 1, a 615-megawatt reactor, began operating in 1969 and was not affected by the incident Tuesday.

Unit 2, a 1,080-megawatt reactor that began operating in 1988, is owned by Niagara Mohawk and four other utilities, including Long Island Lighting, New York State Electric and Gas, Rochester Gas and Electric and Central Hudson Gas and Electric.

The NRC describes a site area emergency, one of four categories of alert, as one in which there are "actual or likely major failures of plant functions needed for protection of the public."

Only twice previously have site area emergencies been declared by utilities. There has never been a general emergency, described by the government as an actual or imminent degradation of the nuclear reactor core, though if the system had been in place in 1979, the Three Mile Island accident would have qualified.

Last year, Plant Vogtle, a nuclear generating station owned and operated by Georgia Power, 26 miles southeast of Augusta, declared a site area emergency after the plant's main power supply failed and backup diesel generators were turned on, the NRC said.

In 1982, a steam generating tube ruptured at the Ginna nuclear plant, operated by Rochester Gas and Electric 20 miles northeast of Rochester, and a similar emergency was declared because of the threat of a worse accident caused by the loss of coolant for the reactor core, said the NRC.

The NRC said Tuesday that emergency incidents at nuclear reactors in the United States were declining, indicating an improvement in management and operations since 1979.

Last year, the number of unusual events, the lowest level of alert, declined to 151 from a peak of 312 in 1985. In 1990, the number of alerts, the second lowest emergency event category, was 10, about the same as it had been for a decade.

Niagara Mohawk said it took just 22 minutes for the plant to restore power to the control room monitors.



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 12: Issue 14**

**Monday 19 August 1991**

## Contents

- [TRW Wrong on Credit Reports for Entire Town](#)  
[Scot Drysdale](#)
- [Computer Crime Bill - S1322](#)  
[Robert E. Van Cleef](#)
- [Bank Shot \(RISKS of automatable documents\)](#)  
[Ed Ravin](#)
- [Misuse of computerized auto registration info](#)  
[Rodney Hoffman](#)
- [Risk of licensing programmers -- lost freedom and creativity](#)  
[John Gilmore](#)
- [A320 revisited](#)  
[Robert Dorsett](#)
- [Re: Procter&Gamble](#)  
[Steve Bellovin](#)
- [Re: FSF machine having to clamp down on security](#)  
[Paul Mauvais](#)
- [Re: "locking" DoD smart weapons](#)  
[Guy Sherr](#)
- [Re: Rumor regarding Soviet calibers](#)  
[Michael Edelman](#)
- [More Credit Bureau Risks](#)  
[Mike Waters](#)
- [RISKS of calling 911 from cellular phones](#)  
[E.M. Culver](#)
- [Book: "Narcissistic process and corporate decay..."](#)  
[Dan Jacobson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ **TRW Wrong on Credit Reports for Entire Town**

*Scot Drysdale* <[scot@moosilauke.dartmouth.edu](mailto:scot@moosilauke.dartmouth.edu)>  
*Tue, 13 Aug 91 11:08:43 -0400*

TRW appears to have decided that every resident of Norwich, VT is delinquent

in paying property taxes. An article in The Valley News from from a couple of weeks ago follows. (I foolishly clipped the article but not the date.)

Company Wrong on Credit Reports, by Roger Carrol and Rich Barlow

NORWICH - The Vermont Attorney General's office is investigating how one of the largest credit-reporting companies in the world came to list every Norwich property owner as a delinquent taxpayer.

Not every taxpayer is delinquent, of course, but Karen Porter - town clerk, treasurer, and collector of taxes - said all 1,500 residential taxpayers are listed that way by the California-based TRW, Inc., which distributes credit information through a nationwide network. ... Porter said she first got wind of the problem about a month ago, when someone from Macoma Savings Bank called the Norwich town office to verify that a customer applying for a loan had paid off a "Norwich County" lien on property. The taxpayer never had a lien on the property, said Porter, who became more suspicious when the phrase "Norwich County" popped up again. "I heard that term three times in two days from various banks and credit bureaus," she said. It stood out because there is no Norwich County. She traced the source of the information to TRW, and it took her a week of calling and writing before she got a company official who could answer her questions. "I had him pull up six or seven records on his computer screen," said Porter. "In each case they (Norwich taxpayers) were listed (on the TRW computer) as having liens. But in each case they had paid in a timely fashion. He's making long sighs on the other end of the phone while I'm telling him there are 1,500 he has to correct." [...]

The article goes on to describe how TRW blames the error on National Data Retrieval of Norcross, GA. An NDR representative came to the town office in February and wrote down the names listed in the town's receipt book. The NDR representative blamed it on a keypunch operator in Georgia.

A couple of days ago Porter published a Letter to the Editor claiming that TRW claims to have fixed all of the incorrect records, but that she has not yet gotten that in writing.

Scot Drysdale scot.drysdale@dartmouth.edu

---

### **✂ Computer Crime Bill - S1322**

*Robert E. Van Cleef <vancleef@nas.nasa.gov>  
Mon, 12 Aug 91 14:35:51 -0700*

Senator Leahy's Computer Crime Bill Would Close Loopholes in CFAA  
(From Government Computer News, August 5, 1991, Page 98)

"Sen. Patrick J. Leahy has reintroduced a computer crime bill that would close loopholes in the existing Computer Fraud and Abuse Act (CFAA) by making it a felony to introduce viruses or other damaging programs intentionally into computers. " [...]

One recent study estimated that computer crime now causes between \$3 billion and \$5 billion in damages a year, [Sen. Hank] Brown said. " [...]

Recognizing that some incidents are neither malicious nor intentional, Leahy said the bill would create a parallel misdemeanor charge for reckless actions that cause harm to computers. " [...]

Bob Van Cleef, NASA Ames Research Center (415) 604-4366 vancleef@nas.nasa.gov

---

### ✂ Bank Shot (RISKS of automatable documents)

*Unix Guru-in-Training <elr%trintex@uunet.UU.NET>*

*Fri, 16 Aug 91 17:40:00 EDT*

Yet another technology-enabled telephone scam -- a telemarketer calls up someone and cons them into reading over the phone the numbers off one of their checks. The cons use this information to print up a "demand draft" which lets them pull any amount of money they want from the victim's checking account. The demand drafts, like checks, are automatable documents, and access to check-printing technology seems to be a plus in pulling this off.

Unfortunately, no one has yet called for changes to the technology used in checks and demand drafts. [Remember the Forbes cover story on how easy it is to fabricate a check -- they were able to clear a forged \$30,000 check that they manufactured with a color photocopier and a desktop publishing system.] It's kind of scary to think that the banking industry so far finds the threat of massive fraud insufficient motivation to change a technology they're comfortable with.

Here's a recent news article on the subject. Note that the words "computer crime" or "hacker" aren't being used, but they would be if the technology involved was owned by a less respectable institution than the U.S. banking industry...

A DEMAND TO GUARD CHECKING ACCOUNTS,  
by Jean Iida, American Banker, NY Newsday, July 25, 1991

A new high-tech telemarketing scam that is stinging banks and consumers is catching the attention of Washington, DC lawmakers. But a proposed law aimed at protecting consumers may do little to limit banks' exposure to the crimes. The drafted legislation would address the problem of fraudulent demand drafts -- a check-like mechanism that can be used to siphon money from checking accounts.

Demand drafts, used legitimately by a variety of businesses to collect recurring payments from their customers, are automatic withdrawals from a checking account. Insurance companies, for instance, often use them to collect premium payments.

The scam has cost banks and their unwitting customers hundreds of millions of dollars since it cropped up late last year, bankers and investigators said.

And despite the big losses, bankers seem to have few ways to combat criminals who use sophisticated check-printing equipment to take advantage of banks' need to quickly process checks and demand drafts.

As a result, Congress may pick up the gauntlet. Rep. Ron Wyden (D-Oregon) is proposing legislation that would register and set bonds of about \$200,000 for each telemarketer. The bill, for which Rep. Wyden is now seeking comment, could even include restrictions on the types of companies that can buy sophisticated check-printing equipment often used in the crimes. ...

Because banks' check-processing operations are so highly automated, it is nearly impossible for a bank to catch a questionable demand draft. "There's no automated way to catch bogus demand drafts," said one banker who asked not to be named. Usually, "you don't know you have a problem until you get the return items, and by then it may be too late."

In the scam, whose victims are frequently older people, a telemarketer obtains checking account and other codes found on the magnetic-ink character line of checks, often promising in return cosmetics, prizes, or trips. Later, the consumer may be charged for the goods but receive nothing, or receive the promised goods but find them shoddy. Or victims may find that their checking accounts have been drained of far more money than expected. The consumer may then turn to the bank, demanding a refund. Once a bank has paid funds from a consumer's account to the telemarketer's, the bank is frequently liable.

Once a telemarketer knows a consumer's checking account and transit routing numbers, he can use demand drafts as a blank check to withdraw almost unlimited sums of money.

But demand drafts are here to stay. Millions of legitimate demand drafts are processed every year.

And the proposed measures, such as requiring telemarketers to post bonds, would protect only the first consumer to notice the fraud. Typically, consumers do not know they have been victimized until after they receive their monthly bank statements.

"The problem is how high do you go" in setting a bond, Barker said.  
"Some telemarketers got \$1.7 million in small amounts in six weeks."

Ed Ravin eravin@panix.com philabs!trintex!elr

---

### **Misuse of computerized auto registration info**

*Rodney Hoffman <Hoffman.El\_Segundo@Xerox.com>  
Mon, 19 Aug 1991 08:15:02 PDT*

Precis of a 'Los Angeles Times' article by Paul Jacobs headlined  
ADDRESSES AT DMV REMAIN ACCESSIBLE (August 19, 1991, page A3):

The California Department of Motor Vehicles regularly opens its address files to 14,000 businesses and individuals, many of whom have direct access to the

DMV's computerized files. Audits found unauthorized use and other problems in more than 25% of a recent sampling of these accounts. None have yet been prosecuted.

In the wake of a 1989 murder of an actress in which the accused killer used automobile registration records to track down the victim, California enacted a new law restricting access to DMV information. However, the law exempts banks, insurance companies, car dealers, wrecking yards, and process servers. Virtually anyone can register as a process server for less than \$100. A black market in DMV data has developed. There have also been some cases of DMV employees altering or misusing data.

In one recent case, Edward Jack Vijfvinkel is alleged to have misrepresented himself as a private investigator and paid \$50 to open a DMV account. He is said to have used license plate numbers to get addresses and other information which he used to write to women he spotted while driving.

One woman received a letter saying in part, "I'll give you one week to respond or I come looking for you." A letter to another woman said, "I looked for you though all I knew about you was your license plate. Now I know more and yet nothing. I know you're a Libra but I don't know what it's like to smell your hair while I'm kissin' your neck and holding you in my arms." The woman called the police. Vijfvinkel bragged to the arresting officer that he could find anyone with a license plate. He had in his possession the book, 'You Can Find Anyone.'

---

### **✂ Risk of licensing programmers -- lost freedom and creativity**

*John Gilmore <gnu@toad.com>  
Sun, 4 Aug 91 04:16:12 PDT*

I can't believe all the people who are posting in RISKS that they like the idea of government mandated licensing of the software craft. (I don't care if you call it designing, engineering, programming, or hacking.) What ever happened to the idea of freedom of speech in software?

Maybe I'm just an old-timer, but while "some of my best friends" came into software through traditional college courses, most of the best, brightest, and most inventive programmers I know became programmers without formal training. The fathers of the computer revolution you are now staring at and typing to, were able to make the great strides they did, in an incredibly short period of time as measured against any other industry, because there was nobody to say "no, you can't do that". Why would anyone who has the equipment and training that permits them to read this message, want to squelch such creativity and productivity gains for the entire society?

I've heard all the drivel about raising standards and driving out the low quality practitioners. Right. What it really does it makes it more painful for *\*everyone\** to enter the industry -- the best *\*and\** the worst. It creates a monopoly, ruled by an old boys' "board of licensing" who entrench their idea of proper programming. It's a good thing this bill didn't pass during the "Goto considered harmful" phase, or it might have ended up "Goto considered illegal"

and stuck us programming in Pascal forever. (I also note that the explosion of C programming in the last ten years was mostly among people on micros who typically hadn't programmed before. E.g. if you were required to go through college to be allowed to try C, you wouldn't bother, since the college courses of the time taught Pascal and Fortran; you'd have already been taught how to constrain your thinking to what was possible in inferior languages.)

By the way, I never went to college at all. Among the three co-founders of my current successful software startup company, only one of us has a degree - and it isn't in computers (I think it's history). And while I am really very talented with computers, if continuing to work with them means getting a government license, I'll just retire on what I've already made in computers, and start exploring one of the other ten or twelve things I've never had time for. I mean, we turn down government contracts now just over the added paperwork!

Did you notice in the bill that it allows people to gain a license to be a programmer even if they don't go to an "approved" college? But it requires years of work experience -- which will be illegal to get after the bill passes. Essentially a grandfather clause disguised as an alternative route. It means that the bright kids and 20 year olds and 30 year olds who currently wander into programming from chemistry or physics or MCAD or library science, or bartending (I know a few!), will be banned from the industry. I'd really rather not replace these talented, motivated people with drones who learned how to take tests and warmed a seat in some state college for four years. We need more interdisciplinary people already -- you want to cut the supply to a tiny trickle of those who're willing to sit through two or three entire courses of formal study?

My reaction to the NJ bill was: O boy. Now the programmers will all get upset at it, and not only can we kill off this stupid bill, but perhaps while we're incensed, we can even repeal some of the other ridiculous occupational licensing that's already on the books -- like hairdressers, barbers, car mechanics, etc.

If you really care about this issue, I recommend that you implement it in your personal life without waiting for the government. Only buy computers designed by licensed and bonded EE's. (Hint: your SPARCstation is not one of them.) Only buy software that was written by programmers who passed the CDP exam. (Better send back Unix, Emacs, Lotus 1-2-3, and Usenet.) I don't think TCP/IP was designed by registered communications engineers either. (Maybe OSI was -- it has that smell.) Well, you can always run DOS -- ahem -- uh, Bill Gates \*started\* college, but I don't think he ever finished it. Too busy making better products than all those people who wasted four years. But maybe he \*hired\* a lot of fully certified licensed degreed people to write the code. Or maybe not.

Don't forget to restrict your reading to government-approved writers, and your thinking to government-approved thoughts.

Sometimes I think the worst mistake the founders of our country made was giving governments the power to control commerce and trade.

John Gilmore, Cygnus Support

---

## **# A320 revisited**

Robert Dorsett <rd@cactus.org>

Fri, 16 Aug 91 13:01:03 CDT

[This is a re-worked sci.aeronautics reply to a comp.sys.mac.programmer post. It's somewhat relevant in its RISKS-of-RISKS aspects...]

And Mr. Finnegan wrote:

>The Airbus suffers from what many software safety experts consider a major  
>design problem - it uses redundant flight computers and a polling computer  
>to pick the 'majority' answer to each input (I forget the technical term  
>for this theory -- it's been way too long since I've been immersed in stuff  
>like this in school/industry). This system is used because some CS people  
>think polling can replace stringent software testing - if 5 s/w teams all  
>write code to the same spec and test just a little, the polling computer (if  
>it is calibrated properly - another issue) statistically should be able to  
>deduce the proper answer and weed out any incorrect input. Needless to say  
>many experts aren't convinced.

The A320 flight control system is comprised of five computers: two elevator and aileron computers (ELAC) and three spoiler and elevator computers (SEC). The computers use diverse software and hardware implementations: the ELACS are based on the 68000 and Pascal, the SEC's on the 80186 and C. At any one time, there is \*one\* and only one "hot" computer, and one standby computer.

Each computer is actually a combination of two "channels," one microprocessor driving each channel. One such channel is a "command" channel; the other is a "monitor" channel. Each is responsible for guaranteeing the output of the other. The command channel was written in a high-level language; the monitor channel was written in assembler.

The ELACS are the higher-level computers, providing all the functionality associated with the complete FBW pilot interface (there are four distinct direct-control flight modes the A320 can be in). ELAC1 is the primary computer. Graceful degradation is accomplished, going from ELAC1 to ELAC2 to SEC1 and so forth. The SEC computers provide a "direct" control law, in which sidestick deflection more or less correlates to control surface movement. SEC3 only controls roll. The pilots can also command switching from one computer to another.

Various means (checksums, range tests, time-outs, etc) are used to determine computer robustness. If the checks fail, the computer takes itself off-line.

SEC and ELAC development teams were isolated, and prevented from communicating with one another. This was intended to prevent teams from "contaminating" each others' code with common approaches. Any problems theoretically will only arise from the \*specification,\* although it's entirely probable that each team opted for similar approaches to solving problems.

The software and hardware verification regime was performed in accordance to

EUROCAE/ED-12A. This is virtually identical to RTCA/DO-178A. The overall system design is fault-tolerant.

Considering the need for hardware and software diversity, I really can't see a credible way of implementing this thing, other than a loosely-coupled, asynchronous network--which precludes anything much more sophisticated than polling by client services. In general, the A320 Electronic Flight Control System (EFCS) is a bit too complex to be condemned by a broad statement that it uses "polling." The A320 does not use a "judging" computer such as you describe; clients are partially responsible for minor things such as parity or range checking on the single inputs from the currently active flight control computer.

What you seemed to be indicating is more akin to how the \*Space Shuttle\* works, i.e., having a "majority rules" system of verifying hardware integrity.

=====

I suppose I should put a big caveat on all my gripes about the A320 over the past three years: yes, I do think the airplane is unsafe. But no, I do not believe that slipshod work went into its design and construction. There is much to suggest that the design of the A320 EFCS represented a quality control system unprecedented in the industry, and which utilized the best techniques of the time. One might quibble with some isolated aspect of it, but the overall approach was sound.

My major problem with the \*reliability\* aspect of the system is Airbus's claim of being able to satisfy the "one catastrophic failure every million hours" clause for flight control systems in the Federal Aviation Regulations. Airbus can't prove it. Moreover, the FAA requirement for the 1e-9 figure explicitly does \*not\* apply to flight control \*software\*, even though it applies to flight control \*systems\*. Draw your own conclusions.

There is also sufficient cause to doubt even our best software engineering techniques. This is an issue that many people like to ignore, assuming that, of course we can produce "perfect" software; if it doesn't work, then somebody must have screwed up. NOT true.

IMHO, this sort of thing doesn't belong in a civilian airliner--yet. Airbus proudly points to its revolutionary airplane, but \*revolutionary\* anythings are rarely well-understood. Related effects of their decision to use FBW--namely, in the form of the pilot interface--will cause other problems.

But Airbus set a precedent, and created a marketing force in the process. Now, other companies have to raise the stakes, too, or risk losing market share. Airbus is extending the A320 EFCS model to include the A330 and A340; Boeing's developing a "tower" (geographically localized hardware) system for the 777.

Lastly, there \*is\* a lot wrong with the A320. But I'm also noticing a lot of scapegoat-bashing going on. The A320's problems are fairly well defined, and need to be corrected. Let's NOT assign our favorite software-engineering pet peeve, arbitrarily, to such a large and accessible target. I'm not addressing this to you in particular, Greg; it's become pretty frequent over

the past few months.

Robert Dorsett rdd@cactus.org ...cs.utexas.edu!cactus.org!rdd  
[References available on request.]

---

**✉ Re: Procter&Gamble ([RISKS-12.13](#))**

<smb@ulysses.att.com>

Mon, 19 Aug 91 15:54:02 EDT

It's not just the computerized risks -- apparently, the police officer running the investigation is a part-time P&G security consultant. And no one at either the company or the police department seems to think that there's any conflict of interest.

---

**✉ Re: FSF machine having to clamp down on security ([RISKS-12.12](#))**

Paul Mauvais <MAUVAIS@psuorvm.bitnet>

Mon, 19 Aug 91 12:24:19 LCL

I have heard from someone that Richard Stallman was interviewed on TV after the anonymous accounts were shutdown, and during the interview, several people noticed that his root password was written on the white board behind him, in plain view of the TV camera.

Needless to say, it was changed soon after this was realized....

Always nice to have one's root password broadcast to a few million people.

Talk about RISKS....

---

**✉ Re: "locking" DoD smart weapons ([RISKS-12.13](#))**

NSIL LCM <0004222127@mcimail.com>

Mon, 19 Aug 91 21:14 GMT

I would rather not spend unbelievable amounts of money on making smart weapons smart enough to know whether they are being fired by the enemy. That runs to the opposite idea, first, that smart US made weapons should NEVER kill the allied forces; thus eliminating Friendly Fire kills.

Instead, let the DoD spend a few dollars making innovative things that will explode WHENEVER they are used, and then tell the allies what to look for in the boobytraps. For example, you could mark alot of hand grenades M27A3 instead of M27A1; the A1 variety go off as expected, but the A3's will detonate when the safety pin is removed (without even losing the spoon). Granted that would be rather rude, however, consider that our enemy would suddenly think, hesitate, and perhaps even abandon the idea of using ANYTHING we leave behind.

Better that than dropping leaflets...

Guy Sherr, Lab Configuration Manager, MCI NSIL, Reston, VA  
Voice: (703)648-8645 (Vnet 262)

---

### **✂ Re: Rumor regarding Soviet calibers**

*Michael Edelman <MEDELMA@CMS.CC.WAYNE.EDU>  
Mon, 19 Aug 91 19:55:08 GMT*

The most recent issue of comp.risks [[RISKS-12.13](#)] repeated a classic bit of modern arms folklore: That Soviet weapons are designed with calibers slightly larger than US arms so that Soviet arms may fire US ammunition, but not vice-versa.

Although this story has been repeated for years, most notably in Alexander Cockburn's book on defense (itself a wonderful source of misinformation), it is most assuredly false. It probably has its origins in the fact that some Soviet arms have odd sizes- like the "121mm mortar". This, according to Suvarov, is to avoid confusion of mortar rounds with gun rounds. While there is a 120 mm gun and a 121mm mortar, both are actually 120mm.

There has never been a Soviet infantry rifle that would safely fire US issue ammunition. Fitting ammunition to a rifle is a critical matter; an error of a few thousandths in headspace can create a lethal hazard.

--mike edelman

---

### **✂ More Credit Bureau Risks**

*Strawberry Jammer <waters@nddsun1.sps.mot.com>  
Thu, 15 Aug 91 08:15:54 MST*

In Risks a few weeks ago was an account concerning someone's problems with the automated credit bureaus. I read it with a little bemusement thinking "it cant happen to me". I soon learned better, that same day I received a rejection notice for a credit card application. The reason? Bankruptcy. BANKRUPTCY? I haven't filed bankruptcy nor do I even plan to, and you would think that \*I\* would know about it.

The credit bureau checked and responded "yes thats correct - tough" (in so many words). It took a letter to my U.S. congressman to get to the bottom of it.

It seems my EX-WIFE had filed bankruptcy and two of our former joint accounts were reporting "a party on the account is bankrupt". TRW interpreted this to mean "liquidated through bankruptcy", and LO! I too had no credit!

TRW (under pressure) has agreed to remove the items from my credit report, but when I next pay my mortgage and they report the on time payment, who knows what will happen!

Watch out, folks, it CAN happen to you!

Mike Waters, waters@nddsun1.sps.mot.com

---

### **✂ RISKS of calling 911 from cellular phones**

"E. M. Culver x5416" <CULVERE%HSDWL@utrcgw.utc.com>

Thu, 15 Aug 1991 08:09 EDT

I have wondered what happens when you call 911 from a cellular phone. In Connecticut, you get the State Police who will (maybe) help you. 911 coverage here approaches 100%, so calling 911 from a cellular phone is not necessarily silly. Somebody tried, nobody got hurt and the human side of the system did not work...

[Digested from "Cellular Caller Gets Runaround Reporting Fire", New Haven (Connecticut) Register, 13 August 1991. I removed the individual names.]

A Wallingford, Connecticut woman called to report a fire in her public housing duplex on August 9 (at about 11:45am) by calling 911 on her cellular telephone. In Connecticut, 911 calls from cellular phones are routed to the nearest state \_State Police\_ barracks. The State Police dispatcher told the woman "This number is for state police emergencies only. You have to call 1-411 {the information number } and get the number of your local fire department." Fine--she did that. The Wallingford Fire Department's dispatcher told her to call 911.....

In frustration, she called the Wallingford Police, told the story and waited. After a few minutes (this was less than a mile from the fire house) she concluded the Fire Department had not been told. She called the fire department again, saying "My house is burning down and nobody's going to come?" and getting agitated. About 25 minutes after the call to 911 the fire trucks arrived. A maintenance worker sent by the housing authority had already put out the fire. There were no injuries.

The Fire Chief said the Fire Department is instituting a policy change so dispatchers will handle emergency calls on non-911 lines instead of directing callers to dial 911.

The State Police get 911 calls from cellular phones because these calls are usually report traffic accidents. State Police dispatchers are supposed to route fire calls to the appropriate local fire department. 911 calls made from regular phones can be traced to the physical address from which the call originated--either the old fashioned way or with an advanced form of caller ID, which give the dispatcher the physical address of the phone originating the call.

---

### **✂ Book: "Narcissistic process and corporate decay..."**

<Dan\_Jacobson@ATT.COM>

Thu, 15 Aug 91 10:01 CDT

Interesting sounding book:

Howard S. Schwartz. Narcissistic process and corporate decay : the theory of the organization ideal. New York University Press, c1990. xiv+151 pp. ISBN 0-8147-7913-1. Corporate culture; Organizational behavior; Challenger (Space shuttle)--Accidents; General Motors Corporation--Management; U.S. National Aeronautics and Space Administration--Management.

PART ONE - The Theory of the Organization Ideal

- 1 The Clockwork or the Snakepit: An Essay on the Meaning of Teaching Organizational Behavior
- 2 On the Psychodynamics of Organizational Totalitarianism
- 3 Antisocial Actions of Committed Organizational Participants

PART TWO - Organizational Decay and Organizational Disaster

- 4 Totalitarian Management and Organizational Decay: The Case of General Motors
- 5 Organizational Disaster and Organizational Decay: The Case of the National Aeronautics and Space Administration
- 6 On the Psychodynamics of Organizational Disaster: The Case of the Space Shuttle "Challenger"

PART THREE - American Culture and the "Challenger" Disaster: A Historical Perspective

- 7 The Symbol of the Space Shuttle and the Degeneration of the American Dream
- 8 Conclusion: Addiction and Recovery



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 12: Issue 15

Thursday 22 August 1991

## Contents

- [Electronic mail beams shuttle's message home](#)  
[Joe Abernathy](#)  
[PGN](#)
- [The RISKS of a national computerized entertainment ticketing network](#)  
[KJPhelan](#)
- [Personal data in California](#)  
[Phil Agre](#)
- [Electronic Library Systems in Airlines](#)  
[Robert Dorsett](#)
- [Microsoft, IBM demonstrating faults in each other's products](#)  
[Jon Jacky](#)
- ["Citicorp Creates Controversy With Plan To Sell Data ..."](#)  
[Jerry Leichter](#)
- [NY Times Letter on Fake Documents](#)  
[Sanford Sherizen](#)
- [ATM videotapes](#)  
[Jyrki Kuoppala](#)
- [Re: Bell V22 Osprey crash -- assembly error](#)  
[Henry Spencer](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Electronic mail beams shuttle's message home**

*Joe Abernathy <edtjda@magic322.chron.com>*

*Wed, 7 Aug 91 20:11:05 CDT*

[I have abridged the following article for RISKS relevance, although I presume its submission by an author could be considered tantamount to our being able to use the entirety with permission. I unfortunately did not get to see it until 22 Aug, or this posting would have been more timely. But, please see the message following this one. Joe, MANY THANKS for sending it in. PGN]

Electronic mail beams shuttle's message home

By JOE ABERNATHY and MARK CARREAU

05AUG91, Houston Chronicle, Page 1A, Copyright 1991, Houston Chronicle

Electronic mail networks, the message medium of the information age, made their debut in the space age Sunday aboard the shuttle Atlantis as part of an effort to develop a communications system for a future space station.

Details of the test were being closely guarded because of concerns over a possible hacker incident or "public free-for-all" on the nation's computer networks, according to one engineer involved with the project. Privacy and medical ethics also loom large as issues. [...]

Electronic mail offers a new way for astronauts to stay in touch with their families, Mission Control, and potentially, the millions of people who use the nation's interlinked computer networks. It could produce far-reaching change in the way scientists and others interact with the space program. Currently, only the shuttle communicator is allowed to talk with the astronauts during a flight, except for a private medical conference each day. E-mail could change that by letting any number of people exchange information, while scientists and engineers on the ground could assume direct control over their experiments in space.

[Bryon] Han and fellow Apple employees Michael Silver and James Beninghaus have donated their time to the project. They are using low-cost, commercially available products, rather than the costly custom products often used in science. [!!!] The e-mail will play a role in controlling experiments, electronic flight information, and transfer of experiment results to the ground, Han said, as well as sending data up to the shuttle.

In the future, the system might be used to transmit and manipulate information from the many medical experiments NASA conducts. But this raises a number of problems regarding privacy and medical ethics. For example, one experiment in this flight seeks to correct a blood-flow problem associated with weightless ness that causes some astronauts to faint upon their return to Earth. But this experiment is being monitored with the same Apple computer that is playing host to the e-mail system. Even though the results aren't being transmitted over computer networks this time, they might be next time -- and computer networks are notoriously insecure.

Inquisitive computer enthusiasts -- hackers -- are in fact one of NASA's chief concerns in regard to the use of electronic mail. The space agency initially sought to conduct the tests without publicity, but word quickly percolated around the nation's computer networks -- perhaps indicating that the concerns were justified. A chorus of calls was heard requesting the e-mail address of the astronauts -- but that raised another problem more pressing than any threat from malicious hacking, that of capacity.

"We have things we need to accomplish with the limited amount of time we have, and we do have a very limited amount of data we can move between Mission Control and the orbiter," said Deborah Muratore, an engineer in the space station support office at Johnson Space Center and the experiment manager.

In addition to voice communication, the shuttles are equipped with Teletype and fax machines for the transmiss ion and reception of printed material and even photo graphs.

"Conceivably, everything they move that way could be moved from computer to computer," Muratore said. "From a space station standpoint it would be much preferable to transfer the information electronically without paper in the loop the way we do today on the shuttle." "Paper is going to be a limited resource, something that has to be thrown away or reused on the space station," she said. "It becomes trash. So the more we can eliminate on the space station the better off we are."

The current experiment does not represent the first time that civilians have had a direct communications link with those in space. Since January, the Soviet space station Mir has maintained a "mail drop" for ham radio operators to use in leaving messages for the cosmonauts. "It's very similar" in function, said Gary Morris, a former member of the Johnson Space Center Amateur Radio Club who now lives in San Diego. "The packet bulletin board system on Mir allows an amateur (ham radio operator) on the ground to leave mail messages. "What they're doing with the Mac is different in that they're going through the whole (electronic mail) network. It's much more complex."

-- Joe Abernathy

[By the way, a sidebar (see next message) is omitted here. PGN]

---

### **✂ Re: Electronic mail beams shuttle's message home**

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

22 Aug 91 09:00:20 PDT

It is worth noting that Joe Abernathy's Houston Chronicle article (the previous message in this issue) included a sidebar (omitted above). This sidebar actually included the EMail address for the shuttle (which I have consciously not included here -- we wouldn't want RISKS to be accused of subverting the Shuttle, even though the address had been widely circulated!).

In [RISKS-12.13](#), Peter J. Scott cited an article by Joshua Quittner (\*Junk Mail in Outer Space\*) and noted that the test of EMail was threatened by "unauthorized" EMail. "The leak behind the E-mail address remains a mystery."

Some mystery! Things like that don't stay "secret" for very long. This is another example of an ostrich-oriented protection policy (OOPP) -- stick your head in the sand and pretend no one will find out what you know.

Furthermore, the old "authorization" paradox has reared its ugly head again. ... ``threatened by "unauthorized" EMail", eh??? Sending EMail to someone REQUIRES NO AUTHORIZATION. (You all recall that in the Internet Worm, the use and misuse of the sendmail debug option, finger and gets, .rhosts, and copying an encrypted password file REQUIRED NO AUTHORIZATION, irrespective of whether they were appropriate acts.) If authorization is to be required, then some form of hard-to-forge identification and authentication must be imposed. It's high time that was better understood. On the other hand, if no authorization is required, no one should be surprised if a mechanism requiring no authorization is misused!!!

---

### **✂ The RISKS of a national computerized entertainment ticketing network**

<KJPHELAN@SUNRISE.ACS.SYR.EDU>

Wed, 21 Aug 1991 3:08:50 EDT

The RISK I wish to address is perhaps much lighter than those we usually consider, but it is one I contend is actually a very serious risk posed by a

national computerized network.

This summer the federal government cleared the way for the privately held Ticketmaster Corporation to acquire Ticketron, its rival. This has led to the existence of one company's computer network having control over the seating of every major entertainment or sporting event in the country. While many would consider this a very inconsequential risk, I contend that the risks are in fact severe.

There are more than 8,000 Ticketmaster locations across the country, each with access to every seat in almost every arena in the country. They are everywhere from convenience shops to record stores, each with several people with access to its functions. Unlike other national networks, there are few restrictions on employees use of the network. With most employees at terminal locations making not much over minimum wage, organized crime, among others have realized that for a few hundred dollars they can buy choice seats that can be brokered for ten times their face value and up. (For more information refer to recent articles in Forbes, The Wall Street Journal, and Rolling Stone Magazine.)

I see a risk here to the principle of fair play, that being first come first served. I would like to know more about the systems that make up these networks.

The RISK is obvious: the next time you end up in the upper tier in Yankee Stadium, or find that seats to a Broadway show are only available from brokers for \$200, it may be because of unauthorized access to a computer network.

---

## **✉ Personal data in California**

*Phil Agre <pagre@weber.ucsd.edu>*

*Tue, 20 Aug 91 18:46:07 PDT*

Three brief notes on the privacy of personal data in California.

1. Having just moved to San Diego, I called the phone and gas&electric companies to get service turned on at my new house. When the clerks on the phone asked me my social security number, I very politely asked them why they wanted that information. Whereupon they both became incredibly hostile, haranguing me and accusing me of disrupting their jobs and giving me pointedly useless answers to the effect of "because it's on the form". After two or three times round this, it finally transpired that there are other established ways to proceed without my SSN, by paying a deposit (to avoid a gas-company credit check) or by showing a picture ID at a company storefront (the phone company wanted my SSN to \*verify my name\*). But to find this out, I had to calmly repeat questions, cite laws (says the phone company person, without skipping a beat: "but those laws are antiquated"), and suffer snide tones of voice for some time. And I'm sure these companies happily tell reporters and members of congress about their established procedures for people who do not want to supply their SSN's.

2. Rodney Hoffman's useful summary of the LA Times article on the failure of

measures intended to prevent abuse of personal information in DMV databases did not mention what I found the most amazing part of the article, the complete indifference of the DMV to the problem. Those who've been following this issue are aware that the DMV has been fighting tooth and nail to avoid having to keep any personal data confidential. (Whether this is because they don't want the attendant legal liability or because they are in cahoots with the people who profit from that data is not clear, at least to me.) I would provide some of the quotes from interviews with DMV officials, but they are so extreme that they ought to be read in full context.

3. It is useful to keep this DMV business in mind when considering the new edition of the state Department of Transportation (Caltrans) proposal (previously described on RISKS) to affix transponders to cars that broadcast VIN's when pinged by roadside transmitters. I'll let others evaluate the technical details and just mention two points. (1) The section specifying the cryptographic scheme to be used is empty. (2) The text, as usual with technical specs, does not address the civil-liberties issues it raises, but it does make a big point of explaining that it's up to *\*other\** parts of the government to decide what to do with the data. "Hey, we just send them up. The legislature decides where they come down." In my own opinion, this device and all other personal tracking devices are wrong and cannot possibly be more beneficial than dangerous, especially given the frightening tendencies of the current Supreme Court majority. Please write a letter to someone in the California state government right away.

Phil Agre, UCSD

---

## ✂ Electronic Library Systems in Airliners

*Robert Dorsett <rd@cactus.org>  
Tue, 6 Aug 91 20:18:43 CDT*

Airbus Industrie and Boeing have petitioned the FAA for permission to develop an automated "reference system" for use in airliner cockpits. Thus far, automation in airliners has been of a purely functional basis: controlling or displaying systems information. In some cases, a crew alerting system has been integrated to display what corrective measures to take by displaying an emergency checklist.

What the Electronic Library System will do is replace most of the normal cockpit paperwork with a computer-based reference system. This would include aircraft operations manuals, maintenance information, checklists, cabin management tools, all systems logs, etc. This would all be integrated into a hypertext database, with a graphics interface.

It could potentially be driven by existing Flight Management System components to provide a dynamic, "nice-to-know" information system. In the case of an engine emergency, for instance, the system could produce relevant checklists *\*and\** the secondary ability to step down into relevant Operations Manual pages, to review the relevant systems.

The 24 July 1991 FLIGHT INTERNATIONAL has a two-page article detailing aspects of this system. Relevant portions:

- An ELS will be integrated into United Airlines 777's after first delivery in 1995. United intends to retrofit its entire fleet with the system soon thereafter. [ We may soon be able to spot United pilots by the heavy briefcases they \*aren't\* hauling everywhere. :-) ]
- Being developed by Honeywell, Bendix, Rockwell-Collins, Sextant Avionique, and Smiths Industries (front-runner Rockwell).
- A "total storage capacity" of "60,000 pages." of information. [ This has to be assumed to include graphics information as well. An airliner usually comes with about 50,000 paper pages of integrated text and graphics in the form of operations, training, and maintenance manuals.]
- No existing standard for the format, display, or control of the data.
- Will use Line-Replaceable Modules (hard avionics, including power module, processor, "magnetic mass-memory" and "magneto-optic" modules), connected to terminals via fiber-optic links.
- Will be developed using a modular approach, adding memory [processors?] as necessary.
- Will use "dispatch disks," created by the airline dispatch department, and carried by pilots and inserted into the system to update meteorological information, flight plans, etc.
- Collins is investigating a hardware interface that would plug into the aircraft at the gate, and download information that way.
- Data enumerated by the magazine is subdivided into operations, maintenance, and cabin applications. Operations: Taxi diagrams, Ops manual, Minimum Equipment List, Preflight info, Company policies and procedures, flight manual, performance data, flight log, check-lists, systems diagrams, approach plates, and navigation charts. Maintenance information includes a maintenance log, illustrated parts list, maintenance manuals, fault isolation and reporting data, trouble-shooting procedures, and equipment location. Cabin data includes check-lists, special passenger needs, announcement scripts, cabin maintenance log, flight schedules, reservations, reaccomodation, and supply inventory.

Personal comments:

The concept is quite exciting. It can potentially give pilots access to an overwhelming quantity of information, only a fraction of which they currently have access to at the moment.

The main problems are that it will undoubtedly promote even more of a heads-down attitude, and that a great deal of tangible "paper" data will be locked up in a computer. Combine this with the obvious complexities of data collection, formatting, and the software reliability issues of the user interface, and we have a potential situation of ELS failures or omissions leaving the flight crew high and dry.

I'd like to see--at the very minimum--an independent, "portable" backup for the operations component of the information. I'm sure some vendor would be more than happy to sell a \$50,000 laptop to the airlines. :-)

The FLIGHT illustration of the top-level user interface is of an overpoweringly primitive touch-screen format. Touch-screens are totally unsuitable for this, IMHO. They need to use trackballs. No comment is made, but I'd bet they plan on using ABCDE keyboards, instead of QWERTY keyboards, too. Avionics manufacturers appear to still be wallowing in the 1970's when it comes to designing user interfaces.

Robert Dorsett Internet: rdd@cactus.org UUCP: ...cs.utexas.edu!cactus.org!rdd

---

### **✂ Microsoft, IBM demonstrating faults in each other's products**

*Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>  
Mon, 5 Aug 1991 22:14:53 PDT*

This excerpt appeared in a long article about the rift between Microsoft and IBM in the business section of the NEW YORK TIMES, Sunday August 4, 1991, pages 1 and 6 (section 3). The article is "One Day, Junior Got Too Big" by Andrew Pollack:

"... Mr. (William) Gates said he is angry about a demonstration by I.B.M. a few months ago in which it showed how easy it was to make (Microsoft's software product) Windows "crash" or stall. Microsoft responded last month by showing securities analysts how easy it was to crash (I.B.M.'s software product) OS/2 as well. ..."

- Jon Jacky, University of Washington, Seattle

[People who fliv in crass grouses shouldn't foe knowns.  
The crashability of both are well known to most enlightened people.

Into the crash can you go.  
Do YOU do Windows?  
You might WIN DEC'S disapproval.  
Or else, let the SUN shine in.  
But don't put all your X in one window.  
PGN]

---

### **✂ "Citicorp Creates Controversy With Plan To Sell Data on ... Purchases"**

*Jerry Leichter <leichter@lrw.com>  
Thu, 22 Aug 91 10:08:42 EDT*

The Wall Street Journal (21 Aug 91, page B1) reports that Citicorp has proposed to give marketers access to files on its 21 million customers. The marketers could use the records of purchases in creating targeted mailing lists.

Privacy advocates "are aghast that outsiders could have access to data as revealing as credit-card records." Georgetown University professor Mary Culnan cited Citicorp's plans in testimony to Congress earlier this year, saying that "These transaction records reflect the most intimate details of our personal lives, yet they do not receive any legal protection."

Citicorp says it intends to disclose data only in broad categories - for example, it might release a list of cardholders who buy goods for children. It does not intend to disclose store-by-store details.

American Express has offered a similar program for ten years, apparently without controversy. Banks and industry officials say they know of no other such programs; however, the Direct Marketing Association says it suspects that similar programs exist. In a curious turn, members of the DMA, and other sellers, are concerned about the privacy aspects of such programs - and about their impact on property rights. Citicorp is, in effect, selling a marketer's customer lists to its competitors. "'The most valuable asset you have is that list,' says John Roberts, president of After the Stork, a mail-order company.... He thinks it's unfair for a credit card company to exploit 'data not generated by them but just recorded and captured by them.' After the Stork rents lists of its 500,000 customers for about 10 cents a name." (Apparently Roberts isn't willing to apply the same kind of standard to the information his customers provide to him.) Citicorp's point of view is that someone who charges an order from After the Stork is as much Citicorp's customer as After the Stork's.

Privacy advocates are very concerned that customers at least understand how their information will be used and have the ability to opt out. American Express explicitly tells its cardholders that it prepares mailing lists "for solicitations from American Express and/or other selected companies" - selected, presumably, but ability to pay. It says surveys show that 85% of AMEX card holders know how to get off its mailing lists.

Citibank claims it also tells its customers how to get off mailing lists. However, its sample notice doesn't mention that outsiders may have access to its lists, offering customers "the option of removing your name from the list we use to inform cardmembers of special Citibank offers...."

-- Jerry

---

### **✂ NY Times Letter on Fake Documents**

*Sanford Sherizen <0003965782@mcimail.com>  
Tue, 20 Aug 91 15:38 GMT*

I have posted several comments on desktop publishing fraud on RISKS. The following is my letter to the editor that was published in the New York Times on Friday, Aug. 16, 1991.

BEWARE OF A BLIZZARD OF FAKE DOCUMENTS

To the Editor:

Your article on the use of computers in photo fakery (July 24) discusses only a relatively small aspect of a much larger computer-fraud problem. Desktop forgery is joining computer crime and computer viruses as negative byproducts of the Information Age.

I have been giving my clients an early-warning alert to be prepared for an onslaught of computerized forgery of important documents that can easily pass as originals. The problem is serious.

Documents previously difficult to forge are now being reproduced at professional printing levels by people using inexpensive computers, printers, scanning devices, and desktop publishing technology. There are two major aspects to the problem.

The first is using computers to make duplicate copies of important documents. Examples of documents that can be copied exactly include checks, identification papers, certificates of deposit, immigration papers, Social Security cards and other valuable documents that are at the heart of business and government. To foil reproduction of U.S. currency on color copiers, the Bureau of Engraving and Printing has announced that it will begin to alter paper money starting this summer.

A related issue is the modification of documents, so that unauthorized changes can be made and distributed on what appears to be authentic official information. Employees and others can obtain documents or create their own documents using computer-generated corporate letterhead and copies of signatures. Official-looking documents can be produced containing false statements, illegal offers and libelous comments that can cause problems for companies or government.

The traditional legal and technical restrictions against this counterfeiting and forgery provide limited protections. Some new techniques are being developed to protect documents from being copied, as well as to detect counterfeit documents.

However, there continue to be serious limitations on determining and legally proving which were the originals and which the illegally made copies.

Seeing is believing may soon become an anachronism from the pre-computer days.

Sanford Sherizen, President, Data Security Systems, Natick, Mass

---

## **ATM videotapes**

*Jyrki Kuoppala <jkp@cs.hut.fi>*

*Tue, 20 Aug 1991 03:05:53 +0300*

In [RISKS 12.13](#), there's an article about a wrong picture from an ATM tape being published in New York Daily News, trying to catch a person who had committed a crime.

Rather than the mixup with the tape, what seems very shocking and RISKy to me is the reported fact that the police requested and got "all relevant records

and materials with respect to ATM transactions on the night in question".

Anybody still remember what was the meaning of the year `1984' ?

---

**✈ Re: Bell V22 Osprey crash -- assembly error**

<henry@zoo.toronto.edu>

Thu, 22 Aug 91 01:26:20 EDT

>From the Aug 5 issue of Aviation Week:

The Navy has found an assembly error caused the fifth Bell-Boeing V-22 full-scale development aircraft to crash June 11 on its first flight... Reversed polarity on a gyro-type device that provided inputs to the flight control system was blamed. The assembly problem was difficult to detect, but it was verified as the cause in a flight simulator and isolated to the one aircraft... V-22 aircraft should resume flying soon.

Tsk. While this doesn't seem to have been a computer problem per se, it does make one wonder about a design that could be mis-assembled like that. The military usually tries to avoid this; somebody goofed.

(To digress slightly... one of the most impressive cases of design-for-correct-assembly I've ever seen was the inside of the Canon CX print engine used in the HP LaserJet and other first-generation small laser printers. We service our own LaserJets, and we've had to dig fairly deep at times. It's complicated and messy and has a lot of connectors... no two of which are alike. I don't mean just little keying pins that are easily forced or overlooked; no two of those connectors are the same \*size\* even. And this is in a unit manufactured by the millions at rock-bottom prices.)

Henry Spencer at U of Toronto Zoology  
henry@zoo.toronto.edu utzoo!henry

[Also commented on by Bob Rahe <CES00661@udelvm.bitnet> and Tim\_Diebert.PARC@xerox.com. 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 12: Issue 16**

**Monday 26 August 1991**

## Contents

- [Pacific Bell "Message Center" failure in San Francisco Area](#)  
[David Schachter](#)
- [More Risks of Computer Billing -- \\$22,000 water bill](#)  
[PGN](#)
- [Risk Perception](#)  
[Rodney Hoffman](#)
- [More on Houston Chronicle spacemail item](#)  
[Joe Abernathy](#)
- [Internal computer fraud at Pinkerton](#)  
[Rodney Hoffman](#)
- [P&G phone record search](#)  
[Mark Seecof](#)
- [RISKS on trusting organizations like CERT](#)  
[Jyrki Kuoppala](#)
- [TCAS sees ghosts](#)  
[IEEE Spectrum article via Jim Horning](#)
- [More on the Lauda Air crash](#)  
[Brian Acohido via Nancy Leveson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***✉* Pacific Bell "Message Center" failure in San Francisco Area, Aug. 1991**

*<llustigldavid@decwrl.dec.com>*

*Sun Aug 25 23:25:21 1991*

[David's comments follow my synopsis of a San Fran Chron article. PGN]

Pacific Bell's Message Center answering service broke down for 21 hours around the San Francisco Bay Area, affecting thousands of customers. Two hardware cards converting voice to digital failed at the same time, just before noon on Thursday. This was the longest outage since service began last November. (There had been a four-hour outage last December.) No messages could be recorded, and no recorded messages could be retrieved. However, no recorded messages were lost. Previous problems had been in

software, attributed to the "newness of the system". Some grumbling was quoted about how "They're finding all these bugs at the expense of the customers. [Source: San Francisco Chronicle, Saturday, August 24, 1991, page A10, headline "Pac Bell Message Center Breaks Down; Electronic answering service out of whack for 21 hours", By Dan Levy, Chronicle Staff Writer]

My comments:

1. Pacific Bell has been touting its residential voice mail as a more reliable replacement for the answering machine. They stopped the promotion for a time after word got out that their system was losing about ten percent (!) of all messages.
2. Pacific Bell's current promotion points out that answering machines are an old technology, but voicemail is new. Apparently, the company expects us to believe that new == more reliable.
3. There are times when centralizing a function makes it more reliable. This doesn't appear to be one. When the voicemail system went down, customers could not even rush to a store to buy their own answering machine as a workaround, it would appear. And what voicemail customer would know about the failure? Unlike an answering machine, which has a light to blink rapidly when the machine detects a fault, residential voicemail does nothing, and since the service is pitched as being "more reliable," why would you suspect it?

David Schachter    uucp: ...!{decwrl,mips,sgi}!!lusting!david

---

### ✂ More Risks of Computer Billing -- \$22,000 water bill

"Peter G. Neumann" <neumann@csl.sri.com>  
Thu, 22 AUG 91 09:18:40 PDT

In Austin TX, Malcolm Graham received a water bill for \$22,000, for using almost 10 million gallons of water in one month. The meter reading for the month was slightly LESS than that for the previous month, which the computer interpreted as wrap-around. (A new meter had been installed between readings, and not set properly.) A manual review of unusually large bills failed to spot that one. A utility company spokesman said ``We have about 275,000 accounts each month. We just missed this one. If we only miss one a month, that's a pretty good percentage." <Source: CITY SOAKS A CITIZEN FOR \$22,000 BILL, Article by Scott W. Wright [who'S got Right on it!], 1991 Cox News Service, 22 August 1991>

---

### ✂ Risk Perception

Rodney Hoffman <Hoffman.El\_Segundo@Xerox.com>  
Mon, 26 Aug 1991 08:22:31 PDT

In a lengthy 'Los Angeles Times' article focusing on AIDS infection from doctor to patient (JUDGING THE RISKS OF INFECTION, 26 August 1991, page A1), writer Janny Scott begins by highlighting recent research findings about risk

perception:

- \* Unusual and unknown risks are more terrifying than familiar ones, even though everyday risks claim more lives.
- \* Risks undertaken voluntarily seem more tolerable and controllable than lesser risks imposed from outside.
- \* Many people have difficulty understanding probability.
- \* Familiar accidents may go barely noticed, while unfamiliar ones may provoke panic, particularly if they seem to set a precedent.
- \* Experts and lay people value risks differently: experts count lives lost while the general public focuses on many other factors, including fairness and controllability.
- \* Once people make a decision about the size of a risk, their minds are difficult to change.
- \* "One thing people care a lot about is dread." (Peter Sandman, Rutgers)

---

**✦ More on Houston Chronicle spacemail item (Abernathy, [RISKS-12.15](#))**

*Joe Abernathy <chron!magic322!edtjda@uunet.UU.NET>*

*Thu, 22 Aug 91 13:56:22 CDT*

I've interviewed the NASA experiment manager since then, and she described NASA's statements as overwrought. The shuttle was not mail bombed; applelink was, and this event was misportrayed to Josh Quittner. The flight director was upset because they didn't want anyone to know they were using applelink; but the atlantis account on applelink was created explicitly to facilitate the interest expressed by the network community. I suspect that the confusion stems from the confluence of divergent interests at work.

[... which can also result in multimile piecemeal spacemail. PGN]

---

**✦ Internal computer fraud at Pinkerton**

*Rodney Hoffman <Hoffman.El\_Segundo@Xerox.com>*

*Fri, 23 Aug 1991 08:36:00 PDT*

A short item from the August 22 `Los Angeles Times':

**PINKERTON WORKER PLEADS GUILTY TO COMPUTER FRAUD**

Pinkerton Security & Investigation Services, the 141-year-old detective agency whose slogan is "the eye that never sleeps," was caught napping by an employee who embezzled more than \$1 million from the firm.

Marita Juse, 48, of Burbank[, California], pleaded guilty to computer fraud

this week in U.S. District Court in Los Angeles. Between January, 1988, and December, 1990, Juse wired \$1.1 million of Pinkerton funds to her own account and accounts of two fictitious companies. Pinkerton discovered the theft through a routine audit conducted after Juse left the firm Jan. 7, said Sally Phillips, assistant general counsel for Pinkerton.

Juse also pleaded guilty to unrelated 1986 charges of conspiracy, theft of government property and false claims in connection with a scheme to submit false tax returns claiming refunds. She faces a maximum sentence of 30 years and millions of dollars in fines.

---

### **✂ P&G phone record search ([RISKS-12.14](#))**

*Mark Seecof <marks@capnet.latimes.com>*

*Thu, 22 Aug 91 13:49:50 -0700*

To add injury to insult, the 2/3 of a million Ohio telephone subscribers who had their records searched by P&G (or the prosecutors P&G suborned) will have to PAY for the computer time and other costs of the search in their "regulated" bills. I think that some of the subscribers ought to petition the Ohio PUC to disallow the charges, on the theory that the telephone company failed to carry out its duty to attempt to minimize regulated costs when it (the telco) did not try to have the subpoena quashed.

---

### **✂ RISKS on trusting organizations like CERT**

*Jyrki Kuoppala <jkp@cs.hut.fi>*

*Thu, 22 Aug 1991 20:28:24 +0300*

The subject of this story is the unresponsiveness of CERT and vendors to security holes and the risk that this creates when someone thinks that the holes will get fixed once they are reported to CERT.

The topic of how Unix system vendors, Unix system user and administrators, and organizations like CERT should react on security holes which are found on widespread Unix systems always seems to cause some controversy and lots of discussion.

If you publish a security vulnerability widely, people will complain that you are giving information on how to break into systems to possible 'crackers'. If you don't publish it, it perhaps will never get fixed.

I'd like to report one story concerning one particular security vulnerability which allows any ordinary user to gain unauthorized superuser privileges - perhaps it can be useful to people studying the problems of what to do in case of a surfacing security hole and how to do it. This article probably has only a small fraction of the facts that have happened concerning this and related vulnerabilities. But it probably isn't very different from many stories of similar security holes.

This article doesn't contain technical information - I'll post the details in a

subsequent article in alt.security, comp.sys.sun & alt.sys.sun.

May 1989

I send a bug report to Sun about SunOS vulnerability concerning the SunRPC service rpc.rwalld, the world-writability of /etc/utmp on SunOS and the fact that tftpd is enabled and able to read and write the root filesystem on SunOS. This bug report concerns SunOS 4.0.1 and previous versions.

The hole allows anyone to get in from the Internet as the superuser in a few seconds on an off-the-box Sun. As one suggested fix I recommend write-protecting /etc/utmp. I don't notify CERT - I think at the time I'm not aware of CERT. The hole is fixed in a subsequent OS release - I'm not sure, but I think a separate fix is also published later.

June 1989

I tell about the hole on the Sun-Spots mailing list (gatewayed as the Usenet newsgroup comp.sys.sun) with some details blanked out and give suggested fixes.

A fix for the hole is published by Sun - I don't have records on when this happened.

September 1989

In a security-related bug report reporting also a few other holes, I send the following to Sun and CERT (the Computer Emergency Response Team, an organization established by the Defense Advanced Research Projects Agency, DARPA, to address computer security concerns of research users of the InterNet):

```
>5. /etc/utmp is world-writable. This was one of the original causes
>ogf the rwall / wall / tftp hole, and probably takes part in other not
>yet surfaced security holes.
>
>FIX : chmod og-w /etc/utmp
```

October 1989

I send a somewhat 'details-blanked' version of the above-mentioned bug report to the Sun-Spots combined mailing list and newsgroup, including the note about utmp.

May 1990

A security hole with the program 'comsat' which is used to report the arrival of new mail to users (enabled by the 'biff' program) is discovered. The vulnerability gives unauthorized users root access. The hole is reported to Sun through JPL's Sun software representative. It is also reported to the Internet Computer Emergency Response Team (CERT) and the DDN Security Coordination Center (SCC).

CERT & Sun publish no notice about the hole, no fix is published. In the NASA internal notice the suggested fix is to just disable comsat.

March 1991

I independently find the hole with 'comsat' and report it to Sun and Cert. They don't say it's been reported before, and seem to be somewhat unresponsive about it. At the same time, I publish a rough outline of the hole on the net, and I am told about the previous bug reports. Meanwhile, Sun talks something about a non-disclosure agreement that I should sign so I could get information on a product which will fix the hole.

No notice to the net is made by Sun or CERT. No fix is made available.

April 1991

As nothing seems to happen, I get a bit frustrated and send more mail to Sun & Cert:

>If you can't come up with at least some kind of a solution to the  
>problem, perhaps someone on the Usenet can. I'll post the detailed  
>bug report & perhaps some additional suggestions of fixes to the  
>Usenet newsgroup alt.security a month from now if a decent fix isn't  
>available then.

There's some answer by email from CERT, some talk about what to do. No answer from Sun. No notice to the net is made. No fix is made available.

August 1991

Nothing has still happened - no notice about the vulnerability has been announced on the net. Someone takes up /etc/hosts.equiv containing '+' on comp.unix.admin. I remember the promise I made and write this article.

Conclusions

>From CERT's press release 12/13/88, the paragraph quoted verbatim:

>It will also serve as a focal point for the research community for  
>identification and repair of security vulnerabilities, informal  
>assessment of existing systems in the research community, improvement  
>to emergency response capability, and user security awareness. An  
>important element of this function is the development of a network of  
>key points of contact, including technical experts, site managers,  
>government action officers, industry contacts, executive-level decision  
>makers and investigative agencies, where appropriate.

In the light of this story (and some other experience about CERT) I don't think CERT is doing a good job on 'identification and repair of security vulnerabilities'. It is a good thing to have a central point to contact when trouble arises or when you have a security hole to report, and apparently CERT is doing a good job in acting as this central point, and distributing bug reports to the vendors.

But I think that it is not enough. We need something more to fix the holes - as with this bug, it seems that when the vendor does nothing to fix things, CERT also sits idle, promptly forwards the bug report to /dev/null and does nothing.

Solutions?

I suggest we make it a policy that anyone who sends a security hole report to CERT and/or a vendor will send it to the Usenet some time (perhaps six months? a year?) after the ack from CERT or the vendor.

Any more suggestions to solve the problem ?

---

### **✶ TCAS sees ghosts**

*Jim Horning <horning@Pa.dec.com>*

*Thu, 22 Aug 91 19:04:59 PDT*

IEEE SPECTRUM, August 1991, page 58, Section "Faults & failures":

#### TCAS sees ghosts

A system that warns pilots of impending midair collisions is finally, after 30 years in development, being installed in the U.S. airline fleet. The system, called TCAS for traffic alert and collision avoidance system, sends a stream of interrogation signals to the same equipment aboard nearby aircraft and from their responses determines the planes' altitude, distance, and approach rate.

Plans call for all 4000 large aircraft in the United States to carry US\$150,000 TCASs by the end of 1993. But the phase-in suffered a short-lived --and embarrassing--setback on May 2, when the Federal Aviation Administration (FAA) ordered a shutdown of 200 of the 700 units that had been installed. The 200 systems were seeing phantom aircraft and instructing pilots to evade planes that simply were not there.

The cause was quickly identified as a software glitch. More precisely, it was a software gap--five lines of code missing from the faulty units.

Not subject to the problem were TCASs manufactured by the Bendix/King Division of Allied Signal Inc., Baltimore, Md., and Honeywell Inc., Phoenix, Ariz. These were allowed to continue in service.

However, TCASs made by Collins Defense Communications Division of Rockwell International Corp., Dallas, were recalled so that the software could be fixed. The fix was simple: the units were reloaded with the correct program.

The problem arose in the course of testing, because Collins engineers had temporarily disabled the program's range correlation function--a few brief lines that compare a transponder's current response with previous ones and discard any intended for other aircraft. Without this filter, the system can misinterpret a response as coming from a fast-approaching airplane.

After testing the systems, Collins shipped them to airline customers without re-enabling the range correlation. For the most part, the systems worked as intended. But in high-traffic areas where many airplanes are interrogating each other--around Chicago, Dallas, and Los Angeles, particularly--ghosts appeared frequently. Pilots were misled, and air traffic controllers were distracted from their routine tasks by the need to handle nonexistent situations.

"A pilot would see the ghost image shoot across the screen because the on-board system was accepting all the replies as other TCAS airplanes in the vicinity interrogated the same TCAS transponder," Thomas Williamson, TCAS program manager with the FAA in Washington, D.C., told IEEE SPECTRUM.

TCAS II, the system currently being installed, tells pilots to climb, dive, or maintain the same altitude to avoid a collision. It also displays nearby planes on a small screen. The system was first demonstrated in the early 1970s, but making it work reliably was difficult because of interference by overlapping signals from multiple aircraft in crowded area. The interference was eliminated by using directional antennas and variable-strength interrogation signals and developing range-correlation software to eliminate multiple responses.

In the range correlation scheme, the system notes the distance at which it first receives a response from another aircraft--say 10 miles. At the next interrogation, the distance may be 9.5 miles. The system would then expect the next response to be at approximately 9 miles, and would set a range gate so that it could look for a signal at that distance and calculate the closure rate. Without this correlation, the system becomes confused.

The FAA emphasized that the software fault did not pose a hazard. TCAS is a backup system; primary responsibility for avoiding midair collisions still remains with the ground-based air traffic control systems. Moreover, the FAA pointed out that TCAS has proved its worth in more than 1 million hours of operation.

"Had the problem involved TCAS software on a generic basis, then we would really be concerned," Williamson said, "But it was a breakdown in the quality control procedures of a specific manufacturer."

For its part, Collins has promised customers that it will correct all 200 systems within 90 days after discovery of the problem. "We'll be fully operational across the board well within that time frame," said Charles Wahag, Collins' manager of TCAS products.

Wahag defends Collins' quality control procedures, which were approved by a team of FAA software experts. "We had a simple human error where an engineer misclassified the changes in the software," he told SPECTRUM. "It didn't show up in our testing because one of the essential elements was absent: you have to have many, many TCAS-equipped airplanes in the sky," as in the high-traffic-density areas where the ghost problem appeared.

To prevent similar omissions, Collins now requires that a committee of software engineers review changes before a program is released. "More than one pair of eyes must review these things and make a decision," Wahag said.

COORDINATOR: George F. Watson

CONSULTANT: Robert Thomas, Rome Laboratory

---

## ✈ More on the Lauda Air crash

<leveson@cs.washington.edu>

Sat, 24 Aug 91 10:06:45 -0700

[The following item was abridged by Nancy Leveson, and further by me.

Also, today's paper indicates the FAA has backed off on some of its restrictions. PGN]

>From the Seattle Times, Friday August 23, 1991 (excerpts)

Flawed part in 767 may be flying on other jets

by Brian Acohido, Times Aerospace Reporter

More than 1,400 Boeing 747, 757, and 737 jetliners may be flying with the same type of flawed thrust-reverser system as the ill-fated Lauda Air 767 that crashed in Thailand last spring. A thrust reverser inexplicably deployed on that May 26 flight, possibly flipping the plane into an uncontrollable crash dive. All 223 passengers and crew members were killed.

Officials at Boeing and the Federal Aviation Administration say only that the matter is 'under review' and that they are conferring about possible safety implications for Boeing models other than 767s. The use of thrust reversers on late-model 767s was banned last week by the FAA. Also last week, Boeing alerted airlines worldwide that it may, at some point, recommend that the reversers of these other models be inspected.

Industry sources say it appears a dangerously flawed safety device that is an integral part of the reversers in question may be the same one that is in widespread use on other Boeing models as well. The device is called an electronically actuated auto-restow mechanism. The flaw was discovered last week, and was considered potentially hazardous enough to prompt the FAA to order reversers deactivated on 168 late-model 767s. The ban is in effect until Boeing redesigns the device. [... lots of stuff deleted about the use of it on other planes, etc.] [...]

'In my estimation, the suggestion is very, very strong that there is the distinct possibility there could be further danger with these other aircraft,' said aviation safety analyst Hal Sproggis, a retired 747 pilot. [... more stuff deleted about arguments between the NTSB and the FAA about what should be done.] [...]

On Boeing jets, reversers work like this: A door on the engine cowling slides open, simultaneously extending panels called 'blocker doors,' which deflect thrust up and out through the cowling opening. In flight, the cowling door is designed to remain closed, with the blocker doors retracted, stowed, and locked. Depending on the engine type, the reverser system is powered either pneumatically using pressurized air, or, like the Lauda jet, hydraulically using pressurized oil.

The flawed auto-restow device is designed to detect the system becoming unlocked in flight and to move quickly to restow and relock the system before any significant control problem can occur. According to industry sources, the

NTSB, and the FAA, here's how the complex device works:

An electronic sensor monitors the cowling and alerts a computer if the cowling door moves slightly in flight. The computer then automatically opens an 'isolation valve' which permits pressurized oil or air to flow into the reverser system. This actuates a very crucial, and -- as was revealed last week by the FAA -- dangerously flawed part called a 'directional control valve' or DCV. The DCV directs the pressurized oil or air to retract the blocker doors and shut the cowling door. The DCV can sit in only two positions: extend or retract. In flight, it is supposed to always remain in the retract position, ready to do its part in auto restow.

In older Boeing aircraft, a mechanical part physically prevented the directional control valve from moving off the retract position as long as the plane was airborne. But in newer Boeing jets, the auto-restow mechanism is controlled and kept in the retract position by electronic means. 'The reason they go for these electronic reversers is strictly economic,' safety expert Sproggis said. 'It saves weight, and, in commercial aviation, weight is money.'

When Boeing certified its electronically controlled reverser system, the company assured the FAA that it was fail-safe. As a result, the FAA never required the company to calculate or test what might happen should a reverser deploy in flight at a high altitude and high speed, as happened on the Lauda flight.

After the Lauda crash, Boeing tested the system anew. An engineer wondered what would happen if a simple O-ring seal on the DCV deteriorated, with small bits getting into the hydraulic lines. A test was run. The result: the DCV clogged in such a way that when the auto restow was activated, the DCV moved off the retract to the extend position. Thus, the computer thought it was instructing the DCV to restow when, in fact, it was deploying the reverser.

'I think they (Boeing officials) expected bits of the O-ring to run right through the system and were shocked when they saw the reverser deploy,' said a source close to the Lauda investigation.

After learning of the results of the O-ring test, the FAA, which to that point had rejected repeated exhortations from NTSB Chairman James Kolstad to ban reverser use on 767s, did just that.

Another revelation likely was a factor in the decision to ban reversers on 767s, sources said.

After the Lauda crash, the FAA ordered reversers inspected on 55 767s powered by Pratt & Whitney PW4000 engines -- the same airframe/engine combination as the Lauda plane. (Later, Boeing revealed that a total of 168 767s actually use the same electronically controlled reverser system.)

As 767 inspection reports came in, a disturbing pattern of chafed wires and out-of-adjustment auto-restow sensors emerged. In fact, nine out of every 10 planes checked had sensors out of adjustment, the FAA reported.

Moreover, a Seattle Times review of five years of 'service-difficulty reports,' or SDRs, filed by U.S. airlines with the FAA shows a similar pattern of reverser troubles for 747s, 737s, and 757s.

Airlines are required to file SDRs with the FAA showing how various problems are dealt with. Problems with reversers on Boeing planes are cited on 118 reports from Jan. 1, 1985 through June 25, 1991, including 44 reports on 737 reversers, 25 on 747s, four on 757s, and three on 767s.

SDRs have been widely criticized for being something less than comprehensive because of the wide leeway airlines are granted in deciding what to report. Even so, the reports ranged from cockpit warning lights flickering inexplicably and sensors repeatedly turning up out of adjustment, to numerous instances of stuck or leaking reverser parts. One case involved a 747 aborting a flight

after a reverser deployed and broke up with a loud bang. The plane landed safely.

A pattern of out-of-adjustment sensors suggests that maintenance instructions provided by Boeing to the airlines are not clear or perhaps that the part is badly designed and susceptible to readily moving out of adjustment, said industry sources. More significantly, it suggests that the auto-stow system may be activating unnecessary -- or more slowly than its supposed to -- due to a sensor that's out of adjustment, sources said. [... more discussion deleted about the risk on other Boeing planes]

During the ill-fated Lauda flight, pilot Thomas Welsh, formerly of Seattle, discussed with this Austrian co-pilot, Josef Thurner, the flickering of a cockpit warning signal indicating a possible problem with one of the reversers. Everything was being handled routinely until a second warning signal indicated the left reverser had somehow deployed. Two seconds later, a loud snap is heard on the cockpit recorder, followed by swearing and the sound of warning tones. Thirty-nine seconds after the snap, the tape ends with the sound of a bang. The left engine was recovered from the wreckage with the reverser deployed, evidence that the DCV was improperly positioned, perhaps because it was contaminated, sources say.

Sources said the valve could have become contaminated by something other than a bad O-ring and that investigators also are exploring the possibility that a stray electrical current, vibration or some other phenomenon moved the DCV to the deploy position. A key piece of evidence that could provide the answer -- the left DCV -- was missing from the wreckage.

This incident brings up some important issues:

- The role of the computer in this particular accident
- The role and procedures of the FAA in regulating aircraft
- The trend to removing mechanical safety interlocks in order to save weight and the way that such cost/benefit decisions are being made.

Note that there will be a session at SIGSOFT '91 (Software in Critical Systems) in December on government standards and regulation and that Mike Dewalt of the FAA (his title is "National Resource Specialist -- Software") will be discussing certification and standards for commercial avionics software.

Nancy

Prof. Nancy G. Leveson, University of California  
(on sabbatical at Univ. of Washington)



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 12: Issue 17**

**Monday 26 August 1991**

## Contents

- [Computer-related problems at Cape Canaveral](#)  
[Steve Bellovin](#)
- [Computer communications and the aborted Soviet coup](#)  
[PGN](#)
- [Medical records for sale](#)  
[Jerry Leichter](#)
- [Citicorp selling of credit card data](#)  
[Bud Couch](#)
- [Automating commodities markets](#)  
[Cameron Laird](#)
- [Re: Bank Shot \(RISKS of automatable documents\)](#)  
[Jerry Hollombe](#)
- [Re: Microsoft, IBM demonstrating faults in each other's products](#)  
[Flint Pellett](#)
- [More about California's Automatic Vehicle Identification spec](#)  
[Steve Bagley](#)
- [California DMV AVI proposal](#)  
[Phil Agre](#)
- [Use of ATM for blackmail in UK TV script](#)  
[Mark Evans](#)
- [Desktop Forgeries](#)  
[John Moore](#)
- [Re: SSNs](#)  
[Brad Templeton](#)
- [Sometimes you can only get there using the long way around](#)  
[Bob Cunningham](#)
- [Re: canopus.stanford.edu goes nova](#)  
[Joe Dellinger](#)
- [FTCS 22--Symposium on Fault-Tolerant Computing](#)  
[Jack Goldberg](#)
- [Info on RISKS \(comp.risks\)](#)

---

✉ **Computer-related problems at Cape Canaveral**

<smb@ulysses.att.com>

Mon, 26 Aug 91 16:31:22 EDT

Last week, the range safety officer at Cape Canaveral had to destroy a rocket because it was off-course. The reason: a technician hit the wrong key while loading the guidance software, and the ground test version was loaded instead of flight software. And that caused the steering nozzles to lock in place. The error was apparently obvious on printouts, but no one checked them.

Even the right code were loaded, the rocket may have malfunctioned anyway. A bug was discovered in the navigation programs of a second rocket of the same model; it would have caused the rocket to head in the wrong direction. Launches have been suspended until they can check things over some more. (It isn't known if the destroyed rocket had the same bug.)

The two rockets were conducting SDI-related experiments. The article I saw made no mention of the irony.

--Steve Bellovin

---

### **✂ Computer communications and the aborted Soviet coup**

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

Thu, 22 AUG 91 08:04:06 PDT

Apprently EMail, Internet, CompuServe, and FAX played a major part in foiling the aborted coup attempt in the Soviet Union. Despite local news blackouts, various communiquees found their way around quite successfully. ``While messages from Russian President Boris Yeltsin and other coup opponents were being sent throughout Asia, Europe and North America this week, the committee that tried to seize power either didn't know about or couldn't keep up with the instantaneous network transmissions. ... The unprecedented connection, made possible by the introduction of thousands of personal computers into the Soviet Union under President Mikhail Gorbachev, put a kink into plans to control the flow of information." [Source: DURING COUP ATTEMPT, SOVIET COMPUTER USERS FED NEWS TO OUTSIDE WORLD, By ROGERS CADENHEAD, c.1991 Fort Worth Star-Telegram, 22 Aug 91]

["Coup" is of course pronounced "coo", the sound of the dove.]

---

### **✂ Medical records for sale**

Jerry Leichter <leichter@lrw.com>

Thu, 22 Aug 91 12:48:38 EDT

No computers seem to be involved in this story, but it's an illustration of modern trends.

The New York Times (14 Aug 91, page A10) reports on a controversy that has arisen in Greenville, South Carolina. It seems that Dr. Donald Miller moved to Michigan not long ago. He tried, but without success, to find another doctor to sell his practice to. Ultimately, it was sold at auction. Bidding against a number of doctors and other salvage dealers, Claude Rogers, an area

businessman who runs an auto body and salvage company, an auto leasing concern, and various real estate ventures, bought the building that held the practice and all the equipment for \$92,000. He was also the only bidder at a separate auction, at which he obtained thousands of patient records for \$4,000.

Mr. Rogers felt the records were a valuable resource, defining a ready made market of some 8,000 to 10,000 potential patients; he intended to sell them, along with the physical pieces of the practice, to another doctor. However, he drew no offers - only cries of outrage that someone who was not a medical provider ended up with access to confidential medical information. Mr. Rogers says he signed a document, at Dr. Miller's request, pledging to maintain the confidentiality of the records. In a move he viewed as a service to the patients - but which many saw as an additional cause for concern - Mr. Rogers ran ads in the local papers offering people copies of their medical records for \$25. Mr. Rogers says the fee is the standard amount doctors charge insurance companies in accident claim cases. (According to a doctor I spoke to, \$25 would be a rather low fee. However, doctors do not normally charge patients for copies of their own records.) He says he's had about 30 requests for copies, about half from people on fixed incomes, for whom he's waived the charge.

There appears to be no clear legal protection for the confidentiality of doctor's records when the doctor dies or dissolves his practice. According to the American Medical Records Association, which represents 35,000 people who maintain medical records (is it my imagination or is there an "Association" for every possible grouping of businesses?), privacy rules are clear regarding hospitals, but less so for private practices. The article doesn't indicate what the rules are, or whether they are voluntary or enforceable under state or Federal law, but the association's spokeswoman implied that hospitals must keep medical records confidential.

According to Mr. Rogers, all that counts is a happy ending, and the story appears to have one: Dr. Kevin Smith bought the records (at a "considerable profit" to Mr. Rogers), and is leasing Dr. Miller's old practice. Mr. Rogers says the ready-made patient pool won Dr. Smith over; Dr. Smith was unavailable for comment.

-- Jerry

---

### **✶ Citicorp selling of credit card data (Leichter, [RISKS-12.15](#))**

*Bud Couch <kentrox!bud@uunet.uu.net>  
Fri, 23 Aug 1991 16:42:58 GMT*

Jerry Leichter reports about Citicorp's plan to sell marketing data on it's credit card customers buying habits, and notes that "American Express has done this for years". When my Amex card comes up for renewal, there is always a little box on the form which allows me to opt out of this plan. I check it.

Bud Couch - ADC/Kentrox

---

## ✂ Automating commodities markets

Cameron Laird <cl@lgc.com>

Mon, 26 Aug 91 13:50:59 -0500

"The Chicago Board of Trade, departing from its 143-year-old tradition of frenzied pit trading, announced plans Wednesday [21 August 1991] for a new steel futures contract to be traded only on computer screens. [...] It also represents a cautious step ... away from the increasingly controversial open-outcry trading technique that the Board of Trade practically invented. [...] Open-outcry trading has been criticized in recent years ... prosecutors alleged corrupt traders used the pandemonium of the pits to cover for illegal schemes. [...]" [AP wire story]

It happens quite often that an organization or individual proposes to sanitize the operation of some market--soybean oil, Impressionist masters, gold coins, ...--by moving the operation on-line. It is EXTREMELY rare for an appropriate discussion of the comp.risks of automation to accompany the litany of benefits.

Among the chief concerns of existing market participants are: privacy; reliability; response time; exception-handling; and synchronicity. Automated data-processing certainly has experience addressing precisely those requirements, but not all the experience has been happy. There are bound to be more problems in the future.

Personal opinion: from the little contact I've had, the Chicago exchanges have been effective in their automation efforts. I expect the BoT will make this latest experiment a success, too. However, it's quite typical of them to present information to the public which includes no hint of the possible negatives.

Cameron Laird +1 713-579-4613 +1 713-996-8546 cl%lgc.com@uunet.uu.net

---

## ✂ Re: Bank Shot (RISKS of automatable documents) (Ed Ravin)

The Polymath <hollombe@ttidcb.tti.com>

Wed, 21 Aug 91 19:10:11 -0700

}... The bill, for which Rep. Wyden is now seeking comment,  
}could even include restrictions on the types of companies that can buy  
}sophisticated check-printing equipment often used in the crimes. ...

They plan to restrict the sale of laser printers?

This month's issue of "Byte" lists a relatively inexpensive software product that prints checks, including the MICR encoding, with a laser printer. Magnetic toner cartridges are available for about \$150. So much for "... sophisticated check-printing equipment ..."

Even if they restrict the sale of magnetic toner, most banks take the occasional unreadable MICR numbers in stride and simply re-encode them on a strip of paper glued to the original document. The sheer volume of

checks processed makes examining even these special cases impractical.

Jerry Hollombe, M.A., CDP, Citicorp, 3100 Ocean Park Blvd. Santa Monica, CA  
90405 (213) 450-9111, -2483 {rutgers|pyramid|philabs|psivax}!ttidca!hollombe

---

**✂ Re: Microsoft, IBM demonstrating faults in each other's products**

Flint Pellett <flint@gistdev.gist.com>

26 Aug 91 15:12:01 GMT

JON@GAFFER.RAD.WASHINGTON.EDU (Jon Jacky) writes:

>"... Mr. (William) Gates said he is angry about a demonstration by I.B.M. a few  
>months ago in which it showed how easy it was to make (Microsoft's software  
>product) Windows "crash" or stall. Microsoft responded last month by showing  
>securities analysts how easy it was to crash (I.B.M.'s software product) OS/2  
>as well. ..."

I don't mind seeing them throw stones: in fact, I hope to see more of it. Then maybe some of these industry giants will put a little money into making products that don't crash or hang instead of piling on more features most of us won't use. (It would be nice if other people, like UNIX developers, spent a little money in that direction as well, since the Dec 1990 CACM article on how 25 to 30% of UNIX utilities could be crashed or hung demonstrates they also need to.)

Flint Pellett, Global Information Systems Technology, Inc. 1800 Woodfield Drive, Savoy, IL 61874 (217) 352-1165 uunet!gistdev!flint

---

**✂ more about California's Automatic Vehicle Identification specification**

Steve Bagley <bagley@parc.xerox.com>

Fri, 23 Aug 1991 14:27:09 PDT

A brief addendum to Phil Agre's note in [Risks 12.15](#) about the State of California's Department of Transportation and Automatic Vehicle Identification (AVI):

The current version (dated 20 Aug 91) of the specifications for the compatibility of the AVI equipment is now a "Notice of Proposed Regulatory Action". There will be a public hearing about this spec in Sacramento on October 18, 1991. Written comments will be accepted up to that date at the address below. "Following the public hearing and comment period, the proposal may be adopted substantially as set forth without further notice."

The section on encryption, in the current version, reads in total: "The encryption methodology to be used is defined with individual data message formats. There is no requirement that subsequent message definitions share encryption method [sic] with previously defined data messages." Elsewhere, the standardized DES encodings are referenced although the requirement to use encryption appears to be outside the boundaries of the technical specification.

Each type of radio message between fixed receiver and mobile transponder has both an encrypted and unencrypted form.

A rather short, but useful, section in the preface entitled "Informative Digest" details some of the history of AVI spec. Basically, in Sept 1990 Senate Bill No. 1523 added some sections to the Streets and Highways Code, that provided, in part, that "The Department of Transportation, in cooperation with the district and all known entities planning to implement a toll facility in this state, shall develop and adopt functional specifications and standards for an automatic vehicle identification system."

"Requests for copies of proposed regulations or the initial statement of reasons, written comments, or proposed regulations and questions concerning the proposed adoption of the regulations and the public hearing should be addressed to:

Les Kubel, Chief, Office of Electrical & Electronics Engineering  
Department of Transportation, Division of New Technology - Materials and Research  
5900 Folsom Blvd., Sacramento CA 95819 (916) 739-2405"

Comments about the Senate Bill are probably best addressed to your state representative and the Governor.

--Steve

---

### **✂ California DMV AVI proposal**

*Phil Agre <pagre@weber.ucsd.edu>  
Mon, 26 Aug 91 13:35:15 pdt*

It would seem that the version of the DMV's AVI proposal to which I was referring was out of date by the time I got around to writing my note. I hope that others with access to the newer version will report on it to Risks.

Phil Agre, UCSD

---

### **✂ Use of ATM for blackmail in UK TV script**

*Mark Evans <evansmp@uhura.aston.ac.uk>  
Fri, 23 Aug 91 12:43:21 +0100*

A recent TV program in the UK shows a police investigation into a crime (Indelible Evidence). A blackmailer worked by requesting that money be deposited into an account, which they then withdrew by ATM. There was a point in the program where a terminal was shown listing the card and account numbers of EVERY use of an ATM. (Such equipment had been set up initially covering all possible machines country wide. Surely it would have been possible to have the Bank's central computer recognise the card and put the location of use on a terminal, without needing to display details of any of the customers who may have used the machine.)

Mark Evans, University of Aston, Birmingham, England

---

**✂ Desktop Forgeries (RE: Sherizen, [RISKS-12.15](#))**

*John Moore <sunburn.West!gtx!anasaz!qip.john@fernwood.UUCP>  
Fri, 23 Aug 91 8:45:18 MST*

Sanford Sherizen posts comments regarding use of desktop publishing to forge paper documents:

>The first is using computers to make duplicate copies of important documents.

One wonders if this is significant in comparison to copies made by high quality copiers.

>A related issue is the modification of documents, so that unauthorized changes  
>can be made and distributed on what appears to be authentic official  
>information. Employees and others can obtain documents or create their own

This would seem to be a serious risk.

In the electronic document world, much work has been done on the issue of cryptographic signatures, which both certify the signature and protect the contents from undetected alteration.

Since most important documents today are generated by computer systems, is there any reason that the same technology could not be used for paper documents? When a document is generated, a cryptographic hashing function would be computed, and the result PRINTED on the document. With certain standardization on what is included in the hash, and what formats are used (no old English script, or whatever), the document could be validated using a scanner with associated crypto algorithm (probably using public keys).

Is any work being done in these areas? Should it be?

John Moore

---

**✂ Re: SSNs (Agre, [RISKS-12.15](#))**

*Brad Templeton <brad@looking.on.ca>  
Thu, 22 Aug 91 23:49:43 EDT*

Phil Agre's not-uncommon story of the hassle he encountered in not giving his SSN to the power company made me wonder about the consequences of such actions. In an attempt to remain private, one is often required to make a big fuss and draw attention to one's self.

I wonder if such contradictory behaviour might have bad consequences. Is somebody keeping a database of people who don't want too much information about them to be on file?

---

**✂ sometimes you can only get there using the long way around**

*Bob Cunningham <bob@kahala.soest.hawaii.edu>*

*Thu, 22 Aug 91 07:48:25 HST*

The primary Internet link between North America and Asia uses circuits in HAW-4 undersea fiber optic cable between California and Hawaii, and from Hawaii, other undersea cable circuits to Japan and Korea (indeed, until recently most Internet traffic between North America and Australia went through HAW-4 as well, then via satellite between Hawaii and Australia; though recently they switched to a direct satellite link with California).

At about 0100HST Saturday, repeater #37 on HAW-4 failed, bringing down all the circuits on the cable. An AT&T cable repair ship was dispatched from Honolulu on Saturday, has been on site since Monday, and at last report was still grappling to try to bring the repeater to the surface for repairs. The precise cause of the failure is not yet known. Estimates of full restoration of HAW-4 service range from several days to as long as a couple of weeks.

Overseas telephone services were switched over to other, older (copper) cables and various satellites in a fairly straightforward manner. And while there's less trans-Pacific phone capacity now, I don't believe there's been much if any noticeable interruption of service. Overseas television flows primarily via satellite anyways, and as far as I know, hasn't been affected at all.

Finding alternative computer network circuits turned out to be considerably more challenging. An alternate circuit using international satellite connections was set up between North American and Japan fairly quickly. But between the limited capability of the older undersea cables and a shortage of U.S. domestic satellite transponder capability (more precisely: an apparent shortage of transponders which can use "spot beam" capability with Hawaii), there didn't seem to be any way to set up an alternative connection between Hawaii and the rest of the United States.

Until someone remembered that the circuits between Japan and Hawaii were still working perfectly well...

As of approximately 1000HST Tuesday, Hawaii was reconnected with North America via: an international satellite link between California and Japan, and an undersea cable link between Japan and Hawaii. Only at 384Kbps (1/3rd of the former HAW-4 circuit speed), and it's a rather roundabout "bypass", but it seems to work quite well.

---

**✂ Re: canopus.stanford.edu goes nova**

*Joe Dellinger <joe@montebello.soest.hawaii.edu>*

*Thu, 1 Aug 91 03:14:58 HST*

On June 18, 1990 I reported how the Hitachi monitor of my color Sun 3-110 workstation had suddenly released enough irritating fumes to prompt the evacuation of our (extremely poorly ventilated) Stanford building the previous

evening. Here is the promised followup...

Stanford Health and Safety was quite concerned about the incident; there are a lot of Suns at Stanford, and the fumes were still powerful enough a day after the event that persons entering my office would develop a headache and watering eyes within a few minutes. People in our building naturally wanted to know what toxic chemicals they were being exposed to. Health and Safety wanted to know if this might happen again. (I wanted to know when I could use my office again.) The Sun front-office people that Health and Safety first contacted insisted that this failure mode was virtually unknown and it would almost certainly never recur. We were suspicious of this claim, since in our research group we owned only six Suns of that particular model, and mine was the `_second_` monitor to fail this way within as many years. (The first one fortunately had failed when the building was empty and when the ventilation was working better, so Health and Safety didn't get called that time.)

My posting to risks which appeared a few days later netted a handful of accounts about similar incidents, mostly in Europe. More importantly, it prompted an immediate response from more informed people within Sun [Health and Safety was still trying to beat past the outermost layer of bureaucracy by telephone with little success]. Sun quickly retrieved the offending monitor from Health and Safety (who had carted it off and stored it as toxic waste) and launched an investigation. Sun determined the part that failed was a capacitor in the high-voltage line. This caused the flyback transformer coils to overheat, which in turn caused "a small amount of the case material of the flyback transformer to burn". Sun asked Hitachi, who made the monitor, to investigate what was in the resulting smoke. The conclusion was "There were trace quantities of a number of chemicals in the smoke. We do not believe that a short exposure to the small amount of smoke emitted represents a hazard to the individuals involved."

Sun helpfully included a copy of Hitachi's lab tests showing what they got when they burned some transformer casing in a test chamber. It showed 10 parts per million CO (with 100 the maximum allowed by the American Conference of Governmental Industrial Hygienists), 800 ppm CO<sub>2</sub> (no limit), 2 ppm Formalin (3 max allowed), 1.2 ppm Toluene (150 max), 1.7 ppm Ethylbenzene (125 max), and 3.4 ppm Styrene (100 max). This seemed strange to me; if the smoke were so innocuous why did breathing the air in my office still make me sick more than a day after the event, despite my best attempts to dissipate the fumes? I wanted to know how big a sample Hitachi had burned, and how much air the resulting smoke had been diluted in!

The contact person at Sun seemed a little annoyed that I still wasn't satisfied, and resignedly explained again and again that "parts per million" was independent of the air volume. It didn't matter what size room the Sun was in, how good the ventilation was, or how much transformer case burned. I pointed out that it was a good thing my sun hadn't been outside, or the entire Earth's atmosphere would be contaminated with 2/3 the legal limit for Formalin. Right? They promised to get back in touch with Hitachi.

Three months later I got another letter. It had the same numbers (in ppm) as before, and again had no information about the volume of the test chamber or the amount of transformer casing material burned in the test. It further patiently explained "All of the measured smoke constituents are significantly

below OSHA's established minimum exposure levels. Since the smoke examined in the analysis is of the same type as emitted during flyback transformer failures at Stanford, no significant concerns are raised by the monitor failures you experienced." I tried calling and asking for clarification again, got the same explanations about ppm being independent of air volume (why couldn't I understand such a simple concept?!). Finally I gave up (after all the smell was gone by this time and there seemed to be no ill aftereffects).

The second letter did have some interesting new information, however. Previously we had been told our monitor failures were practically unique; the new letter stated that "When the flyback transformer failure was discovered the total failure rate per month attributable to the flyback capacitors was only .4 percent. After the process improvement, which was promptly implemented, the failure rate was reduced to .04 percent. Although the newer model is superior, the older model was within the range of reasonable failure. Sun recognizes the frustration and disappointment that you must have experienced as a result of two monitor failures. This is an extremely unusual occurrence [sic] and one that Sun would like to avoid in the future."

Was it unlucky? We had 6 monitors for 3 1/2 years; given Sun's stated rate of .4% per month, the chance of at least one failure was  $1 - (1 - .004)^{(12 * 3.5 * 6)} = 64\%$ . Having 2 failures instead of just 1 was probably a little unlucky. Was our problem unusual? Probably yes; from reading between the lines it sounds like the problem only occurred with certain smaller-sized Hitachi monitors delivered around the same time ours were, Sept 1986 - Jan 1987. Our bad luck was in getting 6 monitors from this batch, and then keeping them in near constant use for several years.

The letter continued "Sun is prepared therefore to replace, at no charge, the four monitors remaining in the Department of Geophysics ... for your understanding that the failure rates are negligible and that in any event, monitor failures are unlikely to pose future problems." Our research group took the deal. Not surprisingly, the Geophysics department at Stanford has had no more such incidents since the monitors were replaced (despite a significant expansion in the total number of Suns in the building).

Since my research group accepted the deal, I thought it was appropriate to wait until I graduated and had left Stanford before posting this. I do have a Sun on my desk here in Hawaii and like it a lot; I don't expect it will go "Nova" like canopus.stanford.edu did! I'll let readers draw their own conclusions about the various sorts of RISKS illustrated by my story...

---

## **FTCS 22--Symposium on Fault-Tolerant Computing**

*Jack Goldberg <goldberg@csl.sri.com>  
Fri, 23 Aug 91 14:09:25 -0700*

CALL FOR PAPERS

22ND FAULT TOLERANT COMPUTING SYMPOSIUM (FTCS 22)  
LAFAYETTE HOTEL, BOSTON, MA  
JUL, 8-10 1992

SUBMISSIONS AND INQUIRIES SHOULD BE SENT TO:

DR. J. H. Lala, MS: 6F, C. S. Draper Lab., 555 Technology Square  
Cambridge, MA 02139 USA (Mark the envelope "FTCS22 Submission")  
Tel: 617-258-2235; e-mail: lala@draper.com; FAX: 617-258-4444

IMPORTANT DATES: ABSTRACTS DUE: OCT. 18, 1991; PAPERS DUE: NOV. 22, 1991  
ACCEPTANCE NOTIFICATION; MARCH 16, 1992

The Fault-Tolerant Computing Symposium is the major international forum in fault-tolerant computing. Represented are specification, design, modeling, implementation, test, diagnosis, evaluation and validation of dependable and fault-tolerant computing systems. The symposium scope spans hardware, software and system issues. Original papers not submitted elsewhere are invited from all these areas. Also, solicited for special sessions are practical experience reports in fault-tolerant computing such as design and deployment of a system, field data on failures and recoveries, and correlation of field data with model predictions.

Major topics include, but are not limited to: Fault-Tolerant Architectures, Safety-Critical Systems, Testing and Verification, On-line transaction Processing Systems, Fault Tolerance in Real-Time Systems, Defect Tolerance, Concurrent Error Detection in VLSI circuits, Software Fault-tolerance, and Modeling issues.

INFORMATION FOR AUTHORS:

Six copies of a 1-page abstract and a list of 5 keywords should be submitted before Oct. 18, 1991. Six copies of the paper (1-1/2 spaced, 12 point font) should be submitted before Nov. 22, 1991 and should not exceed 20 pages including figures and text. The paper should be accompanied by ten copies of a title page which includes: the title, author name(s), affiliations, mailing address, phone number, FAX number and e-mail, a maximum 150-word abstract, five keywords, an approximate word count and a declaration that the paper has been clear through author affiliations. For multi-authored papers principal contact should be indicated. Submissions arriving late or significantly departing from length guidelines, or papers submitted elsewhere must be returned without review.

For industrial experience reports, the contributor(s) should submit six copies of a 5 - 10 page written description of the experience along with a one-page outline for a 5- 10 minute presentation.

For panel session recommendations, submit the topic(s), names, addresses, and biographies of the proposed panelists, and a maximum two-page description of the panel objectives.

This year marks the inauguration of technical exhibits at FTCS. Exhibitors from both industrial and academic communities are encouraged. This will be an opportunity to present advanced products to an informed and sophisticated audience.



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 12: Issue 18**

**Tuesday 27 August 1991**

## Contents

- [13 Aug 91 NY Nine Mile Point 2 Nuclear Plant Incident Reassessed](#)  
[PGN](#)
- [Risks to Computers from Coup Attempt](#)  
[Aldis Ozols](#)
- [Oil Firm Surveys for Data and a Data Interchange Format](#)  
[John F Stoffel](#)
- [Ada beats C++ according to the DoD](#)  
[John F Stoffel](#)
- [Unwarranted equivalence assumptions](#)  
[Andrew Koenig](#)
- [Study Recommends Earthquake Warning Network](#)  
[Fernando Pereira](#)
- [Re: Firefighters won't give first aid to AIDS patients](#)  
[Tim Oldham](#)
- [Re: Cracker charged in Australia](#)  
[Richard A. O'Keefe](#)
- [FAA seems misled \(Re: TCAS Sees Ghosts\)](#)  
[Richard Johnson](#)
- [Risks of CDROM publishing](#)  
[Donald M. Craig](#)
- [The RISKS of a national computerized entertainment ticketing network](#)  
[Steve McDowell](#)
- [New List: C+HEALTH \(Computers and Health\)](#)  
[Judy Smith](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ 13 Aug 91 NY Nine Mile Point 2 Nuclear Plant Incident Reassessed

*Peter G. Neumann* <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

*Tue, 27 Aug 91 10:47:07 PDT*

An AP item today, datelined WASHINGTON, noted that Federal investigators are still trying to determine why backup systems failed at the Nine Mile Point 2 nuclear power plant in upstate New York during the 13 Aug 91 blackout, after a

25,000-volt transformer blacked out. Cutover to the "uninterruptible power" system's standby batteries failed. ``The team issued a preliminary "sequence of events" late last week, which indicated that many more systems had failed than originally reported." Furthermore, the plant actually went into "scram" (emergency shutdown), despite earlier reports to the contrary. The plant operators had apparently not known this at the time, because of the lack of backup power. The feedwater control, radio and public address system, computer systems, and some lighting failed. (The NRC team leader, Michael Jordan, was quoted as saying, "Most of it was monitoring systems. All the ones that failed were not safety related.")

[Good thing Jordan was not in Chicago, or there might have been suspicions of his having something to do with the Bulls... PGN]

---

### ✂ Risks to Computers from Coup Attempt

<peg!aldis@igc.org>

Sat, 24 Aug 91 16:41:57 PDT

>From Aldis Ozols, Sydney, Australia.

During the abortive Soviet coup, several data communications links remained open. Not all computer users were fortunate, however, as the following report from Leningrad attests:

>NorthWest northwest.news 6:49 pm Aug 19, 1991

>(at p2013.f20.n490.z2.Fidonet.Org)(From News system)

>

>LENINGRAD-MOSCOW, August 19 /"NORTH-WEST" Information Agency/

> [coup progress news deleted]

>

> All fax-machines and computers at publishing houses of democratic newspapers

> "Smena" and "Nevskoye Vremya" were burnt by strong electric impulses.

[Beware of opening (electric) charge account, and must not buy on impulse! A truly shocking story. But we now have the inevitability of life, death, and faxes--which transcend all sorts of would-be barriers, as long as they don't get fried. PGN]

---

### ✂ Oil Firm Surveys for Data and a Data Interchange Format

John F Stoffel <john@wpi.WPI.EDU>

Tue, 27 Aug 91 02:02:49 EST

Conoco Inc. wants to redesign the way it keeps track of names and address by consolidating scores of files into one global name and address system. The problem is, it does not know how to do it. In a unique approach, the \$2 billion, Houston Texas based oil and gas subsidiary of E.I. du Pont de Nemours & Co. Inc. sent out a survey to the top 108 companies on the Fortune 500 and a majority of its competitors to garner input on whether they have ever attempted a similar records consolidation and what suggestions they could make. In the survey, Conoco also asks if some of its systems personnel can visit the

corporation's sites. The project is being administered by Conoco's accounting systems group and the Conoco Information Systems group in Ponca City Okla. So far, the response rate has been excellent, according to Walt Drawl training director of the accounting system group. After sending out the surveys on June 28, Conoco has received 35 responses - including some from competitors. "We've been getting some good information on EDI," says Drawl. One of Conoco's biggest concerns in file consolidation and information exchange is maintaining data security. "Network security is one of the those monsters out there we have to be very careful of," says Drawl. Drawl and his associates plan to release their findings by the end of August and present them to Conoco management.

{InformationWeek July 29, 1991}

---

### ✦ Ada beats C++ according to the DoD

*John F Stoffel <john@wpi.WPI.EDU>*

*Tue, 27 Aug 91 01:59:58 EST*

I got this from VNS (The Vogon News Service) an internal news feed from Digital for British people working in the US. I thought this article tied in very nicely with the New Jersey bill trying to license programmers. Mostly in the way they compile and use statistics which are pretty meaningless, or do not give enough of a break down on what kind of errors they are.

[In general I think VOGON has no objections to reuse. However, John, next time please leave their HEADERS intact... PGN]

{ComputerWorld July 29, 1991}

#### Ada Bests C++

The US Department of Defense has released the results of four recent studies showing that the DoD mandated programming language Ada is superior in a variety of ways to its newer rival C++. The studies showed that "there is no compelling reason to waive the Ada requirement [in favor of] C++", the Pentagon said.

A fifth study went beyond a look at the third generation, object oriented languages and said the use of fourth generation languages with good development environments and methods can boost software productivity by a factor of 10.

The studies generally found that Ada is more mature than C++, is more standardized, is supported by more vendors and is accompanied by a richer set of development tools. A TRW Inc. study said that Ada is about three years ahead of C++. TRW found that Ada now offered a 35% cost advantage in development and a 70% in maintenance over C++. After 1994, TRW said, those figures may erode to 10% and 30%. However, TRW said C++ rated better than Ada in compilation and runtime efficiency and support of object oriented design.

Carnegie Mellon University's Software Engineering Institute used a language evaluation methodology developed by IBM in the mid-1980s and concluded that Ada was 23% better than C++ in six categories.

CTA Inc. looked at the productivity of the two languages based on actual projects and found Ada programmers on average produced 210 source lines per month while C++ programmers turned out 187 lines.

---

## ✂ Unwarranted equivalence assumptions

<ark@research.att.com>

Tue, 27 Aug 91 10:34:25 EDT

What do the following statements have in common?

'We don't want any illegal drug users in our company, so we won't hire anyone who doesn't pass a drug test.'

'We can't give you that loan; your credit report shows a poor payment history on one of your credit cards.'

'We want to make sure airplanes that enter the country do so legally, so we will only allow airplanes to clear Customs if they have their original certificates of registration with them.'

'I'm sorry, Sir; but even if you are indeed the Ambassador, we can't let you into the Embassy building without a proper pass.'

The obvious similarity is that they would all be supremely frustrating, especially if made inappropriately. Behind that, though, is that each one is the result of a system that assumes that two things are equivalent even when they sometimes aren't.

Not everyone who fails a drug test is a user of illegal drugs; the test might be in error or, as happened not too long ago, the lab might have deliberately fudged the results so that its statistics would look better.

Not everyone who turns up with a bad credit report has a reason for it; sometimes the negative history actually belongs to, say, someone else with the same name.

Not every airplane without an official registration certificate is illegal; perhaps its present owner bought it only recently and is waiting for the permanent registration certificate to arrive from the FAA (which can take many months).

Perhaps the Ambassador was appointed only a week ago, has been outside the country since then, and therefore hasn't had the opportunity to pick up the pass that has been waiting for him.

All four of these examples are based on real events; all four point up an error that is made all too often by people who should really know better. They reemphasize something that everyone knows who has been working with software for any length of time: it's practically impossible to keep two separate databases in step for any length of time. That's true even when one of the

`databases' is reality itself.

--Andrew Koenig ark@europa.att.com

---

## 🔥 Study Recommends Earthquake Warning Network (AP)

*Fernando Pereira <pereira@klee.research.att.com>*

*Tue, 27 Aug 91 18:08:08 EDT*

AP Science writer Paul Recer reports that a committee of the National Research Council recommended the creation of automatic earthquake warning networks for highly seismic areas. The network would take advantage of the fact that the primary (P) wave train from an earthquake moves faster but is less destructive than the secondary (S) wave train, and can therefore be used as the trigger for an automated alarm system. Even relatively close to the epicenter, P waves precede S waves by a few seconds. Such a system could be used to lower fire risks by shutting down natural gas and power distribution networks, to protect computer systems by retracting disk heads, to start a controlled shut down of factory processes, to divert aircraft, etc. Well trained people could also take advantage of the warning to seek shelter.

Even with the risk of false alarms that could cause blackouts and damage, the committee recommended that such a system should be automatic to achieve the required fast response. The system would involve a network of sensors connected by microwave or satellite to a central computer system.

I guess we need a new Emacs function save-all-buffers-on-quake... More seriously, this poses all sorts of interesting RISKS issues. Does anyone know how reliable such a system might be? I assume it would use some form of spatiotemporal cross-correlation to discriminate real quakes from sensor malfunction or local disturbances (big truck going by?) Are there results relating density of sensors, network topology and probability of sensor or link malfunction to probability of false alarm? What are the legal implications of "alarmist" versus "conservative" decision rules?

Fernando Pereira, 2D-447, AT&T Bell Laboratories, 600 Mountain Ave,  
Murray Hill, NJ 07974

---

## 🔥 Re: Firefighters won't give first aid to AIDS patients ([RISKS-12.12](#))

*Tim Oldham <tjo@its.bt.co.uk>*

*Tue, 13 Aug 91 14:31:23 BST*

This is also the case in Britain. A piece on the (National) Radio 4 news programme "Today" broadcast today 13th August described how the Police National Computer (PNC) stores information relating to \*suspected\* contagious diseases, including AIDS. This information is shown in the form of a warning when a look-up is done. According to "Today", the source of the information is never medical files but prison authorities and "other sources" (presumably hearsay sources).

An example of a woman whose record showed that she had AIDS (presumably HIV, in

actual fact) when she did not was quoted. In order for her record to be corrected she had to undergo an HIV test. The woman stated that she had been ostracised by her friends and community because the police had displayed a photograph of her with the word "AIDS" above it in the local police station. I'm not clear whether the computer record or the photograph came first, but there is certainly every possibility that police units will create incorrect records and others will use these records to discriminate against people. The police have "apologised" to the victim in this case. No other compensation seems to have been offered and it appears that she is not suing.

A police spokesman stated that such records were used to ensure that the police take appropriate precautions when dealing with someone whose record showed that they had a contagious disease. By law, the records should be available, although there a number of police get-out clauses to allow them to refuse to reveal parts of their computer records.

Tim Oldham, BT Group Computing Services

---

### ✉ Re: Cracker charged in Australia ([RISKS-12.13](#))

Richard A. O'Keefe <ok@goanna.cs.rmit.OZ.AU>

22 Aug 91 05:16:05 GMT

Fernando Pereira cites an AP report on Nashon Evan-Chaim. Since I know Nashon (he was in one of my classes here last year), I thought I'd put in a word on his behalf. If there is such a thing as "innocent cracking", where someone goes around logging into computers all round the world without any malicious intent, for the sheer joy of exercising an admittedly reprehensible skill, then in my opinion this is an example of it. Based on my conversations with him, he has exactly the kind of knowledge about security holes that you would expect a bright CS undergraduate who isn't afraid of reading manuals to work out. The particular part of the quote which caught my attention was:

> Execucom Systems Corp. of Austin, Texas, where it is alleged he destroyed  
> important files, including the only inventory of the company's assets.

I don't know Nashon *very* well, but I've spoken with him quite a few times, and it would be completely inconsistent with his character as I know it for him to have done anything like this deliberately. Nashon isn't an anti-social "loner", he is quite a helpful person. I would be very surprised and disappointed if this charge turned out to be true. (What company would not have a backup of their inventory, plus the paper audit trail to bring it up to date?)

Although I do not believe Nashon guilty of any malicious intent, that is not to say that I approve of entering systems which don't display a "Welcome" message for visitors.

---

### ✉ FAA seems misled (Re: TCAS Sees Ghosts)

Richard Johnson <richard@oresoft.com>

*Mon, 26 Aug 91 13:51:39 PDT*

A little correction to the comments made by the FAA in Jim Horning's excerpt from "IEEE Spectrum: TCAS Sees Ghosts".. (By the way, thanks, Jim.)

...

: The FAA emphasized that the software fault did not pose a hazard. TCAS is  
: a backup system; primary responsibility for avoiding midair collisions still  
: remains with the ground-based air traffic control systems.

Not quite. TCAS is a backup system. It's a redundant backup. Primary responsibility for "see and avoid" is with the pilot (FAR part 91). The air traffic control system, with all it's eyes, ears, and radar exists to help the pilot avoid situations that can develop into genuine emergencies.

The concept of TCAS is to give back to the pilot some of the ability to "see and avoid" that goes with the responsibility, in an era where huge aircraft can be atop you before you see them. It puts an electronic eye in the cockpit with the pilot; something to help the pilot, rather than air traffic control.

Of course, the FAA has maintained since around 1946 or so that the ONLY effective way to maintain safe skies is through control from the ground, rather than from the cockpit. Draw your own conclusions. Because of this, in some ways, TCAS and air traffic control are at crossed purposes. TCAS gives authority to the pilot, and ATC takes it away.

It is important to remember, that as much as the FAA likes to calm people's fears by telling them that ATC is in "control", the rules put the pilot in the hot seat. The total and ultimate safety of every flight is the job of the pilot first. Everything else is advice.

And there are some interesting failure modes that I hope "experts" have looked into already (faulty or missing messages, failure to notify ATC, etc.)

Richard Johnson richard@oresoft.com richard@agora.rain.com

---

### ***✂* Risks of CDROM publishing**

*"Donald M. Craig" <dmc@taupe.tv.tek.com>*

*Tue, 27 Aug 1991 15:00:50 -0700*

Last weekend, interested in trying out a SparcStation draw program, I inserted a recently arrived SUN Catalyst CDWare disk, Volume 1, in my CDROM drive and attempted to mount it. No luck. After some mucking about, the disk mounted when I specified High Sierra file format. But none of the advertised browsers or programs were to be seen - instead there were a number of very large MSDOS format files. Inside a text file, I found:

"Dear OncoDisc Customer,  
Congratulations on your subscription to OncoDisc, the cancer information service on CD-ROM! You have chosen a unique information service that will provide you with immediate and unlimited access to the key sources

in oncology. We at Lippincott are pleased to have you as a new subscriber and are sure you will find using OncoDisc very exciting and worthwhile."

The disk had Sun Microsystems Catalyst printing on the front, and the silver lettered text on the back said: MADE BY 3M USA CR14614A 910213

My conclusion from this is that some low probability process at 3M's CDROM pressing(?) plant permutes disk labels and contents - and that somewhere there is an unhappy Lippincott customer.

Sigh. Not only a computer risk, but another cancer risk as well.

Don Craig dmc@tv.tv.tek.com  
Tektronix Television Division

---

## **✂ The RISKS of a national computerized entertainment ticketing network**

*Steve McDowell <mcdowell@exlog.com>  
Mon, 26 Aug 91 14:06:38 CDT*

Re: KJPhelan@SUNRISE.ACS.SYR.EDU, [RISKS-12.15](#)

Back in 1985 I worked for the Ticketmaster Corporation on the then latest-and-greatest ticket selling software. At that time, everything was done on PDP-11's running in a fault-tolerant configuration under a Ticketmaster proprietary operating system (a risk in it's own right). Each data center was then linked via leased lines into a centralized database. I understand that they have ported their operating system now to the VAX architecture.

Extreme consideration was given to eliminating the risks of minimum waged ticket sellers turning an unethical profit. They had a command set of about six commands, most of which dealt with whether the customer was paying cash or credit. The system would generate audit reports and automatically check the arena map against tickets sold and the cash reported for each location each night. If there was a discrepancy or if an unusually large number of tickets were sold for a particular location, then the system would generate an alarm on that location. The promoter for each event also received daily activity reports from the system.

The weak link in this system, as in all systems, is the human element. Though it was very hard to make the computer do something that it was programmed to believe to be unethical, things could be done. The seller could "forget" to program returned tickets, for instance. For the most part, however, very little trouble came from the low paid, low techno-savvy, ticketsellers.

The big risk exists in trusted accounts on the system. It could be fooled, but only by someone with direct access. There was a general manager for Ticketmaster in a rather large urban area who had a cocaine habit. He would trade tickets for drugs. He would come in at three in the morning, after the night operators had run their nightly audit procedure, bring the system up thinking it was some absurd date, sell himself fifty or one hundred tickets, then run the nightly audit reports again, ignoring the alarms generated. He

could tell the computer that the seats he sold himself were available, but to not sell them to any outlet. This went on for about three years before he was caught by the night operators who were just trying to learn what made the PDP-11's tick!

The bottom line is that there is a risk, but not a risk any greater than that of, say, the American Airlines ticket reservation system. Abuses of power happen; very little can deter a super-user from doing what he wants to do. Managers simply have to read the audit reports, not just file them. The computer should do self-audits, as the Ticketmaster system does. Care should be taken, and in the case of Ticketmaster it is.

Steve McDowell

---

### **✂ New List: C+HEALTH (Computers and Health)**

*"Judy Smith" <smithj@a1.relay.upenn.edu>*

*Tue, 13 Aug 91 10:24:01 -0400*

[Sorry for those of you on BITNET who get two copies. Judy double posted.]

This list is intended to promote sharing of information, experiences, concerns, and advice about computers and health. Anecdotal evidence, media reports, and some formal studies suggest that computer users are at risk from misuse and overuse of computers. Eyestrain, headache, carpal tunnel syndrome, and other apparently computer-related maladies are increasing. And, it would appear that colleges, universities, and other institutions have been slow to respond with education, training, office and lab design, furniture purchasing, and other programs that could make computing more healthful -- and productive.

We welcome questions and answers; article and book reviews; hardware, software, and furniture evaluations; approaches to influencing institutional policy; speculation; and humor. Medical, legal, technical, financial, aesthetic, and administrative viewpoints are encouraged. We hope that this forum will be of interest to end users, computing managers, epidemiologists, and policymakers.

Subscribers to this list may also wish to participate in EDUCOM's Project EASI: Equal Access to Software for Instruction, "dedicated to assisting higher education in developing computer support services for people with disabilities." EASI provides information and guidance on campus applications of adaptive computer technology. For information on EASI, contact Carmela Castorina, CSMICLC@UCLAMVS.BITNET.

In general, C+Health will focus on individual and institutional measures for "keeping healthy people healthy" as well as remedies for restoring temporarily disabled people to health. We suggest that computing issues related to those with permanent disabilities be referred to our dedicated colleagues at EASI. Although this distinction will not always be "easy," one goal of C+Health is to minimize the number of casualties in our increasingly computer-intensive campuses, offices, and homes.

This list will not be moderated, at least initially, so we encourage

contributors to be succinct, to include relevant parts of messages to which they are responding, and to append their names, titles, and institutions to contributions. New users are welcome to send to the list a brief statement of their experiences and interests in this topic. Unless stated otherwise, it will be assumed that contributions represent individual opinion rather than institutional policy.

As list owners, we look forward to your contributions to C+Health,

Judy Smith, Data Analyst, Office of Data Administration and Information  
Resource Planning, University of Pennsylvania; SmithJ@a1.relay.upenn.edu.

Kimberly Updegrove, Lecturer, School of Nursing, University of  
Pennsylvania; kimu@dairp.upenn.edu.

\*\*\*\*\*

#### On-line references on Computing and Health:

The following articles from campus computing newsletters are recommended for those interested in issues of ergonomics, radiation, light and glare, work habits and exercise, and related issues and protective measures. Articles can be retrieved by sending a GET FILENAME FILETYPE command to LISTSERV@BITNIC (not IUBVM), where FILENAME FILETYPE are shown below in CAPITAL LETTERS.

COMPHEAL DUBEY\_J Computers & Health (Reed College; 3/91; 520 lines)  
COMPHEAL UPDEGR\_D Computers & Health: Issues & Protective Measures  
(U of Pennsylvania; 1/91; 262 lines)  
CTS SHEEHAN\_M Carpal Tunnel Syndrome (Indiana U; 11/90; 212 lines)  
ERGONOM UPDEGR\_D Computers Don't Belong on Desktops (U of  
Pennsylvania;  
11/90; 90 lines)  
ERGO BALKITS Workstation design (UC Davis; 8/88; 64 lines)  
PAIN BRADLE\_J Computing Pains (U of Houston; 3/89; 135 lines)  
SFVDTLAW UPDEGR\_D San Francisco VDT Safety Ordinance (1/91; 146 lines)  
VDT SHEEHA\_M VDT Health Risks (Indiana U; 11/90; 137 lines)

Thanks to Wendy Rickard-Bollentin of EDUCOM for maintaining the articles archive of CCNEWS, from which these articles were selected.

\*\*\*\*\*

#### Hints for using LISTSERV:

To send a message to all subscribers, address it to C+HEALTH@IUBVM (from BITNET sites) or to C+HEALTH@IUBVM.UCS.INDIANA.EDU (from Internet sites).

For all "list management" commands below, send mail or messages to LISTSERV@IUBVM (from BITNET sites) or (from Internet sites) mail to LISTSERV@IUBVM.UCS.INDIANA.EDU. Do not send LISTSERV commands to C+HEALTH, since they will be distributed to all subscribers

\* To leave the list, send command, SIGNOFF C+HEALTH

\* The amount of acknowledgement you receive upon completion of a mailing operation can be changed by means of a SET C+HEALTH OPTION command, where

"option" may be either ACK (mail acknowledgement), MSGACK (interactive messages only) or NOACK.

\* Contributions sent to this list are automatically archived. You can obtain a list of the available archive files by sending an INDEX C+HEALTH command. These files can then be retrieved by means of a GET C+HEALTH FILETYPE command (where "filetype" is the name following C+HEALTH in the file list) or by using the database search facilities of LISTSERV. Send an INFO DATABASE command for more information on the latter.

\* It is presently possible for other people to determine that you are signed up to the list through the use of the REVIEW command, which returns the network address and name of all the subscribers. If you do not wish your name to be available to others in this fashion, issue a SET C+HEALTH CONCEAL command.

\* More information on LISTSERV commands can be found in the "General Introduction guide," which you can retrieve by sending an INFO GENINTRO command.



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 12: Issue 19

Wednesday 28 August 1991

## Contents

- [Phone Fraud](#)  
[Ed Andrews summarized by PGN](#)
- [\(Assumed\) False Alarm at Nuclear Plant](#)  
[Rodney Hoffman](#)
- [O, Oh, what a difficult name](#)  
[Gene Spafford](#)
- [Programs Pester Public Policy People](#)  
[Jeffrey Sorensen](#)
- [Re: 13 Aug 91 NY Nine Mile Point 2 Nuclear Plant Incident](#)  
[Steve Bellovin](#)
- [Re: Ada beats C++ according to the DoD](#)  
[Brinton Cooper](#)
- [Re: Unwarranted equivalence assumptions](#)  
[Brinton Cooper](#)
- [Re: TCAS sees ghosts](#)  
[Steve Jay](#)  
[Lars-Henrik Eriksson](#)  
[Keith Hanlan](#)
- [pugwash.dcs.ed.ac.uk goes nova too](#)  
[John Butler](#)
- [NIST High Integrity Lecture Series: talk by Laszlo Belady](#)  
[Laura Strigel](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Phone Fraud**

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>  
Wed, 28 Aug 91 10:27:41 PDT

Abstracted by PGN from an excellent article in the New York Times (28Aug91),  
Theft of Telephone Service from Corporations is Surging, by Edmund L. Andrews

Telephone fraud is reaching epidemic proportions, with some companies getting  
billed for hundreds of thousands of dollars in bogus calls. Stolen credit

cards and line tapping are old techniques. The new craze involves cracking into switches and PBXs (private branch exchanges).

``It is by far the largest segment of communications fraud," said Rami Abuhamdeh, an independent consultant and until recently executive director of the Communications Fraud Control Association in McLean, Va. ``You have all this equipment just waiting to answer your calls, and it is being run by people who are not in the business of securing telecommunications."

Mitsubishi International Corp. reported losing \$430,000 last summer, mostly from calls to Egypt and Pakistan. Procter & Gamble Co. lost \$300,000 in 1988. The New York City Human Resources Administration lost \$529,000 in 1987. And the Secret Service, which investigates such telephone crime, says it is now receiving three to four formal complaints every week, and is adding more telephone specialists.

In its only ruling on the issue thus far, the Federal Communications Commission decided in May that the long-distance carrier was entitled to collect the bill for illegal calls from the company that was victimized. In the closely watched Mitsubishi case filed in June, the company sued AT&T for \$10 million in the U.S. District Court in Manhattan, arguing that not only had it made the equipment through which outsiders entered Mitsubishi's phone system, but that AT&T, the maker of the switching equipment, had also been paid to maintain the equipment.

For smaller companies, with fewer resources than Mitsubishi, the problems can be financially overwhelming. For example, WRL Group, a small software development company in Arlington, Va., found itself charged for 5,470 calls it did not make this spring after it installed a toll-free ``800" telephone number and a voice mail recording system machine to receive incoming calls. Within three weeks, the intruders had run up a bill of \$106,776. to US Sprint, a United Telecommunications unit.

The article goes on to document the experiences of WRL, pirate call-sell phone operations, voice-mail cracking, etc., familiar to RISKS readers, and discusses the possibilities of blocking calls by area, shutting down out of hours, verifying callers (!), monitoring for unusual traffic, etc.

In the past, long-distance carriers bore most of the cost, since the thefts were attributed to weaknesses in their networks. But now, the phone companies are arguing that the customers should be liable for the cost of the calls, because they failed to take proper security precautions on their equipment.

[...]

Consumertronics, a mail order company in Alamogordo, N.M., sells brochures for \$29 that describe the general principles of voice mail hacking and the particular weaknesses of different models. Included in the brochure is a list of ``800" numbers along with the kind of voice mail systems to which they are connected. ``It's for educational purposes," said the company's owner, John Williams, adding that he accepts Mastercard and Visa. Similar insights can be obtained from 2600 Magazine, a quarterly publication devoted to telephone hacking that is published in Middle Island, N.Y.

It's a good article for those of you whose telephone systems are being cracked (but good for crackers as well!)...

---

### ✂ (Assumed) False Alarm at Nuclear Plant

Rodney Hoffman <Hoffman.El\_Segundo@Xerox.com>

Wed, 28 Aug 1991 08:44:37 PDT

#### NUCLEAR PLANT'S SIREN WAILS BY MISTAKE

San Juan Capistrano - A high-decibel siren warning of a major accident at San Onofre nuclear power plant sounded by mistake Sunday, Southern California Edison Co. reported.... [T]he siren ... went off during the late afternoon and was reported to Edison about 5:30 pm by Orange County emergency management workers.

By the time a repair crew reached the siren, it had stopped operating. [!] ...[T]he warning device was disconnected [!!] and an investigation begun into why it went off. Edison, which operates the San Onofre Nuclear Generating Station, received no complaints from the public about the mishap.... The siren, which warns of a nuclear accident, is part of a network of 50 such devices in [nearby towns].

- - - - -

This was a brief item in the 26 August 1991 'Los Angeles Times.' No explicit mention is made of computers, but this seems relevant to RISKS on several counts. Unfortunately, the story does not tell why Edison was and remains so certain that it was a false alarm; I presume that the other 49 sirens were silent. As for "no complaints from the public," most people probably assumed it was just a particularly obnoxious car alarm. Perhaps the sirens should be replaced by voice, shouting, "Major nuclear accident underway." That would probably get some public attention!

---

### ✂ O, Oh, what a difficult name

Gene Spafford <spaf@cs.purdue.edu>

Wed, 28 Aug 91 11:10:06 EST

From: The Associated Press (and sharply abridged by PGN)

WASHINGTON -- Oh, woe is O.

For months, Stephen O has been hassled by credit card companies. It's not because he's a bad credit risk. It's simply that his last name is too short. Twice the 23-year-old South Korean native has applied for new credit cards, and twice he's been turned down. The banks say their computers cannot recognize a single-letter last name. His automobile finance company says he's "S.O. Stephen." The computer at the Virginia Division of Motor Vehicles says he's OO, which stymied his efforts to get car insurance for a year. To make matters worse, the computer at the Credit Bureau Inc., which furnishes

merchants with individual credit references, insisted that O was nobody, even though he has carried American Express and Visa cards since he was a college student. Instead, the credit bureau listed him as "Ostephen," which confused everybody.

[... He has now changed his name to Oh. ...]

Since he was a kid, being an O has been both embarrassing and amusing. "I always hated the first day of school," he said. "The teacher would call the roll through the M's and N's and then stumble over the O. 'Is this a typographical error?' he'd ask, and I'd say, 'That's me!'" [...]

[I guess he did not read *The Story of O*, by Pauline Reage.  
But, how about "O'O"? Computers would love it! PGN]

---

## **✂ Programs Pester Public Policy People**

*Jeffrey Sorensen <sorensen@spl.ecse.rpi.edu>*

*Wed, 28 Aug 91 13:35:29 EDT*

In the Aug 24, 1991 issue of *\_Science News\_* p. 127 "Faulting the Numbers":

A brief article discusses the topic of the accuracy of computer models when used as the basis for changes in social and tax programs. "A National Research Council panel warns that these estimates are...of unknown quality and may be seriously flawed."

The problems are lack of objective measures for assessing the reliability and validity of the resulting figures. One example cited is the underestimate of the popularity of the individual retirement accounts which thus led to an underestimate of the subsequent revenue lost.

"Arguing that detailed simulations...are important to the policy process, the panel strongly urges the government to allocate sufficient resources to improve the quality of current computer models used for making cost estimates."

Whether this is a case of the government expanding to meet the needs of an expanding government is left as an exercise for the reader. The problem of bad statistics used as the basis for bad decisions has been with us a lot longer than computers have. For some good examples check out:

*\_Systems Analysis in Public Policy: A Critique\_* by Ida R. Hoos  
Berkeley : University of California Press, 1983.

Also in Science News:

\* "Greenhouse Snow: Melting the preconceptions" about the various different outcomes of computer models that raise questions about the feedback effect of melting snow:

more heat -> less snow -> darker land -> more heat -> less snow...  
may actually turn out to be

more heat -> less snow -> more clouds -> a little cooler -> more snow  
or even

more heat -> less snow -> more radiation to space -> a little cooling

\* "Phone glitches and software bugs" says that the DSC equipment responsible for the June phone problems suffered from three faulty lines of code in a program with several million lines. (a 1E-8 error percentage :-)

\* "String and springs net mechanical surprise" gives details of a problem that has to be seen to be believed. A discussion of problems that are counterintuitive including Braess paradox which demonstrates that adding roads to a congested network can actually increase the amount of congestion. Also an electrical equivalent so that "when you add extra current carrying paths, less current flows."

\* And, the cover story, the risk free :-) buckyballs and fullerenes with about four and 1/2 pages dedicated to research in these new forms of carbon.

Jeff Sorensen   sorensen@ecse.rpi.edu   (518) 276-8202

---

### ✂ Re: 13 Aug 91 NY Nine Mile Point 2 Nuclear Plant Incident Reassessed

<smb@ulysses.att.com>

Tue, 27 Aug 91 20:27:49 EDT

An AP wire story indicates that the problem was dead batteries in the backup power supply. The NRC has no standards for battery replacement, the manufacturer says change them every four years, and these were six years old. Utility officials blame unclear manuals, and say that the backup systems weren't wired the way the manual said they should be.

Also worth noting is that the batteries weren't inspected on schedule. However, the inspection wouldn't have measured their charge level in any event. Some inspection procedure...

---

### ✂ Re: Ada beats C++ according to the DoD (Stoffel, [RISKS-12.18](#))

Brinton Cooper <abc@BRL.MIL>

Wed, 28 Aug 91 10:07:49 EDT

John F Stoffel reports on a set of US DoD studies purporting to show that "... the DoD mandated programming language Ada is superior in a variety of ways to its newer rival C++..."

Of course, consider who conducted the studies: TRW and CMU's Software Engineering Institute, each of which have, no doubt, obtained millions of dollars in DoD contracts associated with the use and promotion of Ada. "Can you say conflict-of-interest, boys and girls?"

"CTA Inc. looked at the productivity of the two languages based on actual projects and found Ada programmers on average produced 210 source lines per

month while C++ programmers turned out 187 lines."

Does this mean "More code is better code?" Perhaps it shows that Ada is less expressive than C++ and requires more source code to say the same thing.

\_Brint

---

**✉ Re: Unwarranted equivalence assumptions (Koenig, [RISKS-12.18](#))**

*Brinton Cooper <abc@BRL.MIL>*

*Wed, 28 Aug 91 10:12:34 EDT*

Andrew Koenig discusses four cases of "Unwarranted equivalence assumptions."

His arguments make a lot of sense, but one is flawed. His fourth example is:

'I'm sorry, Sir; but even if you are indeed the Ambassador, we can't let you into the Embassy building without a proper pass.'

He argues,

"Perhaps the Ambassador was appointed only a week ago, has been outside the country since then, and therefore hasn't had the opportunity to pick up the pass that has been waiting for him."

Suppose the denial had been by computer:

"Incorrect password: Login aborted."

Would he argue that this might have been the \*genuine\* user who had forgot her password and that the "system" should have known better because the login was from site known to her office? In fact, both my hypothetical case and that of newly-appointed Ambassador Strauss are examples of \*Authentication\* systems. They must be left in place. Even if the State Department guard \*knew\* Ambassador Strauss personally, it was proper to deny him admission without a building pass. Who knows why the pass may have not yet been issued?

Did anyone ever hear of Clark Clifford?

\_Brint

---

**✉ Re: TCAS sees ghosts (Horning, [RISKS 12.16](#))**

*Steve Jay <shj@ultra.com>*

*Tue, 27 Aug 91 16:53:05 PDT*

> Wahag defends Collins' quality control procedures, which were approved by  
> a team of FAA software experts. "We had a simple human error where an  
> engineer misclassified the changes in the software," he told SPECTRUM.  
> "It didn't show up in our testing because one of the essential elements was  
> absent: you have to have many, many TCAS-equipped airplanes in the sky,"  
> as in the high-traffic-density areas where the ghost problem appeared.  
>

> To prevent similar omissions, Collins now requires that a committee of  
> software engineers review changes before a program is released. "More than  
> one pair of eyes must review these things and make a decision," Wahag said.

Am I the only one who sees a non sequitur here? "We didn't catch the bug because we didn't test it in realistic conditions, so next time we'll look at it harder before we release it."

Seems like some folks don't learn real fast.

Steve Jay, Ultra Network Technologies, 101 Dagget Drive, San Jose, CA 95134  
shj@ultra.com ...ames!ultra!shj (408) 922-0100 x130

---

**✉ Re: FAA seems misled (Re: TCAS Sees Ghosts)**

*Lars-Henrik Eriksson <lhe@sics.se>  
Wed, 28 Aug 91 09:06:36 +0200*

>Not quite. TCAS is a backup system. It's a redundant backup. Primary  
>responsibility for "see and avoid" is with the pilot (FAR part 91). The air  
>traffic control system, with all its eyes, ears, and radar exists to help the  
>pilot avoid situations that can develop into genuine emergencies.

The "see and avoid" responsibility is only applicable in visual flight conditions. In instrument flight conditions, the pilot don't have any such responsibility (Obviously - since he cannot see much outside his own aircraft).

Also, it is a fact that "see and avoid" doesn't work well with aircraft flying at high speed. Many investigations of midair collisions have shown that although the pilots had a theoretical possibility to see each others aircraft in time, the practical possibility was very slight.

>... TCAS and air traffic control are at crossed purposes. TCAS gives  
>authority to the pilot, and ATC takes it away.

ATC authorities (both FAA and those of other countries) have the legitimate concern that pilots will react unnecessarily to TCAS alerts and cause other incidents by doing unauthorised deviations.

I understand that the TCAS technology and the procedures being applied when a TCAS alert occurs have developed to a point when this risk is at an acceptable level.

Lars-Henrik Eriksson, Swedish Institute of Computer Science, Box 1263, S-164 28 KISTA, SWEDEN Phone (intn'l): +46 8 752 15 09 Internet: lhe@sics.se

---

**✉ Risks of developer testing (was TCAS sees ghosts)**

*Keith (K.P.) Hanlan <KEITHH@BNR.CA>  
28 Aug 91 11:17:00 EDT*

The article on TCAS failure quoted by Jim Horning ([RISKS 12.16](#)) illustrates an deficient software development process:

"The problem arose in the course of testing, because Collins engineers had temporarily disabled the program's range correlation function--a few brief lines that compare a transponder's current response with previous ones and discard any intended for other aircraft. Without this filter, the system can misinterpret a response as coming from a fast-approaching airplane."

"After testing the systems, Collins shipped them to airline customers without re-enabling the range correlation."

The flaw here is that the same group is doing development, testing, and "manufacturing" (loadbuilding). I'd suggest that if the CASE tool I work on uses independent testers and loadbuilders, an aviation safety device merits similar precautions. Designers must of course do their own testing but the code they submit to loadbuilders should be intended for production. The independent testers should only work with this "production" code. And the product should only be produced from the loadbuilder's software.

Thus even if the designer accidently submits test code, the testers should detect the flaw and fail the software. And similarly, if the testers wish to insert faults, those faults can not get back into the production code.

On a related note, inserting faults by changing code is never a good idea and this mistake clearly illustrates why.

Let me add that when I refer to "independent" testers, I mean physically disjoint human beings. I, as a developer with intimate knowledge of the inner workings, \*know\* that if this test-case works then all these others will work as well. This is, of course, until Michelle comes along with her cunning pathological special case. This happens time and time again.

Finally, by "loadbuilding" I mean that the activity of configuration management, compiling, linking and installation. My apologies for using terms that may only have local meaning.

Keith Hanlan keithh@bnr.ca Bell-Northern Research, Ottawa, Canada 613-765-4645

---

** pugwash.dcs.ed.ac.uk goes nova too**

<jhb@dcs.edinburgh.ac.uk>  
Wed, 28 Aug 91 12:57:36 bst

Followup to posting in [RISKS DIGEST 12.17](#)  
from joe@montebello.soest.hawaii.edu (Joe Dellinger) 1 Aug 91

Well I guess we've located the newest way of keeping ourselves warm in the winter nights or at least gassing ourselves so we don't notice.

We have (had) a Sun 3/110 with a Hitachi 15" LC monitor in a lab here. A week or so ago the occupants of the lab evacuated hastily complaining of a strong smell

watering eyes, sore throat etc. I would describe the smell as similar to the sweetish smell you get around a badly ventilated clothing dry cleaners and would guess a halocarbon of some sort. We instantly blamed the air-conditioning units and went looking for coolant leaks. By this time the security services had been called and they in turn called in the Fire Brigade who threw us all out and did a thorough survey in full chemical isolation gear and breathing apparatus. It's not easy to locate the source of a smell in full gear and so it was well into the afternoon before someone noticed this monitor was still on and we traced it. If the smell had been the usual yukky smell you get off any torched electronics we'd have got it instantly - this was a new one on us. Culprit was what looked like a torodial transformer in the EHT side of the monitor which was sitting in a little puddle of plasticised slag.

We have no idea what we've been breathing but the city Medical Officer has requested further tests and we are sending him an intact monitor plus the slagged transformer.

This incident is still in progress here as we have yet to have any extensive talks with Sun but I'm posting this meanwhile as it appears there is a real safety risk.

John Butler, Computer Science, The University of Edinburgh, Kings Buildings, Edinburgh EH9 3JZ UK Telephone: +44-(0)31-650-5181 <jhb@dcs.ed.ac.uk>

---

### **NIST High Integrity Lecture Series: talk by Laszlo Belady**

*Laura Strigel <strigel@swe.ncsl.nist.gov>*

*Tue, 27 Aug 91 11:26:58 EDT*

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY  
COMPUTER SYSTEMS LABORATORY  
LECTURE SERIES ON HIGH INTEGRITY SYSTEMS

The Engineering of Software for High Integrity

Laszlo A. Belady  
Chairman and Director of the Laboratory  
Mitsubishi Electric Research Laboratories

October 11, 1991, 2:00 p.m., NIST Green Auditorium

Software is now paramount in determining the qualities of man-made and man-machine systems. Problems of integrated, networked information systems and of machinery in which software is the significant component are particularly acute. The design of these software-rich systems must be based on combined expertise in computers and in the application domain. This leads to design by teams of many experts whose efforts also need the support of information technology. A few emerging solutions, some still in the research stage, will be discussed, and the importance of technology infusion and education emphasized.

The goal of the lecture series, open to the public free of charge, is to alert federal and industry managers, technical staff, and users of the issues they must be concerned with in the management of valuable information resources.

FUTURE LECTURES:

November 8, 1991: Early Error Prediction: Better Error Management and Improved Process Control; Dr. John Gaffney, Manager, Measurement and Economic Modeling, Software Productivity Consortium

December 3, 1991: Toward a Routine Practice for the Engineering of Software; Dr. Mary Shaw, Professor of Computer Science, Carnegie Mellon University

For further information contact:  
Dolores Wallace (301) 975-3340 or Laura Strigel (301) 975-5248.



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 12: Issue 20

Friday 30 August 1991

## Contents

- ["Thieves Hit Social Security Numbers"](#)  
[Yasmin Anwar](#) via [PGN](#)
- [Jetliners in near-miss over Cleveland](#)  
[PGN](#)
- [More T/CAS](#)  
[Martyn Thomas](#)  
[Robert Dorsett](#)
- [Overseeing dementia patients by computer](#)  
[Urban Fredriksson](#)
- [Heisenberg effect for credit data?](#)  
[Peter G. Capek](#)
- [The story of O \[and Ng\]](#)  
[Jerry Leichter](#)  
[Stuart I. Feldman](#)
- [A number is no name](#)  
[Clifford Johnson](#)
- [The need for utilities to deal with non-standard situations](#)  
[Tom Lincoln](#)
- [Uncle Sam Can't Keep Track of his Trillions](#)  
[Bob Frankston](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ "Thieves Hit Social Security Numbers"

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Fri, 30 Aug 91 10:00:36 PDT

One of the better newsmedia items on the misuse of Social Security Numbers is an article by Yasmin Anwar, Chronicle Staff Writer, in today's San Francisco Chronicle. Front Page. She is a Chron Intern, and I think she is to be commended for a superb job of incisive reportage. The following item is included in RISKS in its entirety because of its keen relevance to our ongoing discussions on this subject in the RISKS FORUM, and the increasingly serious problems that it poses.

Copyright San Francisco Chronicle, 30 August 1991. Reproduced in RISKS with explicit permission of the Chronicle for use by the RISKS Forum. Any further distribution or publication requires explicit permission of the Chronicle.

Thieves Hit Social Security Numbers  
Fouled-Up Benefits and Credits  
By Yasmin Anwar, Chronicle Staff Writer

Debbie Biner knew something was wrong when the Internal Revenue Service demanded back taxes for a job she never had. Then her boss accused her of falsely claiming unemployment. Bewildered, the 36-year-old Moraga woman set out on a two-year investigative trail that led her to a bizarre discovery -- 12 people from as far away as Virginia had been using her Social Security number. "I've never been late on a payment in my life," she said. "Who knows what people are doing with my number?"

Biner is among a growing number of victims stung by Social Security number theft, a crime that can take years to detect. Most often, the felony reveals itself in fouled-up tax records or muddled credit reports. Occasionally, major embezzlement is involved. "Someone can take your number, get a credit card, charge it to the limit and vanish," said Steven Gruel, an assistant U.S. attorney and former immigration fraud prosecutor.

Although many consumers go to great lengths to safeguard their credit-card numbers -- cutting up expired plastic and tearing up carbon receipts -- few realize the dangers of a Social Security number in the wrong hands. In this computer age, where extensive records on a person's background are just a keystroke away, the importance of protecting Social Security numbers is magnified. "If a private eye wants to find somebody, a Social Security number is all he needs," said attorney Fred Gross.

So far this year, 550 people have been convicted of felonies for stealing, selling or using bogus Social Security numbers -- compared with 468 convictions for all of 1989, and 390 in 1988. And federal authorities figure the convictions reflect just a fraction of the problem.

"It's rampant. But the (Social Security) system isn't set up to detect fraud," Gruel said. "You don't know people are using your number unless you try to take out a home loan and your credit file is flagged."

Examples of fraud:

\* Joelle Robert, a waitress at San Francisco's Meridien Hotel, could not figure out how someone opened 16 credit cards in her name -- then ran up \$10,000 in charges. Eventually, Robert learned that someone she considered a friend had been using her Social Security number.

"I don't understand why credit companies don't ask for more IDs when they give people cards," Robert said.

\* A Martinez woman trying to claim unemployment last year was told by the state Employment Development Department that five people using her number had already beaten her to it. The woman, who asked not to be identified, said she gave up trying to claim benefits.

\* Lizabeth Stephens, a.k.a. Elizabeth Ann Borruso, used eight Social Security numbers and six names last year to open accounts throughout Northern California at Citibank, Security Pacific and Great Western Savings. She obtained an Army civilian identification card under a false number and name. Currently in jail awaiting sentencing, she faces a maximum sentence of five years in prison and a \$250,000 fine.

Experts attribute the increasing abuse of Social Security numbers to two main factors: undocumented immigrants seeking work in the United States and the business world's increasing use of the number as a universal ID.

The 1986 Immigration Reform and Control Act -- designed to control immigration and tighten restrictions on illegal workers -- ended up fueling a black market in phony IDs, which contain Social Security numbers.

Illegal immigrants, who now need to present more IDs when they apply for a job, can buy fake green cards and numbers from street corners and stores for as little as \$30. "We created an industry," said Philip Waters, deputy district director for the Immigration and Naturalization Service, who estimates there are 50,000 identification counterfeiters operating in the United States.

Immigration fraud investigators say they seldom pursue workers who have used bogus identifications. "We get the manufacturers and vendors. The bigger the better," Waters said.

#### Uses of the Number

Social Security numbers can be misused in many ways. The computer age has allowed businesses and government agencies to compile extensive and centralized records on Americans. And a Social Security number unlocks that information.

By tapping into computer systems, enterprises as diverse as insurance companies, police departments, hospitals, grocery stores and colleges can dig up details on individuals ranging from unpaid medical bills to cocaine convictions.

"The number is information fly paper. It's basically one step short of putting a bar code on everyone's forehead," said attorney Mark Rotenberg, a former adviser to the Senate Judiciary Committee.

#### Shaky Legal Ground

By law, the only agencies that can demand a Social Security number are the Social Security Administration, the IRS, employers, banks and the military. Other agencies such as credit bureaus, insurance companies, police departments and hospitals have no legal authority to request it. Yet businesses routinely obtain customers' Social Security numbers because people give them out on applications.

"I personally protect my number like it's gold. I keep it locked up in a safe deposit box," said IRS spokesman Larry Wright. "If they choose to deny me the credit card, I don't care. I'll go somewhere else."

The 1974 Privacy Act prohibits government agencies from giving out information from individuals' files. Citing the act, Peter Zilahy Ingerman, a New Jersey computer scientist, sued the IRS for displaying taxpayer Social Security numbers on income tax form envelopes. The case is pending in U.S. District Court in New Jersey.

#### Seeking the Culprits

As Debbie Biner's case illustrates, the search for a number thief can be time-consuming and complex. Biner said government agencies offered no help. "It was so frustrating. Everyone kept telling me my case was out of their jurisdiction." she said.

So Biner asked Transunion, the nation's largest credit bureau, to run her number through a tracing system to determine who was using her nine-digit identifier.

### Slowing the Number Flow

In Washington, D.C., privacy rights advocates and watchdog groups such as Computer Professionals for Social Responsibility are lobbying Congress to write stricter Social Security laws.

They are pushing for a legal guarantee that would state, "No person shall be denied credit, employment or the opportunity to engage in a commercial transaction for failure to provide his or her Social Security number."

Meanwhile, Biner sits in her Moraga apartment, as her 6- and 7-year-old children play, and writes letters. Fraud investigators have advised her to contact the IRS, the Employment Development Department, various collection agencies, banks, department stores and furniture stores where her number mates are doing business. "My name is Debbie Biner," she writes. "I am the original owner of the following Social Security number. Please remove the following 12 names and their attached transaction records from my files. "

---

### ✈ Jetliners in near-miss over Cleveland

"Peter G. Neumann" <neumann@csl.sri.com>  
Fri, 30 Aug 91 9:27:31 PDT

The PGN digesting service notes a NYTimes-originated article in this morning's San Francisco Chronicle (p.A3) regarding the near-miss last Saturday (24Aug91) over a radio navigation marker at 35,000 feet, 20 miles southwest of downtown Cleveland, which somehow did not get into the Cleveland Plain Dealer until yesterday, Thursday (29Aug91). A British Airways DC-10 from London to Atlanta (routed over Toronto and Cleveland) came within 100 feet vertical and half a mile horizontal (only a few seconds separation on closure!) of a Midway Airlines DC-9 from LaGuardia to Chicago. Apparently a controller had accidentally assigned the DC-10 the wrong frequency, the crew had not realized it, and the air traffic controllers observing the two planes on an apparent collision course were unable to contact the DC-10 crew -- which never saw the DC-9. But it was certainly disturbing that the DC-10 crew had not contacted the controllers since passing Toronto. Indeed, NEITHER plane was in contact with the proper controller. Incidentally, neither plane had the collision avoidance system that will be mandatory by the end of 1993. At the last minute (literally) one of the DC-9 pilots spotted the other plane and took evasive action.

---

### ✈ TCAS false alarms

*Martyn Thomas <mct@praxis.co.uk>*

*Thu, 29 Aug 91 11:08:30 BST*

Further to the recent IEEE Spectrum report on problems with the Collins TCAS systems.

Flight International (28/8/91) reports that the US National Air Traffic Controllers Association (NATCA) is claiming that at least half of altitude deviations following TCAS "resolution advisories" are due to malfunctions. NATCA says its estimate is conservative (the FAA disagrees).

The US airline pilots association also says that the problem is not as large as NATCA says.

Problems have mostly been fixed by software changes. They include:

- \* Intruders with a high vertical speed but about to level off
- \* Intruders with adequate vertical separation transponder/encoder errors
- \* Intruders on parallel approaches causing unnecessary go-arounds
- \* TCAS detecting its host aircraft transponder [!!!]
- \* "Descend" advisories issued when the aircraft is only 500ft AGL
- \* High-wing military aircraft with belly-mounted transponders not triggering TCAS.

NATCA say there were 325 TCAS-generated incident reports between 5 May and 12 August. 200 involved altitude changes. Of these 69% reported a deviation of 500ft or greater, 23% reported 1000ft or greater. Pilots are normally advised that a TCAS resolution advisory should result in a deviation of 300ft to 500ft.

I believe that these incidents all involve TCAS II, which only gives vertical advisories. TCAS III will also give lateral advisories - this is computationally harder: whether it will result in more or fewer incidents remains to be seen.

I fear that we are creating an arbitrarily-complex network of systems interacting in real-time, with feedback. I doubt that our technology is capable of assessing the failure probabilities of such a system. Does anyone on the net have a copy of the safety-case justifying the mandatory introduction of TCAS?

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

Tel: +44-225-444700. Email: mct@praxis.co.uk

---

## ***✉* More T/CAS**

*Robert Dorsett <rd@cactus.org>*

*Fri, 30 Aug 91 01:17:45 CDT*

Lars-Henrik Eriksson wrote:

<>Not quite. TCAS is a backup system. It's a redundant backup. Primary

<>responsibility for "see and avoid" is with the pilot (FAR part 91).

>

>The "see and avoid" responsibility is only applicable in visual flight  
>conditions.

...and in IFR conditions, the primary separation responsibility is with the  
air traffic control system. T/CAS is a warning/alert system, and is not  
designed for tactical situational awareness.

<>... TCAS and air traffic control are at crossed purposes. TCAS gives  
<>authority to the pilot, and ATC takes it away.

>

>ATC authorities (both FAA and those of other countries) have the legitimate  
>concern that pilots will react unnecessarily to TCAS alerts and cause other  
>incidents by doing unauthorised deviations.

Currently, it is FAA's policy that it will NOT pursue enforcement of any  
clearance violations by pilots who deviate due to T/CAS alerts. False alarms  
happen often enough, and cause enough pilot concern, that there is now almost  
a monthly reminder in the Air Line Pilots Association newsletter that it is  
still being tolerated.

The controllers resent their organized chaos being disorganized; pilots want  
to stay alive. If I were a passenger on an airliner, I think I'd want my  
captain to err on the side of caution.

Interestingly, many controllers are not completely aware of the FAA's  
lenience on the issue, and continue to write up pilots. ATC currently  
recommends that pilots inform them whether the aircraft has TCAS, so they  
can plan for more lenient separation.

>I understand that the TCAS technology and the procedures being applied  
>when a TCAS alert occurs have developed to a point when this risk is  
>at an acceptable level.

I've seen nothing to suggest that the number of false alarms is falling. In  
fact, as more T/CAS-equipped aircraft come online, the number seems to be  
increasing. In the terminal environment, I'm hearing more discussions between  
pilots as controllers, as pilots attempt to reconcile their T/CAS warnings with  
ATC radar. I have no data to support this, but it's my perception that T/CAS  
warnings are starting to be taken with a grain of salt. This regarding a  
system whose warnings are designed to be obeyed in a time-critical framework!

The design of the T/CAS interface is also fluid. Some systems present a  
"plan" overview on the weather radar screen; another has T/CAS warnings  
built into a funky (and slightly odious) vertical-speed indicator. I had  
hoped that the FAA would standardize display formats, but perhaps not.

To bring this back to RISKS: T/CAS is turning into a classic case of what  
happens when technology is developed and implemented under hysterical political  
pressure, without a concrete grasp of the consequences. T/CAS has been under  
development for years; but it was pushed into service as a result of a mid-air  
collision in the early 1980's.

It did not address the safety issue of the \*much\* higher rate of mid-air collisions BETWEEN general-aviation aircraft, it does not address Mr. Eriksson's observation of ATC/pilot disagreements, and it does not address potential improvements to the ATC system. Ultimately, I suspect there will be more and more restrictions on T/CAS (all it takes is ONE change of the FAA Administrator)--and, at some point, we will find ourselves wondering why we bothered with this very expensive system. The images of drug-crazed pilots and mid-air airliner collisions are quite useful to politicians to rally support around, despite the improbability of either occurring. Few of these politicians attempted to address the real cause of the degradation of air safety in the 1980's: deregulation, and the shortage of experienced controllers caused by Reagan's mass sacking in 1981.

Robert Dorsett Internet: rdd@cactus.org UUCP: ...cs.utexas.edu!cactus.org!rdd

---

### **✂ Overseeing dementia patients by computer**

<Fredriksson\_Urban\_NOK@kista.relay.nokia.fi>

Fri, 30 Aug 91 11:31:41 +0300

"Gunnar, it is night. Don't go out, go to bed!"

"Gunnar, shut of the water tap."

These voice messages are controlled by a computer watching over Gunnar, aged 77 and suffering from senile dementia. They were taken from a Swedish radio program mainly dealing with how to take care of old people while preserving their integrity.

Gunnar doesn't want to stay in a home, so he has food delivered to his apartment and help from time to time.

The computer is part of a highly modified burglar alarm system, which is still in the trial stage. The designer thinks it is better than video surveillance, since now Gunnar isn't watched over, but can get help when he needs it, for example if he is lying on the floor. Or when he doesn't need it, if the new help makes his bed so the sensor gets unplugged, which has happened.

Gunnar doesn't understand there is a computer, any positive reaction is probably because he thinks he's got visitors. His life isn't risk free: He smokes, but isn't very good at putting the cigarettes out, so one message is:

"Gunnar, there is a fire! You must go out  
in the street immediately!!"

But he also runs the risk of being a VERY involuntary beta tester. It took a long time before it was discovered what would have happened if there was a fire in the night.

"Gunnar, it is night. Don't go out, go to bed!"

Urban Fredriksson, Stockholm, Sweden

---

## ✂ Heisenberg effect for credit data?

"Peter G. Capek" <capek@watson.ibm.com>

Thu, 29 Aug 91 10:03:14 EDT

BankCard Holders of America reports that too many inquiries (e.g., to a credit bureau) for an individual's credit report can harm that report by making it appear that credit is being applied for from too many sources, resulting in the individual being over-extended. An example given is that of a person shopping around for a new car: Every dealer visited may use information extracted from the driver's license (for a road test) to obtain a credit report, to determine if the prospect is worth pursuing. Similar effects may occur when shopping around for a bank loan. Bottom Line/Personal, where this was reported, suggests not providing sellers the information they need to make a credit check unless you're serious about buying.

---

## ✂ The story of O

Jerry Leichter <leichter@lrw.com>

Thu, 29 Aug 91 09:00:58 EDT

A recent RISKS mentions the problems of one Stephan O in getting computers to accept his single-letter last name.

This is an OLD problem. "Ng" is a moderately common Chinese name (well, to be more accurate, it's a moderately common rendering of an underlying Chinese name probably more often written as Eng or Ing, and undoubtedly pronounced using a phoneme not present in English). I recall at least one report, probably in Datamation, many years ago - probably early '70's - of the trials and travails of a programmer whose last name was Ng. It seems the payroll computer just would not accept that as a valid name. As I recall, his paychecks were eventually made out to one Damn U Acceptit.

The underlying issue here - and one we haven't gotten any better in dealing with in 20 or more years of trying - is that of "unreasonable" data. A common complaint is that computers accept everything literally; with no knowledge of real-world reasonableness, they are perfectly happy to accept that a homeowner use a million kilowatt-hours in a month (because of a small error in transcription), or what have you. The usual prescription is "Check for reasonableness".

Unfortunately, the world is sometimes "unreasonable"! The "robust" software that avoids accepting random junk produced by line noise for names has problems with Ng and O. The range-checking software that discards "impossible" values suppresses all data about the ozone hole over the Antarctic.

As Mr. O's story illustrates, it's not just computers that run into this problem. A "dumb" program, with no recourse to "common sense", would accept the name with no problems. A "smarter" program, embodying the programmer's model of what names look like, rejects it just as Mr. O's teachers did. The only difference is that, with the teachers, he could convince them that O it

was. The program has no escape hatch.

However, people sometimes have no escape hatch either. Everyone has had to deal with bureaucrats who just would not bend "procedure", even when it was clear that "procedure" just was not working. Everyone has also run into at least one pig-headed individual, operating entirely without the excuse of organizational inertia, who would not bend from his belief in some particular way of doing things, evidence to the contrary notwithstanding.

Probably the most significant effects of this phenomenon are in the many examples of intelligence organizations which ignore what in retrospect are "clear warnings" of problems because the evidence is "unreasonable" in terms of their theory of the world. Or consider the Challenger disaster, and the effects of deliberate blindness to evidence.

-- Jerry

---

## ✂ The Story of O

*Stuart I Feldman <sif@lachesis.bellcore.com>*

*Wed, 28 Aug 91 15:04:47 -0400*

If I remember an NPR item on the problems of Stephen O, he has particular difficulties because programs that launder names to fix up entry errors assume that a single O is part of an Irish name (as in PGN's O'O). An example of the risks either of ethnocentric (Eurocentric?) computer programming or of excessive cleverness.

stu feldman

---

## ✂ A number is no name

*"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>*

*Wed, 28 Aug 91 16:44:19 PDT*

In addition to the story about the computer-related inconvenience of a person having the name "O", it is worth mentioning a California judge's ruling (Marin county, 1984) refusing to permit the name "3", or even its romanized form "III". The person in question had been called "3" since his childhood, being the third child, but the judge ruled that a number cannot be a legal name. Only the spelling "Three" was permissible. Social security fought the name change, arguing that the case presented an exception that would cost them too much to program for.

[Having just seen on PBS a rerun of the old Victor Borge equivalent of the young people's guide to pronunciation, one would assume that if they permit "O" and "3" that someone might try for "!" (Jack Splat?) or "#" (they make calculators!) or "&" (Georges Amper Sand?) or even "~" (ma hatma tilde?). An opportunity to circumflex your imagination! PGN]

---

## ✂ The need for utilities to deal with non-standard situations

Tom Lincoln <lincoln%iris@rand.org>

Thu, 29 Aug 91 17:41:45 PDT

Koenig in [RISKS-12.18](#) states: It's practically impossible to keep two separate databases in step for any length of time. That's true even when one of the 'databases' is reality itself.

It is **particularly** true when reality is to match some formal data structure because reality is full of all sorts of non-standard situations.

The story of (Stephen) O the following day illustrates how pervasive the problem is. See Spafford's contribution to [RISKS-12.19](#), where numerous systems could not accept a letter as a last name. What if he had to be admitted to a hospital with an automated registration and admission system?

The real problem does not lie in the particular cases... those already submitted to the RISKS FORUM are too numerous to count... but rather with the general lack of utilities and procedures to manage non-standard situations wherever they arise in on line computing. The data model will never be completely correct, and the real world is a moving target.

Very commonly, the person at the terminal can see the absurdity, but has no override to do something about it.

Take the case of a nearby hardware store: They have tried to order some power tools from Black & Decker. However, the order has been rejected because there is a non-zero balance of over 60 days. In this case, however, it is not a debit, but a \$8.49 credit! B&D does not send out checks to adjust a credit balance, but rather applies the credit to the next order... But in this case... And there is no override...

Of course this is a bug. The test should be for a balance less than zero. There should be an exception sequence managed on paper by a supervisor.... but there isn't. Clearly, exceptions have not been anticipated. But there are always exceptions. These must be resolved by the direct user (often a clerk) where the transactions are made. At the very least the user must be able to put non-standard material in an exception que to be resolved by higher authority.

Take the case of a physician submitting a missing (?lost) prescription for Medicare patient reimbursement. The instructions are to back date it to the original date. However, the physician, wishing to be accurate, puts down both the original date and the date that the prescription was rewritten, noting that this is a resubmission for a lost document. It is rejected. There is no way to submit a non-standard document.... The only way is to pretend that it is an original. Clearly, the problem is with procedures first, and only subsequently with the computer implementation.

Managing non-standard situations needs to be an integral part of all software that must deal with unstructured aspects of the real world. The idea of managing non-standard situations should be incorporated in the operating system and in the structure of commercial data bases. When this advanced day arrives, life will be much easier, and there will be fewer funny examples in the RISKS FORUM.

TOM LINCOLN lincoln@rand.org

---

## ✂ Uncle Sam Can't Keep Track of his Trillions

<frankston!Bob\_Frankston@world.std.com>

29 Aug 1991 20:25 -0400

So goes the title of a Business Week article (September 2, 1991). I see it is a counterpoint to the Stories of O and Ng. The problem is not so much the risks of technology as the risks of underutilizing technology.

The problem is that there are just too many SMOPs to deal with. Back in the 1950's the banks were saved by computers which made it possible to deal with the huge volumes of checks they had to process. Throwing more programmers at the problems is no better than attempting to hire the entire US population as check sorters or phone operators. (Though throwing programmers at checks did work).

Getting back to the article; the government has underinvested in accounting infrastructure which is no great surprise. What is more surprising was the comment that until 1989 the Treasury couldn't report on which checks were actually presented for payment. (This is the same problem I had with Citibank ebanking which would post a check when issued instead of when presented).

The term "reengineering" is currently in vogue. Change of paradigm is another take on this.

An overriding issue is the question of how to compose large systems out of smaller ones without explicitly building large systems. We can build individual solutions to separate technical problems but how do these interact? These could be the systems within an airplane (and, simultaneously, among planes) or the data exchanges between government departments. If the solution involves project management of large scale software projects, we're doomed. [To head off responses, perhaps there are very large systems, but even they need to cooperate with other VLSs to compose Hyperlarge Systems].

Until we can do this fully, what are the modest standards to adopt so we can exchange data in the interim (i.e., this reality)? (An interesting aside are the competition between SMGL & RTF, X.500 & Domains, TCP/IP & OSI -- is a premature major standard better than a quick & dirty interim solution?) Some of this data will be smart (such as objects with methods -- a Macintosh disk with an INIT operation is a current example). Simple examples involve delivering financial and other data in machine readable form (via email). How does ISDN allow me to interact with the communications infrastructure?

Much of the change simply involves awareness. In accounting we have double-entry bookkeeping, in engineering closed-loop systems are similar concepts. Many problematic systems are open-loop and don't allow for reality checking.

One term I like to use is "federation". Back in the mid70's I reacted to distributed database by proposing federated databases as a better model which

database would be autonomous but cooperative (though not entirely trustworthy).

I'll stop here without going into the many risks we'll encounter as we learn about this systems and without going into how the individual deals with this infrastructure.



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 12: Issue 21**

**Saturday 31 August 1991**

## Contents

- [`Risk perception'](#)  
[Phil Agre](#)
- [Flaming makes the mainstream media \(again\)](#)  
[Charles Forsythe via Gene Spafford](#)
- [Phone Fraud Story a Fraud?](#)  
[Michael Barnett](#)
- [Re: Phone Fraud -- Langley VA](#)  
[anonymous](#)
- [+&\\*#&](#)  
[Bob Frankston](#)
- [Banks, Credit Cards, and Short Names](#)  
[Bill Biesty](#)
- [YASSNS \(Yet Another Social Security Number Story\)](#)  
[S. Peter Loshin](#)
- [Re: Programs Pester Public Policy People](#)  
[Jeffrey Sorensen](#)
- [Police tickets & computers in the Netherlands](#)  
[Ralph Moonen](#)
- [Re: Cracker charged in Australia](#)  
[Gene Spafford](#)
- [Senseless Actions Invite Trouble](#)  
[Charlie Lear](#)
- [A Danger Associated with Intelligent Terminals](#)  
[Douglas Thomson](#)
- [Re: Unwarranted equivalence assumptions](#)  
[Andrew Koenig](#)
- [Old School Reports of the Famous](#)  
[Kernel Mustered via Spaf and Keith Bostic](#)
- [Info on RISKS \(comp.risks\)](#)

---

**`Risk perception'**

*Phil Agre* <[pagre@weber.ucsd.edu](mailto:pagre@weber.ucsd.edu)>

*Wed, 28 Aug 91 18:25:46 pdt*

I reread the LA Times article that Rodney Hoffman helpfully summarized the other day, and suddenly I understood something about the peculiar logic behind the rhetoric of 'risk'. This article described a series of 'findings' to the effect that people are basically irrational about technological risks and other bureaucratic phenomena (in this case, the medical profession). I tend to be suspicious about any theory that treats ordinary people as irrational, and indeed a close reading of this article reveals both better explanations of the data and internal incoherencies in the framework within which these data were reported. The 'findings' summarized by RH, or most of them, are easily explained if we hypothesize that most people disbelieve the claims that are made to them about the risks and benefits of new technologies etc (perhaps because they believe the organizations making such claims to be driven by profit and prestige and getting promoted rather than by genuine concerns for public health and safety), and furthermore that people only believe in risks and benefits they've had the opportunity to evaluate for themselves. This particular article was unusual in that this explanation was given a few lines, though it was quickly dropped and the analysis continued as before.

The point is important because it helps diagnose some of the hidden agenda inside the notion of 'risk'. To talk about 'levels of risk' and the like erases the distinction between the experts' assessments of risk and the assessments that ordinary people are in a position to make. If ordinary people make different assessments from the experts, then that calls for some quasi-biological investigation of 'risk perception'. These investigations will discover all manner of irrationality and ignorance, which will then motivate calls for greater efforts to convince people to leave things in the hands of the experts. The irrationality ascribed to ordinary people helps to draw attention from the open contradictions in the research: the conclusion that ordinary people are unwilling to accept any risk at all is juxtaposed comfortably with the observation that the same people regularly assume large risks out on the highway.

The thing is, though, that the experts have a pretty crude understanding of risk. The LA Times article and many others of its genre are obsessed with death statistics. Levels of risk are routinely equated with the number of people who die each year from a given cause. Thus the obsessive interest in popular assessments of the relative magnitudes of these numbers. It may well be that people falsely believe that many more people die in fires than from drowning, for example, but the question is only interesting once one accepts several premises. Thus as well the obsessive interest in people's skills with word problems from probability theory, which are only germane if you believe (which most people apparently do not) that it's a responsible procedure to assume (as risk theorists so often do, if only because it makes the math simpler) that probabilities are independent unless evidence to the contrary cannot be ignored. Somehow the whole framework associated with the concept of 'risk' derails any attempt to critically investigate these premises.

In my opinion this is not an accident. The whole rhetoric of 'risk' started out as corporate PR. You probably remember the old oil-company ads (from Mobil, right?) decrying those people who supposedly called for a 'risk-free society'. These ads were the laughing-stock of the country, and rightly so. How times have changed. Oil companies no longer have to buy quarter page ads

on the NY Times op-ed page to get such stuff into print. The same ideology, made into a profession, now shows up as `research' in articles in the LA Times. Now we have sophisticated, scientific-sounding ways to ignore the reasonable insistences of normal people -- on being told the truth, on being able to find the world intelligible and sane, being consulted about things that change their lives, on not being subjected to hazards without their consent, and generally on being able to participate in collective decisions about issues of technology and social change -- and remaking them as an irrational aversion to `risk'.

This is why it's so ironic that many of the same people who use the discourse of `risk' also complain about expressions such as ``risks to the public in computers and related systems" which, we are told, encourage a one-sided focus on risks without the balancing context of benefits. Here, surely, is another instance of the irrational aversion to risk. Such complaints are both right and wrong. Technology has certainly been associated with both good and bad in the world, and often at the same time. But it's important not to take `technology' (or `computers' or `credit databases') as package deals. Computer technology is malleable; it can be reshaped endlessly as important social goals are added to its requirements. The problem with the vocabulary of `risks and benefits', as with the vocabulary of `risk', is that it presupposes the unilateral nature of technology, handed down from on high, take it or leave it. But it doesn't have to be that way. Socially responsible technology is technology that is developed *\*with\** people, not just *`for'* them. Can the current social organization of technology even conceive of such a process?

Phil Agre, UCSD

---

### **🔥 Flaming makes the mainstream media (again, I guess)**

*Gene Spafford <spaf@cs.purdue.edu>*

*Thu, 29 Aug 91 07:50:40 EST*

Any RISker's read this book? It sounds like worthwhile reading....

----- Forwarded Message

Date: Tue, 27 Aug 91 21:11:00 -0600

From: forsythe@track29.Ionestar.org (Charles Forsythe)

Subject: Flaming makes the mainstream media (again, I guess)

FLAME THROWERS: Why the heated bursts on your computer network? by Doug Stewart (copied without permission from Omni magazine Sept 1991 issue)

"You are a thin-skinned reactionary jerk," begins the computer message sent from one highly educated professional to another. "I will tell you this, buster, if you were close enough and you called me that, you'd be picking up your teeth in a heartbeat." There follows an obscene three-word suggestion in screaming capital letters.

The writer of the above message, sent over the Byte Information Exchange, was

apparently enraged after a sarcasm he'd sent earlier was misinterpreted as racist. In the argot of computers, his response was a "flame" -- a rabid, abusive, or otherwise overexuberant outburst sent via computer. In networking's early days, its advocates promised a wonderful world of pure mind-to-mind, speed-of-light, electronic conversation. What networks today often find instead are brusque putdowns, off-color puns and screenfuls of anonymous gripes. The computer seems to be acting as a collective Rorschach test. In the privacy of their cubicles, office workers are firing off spontaneous salvos of overheated prose.

Sara Keisler, a social psychologist at Carnegie Mellon University and Lee Sproull, a Boston University sociologist, have observed that networking can make otherwise reasonable people act brash. In studies originally designed to judge the efficiency of computerized decision-making, they gave small groups of students a deadline to solve a problem. Groups either talked together in a room or communicated via isolated computer terminals. The face-to-face groups reported no undue friction. The computerized sessions frequently broke down into bickering and name-calling. In one case, invective escalated into physical threats. "We had to stop the experiment and escort the students out of the building separately," Keisler recalls. Keisler and Sproull documented a tendency toward flaming on corporate electronic-mail systems as well. At one large company, employees cited an average of 33 flames a month over the email system; comparable outbursts in face-to-face meetings occurred about four times a month.

Keisler and Sproull attribute the phenomenon largely to the absence of cues normally guiding a conversation -- a listener's nod or raised eyebrows. "With a computer," Keisler says, "there's nothing to remind you there are real humans on the other end of the wire." Messages become overemphatic -- all caps to signify a shout; "(smile)" or ":-)", a sideways happy-face, to mean "I'm kidding." Anonymity makes flaming worse, she says, by creating the equivalent of "a tribe of masked and robed individuals."

In real life, what we say is tempered by when and where we say it. A remark where lights are low and colleagues tipsy might not be phrased the same under fluorescent lights on Monday morning. But computerized messages may be read days later by hundreds or thousands of readers. Flaming's ornery side is only half the picture, says Sproull, who co-authored *Connections: New Ways of Working in the Networked Organization* with Keisler. "People on networks feel freer to express more enthusiasm and positive excitement as well as socially undesirable behavior," she says. Sproull finds it ironic that computers are viewed as symbols of cool, impersonal efficiency. "What is fascinating is the extent to which they elicit deeply emotional behaviors. We're not talking about zeroes and ones. People reveal their innermost souls or type obscenities about the the boss." What, she asks, could be more human?

---

### **🔥 Phone Fraud Story a Fraud? (Re: Phone Fraud, [RISKS-12.19](#))**

*Michael Barnett <mbarnett@cs.utexas.edu>*

*Sat, 31 Aug 1991 09:46:29 -0500*

Missing from the quotes about the problems WRL has experienced is the

following:

Even more suprising to experts, they [the thieves] had managed to log 129,315 minutes of talking time over one line -- a seemingly impossible feat, because it equaled an average of roughly three calls going out simultaneously every minute of the day

Later in the article a spokesman for Bell Atlantic is quoted as saying, "There simply cannot be a single outgoing line that routes multiple calls at once". Perhaps the problems were not caused by malicious persons at all, but problems in the billing system. How much easier to blame "low-income immigrants" and "drug dealers"! (Anonymous "authorities" claim these are the culprits.) What ever happened to the reports that hackers were responsible for the breakdowns of the AT&T switches? That made headlines until the true causes were discovered.

The real story, I think, which was buried in the article:

In the past, long-distance carriers bore most of the cost [of phone theft], since the thefts were attributed to weaknesses in their networks. But now, the phone companies are arguing that the companies are arguing that the customers should be liable for the cost of the calls, because they failed to take proper security precautions on their equipment.

Michael Barnett (mbarnett@cs.utexas.edu)

---

✉ **Re: Phone Fraud -- Langley VA ([RISKS-12.19](#))**

<[anonymous]>

Thu, 29 Aug 91 12:01:35 XXT

- > The New York City Human Resources Administration lost \$529,000 in 1987. And
- > the Secret Service, which investigates such telephone crime, says it is now
- > receiving three to four formal complaints every week, and is adding more
- > telephone specialists.

Ironically enough, one of the PBX's that was breached was located in Langley, Virginia. This went unnoticed for more than a year (!!). Yes, your very own CIA wuz cracked. I have no information about the amount of fraudulent calls that were made, but I am led to believe that it was a substantial amount.

---

✉ **+&\*#&**

<frankston!Bob\_Frankston@world.std.com>

31 Aug 1991 10:17 -0400

No, I'm not cursing. Just showing a possible New Hampshire license plate. The problem is even worse since other nonASCII graphics such as a bell have been spotted. I'm curious about how various computer systems deal NH plates.

---

**✂ Banks, Credit Cards, and Short Names (Re: [RISKS-12.19](#))**

<biesty@ide.com>

Fri, 30 Aug 91 09:19:25 PDT

Benefits of having a short name?

A friend of mine who works at one of the larger Credit Card issuing Banks, once told me that people whose last names were shorter than \*three\* letters would never get pre-approved credit card letters from them. It seems the program that went through the purchased list of names, addresses and consumer info considered names of less than three letters to be corrupt data.

Before you think that this is a good thing since you'll be getting less junk mail, pre-approved credit mailings often offer you a better interest rate or a deal on the annual fee that you would not get if you applied on a generic application.

Bill Biesty <biesty@ide.com>

---

**✂ YASSNS (Yet Another Social Security Number Story)**

"S. Peter Loshin" <peter@draper.com>

Fri, 30 Aug 1991 17:37:00 EDT

Having recently purchased a used Plymouth, I decided to take over the remainder of the 7 year/70k mile power train warranty. One of the items of information requested was my Social Security number. When asked why that was necessary, the credit manager said "Because it's on the form. If you don't give it to us, we can't transfer the warranty."

I did not give them my SSN. The business manager said that while he had NEVER processed a form without SSN, he didn't know if it really was required. He did say a form was once rejected because it was an out-of-state applicant who did not provide the full 9-digit ZIP code!

He also said he'd call if there were any problems...

Peter Loshin peter@draper.com (617) 258-2480

---

**✂ Re: Programs Pester Public Policy People**

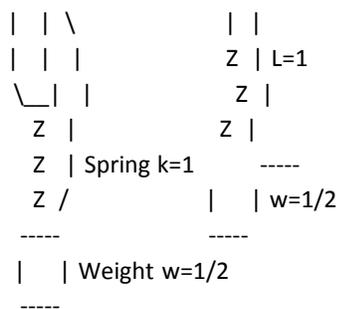
Jeffrey Sorensen <sorensen@spl.ecse.rpi.edu>

Wed, 28 Aug 91 16:22:13 EDT

The Strings and Springs puzzle brought to you in hi-res laughics:

---

Z	Z
Z Spring k=1	Z k=1
Z__	Z



Before                      After

Two springs with  $k=1$  are tied together with a piece of string  $L=3/8$  and the bottom spring is hook to a weight of mass  $1/2$ . Now, two long strings with  $L=1$  are tied from the roof to the bottom spring and from the bottom of the top spring to the weight. These are hanging loose and look like "safety" strings. When the little string in the middle is cut, the weight actually goes up!!!!!!

My calculations:

$F = 1/2 = kx = (1) \cdot 1/2$  So the left weight is  $1/2 + 1/2 + 3/8$  from ceiling

Second case  $F = 1/2 = (kx + kx) = 2kx = 2(1)x$  So the weight is  $1 + 1/4$  from the ceiling.

A circuit can be designed using resistors for springs and Zener diodes for strings according to Science News.

This diagram was adapted from the diagram Science News adapted from Nature

Jeff Sorensen [sorensen@ecse.rpi.edu](mailto:sorensen@ecse.rpi.edu)

## ✂ Police tickets & computers in the Netherlands

*<hvlpa!rmoonen@att.att.com>*

*Thu, 29 Aug 91 12:42 MDT*

>From various newspaper articles in the past couple of weeks in the Netherlands:

The Dutch police is facing serious problems with the paperwork involved with the enormous amounts of tickets for traffic violations. Currently, 4 million tickets per year are being given. However, the police can only handle 2.5 million per year. Last year, simplifications where made to the paperwork, and computers where installed to help the police officers, but it only led to an increase of 500.000 tickets per year, still leaving a gap of an astonishing 1.5 million tickets. Chances are, if you get a speeding ticket or parking ticket, you'll never hear anything from it.

To enable the police to catch up, three methods are being proposed: One, in which ALL unprocessed tickets will be deleted, giving the police the chance of starting with a clean slate, another being: install more computers to do the work, and the third and best: Disallow police officers to give more than a

certain amount of tickets per day.

"I am sorry sir, I can not give you a ticket for this violation. I have reached my quota for today."

And all this, because the installed computers didn't work easily enough to increase the amount of processed tickets with more than 500.000....

--Ralph Moonen

---

### **✂ Re: Cracker charged in Australia ([RISKS-12.18](#))**

*Gene Spafford <spaf@cs.purdue.edu>*

*29 Aug 91 15:19:01 GMT*

In [RISKS-12.18](#), Richard O'Keefe comments on the article in [RISKS-12.13](#) about the Australian indictment of Nashon Evan-Chaim.

I believe Nashon is one of 3 people who had equipment and computer media searched last year under warrant (April or May, as I remember). Nashon allegedly was an active associate of "Phoenix" (or was himself Phoenix) -- the Australian who broke into Cliff Stoll's machine and mine, who then called John Markoff at the NY Times to brag about breaking into our systems (February or early March). In both cases, damage was done to our systems; Cliff claimed his system was thoroughly trashed during the incident, as I remember.

The same gang of crackers are alleged to have broken into systems at a major telecommunications firm (I won't use their name) and caused damage, and I know they raised havoc with machines at LLNL and UT Austin, as well. Breakins occurred many other places, too. System files were altered to insert backdoors for later access, and log files were altered and destroyed to hide the evidence. We saw it happen, as did people at those other sites -- it was not just simple exploration. The breakins were purposeful, and continued over several months despite warnings and attempts to stop them. I'm aware of some of the evidence collected in the case by the Australian Federal Police -- including transcript of hacking sessions -- and it shows that more than "innocent exploration" was involved.

I'm not claiming that Nashon was the principal in this, or was involved in all the activity; the Australian courts will decide the legal aspects of that question. However, if he *\*was\** involved with these activities, he was certainly doing more than harmless exploration (if, indeed, any unauthorized exploration is "harmless"). Some of the damage may have been accidental or incidental, but there was damage nonetheless, and it caused considerable work for our staff here to clean up afterwards, as it did at the other sites involved.

People (in general -- I'm not singling out Mr. O'Keefe) should realize that individuals committing computer crimes don't all look the part....assuming there is any typical "look" to them. Pick almost any kind of "white-collar" crime you wish to name. Then interview victims, friends, and teachers of the accused, and many of them will say "I never would have expected it of him (or

her)! He was such a bright, friendly person from a good family....." (It doesn't even have to be white-collar crime: Ted Bundy comes to mind as an example).

To bring this back around more squarely into RISKS: Bright students are just as capable of stepping outside the bounds of propriety as are dumb students -- maybe even more so, as they often know how to get around the barriers that have been placed to prevent accidental access. Just as we shouldn't always believe what the computer tells us, we should likewise not always believe what our intuition tells us.

Furthermore, those of us who are teachers and role models need to be sure we are teaching all our students (especially the bright ones) where the boundaries of proper usage lie; teaching how computers work is not a substitute for raising questions about how they are to be used. I wonder if this was a topic Mr. O'Keefe and his colleagues every raised in Nashon's classes?

Gene Spafford, NSF/Purdue/U of Florida Softw. Eng. Res. Center, Dept. of Computer Sciences, Purdue University, W. Lafayette IN 47907-1398 (317) 494-7825

---

### **✶ Senseless Actions Invite Trouble**

*<clear@cavebbs.gen.nz>  
30 Aug 91 01:42:00 NZT (Fri)*

The National Library of New Zealand runs an online database service known as Kiwinet. BRS-Search is used to look up a number of databases concerning legal, political and regulatory matters. There are several hundred users and a number of dialup modems.

Users dial into Kiwinet and are charged an average of around \$200/hr for database access. Obviously security is of a major concern to users. Imagine my surprise when the following appeared in with this month's Kiwinet newsletter:

-----begin text-----

ALERT! For smooth transition to Kiwinet's new system on 2 September, please ensure that all Kiwinet users in your organisation read this!!!

The first time you log on to Kiwinet after 2 September, you can NOT use your usual Kiwinet password. Log on with your Kiwinet UserID as usual, then, when prompted to enter your password, type in the default password for all users, which is:

SPRING

It is vital that you change this default password as soon as you have logged on, in order to help prevent unauthorised use of your UserID. Any Kiwinet usage made on your UserID will be charged to you.

-----end text-----

Can you say, "Hackers Paradise"? Reading the above makes me wonder just how some so-called professional system administrators actually get jobs. I know damn well that if Kiwinet tried to bill me for any logins I hadn't made, I would be investigating taking civil action against them for negligence and for unauthorised tampering with my user account.

Charlie Lear, clear@cavebbs.gen.nz

[Charlie's message was also sent to me by Tim Larson, tim@gistdev.gist.com  
Global Information Systems Technology Inc. PGN]

---

## **A Danger Associated with Intelligent Terminals**

*Douglas Thomson <doug@giaea.oz.au>*

*Fri, 30 Aug 91 13:39:25 EST*

Our UNIX system has a console that is left permanently logged in as root. This is convenient for the operators, since they can do things like removing print jobs from queues without having to keep logging in and out. I have more than once queried the advisability of leaving root logged in, but the response has always been that as the console is in the same locked room as the computer itself, it poses no (increased) security risk.

I was never quite satisfied with this answer, and just recently I decided to explore the question a little further. I found there was indeed a major security hole, and one that did not involve any physical access to the computer room.

As I have said, the console is always logged in as root. In addition, the console is writable by everyone, so that anyone can send a message to the operator. So far so good. This works well, and is convenient for everyone. However, the console is an "intelligent" terminal (and perhaps, under the circumstances, I had better not specify which type!). There are several of these terminals around here, and the terminal's user manual may be borrowed from the computer centre. I borrowed one, and checked up on what I could do.

Firstly, it turned out that I could remotely program certain function keys, so that the next time someone pressed the key it would execute my command as root. However, the operator would at least see this happening, so this security hole would be fixed pretty quickly.

However, there was better to come. Naturally it was possible to send cursor addressing escape sequences, and hence to display anything I wanted on any region of the screen. What really caught my attention was that it was possible to instruct the terminal to transmit the contents of a field on the screen back to the computer! So I could define a field at some part of the screen, program the field terminator to be a carriage return, write whatever command I wanted executed to the region of the screen containing the field, and then ask the terminal to transmit the field - thereby executing as superuser any command I chose!

I also looked through the manual to see if there was any way to disable such "intelligent" behavior, but I could not find one.

The moral is obvious: don't allow write access to an intelligent terminal! Any user who can write to such a terminal can do anything they could do by typing at the keyboard!

Doug. (doug@giaea.oz.au) ...!munari!goanna!giaea!doug

---

**✂ Re: Unwarranted equivalence assumptions (Cooper, [RISKS-12.19](#))**

<ark@research.att.com>

Thu, 29 Aug 91 09:31:51 EDT

Brinton Cooper asks [relating to Andrew's four cases in [RISKS-12.18](#)]:

Suppose the denial had been by computer:

"Incorrect password: Login aborted."

Would he argue that this might have been the \*genuine\* user who had forgot her password and that the "system" should have known better because the login was from site known to her office?

No, of course I wouldn't argue that way. Although present-day assumptions have many kinds of bad side effects that result from making incorrect decisions, that doesn't mean they should be replaced willy-nilly with other assumptions that have other, equally bad side effects!

However, the purpose of an authentication system is not simply to keep unauthorized people out -- that could be guaranteed by simply keeping everyone out! For an authentication system to be of any use it must simultaneously let the good guys in and keep the bad guys out.

What I'm trying to point out is that people tend to treat such systems as infallible, which sometimes causes anomalies. The fact that such anomalies are sometimes considered evidence that the system is working as designed doesn't make them any less anomalous.

--Andrew Koenig ark@europa.att.com

---

**✂ Old School Reports of the Famous**

Keith Bostic <bostic@okeeffe.CS.Berkeley.EDU>

Sat, 24 Aug 91 16:27:36 -0700

From: mathew@mantis.co.uk (Kernel Mustered)

Old School Reports of the Famous, #1: Richard Stallman.

"He is an excellent pupil. Our only complaint is that he encourages all the other pupils to copy his work."



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 12: Issue 22

Tuesday 3 September 1991

## Contents

- [Madison mail mess-up](#)  
[Tom Slone](#)
- [RISKS of using electronic mail, and universal addressing](#)  
[David Parnas](#)
- [Re: +&\\*#S](#)  
[Tom Blinn](#)
- [Re: Study Recommends Earthquake Warning Network](#)  
[Floyd Ferguson](#)
- [Re: Risks of Risk Perception Research](#)  
[William P Gardner](#)  
[Craig Seidel](#)
- [Symposium on Reliable Distributed Systems, Advance program](#)  
[Lorenzo Strigini](#)
- [DIAC-92 CALL FOR PAPERS AND PARTICIPATION](#)  
[Douglas Schuler](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Madison mail mess-up**

*Tom Slone <potency@violet.berkeley.edu>  
Mon, 2 Sep 91 17:12:04 PDT*

Madison, Nebraska is reportedly in the midst of automating its mail system, but the automation has reportedly force people to change their addresses repeatedly. The conversion will reportedly be finished by 1995! Meanwhile residents are not use if they're getting all their mail. Residents of the town of Madison are forced to have their mail delivered to boxes rather than their homes, but some rural routes have street addresses. One resident, Mary Duby, has three addresses listed in the phone book due to the apparently due to the postal automation: two boxes and a street address. Duby said, "What a mess. Originally I had a street address. Then I had a mailbox put up and I was put on the rural route." [Source: an AP story reported in the San Jose Mercury News 2Sep91]

---

## ✉ RISKS of using electronic mail

David Parnas <parnas@qusunt.Eng.McMaster.CA>

Tue, 3 Sep 1991 14:24:54 -0400

Many of us have become dependent on electronic mail as vehicle for serious discussions. Our addresses become widely distributed and stored in many colleague's mail files. This is a serious exposure to risk. If one moves one may find that one's former employer feels insulted by the announcement that one has moved on to other pastures and refuses to forward electronic mail. The incorrect mail address may persist in electronic files for many years and those who write to you may find that you are an "unknown user". What is needed is a personal communication system, one where the individual's address is independent of his (or her) location on the computer network.

David Lorge Parnas (no longer at qucis.queensu.ca)

---

## ✉ Re: RISKS of using electronic mail, and universal addressing

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

Tue, 3 Sep 91 11:30:10 PDT

There have been various proposals for life-time unique IDs -- for EMail, for telephone numbers, and even for Postal Delivery, that would transcend geographical locations and relocations, etc. All sorts of interesting problems are raised regarding decentralized implementations and whom you have to trust with what, what happens if one of the decentralized sites is down and whether the implementations are sufficiently fault tolerant to survive multiple outages, what to do about authorizations and junk mail, revocation, etc. But it certainly would be nice. This reminds me of some of the problems experienced long ago in designing capability based systems where capabilities have identifiers that are unique for the lifetime of the system. So, there is actually significant experience in dealing with David's suggestion, in a broader context -- but not yet in the Internet, that wonderful sandbox of the past that is still the sandbox of the future.

---

## ✉ RE: +&\*#\$(RISKS-12.21)

"Dr. Tom @MKO, CMG S/W Mktg, DTN 264-4865 03-Sep-1991 1419" <blinn@dr.enet.dec.com>

Tue, 3 Sep 91 11:19:42 PDT

In RISKS-FORUM Digest (Saturday 31 August 1991 Volume 12 : Issue 21), you asked about "+&\*#\$( as a possible New Hampshire license plate.

While it's true that "+" (plus) and "&" (ampersand) are valid characters on a New Hampshire license plate, as is "-" (dash or minus), I'm pretty sure that the other characters you surmise (\*, #, and \$) are NOT permitted. I'd have to ask the DMV to be sure, however, which I can do if it's important.

I'm amused by your reference to "other nonASCII graphics" -- while it's true

that some other states use bizarre characters on license plates (such as the Lone Star on the Texas plates, or the lobster on Maine plates), usually this is not "user selectable".

New York State allows an embedded space character in license plates. This is as big a problem, I'm sure, for some other states as New Hampshire's use of the printing but unusual characters that are accepted here. [Live Free Or Die!]

Dr. Thomas P. Blinn, Digital Equipment Corporation, Digital Drive -- MKO2-2/F10  
Merrimack, New Hampshire 03054 ...!decwrl!dr.enet.dec.com!blinn (603) 884-4865

---

**✂ Re: Study Recommends Earthquake Warning Network (Pereira, [RISKS-12.18](#))**

*Floyd Ferguson <iphase!coromir!floyd@uunet.UU.NET>  
Sat, 31 Aug 91 13:27:32 CDT*

``More seriously, this poses all sorts of interesting RISKS issues."

In a previous life I had occasion to work with someone who had worked on such a project in California. The system apparently went quite far through the development life-cycle, but then, at the very end was dumped without being deployed.

Such a system could be used to lower fire risks by shutting down natural gas and power distribution networks, to protect computer systems by retracting disk heads, to start a controlled shut down of factory processes, to divert aircraft, etc.

What happened instead was that many of those people responsible for performing these vital functions took advantage of the early warning to leave work to be with and protect their families. Thus, the system ended at "proof of concept", due to the significant risks associated with loss of key personnel at exactly the worst possible time.

Incidentally, the system apparently did use a network of sensors, but took advantage of the fact that the shock wave moves relatively slowly (45 - 60 mph comes to mind, but it has been a few years).

Floyd Ferguson floyd@iphase.com

---

**✂ Risks of Risk Perception Research (Agre, [RISKS-12.21](#))**

*"William P Gardner" <wpg1@unix.cis.pitt.edu>  
Tue, 3 Sep 91 9:46:06 EDT*

Phil Agre (pagre@weber.ucsd.edu) provides some welcome warnings about misinterpretations of risk perception research. I share his concern that findings that lay people evaluate risks differently than experts are often viewed as evidence that "ordinary people are irrational." There are usually several explanations for the discrepancy between lay and expert judgments and the data are rarely conclusive as to which explanation is best. Premature attributions of irrationality are a significant risk in risk perception

research because, as Agre suggests, attributing irrational judgment to ordinary people can make them seem responsible for the morbidity and mortality they suffer.

This said, Agre's diagnosis of a "hidden agenda inside the notion of 'risk'" was inaccurate. Agre says that "The whole rhetoric of 'risk' started out as corporate PR" specifically the well-known advertisements by Mobil Oil. The concept of risk in the sense used in risk perception studies dates (at least) from the beginnings of epidemiology and from the integration of probability into the theory of insurance in the 18th century. Psychological research on risk perception and probability judgments was well established when Mobil ran its ads. Agre believes that it is a conclusion of risk perception research that "ordinary people are unwilling to accept any risk at all." I have never seen a statement like this in the risk perception literature and I wonder if Agre can find one. Agre says that "talk about 'levels of risk' and the like erases the distinction between the experts' assessments of risk and the assessments that ordinary people are in a position to make." The point of this field is to understand how one aspect of our positions in the world -- our cognitive limitations and our limited access to information -- force us to construct simplified models of the world. All of us need to make decisions without the benefit of professional knowledge: how do we cope? Risk assessment research begins with a distinction between the cognitive position of the expert and lay person, it doesn't erase it. By the way, it isn't just ordinary people who construct simplified models: there are many studies showing that experts also have great difficulty in judging probabilities and coping with uncertainty.

Agre describes risk perception research as "ideology, made into a profession." I hope he sees that there are also significant empirical phenomena that need explanations, and quickly if possible. For example, it appears that adolescent gay males have not adopted the safe sex norms accepted by older gay male cohorts. If so, why not? Health psychologists working with these young men think that these kids believe (inaccurately!) that HIV infection risks apply only to older gay men. This is readily understandable: the long incubation period of HIV infection means that an adolescent will rarely encounter a peer with AIDS, and therefore does not perceive himself to be at risk. This explanation is an example of the availability heuristic, the idea that probability judgments are affected by our ability to recall vivid exemplars of the risk in question. Is this really why these kids engage in risk taking? I don't know: it is hard to design a study that can powerfully discriminate among many competing plausible explanations. Agre says that the findings of discrepancies between expert and lay judgments are "easily explained". But if he wants us to believe his explanations, as opposed to the others on offer, he will need some data that show why they are better.

Agre oversimplifies when he reduces the political implication of risk perception research to "corporate PR". Many risk perception researchers share his desire for a "socially responsible" technology in which people are "told the truth, ...able to find the world intelligible and sane, [are] consulted about things that change their lives, [are not] subjected to hazards without their consent, and generally [are] able to participate in collective decisions about issues of technology and social change". All of these goals will require that technical information be communicated to people who are not specialists in the relevant technologies. If risk perception research can

clarify how non-specialists understand risk information, we may get an idea about how to communicate the information more clearly.

William Gardner, Law & Psychiatry Research, Department of Psychiatry,  
University of Pittsburgh School of Medicine (wpg1@unix.cis.pitt.edu)

---

✉ **Re: Risks perception ([RISKS-12.21](#))**

<seidel@puma.sri.com>

Tue, 03 Sep 91 10:17:43 -0700

Phil Agre's posting reminded me of a table in "The Mission Profile," in *IEEE Spectrum*, October, 1981. It describes "consumer" expectations for various systems. I summarize (the original table had more words and a column for availability):

System	Representative Failure Rates	Useful Life of System
Automatic Teller Teller	1 per 18mo.	>15 years
Telephone	3 min/yr	>15 years
Chemical Plant	Less than 3%	>15 years
Electric Power sys.	12 min/mo. during excessive demand or storms	>15 years
Television Set	3-10% during warranty period. May continue with degraded perf.	7-10 years (based on use)
Auto: engine control	1% during warranty	life of car
Air Traffic Control	2.9 unsched. interrupts per month lasting >1 min.	>15 years
Minuteman III missile	1 per 1.9 billion part hours in system with 8000 critical parts	up to time missile is capable of striking a prescribed target
Pacemaker	1 per month among 170,000 devices [I'm tempted to say "lifetime" but that would probably be crude--CHS]	8-15 years depending on type of pacemaker
Operating System	1/hr to 1/mo	runtime of program

I think these figures, although subjective and somewhat dated, illustrate the range of acceptance of failure for various systems. They are not necessarily

rational or related to any more objective ratings, such as the number of deaths caused per year by each system (a figure hard to interpret for a Minuteman III). But, isn't \*acceptance\* of risk by \*definition\* a social phenomenon rather than a scientific one? Death is not the only metric.

The corporate PR firms that started advertising based on risk reduction believed that safety was marketable. Wouldn't our jobs be much easier if more people believed that risk reduction was worth paying for?

Craig Seidel, SRI International

---

## **✂ Advance program - Symposium on Reliable Distributed Systems**

*Lorenzo Strigini <STRIGINI@ICNUCEVM.CNUCE.CNR.IT>*

*Fri, 30 Aug 91 12:05:45 MET*

I am forwarding this from the Symposium chair, Luca Simoncini. [Suggestion: use E-mail or fax for correspondence, regular mail to/from Italy may be very slow. Lorenzo]

THE FOLLOWING IS THE ADVANCE PROGRAM OF SRDS10 COMPLETE WITH REGISTRATION FORM AND HOTEL RESERVATION FORM. THESE FORMS CAN BE USED FOR REGISTRATION AND RESERVATIONS IF YOU NEED WE WILL MAIL REGULAR PAPER ADVANCE PROGRAMS, WHICH ARE GOING TO BE DISTRIBUTED BY REGULAR MAIL IN A FEW DAYS TO ALL COUNTRIES.

INFORMATION AND ENQUIRIES TO: ETTORE RICCIARDI, IEI-CNR, Via S. Maria 46, 56126 Pisa, Italy. tel.: +39 50 553 454, +39 50 553 443 fax: +39 50 554 342  
E-mail: simon@icnucevm.cnuce.cnr.it

### ADVANCE PROGRAM

Tenth Symposium on Reliable Distributed Systems - SRDS10, September 30, October 1-2, 1991, Palazzo dei Congressi, Pisa, Italy

sponsored by: IEEE Computer Society, TC on Distributed Processing, AICA

in cooperation with: TC on Fault-Tolerant Computing, IFIP W.G. 10.4, IEI-CNR, Universita' di Bologna, Universita' di Pisa, with the support of: Olivetti S.p.A, Italy, TANDEM Computers S.p.A., Italy, ANSALDO TRASPORTI, Italy

SUNDAY, September 29, 1991

16.00 - 20.00 Registration

MONDAY, September 30, 1991

08.00 - 09.00 Registration

09.00 - 09.30 Opening Remarks: Luca Simoncini, University of Pisa

Ozalp Babaoglu, University of Bologna

Richard D. Schlichting, Univ. of Arizona

09.30 - 10.30 Keynote Speaker: Brian Randell,

University of Newcastle upon Tyne, UK

10.30 - 11.00 Coffee Break

11.00 - 12.30 Session 1: Checkpointing & Logging Algorithms

Chair: Shaula Yemini, IBM, Yorktown Heights, USA

"Checkpointing Multicomputer Applications"

Kai Li, Jeffrey F. Naughton, James S. Plank, Princeton University, USA

"A Timestamp-Based Checkpointing Protocol for Long-Lived Distributed Computations"

Farnam Jahanian, Flaviu Cristian, IBM, San Jose', USA

"File System Measurements and their Applications to the Design of Efficient Operation Logging Algorithms"

David F. Bacon, University of California Berkeley, USA

12.30 - 14.00 Lunch

14.00 - 15.30 Session 2: Real-Time

Chair: Hermann Kopetz, Technical University of Vienna Austria

"Masking Failures of Multidimensional Sensors"

Keith Marzullo, Paul Chew, Cornell University, USA

"A Statistical Clock Synchronization Algorithm for Anisotropic Networks"

G. Florin, D. Couvet, S. Natkin, Centre D'Etude et De Recherche En Informatique, France

"On the Testability of Distributed Real-Time Systems"

Werner Schuetz, Technical University of Vienna Austria

15.30 - 16.00 Coffee Break

16.00 - 17.30 Panel Session: "Fault-Tolerance in Distributed Systems: how transparent can you get ?"

Coordinator: Shaula Yemini, IBM, Yorktown Heights

USA

19.00 Concert

20.30 Welcome Party

TUESDAY, October 1

08.00 - 09.00 Registration

09.00 - 10.30 Session 3: Backward Recovery Schemes

Chair: Edgar Nett, GMD, Germany

"Optimistic Failure Recovery for Very Large Networks"

Andy Lowry, James R. Russell, Arthur P. Goldberg,  
IBM, Yorktown Heights, USA

"Efficient Communication of Commitment-Dependency  
Information in the PTC Scheme for Cooperative  
Recovery"

Kane Kim, J. H. You, University of California Irvine  
USA

"Flexible Schemes for Application-level Fault  
Tolerance"

Lorenzo Strigini, Felicita Di Giandomenico, IEI-CNR  
Italy

10.30 - 11.00 Coffee Break

11.00 - 12.30 Session 4: Replication & Parallelism

Chair: Fabio Panzieri, University of Bologna, Italy

"A Model for Interface Groups"

Ed Oskiewicz, Michael H. Olsen, John Warne, ANSA, UK

"Formalising Replicated Distributed Processing"

Maciej Koutny, Luigi V. Mancini, Giuseppe Pappalardo,  
University of Newcastle upon Tyne, UK

"On Tolerating Faults in Naturally Redundant  
Algorithms"

Luiz A. Laranjeira, Miroslaw Malek, Roy Jenevain,  
University of Texas Austin, USA

12.30 - 14.00 Lunch

14.00 - 15.30 Session 5: Dependability Modelling

Chair: Jean-Claude Laprie, LAAS-CNRS, France

"Evaluation of Bus and Ring Communication Topologies  
for the Delta-4 Distributed Fault Tolerant  
Architecture"

David Powell, Karama Kanoun, LAAS-CNRS, France

"Flexible Handling of Diverse Dependability  
Requirements in MARS"

Heinz Kantz, Technical University of Vienna, Austria

"Efficient Transient Simulation of Failure/Repair  
Markovian Models"

Juan A. Carrasco, Universitat Politecnica de Catalunya  
Spain

15.30 - 16.00 Coffee Break

16.00 - 18.00 Session 6: Work in Progress

Chair: Miroslaw Malek, University of Texas Austin, USA

(Submissions will be solicited on the spot,  
for short presentations;  
there will be a selection)

20.30 Banquet

WEDNESDAY, October 2

09.00 - 10.00 Session 7: Dependability Assessment

Chair: David Powell, LAAS-CNRS, France

"Performability Evaluation of CSMA/CD and CSMA/DCR  
Protocols under Transient Fault Conditions"  
William Sanders, K. H. Prodromides, University of  
Arizona, USA

"A study of the Reliability of Internet Sites"  
Darrell Long, J. L. Carroll, C. J. Park, University  
of California Santa Cruz, USA

10.00 - 10.30 Coffee Break

10.30 - 11.30 Session 8: Agreement

Chair: Paulo Verissimo, INESC, Portugal

"Ordered Broadcasts for Large Applications"  
Tony P. Ng, University of Illinois Urbana-Champaign  
USA

"Keeping Processes under Surveillance"  
Thomas Becker, University of Kaiserslautern  
Germany

11.30 - 12.30 Session 9: Garbage Collection

Chair: Paolo Ancilotti, University of Pisa, Italy

"A Fault-Tolerant, Scalable, Low-Overhead Garbage  
Detection Protocol"  
Marc Shapiro, INRIA, France

"Copying Garbage Collection for Distributed Object  
Stores"  
Luigi Mancini, Vittoria Rotella, Simonetta Venosa,  
Universita' di Pisa, Italy

12.30 - 14.00 Lunch

14.00 Symposium end.

=====

SRDS10 will be held at the Palazzo dei Congressi di Pisa.

SRDS10 is in connection with the 5th International Conference on Fault-Tolerant Computing Systems (the German FTCS), Nurnberg, 25-27 Sept. 1991 (contact Mario Dal Cin E-mail: DALCIN@INFORMATIK.UNI-ERLANGEN.DE), and with the International Workshop on Responsive Computer Systems, Nice, France, 3-4 October 1991 (contact either Gerard Le Lann E-mail: GLL@SCORE.INRIA.FR or Miroslaw Malek E-mail: MALEK@EMX.UTEXAS.EDU)

INFORMATION and ADVANCE PROGRAM complete with registration form and hotel reservation form for SRDS10: contact: Luca Simoncini, IEI-CNR, Via S.Maria 46,  
56126 Pisa Italy  
fax: +39 50 554342  
E-mail:SIMON@ICNUCEVM.CNUCE.CNR.IT

=====

ELECTRONIC REGISTRATION FORM SRDS-10

SURNAME:

NAME:

AFFILIATION:

ADDRESS:

CITY:

STATE:        ZIP:

TEL.:        FAX:

E-MAIL:

REGISTRATION FEES:

Before September 10,1991:

Members:        Lit. 430.000  
Non Members:    Lit. 550.000  
FullTime Students: Lit. 260.000

After September 10, 1991:

Members:        Lit. 520.000  
Non Members:    Lit. 650.000  
FullTime Students: Lit. 400.000

IEEE/CS Membership number: \_\_\_\_\_

AICA Membership Number: \_\_\_\_\_

Registration fee includes: the Proceedings, three working lunches, coffee breaks, participation to the Concert and Welcome Party on Monday night and Gala Dinner on Tuesday night. Students do not participate to the Social Program.

PAYMENT

AMOUNT OF LIT. \_\_\_\_\_

I ENCLOSE AN INTERNATIONAL BANK CHEQUE FOR THE TOTAL AMOUNT

I ENCLOSE PHOTOCOPY OF A BANK TRANSFER ORDER

PAYABLE TO : SRDS-10 ETTORE RICCIARDI

BANK ACCOUNT N. 13676

BANCA POPOLARE DI NOVARA AG.1 - VIA S.FRANCESCO, 54 - PISA

SEND IN AN ENVELOPE TO: ETTORE RICCIARDI

IEI-CNR

VIA S.MARIA 46

56126 PISA, ITALY

=====

SRDS-10 HOTEL RESERVATION FORM

SURNAME \_\_\_\_\_

NAME \_\_\_\_\_

AFFILIATION \_\_\_\_\_

\_\_\_\_\_

ADDRESS \_\_\_\_\_

\_\_\_\_\_

CITY \_\_\_\_\_

STATE \_\_\_\_\_ ZIP \_\_\_\_\_

TEL \_\_\_\_\_ FAX \_\_\_\_\_

ACCOMPANIED BY (SURNAME AND NAME) \_\_\_\_\_

\_\_\_\_\_

I WISH TO SHARE A DOUBLE ROOM WITH \_\_\_\_\_

\_\_\_\_\_

DATE OF ARRIVAL \_\_\_\_\_

DATE OF DEPARTURE \_\_\_\_\_

TOTAL NIGHTS \_\_\_\_\_

I AM ENCLOSING INTERNATIONAL CHECQUE N.

\_\_\_\_\_

MADE PAYABLE TO: TRE EMME CONGRESSI

PLEASE RETURN THIS FORM WITH DEPOSIT (P.T.O)  
BEFORE SEPTEMBER 2, 1991 TO:

TRE EMME CONGRESSI  
VIA RISORGIMENTO 4  
56126 PISA, ITALY

=====  
COST OF ACCOMODATIONS

HOTEL CAT    SINGLE    DOUBLE    DOUBLE AS SINGLE

\*\*\*\*    LIT.163.500    LIT. 228900    LIT. 190750

\*\*\*    LIT. 74500    LIT. 105000    LIT. 95000

\*\*    LIT. 51000    LIT. 80000    LIT. 65000

PRICES INDICATED ARE PER ROOM AND INCLUDE BREAKFAST, SERVICE CHARGES, TAXES AND VAT. WHEN SINGLE ROOMS ARE NO MORE AVAILABLE DOUBLE ROOMS FOR SINGLE USE WILL BE RESERVED. THE DEPOSIT WILL BE DEDUCTED FROM THE HOTEL BILL UPON DISPLAY OF THE VOUCHER SENT BY TRE EMME CONGRESSI. MAJOR CREDIT CARDS ARE ACCEPTED AT ALL HOTEL IN PISA.

NOTIFY TRE EMME CONGRESSI OF LATE ARRIVAL TO HAVE GUARANTEED RESERVATION.

Lorenzo Strigini, IEI del CNR  
Via Santa Maria 46 I-56126 Pisa ITALY  
Tel: +39-50-553159 ; Fax: +39-50-554342 ; Telex: 590305 IEICNR I  
strigini@icnucevm.cnuce.cnr.it , strigini@icnucevm.bitnet

---

## **✉ DIAC-92 CALL FOR PAPERS AND PARTICIPATION**

<douglas@atc.boeing.com>

Fri, 30 Aug 91 13:08:42 PDT

Call for Papers and Proposals  
DIRECTIONS AND IMPLICATIONS OF ADVANCED COMPUTING  
DIAC-92 Berkeley, California May 2 - 3, 1992

Computer technology significantly affects most activities in society, including schooling, health care, military practice, work, communication, and laws and law enforcement. The DIAC conference considers the implications of technical advancements on society in a broad social context that encompasses ethics, economics, and politics. The conference seeks to address the the relationship between technology and society. Papers that address directly the relationship between technology and policy, and papers on the ethics and values of computing are especially desired. Papers and workshop proposals that build on previous

DIAC presentations are encouraged. Reports on work in progress or suggestions for future work as well as appropriate surveys and applications will also be considered. The following topics should be regarded as general guidelines for paper or workshop topics:

- |                               |                                |
|-------------------------------|--------------------------------|
| RESEARCH DIRECTIONS           | DEFENSE APPLICATIONS           |
| + Research Funding            | + AI & Neural Net Applications |
| + Software Development        | + Autonomous Weapons Systems   |
| Methodologies                 | + Virtual Reality              |
| + Professional responsibility | + Uses of Models & Simulations |

- |                                   |                                     |
|-----------------------------------|-------------------------------------|
| COMPUTING IN A DEMOCRATIC SOCIETY | COMPUTERS IN THE PUBLIC INTEREST    |
| + Community Access                | + Computing for the Disabled        |
| + Computerized Voting             | + Computers and the Environment     |
| + Civil Liberties                 | + Arbitration & Conflict Resolution |
| + Computing & the Law             | + Computing in Education            |
| + Computing & Workplace           | + Software Safety                   |

Submissions will be read by members of the program committee, with the assistance of outside referees. The program committee includes David Bellin (consultant), Eric Gutstein (U. WI), Batya Friedman (Mills College), Jonathan Jacky (U. WA), Deborah Johnson (Rensselaer Polytechnic Inst.), Richard Ladner (U. WA), Dianne Martin (George Washington U.), Judith Perrolle (Northeastern U.) Marc Rotenberg (CPSR), Douglas Schuler (Boeing Computer Services), Barbara Simons (IBM), Lucy Suchman (Xerox), Karen Wieckert (U. CA. Irvine), and Terry Winograd (Stanford).

Accepted papers will be presented on May 2. Accepted workshops will be conducted on May 3. Complete papers should include an abstract and should not exceed 6000 words. Proposals for workshops should include title, purpose, intended agenda, and references. Workshops will be two hours in length. Submissions will be judged on significance, clarity, insight, and originality. Papers and/or proposals (4 copies) are due by November 1, 1991. Notices of acceptance or rejection will be mailed by January 15, 1992. Camera ready copy is due by March 1, 1992. Send papers to Douglas Schuler, Boeing Computer Services, MS 7L-64, P.O. 24346, Seattle, WA 98124-0346. For more information contact Doug Schuler (206-632-1659 (H), 206-865-3832 (W) dschuler@june.cs.washington.edu).

Proceedings will be distributed at the symposium, and will be available by mail. The DIAC-87, DIAC-88, and DIAC-90 proceedings are published by Ablex Publishing Company. Publishing the DIAC-92 proceedings is also planned.

Sponsored by Computer Professionals for Social Responsibility  
P.O. Box 717, Palo Alto, CA 94301

DIAC-92 is co-sponsored by the American Association for Artificial Intelligence, and the Boston Computer Society Social Impact Group, in cooperation with ACM SIGCHI and ACM SIGCAS.



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 12: Issue 23

Tuesday 3 September 1991

## Contents

- [Herb Caen on Computerized Radar](#)  
[via Mike Seibel](#)  
[Brad Templeton](#)  
[Allan Meers](#)
- ["Miser held in record Social Security fraud"](#)  
[Barry Jaspán](#)
- [Re: "Thieves Hit Social Security Numbers"](#)  
[Lars-Henrik Eriksson](#)
- [Computer Abuse Amendments Act of 1991](#)  
[Thomas Zmudzinski](#)
- [Re: A Danger ... with Intelligent Terminals](#)  
[Paul Stachour](#)
- [Complain to Journalists](#)  
[John E. Mollwitz](#)
- [The RISKS of Superiority](#)  
[Arthur Clarke \[!\] via Ellen Spertus](#)
- [NASA severs connection on electronic mail linkup](#)  
[wrapup by Joe Abernathy](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Herb Caen on Computerized Radar

*Allan Meers - Sun Education/Professional Services <Allan.Meers@ebay.sun.com>*  
*Mon, 2 Sep 91 09:05:43 PDT*

From Herb Caen's column in the San Francisco Chronicle,  
via Mike Seibel and Brad Templeton:

A motorist was unknowingly caught in an automated speed trap that measured his speed using radar and photographed his car. He later received in the mail a ticket for \$40, and a photo of his car. Instead of payment, he sent the police department a photograph of \$40. Several days later, he received a letter from the police department that contained another picture -- of handcuffs.

---

✂ **"Miser held in record Social Security fraud" -- UPI, 31 Aug 91**

"Barry Jaspan" <bjaspan@MIT.EDU>

Sun, 1 Sep 91 14:28:27 -0400

(Extracted from the article in clari.news.law.crime from the ClariNet news service. I've left out a great deal of non-RISKS-related information.)

Robert L. Chesney is facing trial in the biggest individual Social Security fraud case in U.S. history. He is accused of receiving retirement and disability checks under at least 29 names. Federal agents found 15 boxes and three steamer trunks full of birth certificates, bank statements, Social Security cards and over 200 CA DMV id cards, each with Chesney's picture and a different name.

The final paragraph in the article:

Chesney allegedly gleaned biographical data about public personalities from the library. Pretending to be those people, Chesney would write to their home counties, give their birth dates and other information and ask for copies of their birth certificates. He then took the documents to the DMV and obtained the ID cars with which he applied for the Social Security benefits.

Barry Jaspan, bjaspan@mit.edu

---

✂ **Re: "Thieves Hit Social Security Numbers" ([RISKS-12.20](#))**

Lars-Henrik Eriksson <lhe@sics.se>

Mon, 2 Sep 91 10:36:08 +0200

One thing that strikes me as strange is when I compare this with the situation in Sweden. We have had "civic registration numbers" since 1947. These numbers are unique identification of every resident in Sweden. Children are assigned their numbers shortly after birth and immigrants as they are given a residence permit.

These numbers are public information and their use permeate the entire society. Even to become a member of a soccer club, you often have to provide your id number. Often a membership number or customer number is simply identical to your id number. While there is a growing resistance to the use of these numbers, they are still such an accepted part of society that they are often requested even when there is no real need for them.

Now the events described in the article, where people are stealing SSN's and using them to get credit etc, virtually never happen in Sweden. This is even more strange as the Swedish id numbers are public information. Of course it \*does\* happen, but it is not seen as an important risk. The important risk is considered to be the possibility of easily compiling lots of information about a single individual. (There is legislation specifically directed against this.)



transmission of a program, information, code, or command to a computer or computer system if-

"(i) the person causing the transmission intends that such transmission will-

"(I) damage, or cause damage to, a computer, computer system, network, information, data, or program; or

"(II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data, or program; and

"(ii) the transmission of the harmful component of the program, information, code, or command-

"(I) occurred without the knowledge and authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and

"(II)(aa) causes loss or damage to one or more other persons of value aggregating \$ 1,000 or more during any 1-year period; or

"(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

"(B) through means of or in a manner affecting a computer used in interstate commerce or communication, knowingly causes the transmission of a program, information, code, or command to a computer or computer system-

"(i) with reckless disregard of a substantial and unjustifiable risk that the transmission will-

"(I) damage, or cause damage to, a computer, computer system, network, information, data, or program; or

"(II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data, or program; and

"(ii) the transmission of the harmful component of the program, information, code, or command-

"(I) occurred without the knowledge and authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and

"(II)(aa) causes loss or damage to one or more other persons of value aggregating \$ 1,000 or more during any 1-year period; or

"(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

(b) PENALTY.-Section 1030(c) of title 18, United States Code is amended-

(1) in paragraph (2)(B) by striking "and" after the semicolon;

(2) in paragraph (3)(B) by inserting "(A)" after "(a)(5); and

(3) in paragraph (3)(B) by striking the period at the end thereof and inserting ", and"; and

(4) by adding at the end thereof the following:

"(4) a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(5)(B)."

(c) CIVIL ACTION.-Section 1030 of title 18, United States Code is amended by adding at the end thereof the following new subsection:

"(g) Any person who suffers damage or loss by reason of a violation of the section, other than a violation of subsection (a)(5)(B), may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage."

(d) REPORTING REQUIREMENTS.-Section 1030 of title 18 United States Code, is amended by adding at the end thereof the following new subsection:

"(h) The Attorney General shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning prosecutions under section 1030(a)(5) of title 18, United States Code."

(e) DEFINITION.-Section 1030(e)(1) of title 18 United States Code, is amended by striking ", but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device".

(f) PROHIBITION.-Section 1030(a)(3) of title 18 United States Code, is amended by inserting "adversely" before "affects the use of the Government's operation of such computer".

---

## ✂ Re: A Danger ... with Intelligent Terminals (Thomson, [RISKS-12.21](#))

Paul Stachour <stachour@SCTC.COM>

Tue, 3 Sep 91 08:41:49 CDT

In original Multics (Unix is supposedly an "improved" derivative of Multics), in the module which has the responsibility for writing messages to the user's terminal (messages which were sent by the Multic-similar function to "write), there is a comment dated 1974 (I enter from memory, the phrasing may not be exact):

This module censors control and escape sequences to prevent users from sending messages that masquerade as coming from the Multics System Operator and other potentially dire consequences.

Notice that:

- #1: The date of this message, showing that the problem was understood even back in 1974.
- #2: The wording of the warning, which gives meaning to the understanding, and not too many hints to the unknowledgeable (Multics source has always, to my knowledge, been publically available).
- #3: As so often is true, the "new improved version" is poorer than the original version.

The mechanism by which Multics sends its mail and messages (which I will

not describe here for lack of my time and space, but is quite clearly documented in the Multics manuals) was well-designed to avoid:

- 1) Forgery
- 2) Spoofing
- 3) Default system style doing bad-things

and designed to allow:

- 1) Good access control over mailboxes
- 2) Ability to retract send-but-not-yet-read-messages
- 3) You to give someone power to send-in-your-name, but with clear indications it was not your userid.

The question (on risks) is:

Why do we (as consumers) continue to buy cut-down products containing significantly less functionality and much higher risks when good products are available? My opinion is that there is inherent difficulty for most of us to evaluate the risks inside of products, and we just take what appears to us to be the path of least resistance.

Paul Stachour, SCTC, 1210 W. County Rd E, Suite 100, Arden Hills, MN  
55112-3739      stachour@sctc.com      [1]-(612) 482-7467

---

## **Complain to Journalists**

*"John E. Mollwitz" <moll@mixcom.com>  
Sun, 1 Sep 91 16:48:00 CDT*

The national convention of The Society of Professional Journalists, an organization of roughly 18,000 members in the United States, Canada and Japan, is meeting Oct. 17-19 in Cleveland. As part of that convention, a seminar will be conducted on writing about computers and computer networks.

Since over the years, cyberspace travelers have bemoaned the accuracy of articles relating to computers, computer networks and even telephones, we ask that you email or snail mail examples of articles that you have found solid and others that you have found less so. Please include a note of explanation.

The panel then will try to compile the examples, and the comments and produce a handout for discussion. Sometime in the week after the convention, we will post the results of the session. The names of the panelists will be disclosed at that time since it is possible that some of the articles that may be submitted may have been written by a panelist.

Mail paper examples to me at the address below. Where possible, the examples should include a copy of the article, the name of the publication and specific comments. If the article is dismissed simply as "nonsense," state that it is because paragraph 5 has failed to adequately explain a concept, and that it would have been better to have said it this way or that.

So, if you go into fits when you see the word "hacker" in print, please mail by Sept. 30.

Thank you for your cooperation.

John E. Mollwitz, Chair, Committee on New Information Technologies  
The Society of Professional Journalists, c/o The Milwaukee Journal  
P.O. Box 661, Milwaukee, WI 53201-0661

Usenet: moll@mixcom.com CompuServe: 72240,131 GEnie: J.Mollwitz Prodigy: CKFB43A

[OK, folks, take him seriously. Here's your chance to have an effect on the SPJ similar to what the net did for Lotus Marketplace? PGN]

---

### **✶ The RISKS of Superiority**

<erspert@ATHENA.MIT.EDU>  
Sun, 1 Sep 91 14:18:45 -0400

I recently rediscovered a science fiction short story, "Superiority" (1951), by Arthur C. Clarke, that would be of interest to RISKS readers. Here are excerpts from the story, which is written in the form of a report by a former military leader:

The ultimate cause of our failure was a simple one: despite all statements to the contrary, it was not due to lack of bravery on the part of our men, or to any fault of the fleet's. We were defeated by one thing only --- by the inferior science of our enemies. I repeat --- by the *\*inferior\** science of our enemeies.

When the war opened we had no doubt of our ultimate victory. The combined fleets of our allies greatly exceeded in number and armament those which the enemy could muster against us, and in almost all branches of military science we were their superiors. We were sure that we could maintain this superiority. Our belief proved, alas, to be only too well founded....

[After an expensive battle victory, the new Chief of the Research Staff, Norden, said:] ``Our existing weapons have practically reached finality. I don't wish to criticize my predecessor, or the excellent work done by the Research Staff in the last few generations, but do you realize that there has been no basic change in armaments for over a century? It is, I am afraid, the result of a tradition that has become conversative. For too long, the Research Staff has devoted itself to perfecting old weapons instead of developing new ones. It is fortunate for us that our opponents have been no wiser: we cannot assume that this will always be so....

``What we want are *\*new\** weapons --- weapons totally different from any that have been employed before. Such weapons can be made: it will take time, of course, but since assuming charge I have replaced some

of the older scientists by young men and have directed research into several unexplored fields which show great promise. I believe, in fact, that a revolution in warfare may soon be upon us."

We were skeptical. There was a bombastic tone in Norden's voice that made us suspicious of his claims. We did not know, then, that he never promised anything that he had not already almost perfected in the laboratory. \*In the laboratory\* --- that was the operative phrase.

Norden proved his case less than a month later, when he demonstrated the Sphere of Annihilation, which produced complete disintegration of matter over a radius of several hundred meters. We were intoxicated by the power of the new weapon, and were quite prepared to overlook one fundamental defect --- the fact that it \*was\* a sphere and hence destroyed its rather complicated generating equipment at the instant of formation. This meant, of course, that it could not be used on warships but only on guided missiles, and a great program was started to convert all homing torpedoes to carry the new weapon. For the time being all further offensives were suspended.

We realize now that this was our first mistake. I still think that it was a natural one, for it seemed to us then that all our existing weapons had become obsolete overnight, and we already regarded them as almost primitive survivals. What we did not appreciate was the magnitude of the task we were attempting, and the length of time it would take to get the revolutionary super-weapon into battle. Nothing like this had happened for a hundred years and we had no previous experience to guide us.

The conversion problem proved far more difficult than anticipated. [Description of problems omitted.] Then two things happened. One of our battleships disappeared completely on a training flight, and an investigation showed that under certain conditions the ship's long-range radar could trigger the Sphere immediately [after] it had been launched. The modification needed to overcome this defect was trivial, but it caused a delay of another month and was the source of much bad feeling between the naval staff and the scientists. We were ready for action again --- when Norden announced that the radius of effectiveness of the Sphere had now been increased by ten, thus multiplying by a thousand the chances of destroying an enemy ship.

So the modifications started all over again, but everyone agreed that the delay would be worth it. Meanwhile, however, the enemy had been emboldened by the absence of further attacks and had made an unexpected onslaught...

And so forth. What are the lessons for RISKS readers?

1. A technological advance doesn't make your equipment obsolete if it still does what you need. For example, if the x86 on your desk meets your needs, you don't need to get rid of it and buy a (x+1)86. I know somebody who is still happily using his TI 99/4 even though any number of people would tell him it's obsolete.

2. I'm sure that all RISKS readers can think of a computer project, either software or hardware, that looked dazzling on paper, far more ambitious and computer scientific than competing projects, that became a disaster. It slipped years because of problems due to its complexity, perhaps never reaching market, while competitors produced products much quicker and met the customers' needs.

3. One shouldn't replace existing tools before learning how to use them. For example, if a novice spent a month studying Pascal, then switched to C++ when somebody said it was better, then switched to Lisp, etc., they would never get any useful work done.

Of course, there are risks in carrying any of these lessons too far (such as carrying the x86 into the next millenium). I am told, at one time, this story was "required reading" at MIT. I never came across it as a student at MIT, which is a shame, because it contains such valuable lessons. I urge engineering/CS professors to consider putting it into a systems-building course. The full story can be found in *\_Expedition to Earth\_*, by Arthur C. Clarke (New York: Ballantine Books).

Ellen Spertus

---

### **✶ NASA severs connection on electronic mail linkup (Houston Chronicle)**

*Joe Abernathy <edtjda@magic322.chron.com>*

*Tue, 3 Sep 91 17:05:01 CDT*

{ This story appeared on Page 1A of the Houston Chronicle on Monday, Sept. 2, 1991. Permission is granted for redistribution in the ACM Risks Digest, Patrick Townson's Telecom Digest, the newsgroup sci.space.shuttle, Computer Underground Digest, and the interesting\_people mailing list. Our thanks to these groups for their ongoing contributions to the online community and our coverage of it. Please send comments and suggestions to edtjda@chron.com. }

NASA severs connection on electronic mail linkup.

By Joe Abernathy, Copyright 1991, Houston Chronicle

Although declaring the experiment a success, NASA has called a halt to a project by which space shuttle astronauts briefly were linked with the nation's computer networks through electronic mail. The e-mail experiment, conducted during the recent flight of Atlantis, was part of a larger effort to develop computer and communications systems for the space station Freedom, which is to be assembled during the late 1990s. The National Aeronautics and Space Administration cited unauthorized access as the reason for severing the network connection, but NASA officials did not provide details. The space agency initially attempted to carry out the project in secrecy, but word leaked out on the nation's computer networks. Details were closely guarded because of concerns over malicious computer hacking and astronauts' privacy.

"Hello, Earth! Greetings from the STS-43 Crew! This is the first Applelink from space. Having a GREAT time, wish you were here!" read the first message home. It went from Atlantis astronauts Shannon Lucid and James Adamson to

Marcia Ivins, a shuttle communicator at Johnson Space Center.

It was the use of AppleLink -- a commercial electronic mail network connected to the global computer matrix -- that apparently contained the seeds of trouble. When an AppleLink electronic mail address for the shuttle was distributed online and then published in the Houston Chronicle, it generated about 80 responses from well-wishers.

Although the address was created just for this purpose, the flight director nearly pulled the plug on the project, according to Debra Muratore, the NASA experiment manager. The project was concluded as scheduled and declared a success. But ultimately, it was decided, at least for now, to cease all interaction with public computer networks. The decision eventually could mean that NASA's premier research facility, the space station, may not have access to its premier research communications tool, the NASA Science Internet -- the space agency's portion of the vast Internet global computer network.

Electronic mail, which is becoming commonplace in offices, is simply the transmission of messages via computers to one or more people, using electronic addresses. Users linked to the right networks can send electronic messages or other data to specific recipients nearly anywhere in the world -- and for a short time, could send them to space. "The problem was that the information had gotten leaked prematurely. There was no problem with security," Muratore said. Even previous to the leak of the address, however, the experiment was structured in such a way that it was vulnerable to hackers, she acknowledged. "As a result of this whole experience, at least my project plans never to use a public (electronic) mail system again," she said. Muratore indicated that the space agency may explore other ways of providing "connectivity" -- communication between orbiting astronauts and NASA's broader collection of computerized resources -- which will become increasingly important as the use of computerized information grows.

The decision to sever the short-lived e-mail connection has drawn strong criticism among computer security experts and other scientists, who charge that NASA was attempting to design "security through obscurity." "This is another example of an ostrich-oriented protection policy -- stick your head in the sand and pretend no one will find out what you know," wrote Peter G. Neumann, moderator of the Association for Computing Machinery's RISKS Digest, a respected online publication that assesses the risks posed by technology. "Things like that don't stay 'secret' for very long."

NASA told Newsday, but would not confirm for the Chronicle, that more than 80 "unauthorized" messages from around the world were sent to the Atlantis address -- which a source told the Chronicle was set up explicitly to handle public requests for a shuttle e-mail address. Private addresses were used for the actual experiments. "The old 'authorization' paradox has reared its ugly head again," wrote Neumann, who prepared a study for NASA on the security requirements of the space station. "Threatened by unauthorized e-mail, eh? Sending e-mail to someone REQUIRES NO AUTHORIZATION."

Muratore defended the use of secrecy as a security tool. "I feel that that was a viable option," she said. She said operators of AppleLink told NASA that it was impossible to keep public e-mail from being sent to the on-orbit address, so the only option was to try to keep it secret.

But network users questioned this viewpoint. "Why is an e-mail system 'in jeopardy' when it receives 80 messages? And what is an 'unauthorized user?'" asked Daniel Fischer of the Max-Planck-Institut fuer Radioastronomie, in Bonn, Germany. "Once the system is linked up to the real world, it should expect to receive real mail from everyone. If NASA can't handle that, it really shouldn't get into e-mail at all," added Fischer, writing in an online discussion group composed of scientists involved with the space program. "Consider that (heavy response) a success, NASA!"

The disposition of the electronic mail sent to Atlantis is still up in the air. A Chronicle message was not acknowledged, and no one has reported receiving a response.

[Chronicle reporter Mark Carreau contributed to this report.]



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 12: Issue 24

Wednesday 4 September 1991

## Contents

- [Radiation therapy machine dose rate doubled by configuration error](#)  
[Lawrence W. Berkley and James A. Purdy](#)  
summarized by [Jon Jacky](#)
- [Salomon Brothers -- Database Design \[anonymous\]](#)
- [Airworthiness Directive for 747-400 electrical system](#)  
[Robert Dorsett](#)
- ['Risk perception'](#)  
[Phil Agre](#)
- [Re: Risk Assesment High Priesthood](#)  
[Robert W. Kerns](#)
- [Re: A number is no name](#)  
[EKristia...](#)
- [Re: Re: +& \\*#\\$](#)  
[Bob Frankston](#)
- [Re: "Thieves Hit Social Security Numbers"](#)  
[Urban Fredriksson](#)
- [Re: Risks of a Universal Identifier](#)  
[Martin Minow](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Radiation therapy machine dose rate doubled by configuration error**

*Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>*  
*Wed, 4 Sep 1991 13:52:02 PDT*

This incident was reported in a poster presentation at the annual meeting of the American Association of Physicists in Medicine (AAPM) held in San Francisco last July 21 - 25. A brief abstract appeared in MEDICAL PHYSICS, 18(3), May/June 1991, p. 608. Some of the material quoted here will also appear in a forthcoming AAPM Task Group 35 Report on Medical Accelerator Safety Considerations. Included here with permission. Jon Jacky, [jon@gaffer.rad.washington.edu](mailto:jon@gaffer.rad.washington.edu), University of Washington, Seattle

=====

Excerpts from Lawrence W. Berkley and James A. Purdy, "The Need for Better Communication between Accelerator Manufacturers and In-House Service Engineers"

... This [incident involved] the switching of the "target and filter" interlock boards between a Varian Clinac 1800 and a Clinac 2100C ... Please note that good quality assurance practices [at the clinic] detected the problem before any significant increased dose was delivered to any patient.

A PC board intended for use on a Varian Clinac 2100C was placed in a Clinac 1800 by an in-house service engineer [an engineer was on the clinic's staff, not the vendor's staff]. ...

The boards for the two machines had the same part numbers. ... EPROM's on the boards for the two machines were programmed differently due to [to accommodate the different characteristics of] different types of ion chambers [present on the two different accelerator models].

When the incorrect PC board was in the Clinac 1800, the calibration changed by over 100% for some beams. [A single therapy machine can produce several types of beams that differ in particle (photons or electrons) and energy]. ... For these beams, the calibration changed from 1.00 cGy/MU [centigrays (a unit of radiation dose) per monitor unit (the indicator on the therapy machine display screen or control panel)] to 2.08, 2.51, and 1.09 cGy/MU for the 9, 12, and 16 MeV [electron] beams respectively. This was due to reduced ion chamber sensitivity. ...

The dosimetry error was detected during a routine constancy check of beam output. [It is usual good practice to check each machine's internal dosimetry system by making frequent independent measurements at the clinic with equipment that is entirely separate from the therapy machine. The "morning constancy check" is usually performed every day.]

When the incorrect Target and Filter interlock board was placed in the Clinac 1800 ... no dosimetry fault was tripped and the machine appeared to be running normally.

Varian was aware of the possibility for this to occur but did not alert new owners of the Clinac 1800's from 1987 to 1990. ... Although notice was sent to users of the equipment in 1986 following a similar incident, new owners were not notified of the potential problem. ...

The fact that the incident described is for a Varian accelerator, is not intended to imply that such problems exist only with the Varian organization. We feel strongly that it is an industry wide problem and a solution must be found rapidly to avoid any serious consequences. ...

The report relating to this incident issued by the Problem Reporting Program of the FDA failed to mention the large change in machine calibration ...

Recommendations:

A cumulative list of problems unique to each model of accelerator should be maintained by all manufacturers for their models. This list should be made

available to all existing users and should be brought to the attention of new purchasers of accelerators. ...

Medical physicists should be constantly aware that accelerators are capable of large changes in calibration with no indication of a problem. This reinforces the need for frequent output checks.

Medical physicists should be aware that manufacturers and the Problem Reporting Program of the FDA may temper their notifications to users such that serious problems appear to be fairly benign.

---

### **✂ Salomon Brothers -- Database Design**

<[anonymous]>

Tue, 3 Sep 91 08:57:07 EDT

The recent Salomon Brothers securities scandal was caused in part by sloppy database design according to an employee in the database programming department. Normally whenever there is a buy or sell order, several "confirmations" are sent to individuals of the represented organization. Four traders were able to exploit this system by setting the number of confirmations to zero and subsequently trading in an unauthorized and unsupervised fashion.

Among the many changes in the Salomon Brothers firm, a new requirement for management to authorize setting confirmations to zero is being implemented in their software along with a new audit trail of the confirmation process. Surprisingly, no confirmation is actually desired by some organizations.

The problem is certainly not new to readers of risks and the proposed solution is not particularly inspired. Another unread audit trail or a scandal at the next level of hierarchy both seem possible, unaddressed, and unacknowledged. What is new is the fact that the Salomon Brothers scandal has been international incident with severe political and economic consequences. Butterfly wings and programmer fingertips can both cause hurricanes.

Of course, had the traders set the confirmations to `O' instead of `0', Stephen could be the most influential man on Wall Street...

It should also be noted that Salomon Brothers does not allow direct access of the programming department to Internet or Usenet and is a company that routinely monitors electronic mail.

---

### **✂ Airworthiness Directive for 747-400 electrical system**

Robert Dorsett <rd@rascal.ics.utexas.edu>

Tue, 3 Sep 91 22:12:04 CDT

>From the Federal Register 56:159, August 16, 1991, pp. 40773-40774. Ties into discussions of common-cause-of-failure cases on RISKS a couple of years ago. The 747-400 is Boeing's newest 747, featuring a glass cockpit with conventional hydromechanical flight controls. The aircraft was

rolled out January 26, 1988.

"Summary: This amendment adopts a new airworthiness directive (AD), applicable to certain Boeing Model 747-400 series airplanes, which requires rerouting and adding shielded wiring associated with the differential protection current transformers in the P6 panel. This amendment is prompted by the results of a Model 747-400 electrical system safety assessment, which demonstrated that the potential exists for a single event causing the loss of all normal sources of airplane electrical power. This condition, if not corrected, could result in the loss of all normal sources of electrical power to the airplane essential busses, limiting power availability to that provided by the standby system.

"...No commenter expressed any technical objection to... the rule... Two commenters requested that the proposed compliance period of 180 days be extended to 12 or 15 months so that the modification could be performed during other scheduled maintenance... One commenter stated that, since this AD is based on a safety assessment, and not an actual occurrence, an increase in the proposed compliance time to 15 months would not compromise safety; and since the airplanes affected by this proposed rule are relatively new and most have been only recently delivered, chafing of the affected wire bundles during that time seems unlikely...

"One commenter ... recommended that ... compliance time be reduced to 60 or 90 days. This request was based on the commenter's stated opinion of the dire consequences of losing all electrical power on a long overwater flight..."

[ FAA doesn't concur with any of these: recommends that rule be adopted as proposed]

"There are approximately 107 Model 747-400 series airplanes of the affected design in the worldwide fleet. It is estimated that 18 airplanes of US registry will be affected by this AD, that it will take approximately 8 manhours per airplane to accomplish the required actions, and that the average labor cost will be \$55 per manhour. The cost of required parts per airplane is estimated to be \$20. Based on these figures, the total cost impact of the AD on US operators is estimated to be \$8,280."

Robert Dorsett           UUCP: ...cs.utexas.edu!rascal.ics.utexas.edu!rdd  
Internet: rdd@rascal.ics.utexas.edu

---

## `Risk perception`

*Phil Agre <pagre@weber.ucsd.edu>  
Tue, 3 Sep 91 16:46:16 pdt*

Wm Gardner's message is helpful in that it makes clear just how much is at stake in accepting or rejecting the basic validity of research on `risk perception'. First a few side issues. I did not mean to suggest that ``attributing irrational judgment to ordinary people can make them seem responsible for the morbidity and mortality they suffer." That may well be true, but I haven't actually encountered that particular interpretation. Also, the LA Times article I cited contained a quote from an interview with

a risk expert to the effect that "ordinary people are unwilling to accept any risk at all" though I am afraid that I no longer have my copy of the article. I doubt if anyone would say this in an official journal, and the rhetorical context was something in the spirit of irony or hyperbole, but I have encountered such opinions regularly in conversation with people who work in industries where 'risk' is a controversial issue. Next, when I said that the 'findings' quoted in the LA Times article are "easily explained" in such-and-such a way, I took that to be a figure of speech meaning, in scientific language, "those findings are equally compatible with the hypothesis that such-and-such, so that (1) no conclusion of irrationality can be drawn at this point and (2) in searching for an explanation, it is necessary to explore other new directions of research." Finally, I want to make sure that WG and others don't take me to be saying that most 'risk' researchers operate in bad faith. I am sure that many such people share a concern with responsible technology, however misguided I may find their approach to it, and I should probably not have put the word 'research' in sneer quotes when discussing this work. However...

WG and I have different views about the social context within which 'risk' research operates -- or, more precisely, about the consequences of that social context. Whereas my argument emphasizes the role of corporate PR and recent history, WG wishes to portray risk research as a scientific field with a history and origins like any other. Every scientific field tries to back-date itself to distant origins and risk research cannot be singled out for any special criticism in this respect. Certainly 'risk' is an old word that has been used in various contexts for a long time. Now, WG says, "The concept of risk in the sense used in risk perception studies dates (at least) from the beginnings of epidemiology and from the integration of probability into the theory of insurance in the 18th century." The examples given here involve a natural phenomenon and a business-risk calculation performed within a single firm. But what is new and distinctive about contemporary 'risk' controversies is that the 'risks' involve dangers to the public at large that result from human (bureaucratic) action. At this point, 'risk' becomes part of something altogether different. Though WG says that "[p]sychological research on risk perception and probability judgments was well established when Mobil ran its ads," I did not mean to imply that the whole thing sprung fully grown from Mobil's ads. What I did mean to imply is that, with the growth of public controversy around the politics and morality of large technology-based organizations, there has evolved a huge ideological machinery that propagates things \*like\* those Mobil ads through all manner of media. This is the important thing to understand about PR. It's not just a matter of quarter-page ads and talking heads spewing reassuring nonsense when things blow up. And it's not just a matter of people being bad. It's a matter of large corporations involved in extremely competitive businesses, where profits or losses can turn on sustained public assent to marginal technological projects. Ten thousand Mobils large and small are at work as we speak, driven by the imperatives of the market to attempt to capture and occupy the workings of civil society. The principal weapon in this battle is not cash or fast talk; rather it is precisely the sort of ideology I outlined in my note.

The people of Bhopal may have some trouble distinguishing between this motivated sort of 'risk'-talk and the properly scientific sort. The readers of the LA Times are probably having a hard time too. Even so, it is important for us to reflect carefully on the conditions under which it is possible to

conduct responsible scientific research. WG's message argues in effect that we can judge 'risk' research in isolation from its social context. Can we? Let us suppose that risk researchers, by and large, are willing to dissociate themselves from (for instance) those Mobil advertisements. (Remember the ones -- cited in Langdon Winner's essay on 'risk' in his book "The Whale and the Reactor" -- about how 'risk-taking' is a good old American value, how 'risk'-avoidance is thus un-American, and how the very essence of the Americanness of companies like Mobil is all of the business risks that made them what they are today? The word 'risk' is uncannily plastic in this sort of way.) Let us also suppose that an audit of the sources of research funding for 'risk' research would also be beside the point. (I don't actually know what such an audit would turn up; and I do indeed think that such an audit would not, all by itself, mean anything.) My own argument would be that the logic of 'risk', however unconscious or unintended, is inherently ideological in the way my note asserted. I do not pretend that this is an easy argument to make.

I am glad that WG has chosen as his test case the sexual lives of young gay men. It is easy to concur with a call (not actually present in WG's note, but presumably implied) for the wide dissemination of accurate information about HIV and AIDS. This is not the issue. The issue is how this process should proceed. The example is an excellent one because the AIDS epidemic itself is a terrific illustration of a non-unilateral, community-based response to a serious public emergency. Gay community activists differ in their beliefs and approaches, but collectively they have been an inspiring model of how people can take scientific, medical, and social issues into their own hands. My own view, which I think many in this community would share, is that phrases like "availability heuristic" are intolerably dull instruments for understanding and acting upon human questions. The world of gay people is a complicated place, shot through with the social and psychological effects of eons of homophobic prejudice, often dressed up as the most extraordinary scientific nonsense. Terms like "availability heuristic" do not begin to scratch the surface of the epistemological situation of a young gay man. Around 1985 the gay community decided that it was not going to wait around while people with generalized expertise about 'risk' and the like designed studies "that can powerfully discriminate among many competing plausible explanations," all of them founded in ignorance and likely to be wrong. Through detailed study, community-based research, and vociferous activism, they changed the conduct of American science for the better. And, to the extent that they have been permitted by the keepers of 'public service announcement' space and the like, they have also been conducting an imaginative and highly successful education campaign, based on their own extensive discussions among themselves, which not only says "sex can give you germs" but also places the epidemic within a broadly drawn political and economic context. \*This\* is what socially responsible medicine looks like -- and it is a success that ought to be replicated by the victims of toxic wastes, unsafe workplaces, and several other horrors of the market as well.

In conclusion, it is my argument that 'risk' research is inherently complicit with the ideology of Mobil oil so long as it persists in understanding 'risk perception' as a narrowly drawn cognitive matter, and not as a reflection of rational responses to corporate sophistry and fundamental disagreements about the social organization of technology and medicine. Probability theory is not

wholly irrelevant, but the numbers only make sense in a very large context. Until 'risk' research decides to start at the beginning, it cannot \*help\* but portray ordinary people as irrational, jumping at shadows and losing out to experts who are paid to tell us why we don't think that everything's alright.

Phil Agre, UCSD

---

## **✂ Risk Assessment High Priesthood**

*Robert W. Kerns <rwk@Crl.dec.com>*

*Tue, 3 Sep 91 22:22 EDT*

In regard to Phil Agre's remarks on PR and the Risk Assessment field: I too am offended by most of what I see in this area. (Note: What I see is a biased sample, and not representative of all research done in the field). I consider the field to be seriously contaminated by self-serving interests, to the point where I don't trust ANY conclusions presented, unless I'm also given the data, methodology, and chain of reasoning.

The most fundamental flaw in my view, and one I haven't seen discussed except peripherally, is the assumption that risk can be reduced to comparing numbers of deaths, with all deaths being equal. Whenever the public at large doesn't agree with this, "public reaction" is labeled as being irrational. It is the strong parallel here between religious dogma and Risk Assessment "professionals", which leads me to term this a High Priesthood. Time and time again, I see results which are surprising when viewed from a "all-deaths-equal" viewpoint, used to argue that people's perceptions of risk are flawed.

I KNOW there's value to scientific methodology in analyzing risk, and I would like to make use of it in forming my opinions. But when most of what I see masquerading as analysis is contaminated with this religious assumption, I am really thwarted in using Risk Analysis.

To take one oft-cited example, coal vs nuclear, and twiddle with it a bit to make what I'm talking about clear. (Numbers invented; I'm illustrating a RA concept, not comparing coal and nuclear).

Coal: 5 death per 10,000 man-years.

Nuclear: 1 death per 10,000 man-years.

Sounds like Nuclear is the clear winner here, right?

But let's consider a couple scenarios:

1) Coal: Equal geographic distribution of risk over area of benefit.

Nuclear: Risk concentration around the plant.

2) Coal: Constant, predictable rate of deaths.

Nuclear: Low rate, except in rare accident, resulting in very high cost of health care, entire families wiped out.

The results I've seen indicating that people's perception of risks are "skewed"

to me indicate that people are more adverse to risks with particular characteristics:

- \* Unfair distribution
- \* High concentration; that is occasional disaster is worse than continual high risk.
- \* High subsidiary cost, such as an area of land rendered uninhabitable, or high health-care costs.
- \* Low amount of individual control over individual risk factors.
- \* Risks whose assessments are based on questionable data or from sources whose veracity is suspect.

To me, this seems to be a much more rational approach than reducing the debate to numbers killed by coal or nuclear.

>From this, you might assume that I am wildly pro-coal and anti-nuclear, which would exaggerate my position considerably. (I'm anti-coal, and consider chemical waste to be more serious than nuclear. Nuclear waste decays, but heavy metals are forever!).

I see the same phenomena operating in assessment of air-travel risks, where people are more concerned with air accidents, which wipe out entire families, and over which there is little personal control and choice, than over automobile travel, which is far more dangerous. This concern is viewed as non-rational, but I find it eminently rational. Killing off and injuring large numbers of people at once overloads our mechanisms for dealing with tragedy, by overloading emergency health-care, wiping out large segments of families, wiping out entire upper-level management of companies, or rock groups, or what-have-you.

There's more structure to risk than a single scalar value; deaths per 100,000 deaths per {man-hours,passenger-miles, etc.}, and these scalar numbers are not what society tries to optimize.

Real scientific research would try to go to the next step, and model and quantify what people really DO try to optimize.

But it's easy to look scientific if you ignore this and say "see, it all reduces to this number, which scientifically PROVES it."

---

**✂ Re: A number is no name ([RISKS-12.20](#)).**

<EKRISTIA@estec.bitnet>  
Tue, 03 Sep 91 08:52:17 CET

In his accompanying note, PGN is musing whether characters traditionally considered non-alphabetic, such as "!" (I hope the exclamation mark translates correctly from my IBM PROFS to the machine running the list) could be a name.

I recall reading in Scientific American some time ago about a people somewhere in Africa named !KUNG. The exclamation mark is part of the name and is pronounced as a [Zulu] "click" (as in Miriam Makeba's "Click song" ).

In fact, this is just an example of a much broader issue: National alphabets. Computer alphabets like ASCII and EBCDIC originated in an English-speaking country and consequently knows only the 26 letters of the English alphabet. Most other countries using, basically, the Roman alphabet, however, have a few more characters. Examples: a, o, u, with two dots on top ("umlaut") in German and Swedish; a with a small circle on top in Danish, Swedish, Norwegian; n with a tilde in Spanish; accents in French, Spanish and Turkish, and many more.

National extensions to e.g. ASCII exist, but unfortunately they tend to overlap and to "steal" characters like the square brackets away from the US-ASCII. The result is that names (or anything else) containing one of the national characters may print quite differently on a computer assuming another national alphabet. I recently printed a C program on a German PC. All the square brackets came out as A-umlaut and o-umlaut, respectively. Not very readable!

With the increasing mobility of people, more and more people end up in places where computers cannot handle their names properly because they contain characters which are not in the alphabet of the country of residence. In practice, of course, there are work-arounds like representing special letters by letter combinations which are phonetically reasonably close. But this is not very satisfactory.

I wonder how your legal situation is if you refuse to accept documents, say, from public authorities, as long as they cannot spell your name properly?? (I am a Dane living in Holland, but I have no "non-standard" letters in my name, so I cannot put it to a test).

---

**✉ Re: Re: +&\*#\$(Blinn, [RISKS-12.22](#))**

<frankston!Bob\_Frankston@world.std.com>  
3 Sep 1991 20:56 -0400

Admittedly I wasn't trying to be exact in my representation of NH plates. But the response reminds us that the Risks of Technology makes us understand existing risks better. The problem of encoding license plates is present even in paper systems. Is a "-" significant? Might there be both 12-134 and 121-34 or, even, 12<space>13-4? How about +RMF+ (which I've seen on an NH plate)? Obviously the Maine Lobster is decoration. Or is it? Does NH purposely create a situation that makes it less likely for their drivers to get out of state tickets since other states can't refer to the plate numbers?

I once had my office manager order property stickers. Since there were to be both removeable and nonremoveable stickers I ordered some of each in different colors. I didn't expect her to order the same series of numbers (1 to 1000) on both sets. Obviously she saw the color as a significant distinction while I was assuming it was unrelated to the actual numbering.

In Massachusetts the number series are reused for each class of plates. Thus the Taxis are numbered from 1. (The Governor, however, is G-1 because one of the previous Governors refused to return his "1" plate -- politics triumphs over technology). Of course the fact that there aren't check digits in

license plates is also naive considering the importance of accuracy in recording the numbers.

---

**✉ Re: "Thieves Hit Social Security Numbers" ([RISKS-12.23](#))**

*Urban Fredriksson <urbanf@yj.data.nokia.fi>*

*Wed, 4 Sep 91 10:49:58 EET\_DST*

One reason SSNs are seldom 'stolen' in Sweden is the fact that they are public. For important things, nobody [should] think I am I, just because I know my number.

If I take out a loan card at a library, they will want my number (so if I don't return books and move they can track me), but they won't give me a card without seeing an ID.

When I started accounts in a bank I hadn't done business with before, they asked me for my number, but no ID. Unsafe you say? Well, they also didn't ask me for my address, and didn't give me anything at their office. They sent all confirmation papers to my address anyway, so I had to sign for them at the post office.

But there have been cases of serious SSN abuse: One man, a drug addict, went to a hospital wanting aid, and gave them his brother's SSN. For security reasons, no hospital computer records may be erased, so now the brother has got a permanent record of being a drug addict.

And at the same time, the health services doesn't use our SSNs for keeping track of what prescribed drugs we are given, so you can go to 20 doctors, and be given 20 prescriptions for the same (mildly) narcotic drug.

Urban Fredriksson, Stockholm, Sweden.

---

**✉ re: Risks of a Universal Identifier**

*Martin Minow <minow@ranger.enet.dec.com>*

*Tue, 3 Sep 91 13:11:41 PDT*

I used to live in Sweden where there is a universal identifier, assigned to natives at birth, and to immigrants when they get a residence visa (but not to tourists). There are a number of advantages:

- when you move, you fill out one postcard and all of your magazine subscriptions (etc.) change, since all of the publishers subscribe to the "change of address tape."
- since the "personnummer" is an official id and Sweden has an extremely strong data privacy law, there are safeguards surrounding its use. The Swedish data privacy law controls information processing where there is a "risk for personal integrity." (For example, when I applied for an American Express card, I gave my bank reference. Two weeks later, my bank

sent me -- unsolicited -- a copy of the credit report they sent AmEx. This wasn't because of the d.p. law, but illustrates the way private information s disclosed in Sweden.)

There are also risks -- fewer, however than there would be in America, with it's reliance on industry to do the right thing without unnecessary government meddling in the workings of the free enterprise system.

By the way, and not entirely off the subject, there is an interesting background to the now twenty-year-old Swedish data privacy law. The "change of address tape" contains public information which MUST be made available to any requestor. Public information, in Sweden, includes civil status, profession, age, sex, weapon-license possession, and taxable income. As I recall the story (from a Swedish newspaper), one of the incidents that led to the d.p. law was the monthly purchase of the change of address tape by a large American company in the credit-bureau business. When the government discovered this, they realized that this was ideal material for "economic espionage." Since access couldn't be restricted under the "Sunshine Laws," they restricted its use.

Like most laws, the Swedish d.p. law is only a few pages long. If someone could get me a current copy, I could try to knock together a translation for Risks (or perhaps CACM).

Martin Minow    minow@ranger.enet.dec.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 12: Issue 25

Thursday 5 September 1991

## Contents

- [A kludge too far? FAX-to-OCR-to-speech](#)  
[Bob Frankston](#)
- [LA Times Article on E-mail](#)  
[Mike Kimura](#)
- [Re: RISKS of using electronic mail](#)  
[Brian Clapper](#)  
[David Parnas](#)
- [More on SSN risks](#)  
[Glen Osterhout](#)
- [Universal Email addresses and SSN](#)  
[Jim Anderson](#)
- [Re: "Thieves Hit Social Security Numbers"](#)  
[Bob Frankston](#)
- [Re: National Character variations in ASCII](#)  
[Jim Haynes](#)
- [Pork barrel software validation](#)  
[Paul Eggert](#)
- [Multics/UNIX Lessons](#)  
[Edward Rice](#)
- [Call for Papers, FICS 92, Singapore](#)  
[Harold Joseph Highland](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **A kludge too far? FAX-to-OCR-to-speech**

<[frankston!Bob\\_Frankston@world.std.com](mailto:frankston!Bob_Frankston@world.std.com)>

4 Sep 1991 22:55 -0400

In the New York Times, Sept 4th, there was a blurb titled "Fax Machines Are Getting a Voice". The article describes a product (from Malibu Software Group) that OCRs incoming FAXes and then converts them to speech. So one dictates a message to someone who enters it into a Word Processor and then prints it on paper, sends it as a FAX, it gets scanned into a computer, OCRed and then converts it (or something loosely related to the original) to speech.

Computers are wonderful, they allow one to keep layering technology on top of technology. Actually this is nothing new, bureaucracies have been using this kind of approach for many years.

There are many risks associated with situations in which the original rationale is lost as layers get added. Technology increases the opportunities and adds new elements of mystery and credibility to these kludges.

---

### ✂ LA Times Article on E-mail

Mike Kimura <MNK@PYXIS.RSG.hac.com>

Wed, 4 Sep 1991 16:20:00 PDT

On page 1 of the View section of today's (Wednesday, September 4, 1991) LA Times there is an interesting article written by Amy Kuebelbeck entitled:

#### Getting the Message

E-mail is fast and efficient. But it isn't always private -- and that can mean big trouble for users.

The article describes the growing use of E-mail in American business and describes how it is raising sobering questions about workplace privacy vs. accountability. It describes the risks of accidentally sending E-mail to the wrong person or to a huge list of people. It quotes several authors and professors. Some important advice was

- o Be careful about expressing emotion
- o Assume messages are forever

The article describes the lawsuits pending against Epson America and Nissan Motor Corp. USA. There is an interesting section on the LAPD's use of E-mail where the Christopher Commission, investigating the Rodney King beating, deemed about 700 messages improper apparently sexist or racist. Interesting reading considering it was written for the people who have probably never used E-mail.

Mike Kimura, Hughes Aircraft Company, mnk@rdac.dnet.hac.com

---

### ✂ Re: RISKS of using electronic mail

Brian Clapper <bmc@hutch.rabbit.com>

Wed, 4 Sep 91 17:45:24 EDT

In [RISKS-12.22](#), David Parnas writes about the electronic mail problems one incurs when changing jobs. I ran into the problem myself when I left my former employer; they refused to forward electronic mail for reasons that struck me as specious as best.

Establishing a location-independent personal communication system could solve the problem; however, I wonder who would be responsible for

maintaining such a system, assigning addresses, etc. In any case, I'm not sure it's necessary.

When I move my residence, I have many of the same problems with physical mail. The consequences of not forwarding my mail to my new residence can be catastrophic. The primary difference between that arena and the electronic one -- at least in the U.S. -- is that most physical mail can legally be transported only by a central postal authority. The postal authority currently allows me to instruct my old post office to forward all my mail to my new post office for a few months. Electronic mail "post offices" are typically the property of the owner of the machine; as demonstrated by Mr. Parnas's post, the owner really has no incentive to forward anyone's mail. Some do so as a courtesy; some flatly refuse. If the postal service were to stop forwarding mail (say, because it costs too much), the difference between these two situations would disappear.

In the physical world, I have two ways to ensure that I don't lose mail when I move. Each method has its analog in the electronic arena.

- 1 - I can have my old post office forward the mail during the transition period. In the electronic world, this is analogous to having my old employer forward my mail, which they may or may not do.
- 2 - Rent a post office box (from the postal service or from a private mail service company) before I move, and notify those who send me mail to use the post office box address instead. In the electronic world, this is analogous to opening an account on a public access computer system like CompuServe or The Well and notifying people to use that address instead.

In both worlds, #2 has a problem: I may forget to notify someone, and mail from that person will eventually be returned with an indication that the address is invalid. I'm not convinced that this problem is sufficiently serious to warrant restructuring the system. For the professional who needs a dedicated, reliable, permanent electronic mail feed, renting an electronic post office box can be viewed as a cost of doing business, much the way dues in professional societies are viewed. (I wonder what the IRS would do if I tried to write off a CompuServe account as a business expense?)

As an aside, the electronic world also provides a third alternative: I can buy a machine, contract with a supplier for a network feed, and establish my own "post office". That's a little hard to do in the real world.

The difficulties associated with changing one's address aren't new; changing the message medium doesn't change the problem. The risks that Mr. Parnas outlines don't seem to differ from risks we already accept when we deal with "real" mail.

Brian Clapper, Rabbit Software Corporation, Malvern, PA    bmc@rabbit.com

---

 **Re: RISKS of using electronic mail ... ([RISKS-12.22](#))**

David Parnas <parnas@qusunt.Eng.McMaster.CA>

Wed, 4 Sep 1991 22:38:05 -0400

[In response to Brint Cooper]

1) I do keep a mailing list and have notified all who are on it of my move. It is an obvious thing to do. However, I regularly get mail from people who are not on that list.

2) I personally feel no need for the kind of privacy that involves not having a personal net address. I would strongly oppose a requirement that every individual have such a personal address, but those who chose to have one should be able to have one.

Dave

---

### **✂ More on SSN risks**

Glen Osterhout <glen@tegra.com>

5 Sep 91 14:53:54 GMT

This article was taken from the new products section of the July/August issue of ISPNews. This company is apparently marketing a software product that incorporates a database of social security numbers!?

"Veris is a computer program designed for the financial institutions that need to verify social security numbers as part of their business. The product will determine if a number is valid for the person using it. Along with a valid number, the product lists the state or territory where it was issued and the year(s) in which that set of number series were issued. In the event of an invalid number, warning and advisory messages are given. The product runs on Macintosh and IBM PC compatibles or networks."

Glen Osterhout, Tegra-Varityper, Inc., Billerica, Massachusetts glen@tegra.com

---

### **✂ Universal Email addresses and SSN**

Jim Anderson <jim@saylor.saylor.mn.org>

Wed, 4 Sep 91 18:49:41 CDT

Somehow, I find a contradiction in the last couple Risks Digests. On one hand, we are told to protect our SSN, and that it is a BAD thing to use as a universal ID number. On the other hand, we have a message saying that we need a universal EMail addressing scheme. Why not combine the two and make your SSN the email address? Or if that isn't acceptable, how many 'universal' ids should we have?

Jim Anderson, Saylor's Software First, 6532 Edenvale Blvd, Eden Prairie, MN 55346 612-636-7451 jim@saylor.mn.org or jim@aob.mn.org

[Of course there is a contradiction. You cannot optimize for privacy and

universal accessibility at the same time. If a unique ID is used to link databases universally, that is risky. If a unique ID were used only for identification, then that has some merit. It is the controls on potential use that present the problems, not the unique identifier itself. PGN]

---

✂ **Re: "Thieves Hit Social Security Numbers" ([RISKS-12.23](#))**

<frankston!Bob\_Frankston@world.std.com>  
5 Sep 1991 09:40 -0400

Simple reason for less abuse of SSN's in Sweden? Less diversity and poverty? Be careful about generalizing across societies.

---

✂ **Re: National Character variations in ASCII ([RISKS-12.24](#))**

Jim Haynes <haynes@cats.UCSC.EDU>  
5 Sep 91 06:01:15 GMT

Perhaps it's worth discussing a bit of history here. One of the precursors of ASCII was a military character code called Fieldata. If I remember correctly this was an upper-case-only, and used 6 bits to represent all the printing characters. A seventh bit was part of the code (and there was a parity bit, so 8 bits were transmitted). At any rate a lot of the code combinations were deliberately left unassigned, so that designers of systems using Fieldata had plenty of codes available for control purposes, or for extra printable characters if they so desired.

The committee that designed ASCII decided this was not such a good idea, as different systems used different characters for the same purpose, or the same character for different purposes. They therefore took pains to insure that in ASCII every code combination was used for something, leaving no room for expansion. (That's not precisely true; ASCII was standardized in two phases, first upper-case-only and later upper-lower; and the character that prints as dollar sign in the U.S. was designated "currency symbol" so it could print a sterling sign in the U.K., or other signs in other countries; and there were a few others designated for national characters.)

When a character set is designed by a committee and ratified by majority vote, as was ASCII, there is naturally a certain amount of pushing and shoving to get various companies' favorite features in there. ASCII includes shift-out and shift-in characters, analogous to the figures and letters characters of Baudot, which could be used to shift to an alternate printable character set. It also includes escape, to mean that the following character(s) is not to be interpreted as ASCII. (There were some truly frightful proposals for getting back to ASCII after an escape, such as using a character with deliberate incorrect parity.) There are Cancel and Substitute; I've never heard anybody able to explain unequivocally exactly what they are supposed to mean.

Not that it matters much. Once the computer people got hold of ASCII they made up their own interpretations. Delete, the all 1s character, was intended for

erasing mistakes in paper tape. A character deleted this way should be simply ignored altogether; but the computer people gave it the entirely different interpretation of "discard the previous character." Backspace was meant to work exactly like backspace on a typewriter. With a hard copy terminal you could type o backspace / to get an o with a slant through it. But certain computer people decided to use backspace in the same way that others use delete; and few video terminals are able to do backspace and overstrike the way a hard copy terminal can. Control-C was meant to indicate the end of text in a message; but computer people widely use it to mean "interrupt the currently running program, or the program currently attached to the terminal." And so on, so in the end we have exactly what was had with Fieldata.

haynes@cats.ucsc.edu haynes@ucsccats.bitnet

---

### **✂ pork barrel software validation**

*Paul Eggert <eggert@twinsun.com>*

*Wed, 31 Jul 91 21:13:00 PDT*

Research in computer software validation is not immune to the increasing trend by the US government to fund projects for merits that are political, not technical. Eliot Marshall reports (*\_Science\_*, 19 July 1991, p. 257) that a bill passed by the Senate Appropriations Committee on 11 July includes \$10 million for a new software validation center at West Virginia University. It is not a coincidence that the committee is chaired by Robert Byrd (D-WV). Regardless of WVU's merits, the public would be at less risk if the government funded software R&D's best technical opportunities instead of succumbing to political opportunists.

Paul Eggert <eggert@twinsun.com>

[Yes, this item is over a month old -- I was finally trying to catch up with some of the backlog from my three-week absence. But it is still timely. NPR had a rather acerbic piece on 4Sep91 on some of Senator Byrd's successes in getting some substantial chunks of the USGovernment moved to West Virginia. PGN]

---

### **✂ Multics/UNIX Lessons**

*Edward Rice <Edward.Rice@p0.f716.n109.z1.fidonet.org>*

*04 Sep 91 19:56:27*

An article by Paul Stachour in the v12, n23 issue of RISKS DIGEST, contained several statements that I feel deserve comment. His recollection of the recognized need to filter out control sequences in inter-user messages is essentially correct, although the actual date may be a year or two later. The problem in question arose when Delta Data 4000 terminals capable of "smart answerback" were in use at the University of Southwestern Louisiana, and users were coding their login passwords into those answerbacks. Another issue, which was dealt with even later, was the concern that in a shared-terminal environment, a user could leave the terminal not with a logout, but by

executing a malicious program that would issue what appeared to be a standard system logout, appear to respond correctly to a new user, and would record the new user's name and password on behalf of the hacker. (It could then claim the password type-in was in error, issue a logout-with-no-messages, and let the real operating system respond correctly to the user's next attempt to log in.)

Paul's comments reflect the hindsight of the intervening years in two ways. First, his comments indicate that "Unix is supposedly an 'improved' derivative of Multics [sic]" is not correct. A tripartite design group consisting of General Electric, M.I.T., and Bell Labs designed the original Multics system; when it came time to start building Bell removed itself from participation in MULTICS, and developed UNIX as what it perceived a more cost-effective and achievable system. By then, Honeywell had acquired GE's large-scale computer division (and in a later acquisition of the rights to MULTICS, was required by M.I.T. to rename their operating system "Multics," for all you trivia fans) and continued with Multics for the next fifteen or so years. UNIX was indeed a derivative of MULTICS, but intended as a cut-down, quicker, less-elegant project better suited to Bell's needs. In later years, of course, UNIX was improved.

Second, "The mechanism by which Multics sends its mail and messages ... was well-designed to ..." gives somewhat too much credit to the design. The original Multics mail scheme not only permitted inter-user messages and mail to contain control characters, but used a shared-stored method of holding the messages while they awaited delivery that let message forgeries be as simple as using a text editor. Literally: in the original scheme, you could use a text editor to take a message that was "in transit" and freely change the contents, including sender ID and all other header fields. Security was enhanced, later, to provide for mailboxes that required outer-level operating system intervention to place or retrieve messages. In that development, undertaken in part to satisfy Air Force requirements for a secure, multi-security-level computer utility, the resolution to the smart terminal/control codes problem became feasible and was implemented. (The problem of forgery of the operating system's login sequence turned out to be a great deal more difficult, as it was a much simpler hack.)

Finally, the comment that "Multics source has always, to my knowledge, been publically available" requires comment. Paul's belief is not precisely correct, but it is true that Multics source has been available to users of the system and to the research community without major limitation. Within the Multics community, anything less than a complete willingness to hand critical code over to any hacker who asked for it was demeaningly referred to as "security through obscurity," and was avoided at all cost (generally, however, at NO cost, and often with distinct benefit).

Edward\_Rice@p4124.f716.n109.z1.fidonet.org

[By the way, you can probably still get a Multics from Bull, if you hurry. PGN]

---

## Call for Papers

"Dr. Harold Joseph Highland, FICS" <Highland@DOCKMASTER.NCSC.MIL>

*Wed, 31 Jul 91 11:39 EDT*

CALL FOR PAPERS  
THE IFIP/SEC'92 INTERNATIONAL CONFERENCE on COMPUTER SECURITY  
May 27-29, 1992 Singapore

The purpose of the 1992 International Federation for Information Processing Security Conference [IFIP/Sec'92] is to provide a forum for the interchange of ideas, research results, and development activities and applications among academicians and practitioners in information, computer and systems sciences. IFIP/Sec'92 will consist of advance seminars, tutorials, open forums, distinguished keynote speakers, and the presentation of high-quality accepted papers. A high degree of interaction and discussion among Conference participants is expected, as a workshop-like setting is promoted.

IFIP/Sec'92 is co-sponsored by The International Federation for Information Processing, Technical Committee 11 on Security and Protection in Information Processing Systems [IFIP/TC11] and The EDP Auditor's Association. IFIP/Sec'92 is organized by the Singapore Computer Society and IFIP/TC11 and is sponsored by the National Computer Board, Singapore, Singapore Federation of Computer Industry, Microcomputer Trade Association of Singapore and the EDP Auditors Association of Singapore

Because IFIP/Sec'92 is a non-profit activity funded primarily by registration fees, all participants and speakers are expected to have their organizations bear the costs of their expenses and registration. Presenters of papers will pay a reduced conference fee.

#### WHO SHOULD ATTEND

The conference is intended for computer security researchers, managers, advisors, EDP auditors from government and industry, as well as other information technology professionals interested in computer security.

#### CONFERENCE THEME

The Eighth in a series of conferences devoted to advances in data, computer and communication security management, planning and control, this Conference will encompass developments in both theory and practice. Papers are invited in the areas shown and may be theoretical, conceptual, tutorial or descriptive in nature. Submitted papers will be refereed, and those presented at the Conference will be included in the proceedings. Submissions must not have been previously published and must be the original work of the author(s).

The theme for IFIP/Sec'92 is "Computer Security and Control: From Small Systems to Large." Possible topics of submissions include, but are not restricted to:

- o Auditing the Small Systems Environment
- o Auditing Workstations
- o PC and Microcomputer Security
- o Security and Control of LANs and WANs

- o OSI Security and Management
- o GOSIP - Government OSI Protocol
- o Electronic Data Interchange Security
- o Management and Control of Cryptographic Systems
- o Security in High Performance Transaction Systems
- o Data Security in Developing Countries
- o Software Property Rights
- o Trans-border Data Flows
- o ITSEC (IT Security Evaluation Criteria - The Whitebook)
- o Database Security
- o Risk Assessment and Management
- o Legal Responses to Computer Crime/Privacy
- o Smart Cards for Information Systems Security
- o Biometric Systems for Access Control

#### THE REFEREEING PROCESS

All papers and panel proposals received by the submission deadline will be considered for presentation at the Conference. To ensure acceptance of high-quality papers, each paper submitted will be blind refereed.

All papers presented at IFIP/Sec'92 will be included in the Conference proceedings, copies of which will be provided to Conference attendees. All papers presented, will also be included in proceedings to be published by Elsevier Science Publishers B.V. [North-Holland].

#### INSTRUCTIONS TO AUTHORS

- [1] Three (3) copies of the full paper, consisting of 22-26 double-spaced (approximately 5000 words), typewritten pages, including diagrams, must be received no later than 1 December 1991. Diskettes and electronically transmitted papers will not be accepted. Papers must be sent to the Program chairman.
- [2] Each paper must have a title page which includes the title of the paper, full name of all authors, and their complete addresses including affiliation(s), telephone number(s) and e-mail address(es). To facilitate the blind review process, these particulars should appear only on a separate title page.
- [3] The language of the Conference is English.
- [4] The first page of the manuscript should include the title and a 300 word abstract of the paper.

#### IMPORTANT DATES

- o Full papers to be received by the Program Committee by 1 December 1991.
- o Notification of accepted papers will be mailed to the author on or before 1 March 1992.

- o Accepted manuscripts, in camera-ready form, are due no later than 15 April 1992.
- o Conference: 27-29 May 1992.

#### WHOM TO CONTACT

Questions or matters relating to the Conference Program should be directed to the Program chair:

Mr. Guy G. Gable  
Department of Information Systems and Computer Science  
National University of Singapore  
Singapore 0511  
Telephone: (65) 772-2864 Fax: (65) 777-1296 E-mail: ISCGUYGG@NUSVM

For information on any aspect of the Conference other than Program, panel, or paper submissions, contact the Conference Chair:

Mr. Wee Tew Lim  
Organising Chairman  
c/o Singapore Computer Society  
71 Science Park Drive  
The NCB Building  
Singapore 0511  
Telephone: (65) 778-3901 Fax: (65) 778-8221

Papers should be sent to:

The Secretariat  
IFIP/Sec '92  
c/o Singapore Computer Society  
71 Science Park Drive  
The NCB Building  
Singapore 0511

In the States and Canada, inquiries about the Conference can be sent to:

Dr. Harold Joseph Highland, FICS  
Chairman, IFIP/WG11.8 - Information Security Education and Training  
562 Croydon Road Elmont, New York 11003-2814 USA  
Telephone: 516 488 6868 Telex: 650 406 5012 [MCIUW]  
Electronic mail: Highland@dockmaster.ncsc.mil  
X.400: C=US/A=MCI/S=Highland/D=ID=4065012 MCI Mail: 406 5012



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 12: Issue 26

Friday 6 September 1991

## Contents

- [The Dead Sea Scrolls and Data Security](#)  
[Jerry Leichter](#)
- [Charging batteries](#)  
[Erling Kristiansen](#)
- ["Returns for Senders" \(US Postal Service handling of forwardings\)](#)  
[Dinah Wisenberg Brin in Common Cause](#)  
[via PGN](#)
- [Re: Portability of E-mail Addresses](#)  
[Robert Neff](#)
- [DDN Management Bulletin 84 on NIC transfer](#)  
[NIC](#)
- [Re: +&\\*#S](#)  
[David J. Fiander](#)  
[Tom Blinn](#)
- [Re: Story of O](#)  
[Will Martin](#)
- [Re: A number is no name](#)  
[Merlyn LeRoy](#)  
[Bob Frankston](#)
- [Re: RISKS of using electronic mail...](#)  
[Brinton Cooper](#)  
[Bob Frankston](#)
- [Re: National Character variations in ASCII](#)  
[Bob Frankston](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ The Dead Sea Scrolls and Data Security

*Jerry Leichter <[leichter@lrw.com](mailto:leichter@lrw.com)>*

*Thu, 5 Sep 91 22:04:34 EDT*

Today's New York Times contains a front-page article on an event also widely reported elsewhere: The use of a computer to "re-construct" one of the Dead Sea Scrolls.

As readers may recall, the Scrolls were found in a series of caves in the desert in Israel over forty years ago. Some of the Scrolls contain the earliest known texts of books of the Bible; at least one is apparently a sixth book of the Old Testament, which along the way was lost.

Control of the Scrolls was given to a small group of scholars, who've been slowly - very slowly - publishing them. Their practices have led to many protests by other scholars, who have been denied any access to the unpublished Scrolls - at this point, more than half of them.

While much of the material remains unpublished, the controlling group has published extensive concordances of most of it. (A concordance lists each word that occurs in the text, together with an indication of exactly where it occurs - i.e., it's a cross-reference map.)

A group at Union Hebrew College in Cincinnati realized that a concordance contains all the information necessary to reconstruct the text. They wrote a program for a Mac to do just that, and have just published their first reconstructed version of a previously-unpublished Dead Sea Scroll.

A controversy has, of course, been ignited by this action. The group that control the Scrolls claim this is plagiarism, for example.

What I find interesting about the whole business is the way it brings to attention the degree to which the widespread availability of computation make it very hard to release partial information. Partial information about some set of data usually implicitly constrains additional information about the same set of data, information that the releaser may not have intended to make release. Actually determining the implicitly-specified information may involve a very large amount of work - but computers make it quite practical.

This issue has, of course, come up before. Much work has been done on the problem of allowing access to broad statistics from large databases without allowing information about individual records to be determined. This work is too technical for most people to integrate.

The Reagan administration tried to create a new class of "unclassified by sensitive" information, which would be protected in some way because when pooled it could reveal valuable, perhaps classified, data. The broad mistrust of administration motives in the national security area, coupled with a lack of convincing examples, kept this from really entering the national consciousness either.

The Dead Sea Scrolls case is easy for people to understand - they can clearly see how the approach works. It will certainly be the example I use in the future for explaining the difficulty of security problems. How much of an impact it will have on people's understanding and views, I don't know - I suspect little. But a few more instances of this use of computers - perhaps in more threatening circumstances, for example a data-matching program that led to large numbers of IRS actions against "the common man" - and the impact could become significant. How people will react when the realization comes home, and what kind of protections they will want, I have no idea.

-- Jerry

---

## ✂ Charging batteries

*E. Kristiansen - WMS <EKRISTIA@estec.bitnet>*

*Fri, 06 Sep 91 08:51:51 CET*

We use several small, portable computers to control some mobile communication equipment. These computers are powered by rechargeable batteries.

We have had problems charging the batteries of some units, even some brand new ones. We consulted the supplier who told that the battery charging is UNDER SOFTWARE CONTROL, as is the charging indicator LED.

So, if you discharge far enough for the processor to stop operating, you can sometimes not charge the batteries! There is some bypass circuitry which allows very slow charging, it takes about 4 days to charge to operating condition. Since the LED is also non-operational, you do not know whether you are charging or not.

Erling Kristiansen, ESTEC, Noordwijk, The Netherlands.

---

## ✂ ``Returns for Senders'' (US Postal Service handling of forwardings)

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

*Fri, 6 Sep 91 10:38:39 PDT*

[The following article by Dinah Wisenberg Brin appeared in the July/August issue of the Common Cause Magazine, vol.17, no.4, pp.8-9, and is reprinted with permission of Deborah Baldwin, Common Cause, 2030 M St. NW, Washington DC 20036, 202-833-1200. PGN]

The U.S. Postal Service -- the butt of so many complaints about inefficient service -- is on its toes in one way the average mail recipient might not appreciate. The same system that enables the Postal Service to forward your mail to a new address also alerts scads of direct marketers -- from the folks at your favorite mail-order company to those pesky tricksters who say they have a special gift waiting if only you'll call - to your new whereabouts. The system seems to work for better and for worse. For better: You get the mail you want and the Postal Service saves time and money by not delivering mail to the wrong address. For worse: Junk mailers you never wanted to hear from discover your new address and waste no time making use of it.

Postal officials insist that they share change-of-address information only with those who already have your old address. But thanks to the large-scale selling and renting of customer lists among direct mail marketers, some companies that never knew you existed will have your particulars. The Postal Service forwards about 2.3 billion pieces of mail a year for the 40 million Americans who move annually, at a cost of some \$1 billion, says Bob Krause, director of the Postal Service's National Change of Address (NCOA) system.

Meanwhile 19 companies, including some of the largest direct-marketing list

management firms, pay the Postal Service an annual fee of roughly \$48,000 to receive computerized NCOA updates every two weeks. These "licensees" then provide the updated information to their customers, who pay for address changes for consumers already on their mailing lists.

The Post Office places great importance on keeping address-correction information secure, Krause says, and the licensees must follow strict guidelines on what they can do with it. They may not use the information to develop mailing lists. But direct marketers who properly obtain the information from the Post Office or its licensees can make it available to others with impunity.

Ann Zeller, vice president for information and special projects of the Direct Marketing Association, concedes that firms can buy names from a direct mailer who has a consumer's new address.

Evan Hendricks, editor of the Washington-based Privacy Times newsletter, is "very suspicious" of the system. Without realizing it, individuals who complete change-of-address cards are "permanently giving away their addresses to anyone who asks for them," he says, and that should be clearly explained on the card.

Of course a change-of-address card is only one of many methods direct mailers have for learning a person's new address. Those who would sell you their wares also mine motor vehicle records, voter rolls, magazine subscription bases, home purchase records and other sources.

There is a way out. Individuals who want their names removed from various mailing lists can contact the New York-based Direct Marketing Association, which runs a name and address "suppression" service. But, Krause notes, "If you buy something at your new address from any direct marketer, your name will be on a number of lists within weeks."

-- Dinah Wisenberg Brin (a freelance writer now living in Hollidaysburg PA)

---

## **✉ Re: Portability of E-mail Addresses**

*Robert Neff <neff@janus.Berkeley.EDU>*

*Thu, 5 Sep 91 15:17:57 -0700*

A previous post on this topic notes that in the snail-mail world we have one central Post Office, and they perform services for us such as mail forwarding, and that many companies do not extend such courtesies with E-mail.

In my view, there is no reason why should we expect private firms to provide us with a full service E-mail address. It is not their business. It is the business of the post office to forward the regular mail. If you want an E-mail service which will be a universal address, from one job to the next, then it is available on public access bulletin boards (or whatever you call them) such as the Well in San Francisco, or Portal Communications in the South Bay. Just have everyone send mail to you at those addresses, and have it forwarded to your work account automatically.

My point is that free access to the internet is a service we have all come to expect, even though we don't pay for it (at least not directly). If you really want the service, all the time, you'll have to pay for it.

-- Robert

[Several people noted that NIC.DDN.MIL provides a "whois" service. It seems appropriate that everyone should register, although its primary charter in the past has been to include all MILNET folks (and earlier, all ARPANET folks), and it is not at all clear what would happen if everyone in internetland were to register. I see that David Parnas is NOT listed, but I am, for example. If you wish to be added, send mail to NIC@NIC.DDN.MIL and see what happens. Following is an excerpt from the latest DDN bulletin, put out by DISA (formerly DCA), which suggests that the transition on 1 Oct 91 is supposed to be almost seamless... PGN]

---

## **DDN Management Bulletin 84**

*DDN Reference <NIC@NIC.DDN.MIL>*

*Wed, 4 Sep 91 13:28:18 PDT*

\*\*\*\*\*

DDN MGT Bulletin 84            DCA DDN Defense Communications System  
4 Sept 91                      Published by: DDN Network Info Center  
                                  (NIC@NIC.DDN.MIL) (800) 235-3155

DEFENSE DATA NETWORK  
MANAGEMENT BULLETIN

The DDN MANAGEMENT BULLETIN is distributed online by the DDN Network Information Center under DCA contract as a means of communicating official policy, procedures and other information of concern to management personnel at DDN facilities. Back issues may be read through the TACNEWS server ("@n" command at the TAC) or may be obtained by FTP (or Kermit) from the NIC.DDN.MIL host [192.67.67.20] using login="anonymous" and password="guest". The pathname for bulletins is DDN-NEWS:DDN-MGT-BULLETIN-nn.TXT (where "nn" is the bulletin number).

\*\*\*\*\*

The transition of the Network Information Center from SRI International in Menlo Park, CA, to Government Systems Inc. in Chantilly, VA, is officially scheduled for 1 October 1991. This includes the transition of services currently offered to DDN and Internet users by SRI, such as network/user registration, on-line information services, and Help Desk operations. SRI will continue to provide all NIC services, to include responding to all user calls and requests, until 30 September 1991.

DISA and GSI will make every effort to ensure a smooth and timely transition of NIC services from SRI. Network users should be minimally impacted. With a few minor exceptions, all on-line services currently offered by SRI will appear the same to the user when a

connection is established to the new (GSI) NIC host. These exceptions are due to the change from the TOPS20 operating system to the SunOS operating system. The new NIC host is a Sun 470 SPARCserver running SunOS 4.1. All users on the DDN and the Internet should carefully note the following changes:

Government Systems, Inc., Attn: Network Information Center,  
14200 Park Meadow Drive, Suite 200, Chantilly, VA 22021

Help Desk Telephone Numbers [after 1 Oct 1991]:

1-800-365-3642 (1-800-365-DNIC)

1-703-802-4535

Help Desk Hours of Operation: 7:00 am to 7:00 pm Eastern Standard Time

Fax Number: 1-703-802-8376

Network Address: 192.112.36.5 (NIC.DDN.MIL)

Root Domain Server: 192.112.36.4 (NS.NIC.DDN.MIL)

During the period of 26 to 30 September 1991 the ID (WHOIS) database will not be changed. All registration actions for this five day period will be suspended. This action is necessary in order to transfer the master database to GSI. Starting 26 September 1991, all U.S. mail and fax requests should be addressed to the GSI address and fax number shown above. All electronic mail requests should continue to be directed to the "HOSTMASTER" and "REGISTRAR" mailboxes at NIC.DDN.MIL. As appropriate, SRI will redirect electronic mail to GSI. On 1 October 1991 all registration activities will resume to include the normal generation of DDN TAC access cards. Currently-valid TAC access cards will remain valid until the normal expiration date.

IMPORTANT! Hosts not using the domain naming system should edit their host tables prior to 1 October 1991 to reflect the change in GSI's domain name DIIS.DDN.MIL (192.112.36.5) to NIC.DDN.MIL and delete the current NIC.DDN.MIL (192.67.67.20) from their tables. The GSI IP address, 192.112.36.5, will not change and may be used in lieu of the domain name. GSI will re-generate all informational and network tables (i.e., host tables) no later than 8 October 1991. All tables will be available using the same access method currently used to download from the SRI NIC.

We hope that the transition and its accompanying changes will not greatly inconvenience network users, and we thank you in advance for your patience and understanding. For general questions regarding the transition, users may call the new NIC Help Desk after September 1, 1991 at 1-800-365-3642. Questions regarding NIC operations policy should be referred to Mr. Wil Pitre of DISA/DODS at (703) 692-2771 (DSN) 222-2771. Questions regarding NIC contractual matters should be referred to Mr. Tyrone Smallwood of DISA/DISCA.

---

✉ **Re: +&\*#\$( [RISKS-12.21](#))**

"David J. Fiander" <david@scocon.sco.com>

Thu, 05 Sep 91 10:44:44 -0400

In Ontario, the "bizarre character" is a small crown. Every non-vanity plate has one, which is used as a separator between the first three-character group

and the second. However, the crown \_is\_ user-selectable in vanity plates, so it is quite possible to have a plate reading "M\*A\*S\*H" (where stars are substituted for the crowns). According to some local discussion, however, they are identical to spaces (but not identical to nothing). Hence "M\*A\*S\*H" == "M A S H" != "MASH".

You can guess how much trouble this causes.

David J. Fiander, SCO Mail Technology Group, SCO Canada, Inc.

---

**✉ More RE: +&\*#\$(RISKS DIGEST 12.21 et. seq.)**

*Tom Blinn <blinn@dr.enet.dec.com>*

*Thu, 5 Sep 91 17:30:55 PDT*

I was not aware that NH allows spaces in license plates (when I asked for the plate "DR TOM" I was told I could not have an embedded space, and got the plate "DR-TOM" instead; my NY plate used to be "DR BLINN", which I've embellished with a "::" to match my node/user name and have posted on the wall in my office). [...]

On the matter of unusual characters (both on and off license plates):

In New Hampshire, "handicapped" plates have a graphic representation of a wheelchair on them -- all the ones I've seen have it at the front, with a sequence of letters and digits following. I have no idea how this gets represented on, say, a parking ticket.

In Massachusetts, some plates have "EX POW" (stacked "EX" over "POW"), and then a three or four-character plate number. I somehow doubt the standard ticket blanks can readily record this, and I also doubt that the automated systems can easily cope with it -- especially outside Massachusetts.

And so on..

There's a rumor that John Sununu's personal NH license plate bears the legend "Fly Free or Drive", but I can't confirm that one, either..

Dr. Thomas P. Blinn, Digital Equipment Corporation, Digital Drive -- MKO2-2/F10  
Merrimack, New Hampshire 03054 ...!decwrl!dr.enet.dec.com!blinn (603) 884-4865

---

**✉ Re: Story of O**

*Will Martin <wmartin@STL-06SIMA.ARMY.MIL>*

*Thu, 5 Sep 91 10:30:03 CDT*

While Mr. O's particular problems may have been exacerbated by the referenced software that looks at "O" as part of "O<something>" names, I do find it surprising that single-letter last names would have not been considered and programmed for in current versions of software. How many years ago was it that Malcolm X was a national figure? There have been decades since then! Plenty of

time for the accommodation of such "initial-names" to have percolated throughout the banking/billing/governmental computer systems, one would think...

Or is it part of the mentioned ethnocentrism to assume that people with single-letter names would not wish to participate in the established economic and social systems? Someone who was angry enough to change their name to "X" wouldn't want a driver's license, or to borrow money, or to be on any computerized records or database? Seems a rash assumption...

Will

---

**✉ Re: A number is no name**

*Merlyn LeRoy <merlyn@digibd.com>*

*Fri, 6 Sep 91 14:15:12 CDT*

A similar case (somewhat earlier) of a Minnesota man who wanted to change to 1069; his legal name had to be One Zero Six Nine.

Merlyn LeRoy

---

**✉ Re: A number is no name ([RISKS-12.20](#))[EKRISTIA@estec.bitnet]**

*<frankston!Bob\_Frankston@world.std.com>*

*5 Sep 1991 09:35 -0400*

There is a proposed character set, Unicode, that is intended to encode all glyphs. That is a bit ambitious since a lobster picture will still present a problem, but does go a long way towards dealing with national alphabet problems.

Don't forget that Risks Digest is mired in limited AmericanSCII and thus cannot provide an effective representation for much that we talk about. Of course, we have some workarounds such as saying "Umlaut" (I can't even backspace to use a " as an umlaut as per ASCII conventions!).

---

**✉ Re: RISKS of using electronic mail, and universal addressing**

*Brinton Cooper <abc@BRL.MIL>*

*Wed, 4 Sep 91 13:13:07 EDT*

David Parnas writes:

What is needed is a personal communication system, one where the individual's address is independent of his (or her) location on the computer network...

Peter Neumann adds:

But it certainly would be nice...

Gee, fellows, it sounds very much like an Internet Social Security Number, and we've had endless discussions over the years about the computer-oriented (and other) risks of having and using universal identifiers!

In the context of "privacy," which also commands attention in this and other forums (fora?), perhaps one need only keep a list of those folks with whom he/she wishes to maintain communication and send them "change of address" notices.

\_Brint

---

### ✉ Re: RISKS of using electronic mail

<frankston!Bob\_Frankston@world.std.com>

5 Sep 1991 21:55 -0400

There is a simpler way to confuse electronic mail. Change your last name. Often happens when people get married. Trivial to overcome the problem, but my impression is that corporate mail managers don't think about these things.

A closely related issue is role vs personal addresses. In paper mail systems people will guess at whether mail is addressed to the current "Sales Manager" or the previous one. Email systems can force one to do it "right" by mindlessly forwarding based on the exact address given, but the corresponding social conventions don't exist -- people will bind to whichever address works once and irregardless of the official purpose of the given address (I call this the "turn left at the cow" syndrome). The Risk here is that the technology exists for a more elegant solution that the users are ready to understand.

---

### ✉ Re: National Character variations in ASCII ([RISKS-12.24](#))

<frankston!Bob\_Frankston@world.std.com>

5 Sep 1991 22:07 -0400

We have a curious mixture of various interpretations of ASCII. ^C, for example is ETX (End of Text) and has evolved into an interrupt key on some systems. But keys on a PC labelled ESC and Break (for example) have an obvious semantic meanings. Since ASCII is utterly meaningless in PC keyboard (VS TTY Keyboard) decoding, it is better design to feed into user's naive interpretations than to try to teach them arcane history. Actually, the battle between ASCII and UI designers has been going on for a long time. Back in the 60's the QED editor on the SDS-940 used mnemonic bindings of control keys (predated Emacs by nearly a decade). Of course, violating ASCII has its costs, the use of ^S/XON and ^Q/XOFF be Emacs is rather unfortunate.



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 12: Issue 27**

**Sunday 7 September 1991**

## Contents

- [Play the lottery via Nintendo](#)  
[Mike Cepek](#)
  - [Re: Salomon Brothers -- Database Design](#)  
[Jeff Berkowitz](#)
  - [The REAL RISKS and REWARDS of E-Mail](#)  
[Larry Press via Tom Lincoln](#)
  - [Re: ``Returns for Senders''](#)  
[Willis H. Ware](#)
  - [Re: +&\\*#&](#)  
[John Moore](#)  
[Andy Goldstein](#)
  - [Re: A number is no name](#)  
[RMRichardson](#)  
[Bob Frankston](#)
  - [Re: Unusual characters in addresses](#)  
[David Lamb](#)
  - [Re: A permanent EMAIL address](#)  
[Mike Van Pelt](#)
  - [Re: RISKS of using electronic mail''](#)  
[David Parnas](#)  
[John Sloan](#)
  - [Re: The Dead Sea Scrolls and Data Security](#)  
[Chuck Karish](#)
  - [Re: WHOIS](#)  
[David A. Curry](#)  
[Chuck Karish](#)
  - [A better model for cracking](#)  
[Scott Draves](#)
  - [Prize for Most Useful Computer Virus](#)  
[Cliff Stoll](#)
  - [15,000 Cuckoo Letters \[Another RISK OF EMAIL?\]](#)  
[Cliff Stoll](#)
  - [Info on RISKS \(comp.risks\)](#)
-

## **Play the lottery via Nintendo**

"Mike Cepek, MGI" <cepek@vixvax.mgi.com>

Fri, 06 Sep 1991 18:23:01 CDT

[ From the Minneapolis Star Tribune, 1-Sep-1991, Section B. I will let it speak for itself. See if you can keep from laughing. - mkc ]

### LOTTERY MAY USE NINTENDO AS ANOTHER WAY TO PLAY

Several kinks have yet to be worked out

[...] Minnesota gamblers soon could be winning jackpots as early as 1993 from the comfort of their own living rooms... the state will begin testing a new system next summer that will allow gamblers to pick numbers and buy tickets at home by using a Nintendo control deck. [...] The system, to be created by the state and Control Data Corp., would be somewhat similar to banking with an automated teller machine card. Gamblers would use a Nintendo control deck and a state lottery cartridge [...] The cartridge would be connected by phone to the lottery's computer system, allowing players to pick Lotto America, Daily 3 and Gopher 5 numbers, and play the instant cash games. Players would gain access to the system by punching in personal security codes or passwords. Incorrect passwords would be rejected. Only adults would be allowed to play. [...] A number of kinks, including setting up a pay-in-advance system for players to draw on, computer security and adult registration, must be worked out. [...] 32% of Minnesota households have Nintendo units. About half of those who use the units are older than 18 [...] [...] Those chosen to participate [in the summer experiment] will be given a Nintendo control deck, phone modem and lottery cartridge.

---

## **Re: Salomon Brothers -- Database Design ([RISKS-12.24](#))**

<jjb@sequent.com>

Sat, 7 Sep 91 22:35:58 GMT

>The recent Salomon Brothers securities scandal was caused in part by sloppy  
>database design according to an employee in the database programming department...

I can't let this this abuse of the concept of "responsibility" go by. Saying that Salomon's DB programmers in any way "caused" the scandal, even "in part", is like saying that police "caused" an automobile accident because they didn't happen to catch the speeder before s/he hit somebody! After all, the police \*do\* have "responsibility" for catching speeders.

It is incredible to me how we have moved away from the concept of individual responsibility and toward reliance on various societal "mommies and daddies" to watch over behavior. I can't help but think that our newfound ability to create computerized "mommies" encourages this trend.

Jeff Berkowitz, Sequent Computer Systems: uunet!sequent!jjb or jjb@sequent.com



## The REAL RISKS and REWARDS of E-Mail (By Larry Press)

Tom Lincoln <lincoln%iris@rand.org>

Fri, 06 Sep 91 21:19:16 PDT

The LA Times of Sept 6 ran an article on the DEMOS network in Moscow as it operated during the coup attempt. Larry Press, who played a major role, felt that this article did not do justice to the full set of facts. Here is his version:

----- Forwarded Message

Date: Fri 6 Sep 91 11:46:51-PDT

From: Laurence I. Press <LPRESS@ISI.EDU>

To: lincoln%iris@rand.org

Copyright, Larry Press, August 26, 1991, do not reproduce or quote without permission. This file may be forwarded around the net as long as this note is attached.

A Computer Network for Democracy and Development  
Larry Press

"Oh, do not say. I've seen the tanks with my own eyes. I hope we'll be able to communicate during the next few days. Communists cannot rape the Mother Russia once again!"

This message was sent from Moscow at 5:01 AM on August 19. It was written by 26 year-old Vadim Antonov, a senior programmer at the Demos Cooperative in the Soviet Union. Demos operates a computer-based communication network which spans the Soviet Union, and within a few hours, Vadim's message had been relayed to computers in 70 Soviet cities from Leningrad in the West to Vladivostok in the East.

The message had also been sent to a computer in Helsinki Finland, which is connected to the non-Soviet computer networks. From Finland, the message was relayed to networks such as The Internet, serving millions of users on all continents. Seconds after it reached Finland, I could read it at my computer in Los Angeles, California. The message was particularly important to me because the week before the coup attempt I had been in Moscow and spent several days with Vadim and his colleagues at Demos. We met professionally and as friends.

Demos' RELCOM (RELIable COMmunication) network celebrated the first birthday of its link to Finland on August 22. During that first year, RELCOM spread to 70 Soviet cities, and over 400 organizations were using it -- universities, research institutes, stock and commodity exchanges, news services, high schools, politicians, and government agencies. As is typical with computer networks, noone knows how many users RELCOM actually reaches.

During the Coup

During the days of the coup, RELCOM was pressed into service in support of the

constitutional government. The junta moved quickly to control mass media. When I learned of the coup, I immediately sent a worried message to Vadim's wife Polina Antonova, who also works at Demos. I did not receive her answer until August 20 at 12:17 AM Moscow time:

"Dear Larry,

Don't worry, we're OK, though frightened and angry. Moscow is full of tanks and military machines -- I hate them. They try to close all mass media, they stopped CNN an hour ago, and Soviet TV transmits opera and old movies. But, thank Heaven, they don't consider RELCOM mass media or they simply forgot about it. Now we transmit information enough to put us in prison for the rest of our life.

Greetings from Natasha.

Cheers,  
Polina."

The Demos staff had learned of the coup around 6 AM on the 19th, and immediately began sending political information to the Soviet Union and the outside world. By 12:30 PM, Moscow time, I was reading news releases from the independent Soviet news agency Interfax. Although outlawed by the junta, news from Interfax, the Radio Moscow World Service, the Russian Information Agency, Northwest Information Agency (Leningrad), and Baltfax was disseminated by RELCOM throughout the coup attempt.

RELCOM also distributed news from official sources opposed to the coup. For example, a copy of the letter Boris Yeltsin read from a tank turret in front of the Russian Parliament building was brought to Demos headquarters (a short trip), entered into a computer, and forwarded across the network. By early evening, several people in the United States had also translated it, and an English-language version was broadcast to the non-Soviet networks.

There were also many eye-witness reports. Pay phones were working in Moscow, and people in the streets could phone news in. At one point, Polina told me she was leaving for the Russian Parliament Building with a portable computer so she could report from there. Later I learned that she had not gone because the phone service to the building was unreliable.

Of course all the news did not come from Moscow. The network was buzzing with reports and official notices from Leningrad, Kiev, the Baltic capitals, and many other Soviet cities.

News also came in from the West. I wrote regular summaries of the news as broadcast on radio and television in the United States. Jonathan Grudin, a colleague in Denmark, did the same for BBC news. Regular reports were also posted from Finland, giving both Finnish and Baltic news summaries. These were translated into Russian by Polina and others, and transmitted throughout the Soviet Union.

Western news was welcome, but the link to Finland became a bottleneck. Before the coup, 6,000 messages were passed between Finland and RELCOM on a typical

day. After the coup began, traffic increased substantially, prompting Vadim to broadcast this message at 6:44 PM on the 19th:

"Please stop flooding the only narrow channel with bogus messages with silly questions. Note that it's neither a toy nor a means to reach your relatives or friends. We need the bandwidth to help organize the resistance. Please, do not (even unintentionally) help these fascists!"

This plea notwithstanding, traffic rose to a high of 13,159 messages on the 21st.

While news of tank movements, demonstrations, and official political statements was of practical value, it also provided emotional support. When the coup was finished, and there was time to rest, I received a message from Polina that said in part "You can't even imagine how grateful we are for your help and support in this terrible time! The best thing is to know that we aren't alone." That message paid me 1,000 times for the hours spent at my computer keyboard.

#### Danger

At the beginning of the coup, memories of the Hungarian revolt, Kruschew's ouster, the Prague Spring, and Tiananmen Square did not give one much hope. Had the coup succeeded, the Demos staff and people using their network would have been in great danger. As Vadim noted in a message to Doug Jones, a professor at the University of Iowa:

"If these dogs win, for certain they'll throw us in prison -- we distributed the proclamation from Yeltsin and the Moscow and Leningrad Soviets throughout the entire Soviet Union, together with the forbidden communiques from Interfax ... Greetings from the underground."

Demos headquarters is in a small building near the Kremlin. The KGB knew of RELCOM, and had they decided to, they could have easily shut the network off early in the coup. When a friend asked why they didn't, Polina replied "Thank Heaven, these cretins don't consider us mass media!" After the coup, she and others speculated that the KGB was generally passive because they were not confident the coup would succeed.

Sensing danger, the Demos staff arranged for backup computers to substitute for the vulnerable headquarters machine if necessary. On the 20th at 8:30 PM Moscow time, Vadim sent this message to Doug Jones:

"Yes, we already prepared to shift to underground; you know -- reserve nodes, backup channel, hidden locations. They'll have a hard time catching us! Anyway, our main communication line is still open and it makes us more optimistic."

They not only hid the computers, many people left Demos headquarters and communicated from their homes and other locations. Polina told me:

"Don't worry; the only danger for us is if they catch and arrest us, as we are sitting at home (valera is at Demos) and distributing all the information we have."

When the coup was finally defeated, George Tereshko, broadcast the following thanks for the risk taken by the Demos staff:

"When the dark night fell upon Moscow, RELCOM was one source of light for us. Thanks to these brave people we could get information and hope."

Of course, for now, the story appears to have had a happy ending. At 3:07 PM on the 21st, I received this from Polina:

"Really good news. Right now we're listening to Radio Russia (without any jamming!); they told that the eight left Moscow, noone knows where ... Hard to believe ... Maybe, they've really run away?"

And on the 22nd at 1:31 PM she wrote:

"Now Vadim and I have to do our usual work (that's so nice!) and Valera and Mike Korotaev went to sleep. They were on duty the whole night. Now there is celebration in Moscow. We just watched president Gorbachev on TV."

#### RELCOM in Peace Time

In the past, a network like RELCOM would have been prohibited in the Soviet Union. Like any communication media, it is incompatible with repressive dictatorship. Gorbachev's Glasnost made RELCOM possible, and in one year, it became a significant segment of the Soviet communication infrastructure.

Part of the reason for RELCOM's success is the fact that postal and telephone service in the Soviet Union are poor, making electronic mail very attractive. Another element of their success is that they use low-cost, appropriate technology. The primary technology used by RELCOM is the voice phone system, low cost modems, and standard personal computers. The final element in their success is the people at Demos. They are very skillful as technicians and as entrepreneurs (Demos is 100% free enterprise), yet they are different than their counterparts in the United States. They are more idealistic and less competitive. If they were in the US, my guess is they would either be graduate students in computer science or they would be driving BMWs and sipping Perrier.

As such, RELCOM may be a good model for other countries with poor telephone and postal systems, little capital, and well educated, motivated young professionals. Networks like RELCOM, probably using satellite technology, may change the face of the earth in peace time as well as helping to keep the peace.

[Larry Press is Professor of Computer Information Systems at California State University at Dominguez Hills. He has visited Chile several times, most

recently as an organizer of the EIES held last July. The week before the coup, Press co-chaired a conference on human-computer interaction in Moscow. While there, he spent several days visiting the Demos Cooperative, which operates RELCOM, an important Soviet computer network. During the coup, he relayed news to his friends at Demos.]

---

**✉ Re: "Returns for Senders" ([RISKS-12.26](#))**

"Willis H. Ware" <[willis@rand.org](mailto:willis@rand.org)>

Fri, 06 Sep 91 15:11:26 PDT

I'm afraid that the author chases a vacuous ghost. She apparently doesn't really understand how the direct mail business works but evidently hopped onto a seemingly significant process. The true situation is the quote from Krause in the final paragraph.

Her facts are correct but the implications are not. If one moves, there will be some collection of mail that he will want forwarded. Among the set will be journal and technical magazines subscriptions, favorite mail order outlets, the family's hobby magazines, the children's items, charitable organizations that one supports and wishes to hear from, -- on and on.

Address information is traded and exchanged on a huge basis and any legitimate address change will readily and quickly find its way into the whole direct mail system.

Try the following experiment. Move but have no mail forwarded to the new residence; route it to a POBox. Then place just one order from some mail order house and have it delivered to the new residence address. Sit back and log the buildup of direct-mail materials. It will startle you how quickly your address gets around.

Such a phenomenon is of course the fallacy, if not silliness, of writing to the Direct Mail Marketing Association and asking to be removed from circulation. It will only do some good if one also forswears to never again order anything by mail.

The most that the USPS update-list sales will do is possibly shorten the response time of updating mailing lists -- although it isn't certain that the USPS is indeed swifter than other methods; and it facilitates the job of the list maintainers by providing material in machine readable form from a single source. These are, to be sure, important points but not the ones that the author identified in the article.

For an extensive treatment of direct mail marketing and its list ramifications, see the report of the Privacy Protection Study Commission.

Willis H. Ware

---

**✉ Re: +&\*#\$([RISKS-12.21](#))**

<anasaz!qip!john@asuvax.eas.asu.edu>

Sat, 7 Sep 91 00:15:37 -0700

As a ham radio operator, for years I have had an amateur radio license plate. In the late '60s, when motor vehicle departments were first computerizing, I was pulled over one night by a policeman. When I asked why he had stopped me, he said that my license number was not valid - the computer (in Topeka, KS) would not accept a license number of WA0DVD - although I suspect that this same computer had originally issued the registration. This took some explaining, and if the police dispatcher that night had not been a friend of mine I might have had an even tougher time of it.

John Moore anasaz!john@asuvax.eas.asu.edu

---

**RE: +&\*#&**

Andy Goldstein - VMS Development 06-Sep-1991 1609 <goldstein@star.enet.dec.com>

Fri, 6 Sep 91 22:15:20 PDT

Bob Frankston's posting about strange characters on New Hampshire license plates reminds me of one of the little bits of dirt that came out about the Ed King administration in Massachusetts back when Dukakis was elected for the second time. Seems the registry of motor vehicles had been issuing special license plates to friends of the governor that contained stars, squiggles, and other symbols expressly chosen because they had no representation on the registry's computer system. Talk about diplomatic immunity!

---

**Re: A number is no name (Frankston, [RISKS-12.26](#))**

<RMRichardson.OSBU\_North@xerox.com>

Fri, 6 Sep 1991 20:00:02 PDT

> There is a proposed character set, Unicode, that is intended to encode  
> all glyphs.

Sorry, this is not quite correct. Unicode is an attempt at a universal character set, not a glyph set. In some cases a Unicode character may be represented by more than one glyph; choosing which glyph is then a rendering (font, maybe?) problem.

Rich

---

**Re: A number is no name ([RISKS DIGEST 12.26](#))**

<frankston!Bob\_Frankston@world.std.com>

7 Sep 1991 01:31 -0400

I was, perhaps, a bit sloppy in my use of the term "glyph". I did indeed mean to say that each numeric code stood for a canonical character not a rendering. Unicode is a great improvement over ASCII but doesn't solve all the encoding

and representation problems. While Unicode doesn't preserve font distinctions it does preserve case distinctions but sometimes the case distinction is not significant but the font distinction might be or the shading or ...

---

**✉ Re: Unusual characters in addresses (Re: [RISKS-12.26](#))**

*David Lamb <dalamb@avi.umiacs.umd.edu>*

*7 Sep 91 12:25:15 GMT*

Regarding the discussion of unusual characters in licence plates: it's not surprising there should be difficulties interfacing with the "real world" when we can't even interface with our technically-defined software world. Back in the late 70's and early 80's I maintained Carnegie-Mellon's RDMAIL system; when we shifted to supporting RFC733, we implemented the whole thing (there was even a hack for handling :postal:) except for retrieving foreign mailing lists on :include:. We immediately broke most other mailers on the net, and got so much flack that we had to turn off half the stuff in the RFC for outgoing mail. I wasn't too surprised that folks didn't want to parse :include:, but was a bit more suprised nobody wanted to handle spaces in names (at the time we were the only site we knew of that would let your mail name be "David Lamb@cmu-10a" (if that's who you really were, of course)).

I'm not sure what this has to do with RISKS, unless it's something along the line of "forall x,y, x wants y to adhere to x's standards".

---

**✉ Re: A permanent EMAIL address**

*Mike Van Pelt <mvp%hsv3@apple.com>*

*Fri, 6 Sep 91 19:21:27 PDT*

One way to have a permanent email address is to subscribe to one of the more stable and inexpensive services (say, The Well) and put in a .forward file to wherever you happen to be at the moment. If you change jobs, delete the .forward file and read your mail on the public access site until you get a new address.

---

**✉ Re: "risks of using electronic mail" ([RISKS-12.26](#))**

*David Parnas <parnas@qusunt.Eng.McMaster.CA>*

*Fri, 6 Sep 1991 17:31:09 -0400*

The discussion of "risks of using electronic mail" that I started, began at the trivial level and seems to be descending even further. I wished to remind users of a simple risk, not to suggest that an employer had any obligation for forward the mail of former employees or that there was no solution for people who had advance warning that they would be leaving. Those things are obvious.

There is however one difference between the situation with "snail mail" and that for electronic mail. In the former case it is not necessary that the

owner or new occupant of your house or apartment be cooperative. In the electronic mail situation they are involved. They can discard your mail, store it in a deep electronic well, read it, respond to it, etc. If you tell your snail mail service that you are moving, the new occupants need not be involved at all and cannot intercept your love letters.

Dave

[Well, mail for the former occupant tends to get (mis)delivered anyway, including after the one-year forwarding expires. Worse yet, my mailman apparently cannot read English, although he is pretty good at numbers. I often get mail for neighboring streets for which the street number matches! PGN]

---

**✉ Re: RISKS of using electronic mail (Cooper, [RISKS-12.26](#))**

*John Sloan <[jsloan@niwot.scd.ucar.EDU](mailto:jsloan@niwot.scd.ucar.EDU)>  
Sat, 7 Sep 91 10:05:05 MDT*

Will we have this same discussion ten years from now when cellular phones are cheap, and the expanded cellular communications infrastructure means we all have one in our hip pocket? Our cellphone numbers won't be tied to geographic locations, as they are with wired telephones, but rather associated with an individual. I have a bad feeling that we'll all be arguing about the risks of universal identifiers like SSNs while publishing our universal telephone numbers in our network signatures. (We'll also need voice mail built into those hip pocket cellphones!)

John Sloan NCAR/SCD, P.O. Box 3000, Boulder CO 80307 +1 303 497 1243

---

**✉ Re: The Dead Sea Scrolls and Data Security (Leichter, [RISKS-12.26](#))**

*Chuck Karish <[mindcrf!karish@decwrl.dec.com](mailto:mindcrf!karish@decwrl.dec.com)>  
Sat, 7 Sep 91 16:22:39 PDT*

A security system that implements the 'born classified' doctrine must try to deny access to information which, if properly related to other marginally sensitive information, will allow conclusions to be drawn which will compromise the national interest. The act of declaring a particular piece of information to be sensitive alerts the bad guy to its importance. Since the information is protected by only the very lowest levels of national security restrictions, it is likely to be available to moderately well-connected information brokers.

Two consequences: First, modest restrictions on the availability of data impact the ordinary citizen's access to information about how the world works much more than it protects 'us' from the bad guys. Second, material that's completely innocuous must also be declared sensitive, to avoid giving the bad guys information about which data the security establishment considers to be important and providing them with a starting point in using the powerful correlation techniques that will turn these hints into solid intelligence.

Note that I use this last word in a technical sense; no judgement as to the wisdom of playing this game is intended.

---

**✂ Re: WHOIS**

"David A. Curry" <davy@ecn.purdue.edu>  
Fri, 06 Sep 91 21:02:56 -0500

You're going to have the NIC very mad at you; registrations for WHOIS are sent to REGISTRAR@NIC.DDN.MIL, not NIC@NIC.DDN.MIL. Furthermore, there is a special template to use. I presume the newest template is in the NETINFO: directory somewhere; here's a slightly old one:

FULL NAME:  
U.S. MAIL ADDRESS:  
PHONE:  
AUTHORIZING HOST:  
PRIMARY LOGIN NAME:  
PRIMARY NETWORK MAILBOX:  
ALTERNATE NETWORK MAILBOXES (if any):  
MILNET TAC ACCESS? (y/n):  
TERMINATION DATE:

--Dave

---

**✂ Re: whois ([RISKS-12.26](#))**

Chuck Karish <mindcrf!karish@decwrl.dec.com>  
Sat, 7 Sep 91 16:22:39 PDT

My understanding of the charter of the `whois' database is that it is meant to provide a directory of the people who make the Internet work, not of all the people who use the Internet. I'm in the database because I'm the zone technical contact for the mindcraft.com domain.

The NIC is not in the business of providing a directory service for everyone on the Internet. Maybe there's a business opportunity here ...

Chuck Karish, Mindcraft, Inc karish@mindcraft.com (415) 323-9000

---

**✂ a better model for cracking**

<Scott\_Draves@WOOZLE.GRAPHICS.CS.CMU.EDU>  
Sat, 07 Sep 91 13:34:54 -0400

Cracking systems is often called the electronic equivalent of breaking and entry. I'd like to propose another model:

Say I telephone your residence, and your six year old child answers. I tell her to go to a filing cabinet, and retrieve a document. She does so. I tell her to read the document to me over the phone. She does so. I hang up.

Models like these are an important part of deciding how to penalize crackers. We must be careful to base our laws on the right model.

My opinion is that organizations (eg att) are using the "breaking and entry" model to shift public perception of the problem. Instead of "our vulnerable systems are being compromised" we have "our systems are being victimized by criminals".

---

### ✂ Prize for Most Useful Computer Virus

*Cliff Stoll <stoll@ocf.Berkeley.EDU>  
Sun, 8 Sep 91 00:33:24 -0700*

Prize for Most Useful Computer Virus

Computer virus specialist Fred Cohen writes an intriguing article in the September/October 1991 issue of The Sciences (published by the New York Academy of Sciences). In short, Dr. Cohen describes ways in which computer viruses and virus-like programs can be beneficial.

These include automated bill-collectors, where, "each bill collector virus is a small program designed to collect one bill"; this program modifies itself depending on the debtor's response. Another instance is maintenance viruses which dispose of temporary files or hung programs.

Dr. Cohen has published "A Short Course on Computer Viruses". Curiously, his publisher is offering a \$1,000 prize for the most useful computer virus. However, "contest rules prohibit any entries that have been released into a computing environment without the permission of the owner or without mechanisms to control their spread"

He points out that malicious and unauthorized viruses have given a bad name to viruses. I'll say! Strangely, though, I've heard less of viruses in the past year than in years past. I wonder if the fad is finally passing?

-Cliff Stoll    cliff@cfa.harvard.edu

[Cliff, I guess you have not been reading VIRUS-L, which documents the continuing incidents and the continuing proliferation of new strains. PGN]

---

### ✂ 15,000 Cuckoo Letters [Another RISK OF EMAIL?]

*Cliff Stoll <stoll@ocf.Berkeley.EDU>  
Sun, 8 Sep 91 00:29:08 -0700*

In 1989, I wrote, "The Cuckoo's Egg", the true story of how we tracked down a computer intruder. Figuring that a few people might wish to communicate with me, I included my e-mail address in the book's forward.

To my astonishment, it became a bestseller and I've received a tidal wave of

e-mail. In 2 years, about 15,000 letters have arrived over four networks (Internet, Genie, Compuserve, and AOL). This suggests that about 1 to 3 percent of readers send e-mail.

I've been amazed at the diversity of the questions and comments: ranging from comments on my use of "hacker" to improved chocolate chip cookie recipes. Surprisingly, very few flames and insulting letters arrived - a few dozen or so.

I've tried to answer each letter individually; lately I've created a few macros to answer the most common questions. About 5% of my replies bounce, I wonder how many people don't get through.

I'm happy to hear from people; it's a gas to realize how far the book's reached (letters from Moscow, the South Pole, Finland, Japan, even Berkeley); but I'm going to spend more time doing astronomy and less time answering mail.

Cheers, Cliff Stoll [cliff@cfa.harvard.edu](mailto:cliff@cfa.harvard.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 12: Issue 28**

**Monday 9 September 1991**

## Contents

- [FAA on 755 thrust reversers](#)  
[PGN](#)
- [Inmate, working for TWA, steals credit card numbers](#)  
[Rodney Hoffman](#)
- [Re: Salomon Brothers -- Database Design](#)  
[William Dye](#)
- [Fax machine IDs](#)  
[Robert Morris](#)
- [Re: Unusual characters in addresses](#)  
[Bob Frankston](#)
- [Failsafe mode for 3.5" Floppies](#)  
[Don Phillips](#)
- [Re: The RISKS of Superiority](#)  
[John Hobson](#)
- [Re: A Danger ... with Intelligent Terminals](#)  
[Randolph Bentson](#)
- [Risk assessment: a specific experience](#)  
[Mark Fulk](#)
- [Re: Risk Perception](#)  
[Geoff Kuenning](#)  
[Chuck via Phil Agre](#)  
[David Chase](#)  
[Dan Drake](#)  
[Craig Partridge](#)  
[William P Gardner](#)  
[Phil Agre](#)  
[Fred Heutte](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **FAA on 755 thrust reversers**

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Mon, 9 Sep 91 10:23:36 PDT

Today's New York Times notes that the Federal Aviation Administration is expected this week to require changes to the design of the engine thrust reversers on some Boeing 757s, based on computer simulations at Boeing that indicate "the accidental activation of thrust reversers could be a far worse problem than previously believed." That is, the plane may not be aerodynamically controllable, despite previous thinking. The cause of the crash in Thailand is still unknown, however.

---

**✂ Inmate, working for TWA, steals credit card numbers**

*Rodney Hoffman <Hoffman.El\_Segundo@Xerox.com>  
Mon, 9 Sep 1991 07:58:58 PDT*

Writing in the September 8, 1991 'Los Angeles Times' (page A3), Mack Reed reports that Carl Simmons, a 20-year-old California Youth Authority inmate, working as a TWA telephone reservation agent, stole dozens of customer credit card numbers and used them for thousands of dollars of personal charges. He is now serving two years in state prison for the thefts.

TWA has used CYA inmates in a special program since 1986. The story says the program "has been touted as a way to help young criminals learn a trade and repay their debt to society. It has raised more than \$500,000 for victims' restitution and the cost of incarceration. And the program's 213 graduates, many of whom now work at airlines and travel agencies, are one-tenth as likely to commit new crimes as nongraduates, CYA officials said." [Sure makes ME feel secure about making airline reservations!]

CYA has tightened security, including more frequent searching of rooms and occasional strip-searches. Inmates have always been forbidden from taking pen and paper into the computer room, and now not even instruction manuals can be taken out. But Simmons and another inmate said that won't stop inmates from stealing card numbers or illegally charging airline tickets.

Fred Mills of the CYA says, "There's always going to be an exception, but 99.9 times out of a hundred in a program you're not going to get that. For every person we can keep out of the institution for a year, that's saving the state about \$31,000. That's the thing we have to look at and balance."

One victim, New Hampshire businessman Phillip Parker, said, "I don't want to begrudge someone a chance to make it back into a productive life, but giving them a chance where there's a significant amount of potential for financial fraud or risk -- maybe there's other things that would make more sense."

TWA says it will now re-evaluate the program.

---

**✂ Re: Salomon Brothers -- Database Design ([RISKS-12.24](#))**

*William Dye <wdye@cse.unl.edu>  
Mon, 9 Sep 1991 18:14:41 GMT*

Jeff Berkowitz writes:

>It is incredible to me how we have moved away from the concept of individual  
>responsibility and toward reliance on various societal "mommies and daddies" to  
>watch over behavior.

Bravo. The database programmers made a mistake. The Salomon traders committed a crime.

---

### **✂ Fax machine IDs**

*Robert Morris <ram@cs.umb.edu>  
Sun, 8 Sep 91 20:10:04 EDT*

Recently I faxed highly confidential information to a bank. Following their instructions, I telephoned their switchboard and asked for the extension with the fax machine on it, then connected my fax and sent my material. I telephoned a few minutes later to verify that my material had arrived and it had. The arrangement was slightly annoying because my "manual" long distance call had to wait on hold for several minutes (at my expense) waiting for the fax to become free. Shortly afterwards, I needed to send additional material to the same fax machine. Thinking myself quite clever, I simply telephoned the number with which the first fax identified itself (it was in the right area code and central office, so I assumed it was really the same machine). My machine connected to a fax at that number and my new material was transmitted. But it was never received at the bank! The bank's fax was identifying itself with the number of another machine (the fax machine vendor who delivered the machine configured for testing? a fraudulent information thief? I have no idea, but in retrospect I can see that one machine was identifying itself with the number "aaabbbccccc" and the other "aaa bbb cccc").

Fortunately for me, my second transmission was not sensitive information. It's also true that I did not follow the bank's instructions in sending the second fax. But in any case, as with "automatic replies" to email, it is clear that a fax sender is at risk sending to a telephone number with which a machine identifies itself. And the owner of a fax machine might potentially be liable for the consequences of a machine mis-identifying itself.

By the way, another small risk became evident in this case. In order not to bill the owner of the sending fax, I made the call using the local access number of my long distance calling card. The fax audit report produced by the Canon fax machine reflected the answering (long distance) fax machine number, not the local number I actually called. That number will not appear on the telephone bill of the originating fax, and it may be difficult to reconcile the fax audit trail with the telephone bill.

[Nice opportunity for scams with call forwarding, user settable identifications, hidden twin-tailed conferencing, etc. PGN]

---

### **✂ Re: Unusual characters in addresses (Re: [RISKS-12.26](#))**

<frankston!Bob\_Frankston@world.std.com>

8 Sep 1991 22:37 -0400

The issue of spaces in a name deserves a long (and thoughtful) response because it gets into serious issues of representation. But I'll be (relatively) brief.

One cause is the accidental sharing of command line parsers (in particular, the Unix one) because they work "well enough". In common programming languages the values are stored within variables and the names are the handles for the variables. In macro languages there isn't a distinct separation between the handles and the values. One is supposed to get around this problem using quoting, but multilayer quoting combined with expanded character sets wrecks havoc on this approach. Especially when the simple solution worked for the first few years.

More to the point, the ability to build a system out of text streams is a very powerful construction technique and eliminates the need for "professional maintenance". The consequence is that when the systems break there is no one to fix them. The fact that these systems are cobbled together and the components "not aware" of their context also means that failures are not diagnosed. (Email to the bit bucket)

Instead the problems are solved by layering additional workarounds such as "sendmail", `_`, and `%!`. These actually exacerbate the problem by eliminating the acuteness of the pain and thus forestall solutions.

Now try pushing Unicode addresses through the usenet mail network! CCITT is no better, unless you view 10 years for changes as quick turnaround.

To be fair, try extending the North American Number Plan phone numbering scheme. You can, but it will take 40 years.

Welcome to the world of Ad Hoc solutions that allow us to be fleet of foot until we stumble and of standards that allow us to run fast as long we don't try to turn.

Back to the Story of O, it isn't just naive programmers but those who are trying to be helpful by adding "smart" heuristics.

---

### **✂ Failsafe mode for 3.5" Floppies**

Don Phillips <don@blkhole.resun.com>

Mon, 9 Sep 1991 00:00 PDT

Recently, in another newsgroup there was a plea for help from somebody that had a floppy drive that was writing on write-protected floppies! After thinking about the use of opto-electronic sensing mechanisms for write-protect detection, it seems to me that the position of the plastic tab in the open position signifying "protected" is backwards from a fail-safe point of view. If dust prohibits sensing the position, or the detector/light source fails, the drive will incorrectly assume that the disk should be writable. In the days of the 5 1/4" diskettes, the sensing was in the opposite way; an open notch implied writable, closed implied protected.

Don Phillips, Research Unlimited, Escondido, Calif. ...!ncr-sd!blkhole!don

---

## **Re: The RISKS of Superiority**

*<sp1!hcfeams!hobs@dale.cts.com>*

*Thu, 5 Sep 91 14:48:57 GMT*

I can give you a specific example of the problems of rushing a weapons system into combat before it is completely tested. It also gives a good example of how political considerations can screw things up.

In the mid to late '60s, I was an infantry officer in the US Army. At the time that I went into the army, the standard infantry rifle was the M14. The M14 was developed by taking a successful rifle, the M1 Garand, and saying "how can we improve this?" They made it lighter, increased the size of the magazine from 8 to 20 rounds, made reloading simpler and quicker, and made the gas system more robust. There were only two major flaws -- it could only be fired semi-automatically (well, there was the M14A1 which was capable of fully automatic fire, but they were few and far between), and the stock was made for people with long arms (at 5'7", with a sleeve length of 32", the stock was about 3" too long for me).

Well, simultaneously, the US was involved in supplying the Army of the Republic of Viet Nam (ARVN) with weapons. (I'm sure you remember the Viet Nam War, it was in all the papers :-). Unfortunately, the average height of Vietnamese men is about 5'5", so that if the stock of the M14 was too long for me, consider what it must have been like for them. The ARVN wanted another rifle, something a bit smaller.

Some years previously, a Mr. Stoner, working for the Armalite company, developed a rifle called the AR-15. This was shorter and lighter than the M14, fired a 5.56mm round (.223 in), as opposed to the 7.65mm (.308 in) round of the M14, and could be fired either semi-automatically or fully automatically. The US Air Force got a few of these for use by its Air Police. When the ARVN saw these, they said "We want these rifles."

So, some were given to the US Army to test -- I personally was not involved in the testing and evaluation. The Combat Arms Development Board has traditionally suffered from a bad case of the NIH disease -- Not Invented Here. They saw the AR-15 as a weapon that had been wished on it by others, and even worse, was used by the AIR FORCE! Also, the Army Special Forces (Green Berets), loved the AR-15, and the Green Beanies (the polite nickname) were despised by most of the Army establishment (while I was an Airborne Ranger, I was never a snake eater (the less polite nickname)). Thus, while it was obvious that the AR-15 was going to be accepted in some form or other by the Army, it had a number of strikes against it. So, the CADB OKed the rifle, but put in a long list of changes that it wanted made. These changes were made, over the strenuous objections of Stoner, and the rifle came out as the M16, and immediately rushed into combat.

Let me tell you of my first experience of the M16 under combat conditions. My

platoon was dropped off our helicopters into an ongoing firefight -- what was called a "hot LZ". It was a hot, dry day, and the helicopters were kicking up a lot of dust. As soon as I hit the ground, I started firing. I got off one burst, then my rifle jammed.

You see, right next to where the bolt and the end of the barrel join, there is the ejection port, which is a hole in the side of the rifle where the spent cartridges go out. In most rifles, there is a small gap between the bolt and the end of the barrel, called "headspace". The M16 does not have headspace -- rather, it has lugs on the end of the bolt which fit into matching lugs on the barrel. Some of the dust and dirt kicked up by the helicopters had gotten in through the ejection port and between the lugs on the bolt and the barrel, and the bolt could not close.

Fortunately, I survived the experience, but I was no fan of the M16. Within a few years, an improved version of the M16 -- the M16A1 -- which was much closer to Stoner's original design came out. But we who had to use the old original M16 had to make sure that it was kept scrupulously clean, not always the easiest thing to do in a combat situation. And it was the good old boys of the CADB, who never took the rifle outside of Georgia and who insisted on all sorts of design changes apparently more to gratify their own egos than because of any real combat requirements.

John Hobson, Ameritech Services, 225 W Randolph HQ 17B, Chicago, IL 60606  
312-727-3490 hobs@hcfams.chi.il.us

---

**✉ Re: A Danger ... with Intelligent Terminals (Stachour, [RISKS-12.23](#))**

*Randolph Bentson <bentson@grieg.UCAR.EDU>*  
*4 Sep 91 04:29:28 GMT*

The good products are usually (and rightly) more expensive. Sometimes that price inhibits their selection. Good features that are seen as unneeded, can't overcome this.

Any risk assessment must factor possible damage by likelihood, but the list of failures can never be complete. Initial approximations are often focussed on the "more likely" failures. At some point, the effort to get good numbers becomes insurmountable. "Disasters" are assigned zero likelihood, or their costs aren't seriously investigated. As a consequence, the cost of "normal use" of the system is used for further price/performance comparisons.

I worked for a time-share/computer service firm in the mid-1970's. At that time we were evaluating a Multics system for use by a client currently using a DECsystem-10. The '10 could support 50 concurrent users with about 10-15 running jobs. Our purchasing agent fell out of his chair when he heard that the comparably priced Multics system could support only six users.

While I appreciate the Multics system (and believe Unix will one day recover most of the Multics features it had lost), there is often a cost associated with these features. In our case, the cost of "doing it right" was far too costly. Another DECsystem-10 running Tenex was

added to our machine room.

Before one counters with lists of things wrong with Tenex, remember that Multics *could* have had comparable undiscovered failures and there was no good way to determine the likelihood of their discovery.

Randolph Bentson                      Colorado State University  
bentson@grieg.CS.ColoState.Edu   Computer Science Department  
303/491-5792                              Ft. Collins, CO 80523

---

**✶ Risk assessment: a specific experience.**

<fulk@cs.rochester.edu>

Thu, 05 Sep 91 09:06:28 -0400

The Maternal Serum Alfa-fetoprotein (MSAFP) test is administered to pregnant women in order to screen for a broad range of congenital defects of the fetus. It is primarily useful against neural tube defects (spina bifida, hydrocephaly), secondarily against Down's syndrome. When my son was on the way three years ago, our doctor suggested we have the test done.

Unfortunately, the MSAFP has a fairly high false positive rate; about 10%. (It has a higher false negative rate, but that is not especially germane here.) A positive result, false or not, tends to be repeated on retest. The response is amniocentesis, which has about a 1% probability of inducing an abortion. The probability of a 29 year old woman having a child with Down's or a neural tube defect is quite a bit less than 1 in 10000.

It was very hard for us to assess whether or not we wanted the test. Certainly, if we didn't intend to have amniocentesis for a positive, we shouldn't bother with the MSAFP. Since it was hard to sort things out, I decided to do some utility calculations, which clearly indicated that the MSAFP was a loser for us. This was because of the .1% or so probability that we would have a false positive, have amniocentesis, and lose the baby to an induced abortion. (We wanted the baby, very much.) That expected negative utility easily outweighed the expected negative utility of having a baby with a problem; especially since the MSAFP's false negative rate was so high. The result was quite insensitive to the numbers I used, within a factor of 10 or so; the differences were so large.

So why did the doctor suggest the test? Why were hospitals and doctor's offices full of ads for it at the time?

The answer is simple: they, and perhaps society at large, considered induced abortions as essentially neutral, and did not assign them the large negative utility that we did. Of course, they didn't say that in their literature, but it was not hard to figure out. I called a genetic counsellor at the hospital and asked about this. She was dumbfounded that I had even done the calculation, and a brief conversation quickly confirmed my explanation.

The point is this: risk assessment depends not only on probabilities, but on the perceived utilities of various outcomes. A risk assessment by someone who

doesn't care about spotted owls won't impress a member of Earth First!, simply because they have different values. This point is often ignored in risk assessments! Nearly all of the published assessments I've seen assume that everyone shares the same utilities for various outcomes. The above example is meant to illustrate the pervasiveness of this phenomenon.

Mark Fulk

---

**✉ Re: Risk perception ([RISKS-12.24](#))**

*Geoff Kuenning <desint!geoff@uunet.UU.NET>*

*Sat, 31 Aug 91 17:06:42 PDT*

pagre@weber.ucsd.edu (Phil Agre) writes:

> I tend to be suspicious about any theory that treats ordinary people as irrational ...

In a world where tabloids like the National Enquirer have a larger circulation than any "serious" newspaper, I find this suspicion surprising. Remember that, by definition, 50% of the population is of below-average intelligence, and that even intelligent people are often irrational. To a first approximation, I'd take such a theory as true.

My own observation is that many people only believe in risks they have personally experienced. A college friend only started wearing his seat belt after he was thrown to the floor in a minor accident, even though he knew all of the equations involving inertia and friction. My firefighting friends are nuts about fire safety, in sharp contrast to others who have no personal contact with fires.

Although Mr. Agre's comments about public suspicion of large organizations are well-considered and valid, I think that this relatively recent phenomenon is merely an aggravating factor. In the not-so-early days of nuclear power, utilities had to fight public association of the word "nuclear" with bombs. It is now generally known that, while nuclear plants pose many serious risks, massive explosions are not high on the list.

My favorite example of public misperception of risks is magnetic resonance imaging, MRI, which was formerly called nucleo-magnetic resonance, NMR. The name had to be changed to keep patients from getting nervous about the word "nuclear." Yet many of those same patients will happily sit down in a dentist's chair and don a lead apron for a full-mouth X-ray, without giving a moment's thought to the possible negative effects of the radiation dose on their brain.

So yes, I tend to believe a theory that treats ordinary people as irrational. All of us are, at least occasionally.

Geoff Kuenning geoff@ITcorp.com uunet!desint!geoff



## Corporate vs. individual risk perception (Agre, [RISKS-12.24](#))

<paussav@sc.lafb.af.mil>

Thu, 05 Sep 91 10:08:00

Phil, I read your recent post to RISKS re: risk assessment etc. etc. This is an area that has bothered me for some time. I came up with the following formula you might be interested in:

Corporate perception:

Anxiety of Individual    Actuarial Statistics    Individual    Fears of individual can be discounted or negated through education

Individual perception:

Anxiety toward risk    Inconvenience to negate the risk    Individual    It is necessary for the corp. to come to an agreement with the individual on how to lessen the risk or lessen the inconvenience.

Example where the customer is not the complaining party:

(let's say) a nuclear power plant. The actuarial risk of a nuclear meltdown or serious release of radiation is very low (just ask your local power provider.) But the inconvenience caused to the individual attempting to avoid that possibility is very high. Plot all nuclear power plants on a map and then move 200 miles away from any plant and 50 miles from the air and water contamination vectors. You end up outside of most of the U.S. (The customer is the utilities regulators not the citizen)

Solution: The utilities and government ignore complaints and attempt to educate the public as to the real risks of a meltdown.

Example where the customer is the complaining party:

Alar contaminated apples. The inconvenience is, you can't eat any apples. There is no way to tell if the apple is contaminated by looking at it.

Solution: Growers stopped using it, regulations were passed etc. etc.

Note that corporations formulate their response based on actuarial risk. If the person complaining does not affect the corporation's bottom line then that person will be ignored. If the complainer can act to reduce the corporation's profit then those concerns are accommodated. (Accommodation vs. Ignorance.)

That is because, IMHO, decision makers rarely have the technical knowledge to rationally evaluate technical risks but, they do have the knowledge to evaluate monetary risks.

Chuck

[I think that something like what you say is right. The puzzle is how to make something so technically complicated into a more participatory activity, so that people can know what risks they're getting into and so forth, and so that they're freely chosen risks and not things that descend from the heavens with actuarial labels on them. Phil]

---

**✶ re: Risk assessment high priesthood**

*David Chase <David.Chase@eng.sun.com>*

*Wed, 4 Sep 91 18:19:20 PDT*

I think there are some simpler explanations for apparent public distrust of "risk assessment".

First, sometimes the claims are misleading in that they confuse the average with the individual.

Second, in those cases where a constant low rate of deaths is compared to occasional catastrophe, note that the constant stream of deaths provide data against which the risk assessors must be checked, and provide additional information that people can use to reduce their own risk of death. People don't compute the crash-safety of new automobiles (well, I'm sure that they do at some early stage), they run them into walls to see what happens.

As an example of individuals and averages, consider the safety of driving to the airport versus flying in the airplane. Airplane crash statistics are fairly generic, and thus here the average makes some sense (some airports are more dangerous than others, of course, but we can get that data). However, auto death/injury statistics are not. Lumped into the average are those people driving drunk, those people driving sleepily, tailgaters, lanehoppers, seatbelt non-users, and Single Young Men Under the Age of 25. I'm none of those people, yet I have no doubt that someone advising me on the risks of driving would quote a figure based on a sample that included them.

David Chase, Sun

---

**✶ Risk research & risk takers: the aphorism (Kerns, [RISKS-12.24](#))**

*Dan Drake <autodesk!gilroy!drake@fernwood.mpk.ca.us>*

*Thu, 5 Sep 91 09:57:06 PDT*

Robert W. Kerns <rwk@Crl.dec.com> lists among the characteristics that make people risk-averse,

- \* Low amount of individual control over individual risk factors.

The importance of this point cannot be exaggerated. And the risk-assessment-as-PR people avoid exaggerating it by consistently and completely ignoring it.

The last word on the subject of the Mobil attitude of "We risk our money, the world's whales, and your lives" was spoken in the 1930's by the woman who swept

David Low's office. As he quoted it in a notable cartoon,

The trouble with that Mussolini is that he not only bets his shirt, he bets everyone else's, too.

---

**✂ Re: Risk Assessment High Priesthood (Kerns, [RISKS-12.24](#))**

*Craig Partridge <craig@sics.se>*

*Thu, 5 Sep 1991 09:22:17 GMT*

> ... Whenever the public at large doesn't agree with this, "public reaction"  
> is labeled as being irrational....

Adding to this comment, I'd point out that deaths are not the only metric by which to measure risk. For example, I'm currently living in Sweden, which has a public-access law which, among other things, permits anyone to pick wildberries and mushrooms on anyone's property (I'm slightly simplifying the rules). One effect of Chernobyl, even now, is that if one does pick some types of mushrooms, you have to take them to a testing center to check their cesium levels. Quality of life issues like these also matter (one might also talk with the Lapps about the effects of radiation on their reindeer herds and their economic livelihood).

Craig Partridge

---

**✂ Re: `Risk perception`**

*"William P Gardner" <wpg1@unix.cis.pitt.edu>*

*Fri, 6 Sep 91 7:49:00 EDT*

Phil Agre's (pagre@weber.ucsd.edu) rejoinder ([RISKS-12.24](#)) to my posting ([RISKS-12.22](#)) has three sections. First, he gracefully qualifies his previous posting ([RISKS-12.21](#)) and makes it clear that he was not suggesting that risk perception researchers work in bad faith. Next he attributes a belief to me -- ``WG's message argues in effect that we can judge `risk' research in isolation from its social context'' -- that I did not state and do not hold. Finally, Agre discusses an example that I proposed concerning risk perception and sexual risk taking among gay adolescents. The example showed how concepts from the risk perception literature are used by public health scientists doing AIDS prevention research, as opposed to the pernicious uses that Agre discussed in his posting and I discussed in mine.

Agre's comments, however, suggest that this research is also pernicious: ``About 1985 the gay community decided that it was not going to wait around while people with generalized expertise about `risk' and the like designed studies `that can powerfully discriminate among many competing plausible explanations' all of them founded in ignorance and likely to be wrong.'' There is a lot of invective here and a claim that Agre has knowledge not shared by AIDS prevention researchers. A couple of sentences later, there is also a significant risk.

The risk is premature declaration of victory in the effort to prevent HIV

infection. Agre says that this campaign has been "highly successful", but what terrifies a lot of us is that it isn't clear, from the data, whether this is true. Recent reviews of the epidemiological and behavioral studies -- Phil, you did read this literature before you disparaged it, right? -- show that there have always been groups of men who have not changed their behavior, others who have relapsed, and little evidence that AIDS education works with young men. The lesson I derive, one that may be relevant to many other risks, is that both AIDS prevention efforts and the empirical study of their efficacy must be perpetual.

William Gardner, Law & Psychiatry Research, Department of Psychiatry  
University of Pittsburgh School of Medicine (wpg1@unix.cis.pitt.edu)

---

**✉ Re: risk perception (Gardner, this issue)**

*Phil Agre <pagre@weber.ucsd.edu>  
Mon, 9 Sep 91 10:27:22 pdt*

I do have some familiarity with the literature on AIDS 'risk perception' though I am not an expert. My point is not that existing education programs solve all problems, but that the process by which gay community activists have developed education programs in the past is a good model for future work. People should, wherever possible, be studied by their own, using concepts geared for their particular complicated situation, and not generic concepts like 'risk perception' which only support very crude generalizations. My language was no doubt unduly harsh in arguing this view, but the point is terribly important.

Phil Agre, UCSD

---

**✉ Re: Risk Perception**

*Fred Heutte <wellphred@well.sf.ca.us>  
1 Sep 91 02:21:17 GMT*

The research findings referred to by LA Times writer Janny Scott are valid but hardly 'recent.' Similar findings were made by Decision Research (a Eugene, Oregon research firm) and others who did risk assessment studies for the AEC/NRC and nuclear utilities in the mid-1970s.

See, for example, "Report to the US Nuclear Regulatory Commission," Risk Assessment Review Group, NUREG/CR-0400, 1978.



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 12: Issue 29**

**Tuesday 10 September 1991**

## Contents

- [CIA dumps on the National Security Archive](#)  
[Tom Slone](#)
  - [CAA grant Cat IIIB autoland clearance for 747/767](#)  
[Martyn Thomas](#)
  - [Follow-up on Hobson's M16 story](#)  
[Jim Purtilo](#)
  - [Risks of Incompatibilities](#)  
[Harry Erwin](#)
  - [Crackers for hire](#)  
[Mark Seecof](#)
  - [Re: Salomon Brothers -- Database Design](#)  
[Dan Drake](#)
  - [Re: Risk assessment: a specific experience](#)  
[Peter Wayner](#)
  - [Re: The risk of thinking we are in control](#)  
[Larry Seiler](#)
  - [Re: National characters on car plates](#)  
[Torsten Lif](#)
  - [Re: Failsafe mode for 3.5" Floppies](#)  
[BartMassey](#)  
[BruceHamilton](#)  
[AndrewKlossner](#)
  - [Re: Number of virus events dropping](#)  
[Mark Hittinger](#)
  - [Re: Prize for Most Useful Computer Virus](#)  
[Raymond Chen](#)  
[Richard A. Schumacher](#)  
[Dave Butterfield](#)
  - [It is RISKy to believe that Averages are 'average' \[!\]](#)  
[David Paschall-Zimbel](#)
  - [Seventh Annual Conference on Computer Assurance](#)  
[James Bret Michael](#)
  - [Info on RISKS \(comp.risks\)](#)
-

## ✂ CIA dumps on the National Security Archive

Tom Slone <potency@violet.berkeley.edu>

Mon, 9 Sep 91 18:43:50 PDT

The National Security Archive (NSA), a non-profit clearinghouse for Freedom of Information Act (FOIA) materials, requested from the Central Intelligence Agency (CIA) a list of materials that the CIA had released under the FOIA. The CIA responded to the request by producing "a random dump", 5000-pages long summarizing the released material. The NSA and the CIA are frequently at odds with each other, hence the "hostile" reply by the CIA. Under the FOIA, agencies are not required to create (i.e. organize, sort, or merge) data, merely to provide information that already exists. So, it is unlikely that the NSA would have any recourse other than to attempt to reconstruct the index from the info-garbage it was given. [Common Cause 17(4): 20 (1991)]

---

## ✂ CAA grant Cat IIIB autoland clearance for 747/767

Martyn Thomas <mct@praxis.co.uk>

Tue, 10 Sep 91 12:02:06 BST

Flight International (11 Sept 1991) reports that British Airways has been granted Category IIIB autoland clearance for its 747-400s and 767s by the UK CAA.

Cat IIIB means that autolandings are permitted where the decision height is touchdown (zero altitude cloud ceilings) and the forward visibility is zero. BA are requiring 100 metres visibility for the 747 to taxi (75m for the 767).

The clearance was granted after the CAA has monitored "almost flawless" autoland trials. 440 approaches were demonstrated on the 747, 520 on the 767.

"At the heart of the system in both types is the Collins FCC132 flight control computer".

The 747 clearance includes 3-engine operation. The single-engine limits for the 767 are 14m decision height and 200m visibility.

BA expects FAA clearance for Cat IIIB in about six months.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

Tel: +44-225-444700. Email: mct@praxis.co.uk

---

## ✂ follow-up on Hobson's M16 story ([RISKS-12.28](#))

Jim Purtilo <purtilo@cs.UMD.EDU>

Mon, 9 Sep 91 18:58:27 -0400

John Hobson gives a nice summary of the risks associated with rushing a weapons system into use either prematurely or after lots of modifications are mandated by paper-pushers. He makes passing reference to the greater-than-usual need

for cleaning of the firearm in its second major ... umm ... "distribution" (the M16A1). The detailed story behind that is itself a study in mismatched specifications.

The cartridge ultimately chosen for the M16 was originally a "wildcat" round, and to some extent it evolved with the light rifle designs (some of which are referred to as the Stoner system, although Eugene Stoner's ideas affected to several products of the era ... the designs were successively owned by several companies during early 60's.) One of the goals for this combination of rifle and cartridge --- as inspired by those nice folks at DARPA, I believe --- was to have a system that we average users would not have to waste time cleaning at all.

The system as rapidly tested and then fielded achieved this goal. Then government procurement got into the act. When the contracts for large quantities of ammunition were written, the part of the specification about not needing to clean the rifle was violated: to serve manufacturing needs, companies used a slightly different formula for the powder than was used in the original cartridge. Its use resulted in much greater accumulation of residue in the rifle's gas system, in turn increasing failure rates (often with consequences that didn't have as happy an ending as Hobson's story). The whole mess was made worse since everyone was told \*not\* to clean the rifle, and no cleaning kits were shipped with the first rifles delivered. Before the problem was sorted out, congress got involved and the reputation of an otherwise serviceable system was permanently damaged.

For what it's worth, those of us who actively compete in this class of shooting sports use the M14, which led off Hobson's article. I guess we either view the committee-designed tweaks to the Garand design as "features" or we have longer arms than he does.

Jim

---

## **✂ Risks of Incompatibilities**

*Harry Erwin <trwacs!erwin@uunet.uu.net>  
9 Sep 91 12:30:01 GMT*

I'm interested in identified incompatibilities between the various US Government standards, beginning with

POSIX  
GOSIP  
Ada  
B2 Security  
(etc.)

in various applications. I know of one between UNIX-based POSIX implementations and Ada tasking that makes the combination inappropriate in safety-critical real-time and near-real-time applications, and I'm interested in identifying any others that are known for specific applications.

[NOTE ADDED LATER IN REPOSE TO A QUERY FROM PGN:]

There is a real issue. Ada running over UNIX can't handle data enablements of tasks reliably--the problem being that you don't have access to a test-and-set instruction and you can be interrupted in the middle by the arrival of data from outside. The result is spurious enablements and the loss of other enablements. That can be disastrous in a safety- or nuclear- critical system. How many nuclear-capable systems have been written using Ada tasking over UNIX? How many other problems have been created by incompatible standards? If you want a background brief, call me at (W)703.734.6092 or (H)703.758.9660.

Harry Erwin Internet: erwin@trwacs.fp.trw.com

---

## **Crackers for hire**

*Mark Seecof <marks@capnet.latimes.com>*

*Tue, 10 Sep 91 10:50:05 -0700*

In the September 19th Rolling Stone at page 67 an article titled "Samurai Hackers" by Lynda Edwards tells us that a "new breed of hacker has been finding a niche in the corporate world in the last two years. These hackers are hired by white-collar professionals at ad agencies, law firms, newspapers, and investment houses who want to steal co-workers' ideas and clients or pillage supervisors computer files for marketing strategies, performance evaluations and managerial gossip."

Ms. Edwards presents several tales of crackers hired by unethical people in business to snoop in or sabotage other peoples' computer files. She also describes how victims sometimes hire their own crackers to mount a counter-attack. The crackers use their knowledge and skills to ferret out information from companies' networks and minicomputers. They usually receive a leg up from their employers, who get them modem 'phone numbers and basic account/password info. The crackers then overcome or bypass the often trivial security on the target systems. Most of what they do could be done by any jackleg expert with a given system, but the crackers are the agents of computer illiterates and thus constitute a threat unconsidered by the managers of systems in non-computer businesses.

These crackers are seen to be somewhat akin to the wandering samurai of Japan's past. They work as mercenaries, honing their own skills and testing them in combat on behalf of employers they often hold in contempt. (The crackers are said to refer to ignorant computer users as "Stupids.") The samurai image is distorted and romanticized but the jobs the crackers take on are very real.

These crackers are well paid by those who hire them through bulletin boards or by word-of-mouth. Tales of their exploits circulate on BBS's and they are getting some notice in 2600 magazine.

[Begin Mark S.'s comments.] Of course, the notion of the computer whiz employed by some nefarious scheming man or woman of business is not new. What is new is the increasing dependence of service businesses on networked PC's. In the past non-computer firms tended to rely on computers and software dedicated to certain business tasks like accounting, process control,

engineering, printing paychecks. These were often vulnerable to cracking for one purpose or another, but they weren't much of a resource for "fuzzy" information like supervisors' memos or private e-mail. Even offices using word- processing systems often relied on stand-alone machines which were easy to crack if you had the office key but impossible to crack by 'phone or from another office because they were not connected to any communication links. Only recently have PC networks become all-purpose communication tools in places like law or advertising offices where you can find memos, workups, payroll info, private diaries, electronic mail, etc. all lurking in the system.

All in all, this sort of thing seems to bolster the argument that systems should be designed with security features even if the end customer doesn't know to ask for them. A cracker given access to one employee's account should not be able to use that access as a springboard to crack all of the other accounts or data on the system.

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

---

**✉ Re: Salomon Brothers -- Database Design (Dye, [RISKS-12.28](#))**

Dan Drake <autodesk!gilroy!drake@fernwood.mpk.ca.us>

Tue, 10 Sep 91 09:43:39 PDT

>Bravo. The database programmers made a mistake. The Salomon traders  
>committed a crime.

Not quite. The programmers implemented a design that was laid down in detail (you may assume, and hope) by analysts working under the direct orders of executives from Operations and Finance. It's the job of those gentlemen to ensure controls and audit trails. Their failure to do so is much more serious than an error by programmers: it is more evidence of incompetence and/or corruption, most likely both, pervading the company.

Dan Drake drake@Autodesk.com

---

**✉ Re: Risk assessment: a specific experience.**

Peter Wayner <wayner@cs.cornell.edu>

Tue, 10 Sep 1991 13:37:05 GMT

Mark Fulk's article on the fetal tests on pregnant women brought back memories of my younger days several years ago when I was in Yale Med School. Well, it was only for a day and I was visiting friends and they took me to one class which was on pre-natal diagnosis.

I remember a very practical and straight-forward professor discussing all of the possible techniques for checking out the womb and making sure everything was okay. He would carefully explain the technique and all the facts you could discern from the various bits of bio-matter you could snag from the womb. The Maternal Serum Alfa-fetoprotein test is only the beginning of their bag of tricks. It turns out that the doctors can't learn too much from this one because the fluid comes from the mother and contains only a very dilute amount

of the child's bio-matter. The next step up was to get some of the chorion (sp?) which is essentially the boundary layer between the placenta and the uterus. All the nutrients pass through this membrane so it is rich in data. The most aggressive procedure, though, was when they poked around with a needle until they managed to find the placenta. Then they grabbed a bit of fetal blood. This, the professor explained, was a data gold mine.

The rub was inserted very parenthetically at the end of each section of the lecture. He would say things like, "the amniocentesis test is the most successful and we find we only induce miscarriages in 1 to 2% of the time." (All numbers in this section are subject to bad memory fudging. They are approximate.) I remember thinking to myself, "Wow! 99% that's great!" because I think I was lead on by the can-do tenor of the lecture.

About 5 minutes later I realized that "inducing miscarriages" was not the same as failing to cure cancer or a cold. It was a big deal. Statistically it was a violation of the Hippocratic oath. The patient died because the doctor was curious. And as it was the only "cure" they have for Down's Syndrome or other tri-somic babies is abortion. The tone of the lecture, though, was much worse than the attitude that you couldn't make an omelette without breaking eggs. They didn't do any of the risk analysis or any number crunching what-so-ever. The lecturer just ploughed on and his manner and diction was just saying, "We're doctors. This is what we do."

Peter Wayner Department of Computer Science Cornell Univ. Ithaca, NY 14850  
EMail:wayner@cs.cornell.edu Office: 607-255-9202 or 255-1008

---

✉ **Re: The risk of thinking we are in control (Kerns, [RISKS-12.24](#))**

LARRY SEILER <seiler@rgb.enet.dec.com>

Tue, 10 Sep 91 12:35:50 PDT

Robert W. Kerns lists this point that makes people dislike certain risks:

- \* Low amount of individual control over individual risk factors.

This is a very important point but not quite accurate. It is *\*perceived\** control or *\*perceived\** lack of control that affects risk aversion, and it is the difference between perception and reality that injects a lot of the irrationality into most people's risk avoidance behavior (myself included).

For a simple example, one of the effects of being drunk is thinking that one isn't -- hence many people at great risk of injuring themselves and others go ahead and drive anyway, because feel that they are in control. I think people's apparent preference for old familiar risks over new risks is in the same category -- familiarity breeding a false sense of control.

But preferring risks where one has individual control is, indeed, rational, provided that one really has control, and doesn't just feel one has control.

Larry

---

**✂ Re: National characters on car plates**

<Torsten.Lif@eos.ericsson.se>

Tue, 10 Sep 91 11:10:08 +0200

As has been said before, the Scandinavian alphabets contain letters "alien" to Anglophones. One such is often referred to in English as "A-ring". In Danish it is written "aa". You can get it on a SUN keyboard by hitting "<compose>A\*". It has ISO8859-1 codes 0xc5 (upper case) and 0xe5 (lower). On a PC it has character codes 0x81 and 0x8c.

Vehicles from the Finnish archipelago A\*land all have numbers starting with "A\*L", followed by some digits. Since they are part of Finland, they may use the "SF" identification marker when travelling abroad, but some prefer to underline their regional identity by using an "A\*L" sticker. I wonder how French police computers are set up to handle all this. The possible permutations of confusing mistakes here are fascinating.

Torsten Lif, Ericsson Telecom AB, EO/ETX/TX/ZD, S-126 25 STOCKHOLM, SWEDEN  
Phone: +46 8 719 4881

---

**✂ Re: RISKS of floppette write-protect systems (Phillips, [RISKS-12.28](#))**

Bart Massey <bart@cs.uoregon.edu>

Mon, 9 Sep 91 16:53:26 PDT

> ... In the days of the 5 1/4" diskettes, the sensing was in the opposite way

Worse than that, \*both\* senses of write protect existed! If I recall correctly, the 5.25" floppies sold by a certain major retail electronics outlet differed from those sold by a certain major mainframe and microcomputer manufacturer in this respect! I was working with both kinds of equipment at the time (sigh) and, if I remember right, trashed a diskette by getting confused by this at one point.

> ... it seems to me that the position of the plastic tab in the open  
> position signifying "protected" is backwards from a fail-safe  
> point of view. If dust prohibits sensing the position, or the  
> detector/light source fails, the drive will incorrectly assume  
> that the disk should be writable.

Ahh, but the chief failure mechanism for the 5.25" diskette write-protect system was for the little "sticker" which was commonly used to write protect/enable the diskette to fall off -- this failure should make the disk write-protected, no? :-)

Probably the 3.5" diskette emulates the argument of the above paragraph, even though it is no longer valid. What it \*should\* do, IMHO, is have the whole slider open, and use 2 LED/sensor pairs to write-enable the disk, with the obvious state table. Of course this would add \$5 or more to the disk drive cost, for a possibly rare failure mode...

Bart Massey bart@cs.uoregon.edu

---

**✂ Re: Failsafe mode for 3.5" Floppies**

*<Bruce\_Hamilton.LAX1B@xerox.com>*

*Mon, 9 Sep 1991 19:19:46 PDT*

5.25" floppies' copy-protect is a risk because it is backwards from every other magnetic medium I have ever encountered. The standard is: You insert something to permit writing and remove it to protect. This is true for:

- 9-track tape (write rings)
- VHS video cassette
- audio cassette
- 8" floppy
- 3.5" floppy

How come 5.25" floppies are backwards?

--Bruce 213/333-3538

---

**✂ Re: Failsafe mode for 3.5" Floppies**

*Andrew Klossner <andrew@frip.wv.tek.com>*

*Tue, 10 Sep 91 13:03:38 PDT*

"If dust prohibits sensing the position, or the detector/light source fails, the drive will incorrectly assume that the disk should be writable."

The RISK of assuming a particular implementation. My Panasonic 3.5" floppy disk drive senses the tab position by attempting to insert a metal probe into the hole. A successful insertion means that the disk can be written. The likely failure modes would falsely indicate unsuccessful insertion, i.e., write prohibited.

-- Andrew Klossner (andrew@frip.wv.tek.com)  
(uunet!tektronix!frip.WV.TEK!andrew)

---

**✂ Re: Number of virus events dropping**

*Mark Hittinger <an288@cleveland.freenet.edu>*

*Sun, 8 Sep 91 21:06:36 -0400*

I noted a comment in Cliff Stoll's message that he had the perception that virus events and interest were kind of winding down. I just wanted to comment that, indeed, the messages-per-week posted on some of the local hacker bbs virus groups has been dropping off steadily for months. In one case the "group" was deleted to make room for something else!

Humanity can only write so many payroll programs right? Most viruses seem to be re-hashes of existing ones. Perhaps the fun is deflating?

The idea of a helpful virus is an interesting one. Perhaps one that would sense when your PC is locked up and warm-reboot? HA. I suppose that a helpful virus would really be called a commercial TSR?

Mark Hittinger [answ.machine] (606)-272-2424 PO BOX 43358 Middletown, KY 40243

---

**✂ Re: Prize for Most Useful Computer Virus**

*Raymond Chen <raymond@math.berkeley.edu>*

*Sun, 8 Sep 91 18:48:15 PDT*

In [<RISKS DIGEST 12.27>](#) Cliff Stoll retells Fred Cohen's article which describes how viruses and virus-like programs can be beneficial.

>automated bill-collectors, where, "each bill collector virus is a  
>small program designed to collect one bill"; this program modifies  
>itself depending on the debtor's response. [...] maintenance  
>viruses which dispose of temporary files or hung programs.

I fail to see how these programs are virus-like. The first is a self-modifying program, and the second is what might be called a daemon. Neither program is (or in the second example, needs to be) self-reproducing.

The only example of a 'beneficial virus' I can think of is the one that was released to fight another virus, namely the 'Animals' program. The problem with viruses of either sort (in my unqualified opinion) is that once released, they are hard to exterminate.

Another (more likely?) possibility is that I'm completely misunderstanding the brief excerpt from Dr. Cohen's article.

---

**✂ Re: Prize for Most Useful Computer Virus**

*Richard A. Schumacher <schumach@convex.com>*

*Mon, 9 Sep 1991 17:56:02 GMT*

I wonder whether Dr. Cohen's bill collector virus included a provision for an audit trail, say by appending a record of every transaction to a database? His "The Sciences" article mentions no such device, and indeed boasts the lack of any large permanent database as an advantage. Feature or bug?

---

**✂ RE: Prize for Most Useful Computer Virus**

*Dave Butterfield <dave@prodnet.la.locus.com>*

*Mon, 9 Sep 91 15:20:32 -0700*

I don't know about the \*most\* useful, but one very useful virus would be a virus that identifies and destroys other viruses. I suppose it would have to be more virulent than the others.

Whoever implements this, please don't forget to program in some appropriate self-destruct condition...

(Maybe there should be an RFC to cover that topic.)

Dave

---

### ✂ It is RISKy to believe that Averages are 'average'

David Paschall-Zimbel <DAVIDLI@SIMVAX.LABMED.UMN.EDU>

Tue, 10 Sep 91 12:52 CST

desint!geoff@uunet.UU.NET (Geoff Kuenning) writes:

"Remember that, by definition, 50% of the population is of below-average intelligence,"

[David goes on to shoot down this old war-horse... once again... I truncated the rest of his message, but would like to remind our contributors that it really helps if you are alert enough to avoid the mistakes that have already been kicked around in back issues. See Mark Seecof's note in [RISKS-12.11](#) that included counterexamples from Tim Smith and Jeremy Grodberg... And thanks to those of you who are on your toes. PGN]

---

### ✂ Seventh Annual Conference on Computer Assurance

James Bret Michael <jmichael@gmuvax2.gmu.edu>

Mon, 9 Sep 91 11:32:59 -0400

#### CALL FOR PAPERS

Seventh Annual Conference on Computer Assurance

The Seventh Annual Conference on Computer Assurance (COMPASS), sponsored by the Institute of Electrical and Electronic Engineers and IEEE Aerospace and Electronic Systems Society, in cooperation with the British Computer Society, will be held at the National Institute for Standards and Technology in Gaithersburg, Maryland, USA, June 15-18, 1992. The purpose of this conference is to bridge the gap between emerging technology for computer assurance from research laboratories into industrial computer systems development. Papers may present original research on theoretical aspects and applications of technology to assured computing, or may be reports detailing experiments, evaluations, and open problems in the use of new technologies for computer assurance. Typical but not exclusive topics of interest include:

- \* Models and modelling (process, mathematical, and requirements models)
- \* Formal approaches (proofs of correspondence, formal specifications, and IV&V)

\* Experiences with assurance (illustrative examples from communications, energy, financial, medical, military, transportation, and other types of systems)

**PAPER SUBMISSION:**

Authors are requested to send five single-sided copies of their papers (not exceeding 7,500 words) to the program chair by January 10, 1992. If available, an electronic mail address for the contact author should be included. Papers submitted simultaneously to another conference with published proceedings are disqualified. Papers will be refereed by the Program Committee and will be returned with comments. Accepted papers will be published in the proceedings.

**IMPORTANT DATES:**

Papers due: January 10, 1992

Notification of acceptance: March 7, 1992

Camera-ready paper due: April 1, 1992

Conference: June 15-18, 1992

Additional information about the COMPASS '92 can be obtained from the General Chair. All inquiries concerning paper submissions should be addressed to the Program Chair.

**GENERAL CHAIR:**      **PROGRAM CHAIR:**

Robert Ayers

Dr. Edgar H. Sibley

ARINC Research Corporation      Department of Information and

2551 Riva Road      Software Systems Engineering

Annapolis, MD 21401 USA      George Mason University

voice: (301)266-4741      4400 University Drive

fax: (301)266-4040      Fairfax, VA 22030-4444 USA

(703)993-1640, or [esibley@gmuvax.gmu.edu](mailto:esibley@gmuvax.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 12: Issue 30**

**Wednsdy 11 September 1991**

## Contents

- [Export controls on workstations](#)  
[John Markoff via PGN](#)
- [Re: Multinational Character sets](#)  
[Hugh Davies](#)
- [Re: National Character variations in ASCII](#)  
[Kim Greer](#)
- [Re: Risks of sloppy terminology](#)  
[Geoff Kuenning](#)
- [Re: M16](#)  
[Ty Sarna](#)
- [Re: Failsafe floppies?](#)  
[Jordan M. Kossack](#)  
[Bob Jewett](#)  
[Doug Krause](#)  
[David Palmer](#)  
[Mike Berman](#)
- [Re: Beneficial viruses considered harmful](#)  
[Brian Rice](#)
- [Re: Prize for Most Useful Computer Virus](#)  
[Joe Dellinger](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Export controls on workstations**

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>  
Wed, 11 Sep 91 9:55:12 PDT

In an article in this morning's New York Times, John Markoff discusses the US DoD's "quietly proposing strict new controls on the export of inexpensive but powerful computer workstations that can have military uses." [See my Note, below.] The article highlights a DoD meeting yesterday with industry executives, at which the DoD expressed concerns "about cheap high-speed computers being diverted to the IRA and the Cambodian Resistance Movement as well as traditional worries that such computers might be used in anti-submarine

warfare applications" -- according to one executive. The proposed "Draconian" controls would require hardware and software changes that would restrict the applications that could run on inexpensive engineering workstations, audit all programs run on the machines, and limit their ability to connect to computer networks. These restrictions "appear partly to reverse the effort by the Coordinating Committee for Multilateral Export Controls, known as COCOM, to ease the limits on many high-technology goods, including computers."

[Note: Yeah, sure. ALL computers can have military uses. But there must also be some folks who are most scared by the PEACEFUL uses! PGN]

---

## **Re: Multinational Character sets**

<hugh\_davies.wgc1@rx.xerox.com>

Wed, 11 Sep 1991 01:48:34 PDT

I have been following this debate with interest and amusement. Why? Because I work in the Systems Group of the Technical Publications arm of a well known photocopier manufacturer (look at the email address!).

We spend a large part of our time manipulating character codes between the various hosts we use. A large part of our work is machine aided translation, and it is essential that we can handle (effectively) any character that anyone, anywhere might wish to use. We have actually standardised on the Xerox Character Code Standard (XCCS) o0, partly because it's our own standard, and partly because (so far as I know) it's the only comprehensive character set standard. We await the Unicode standard with some interest.

So what are the RISKS?

- ASCII is woefully inadequate. I suppose it was barely adequate in the days of punch cards, but today it is unacceptable. Increasingly, European consumers demand that their consumer products "talk" to them in their language. ASCII can't even do plain accented characters, much less an 'L' ogonek! In several European countries it is legally mandated that products must deal with the host language correctly.

- Manufacturers extensions to ASCII are even worse, because they're all different, still inadequate and sometimes wrong. Further, they generally steal "rarely used" character codes from the standard set, for example the open and close square bracket are generally re-used for the AE and A-circle digraphs in Scandinavia. This makes Scandinavian VAXen a pain to use! And did we ever find out what the IBM PC's y-umlaut is actually for? So far as I know it's not used in any language, and appears to be a corruption of the Dutch ij digraph.

- With the freeing of Eastern Europe, the demand for products that can deal with Cyrillic and Eastern European characters is going to rocket.

- Much of the conversion software available is very poor. Can I make a plea to word processor designers to have an option in their "export file" commands to retain character codes they don't understand, in some form (for example in form <nnn>, where nnn is the octal/hex character code?). To be presented with a file

in which every accented character, or sometimes every character, has been replaced with a question mark and asked "Can you do anything with this" (as I have been) is a considerable pain.

- Since we cannot even agree how to convert ASCII into EBCDIC and back, I am not greatly encouraged

- I don't like to think about the costs to industry associated with all the effort involved in translating between character sets. (Of course, the costs of doing the translation itself are another matter!)

What we need is a single, centrally administered, extensible character set standard. Getting people to use it will be a different matter. The Unicode effort has already run into political problems where the Japanese and Chinese will not share a character code for the same kanji character.

If the world is ever to become a global village, it would be nice to be able to send each other email and have it readable at the other end!

Regards,

Hugh Davies, Rank Xerox, Multinational Customer & Service Education- Europe, Welwyn Garden City, Herts. England.

(o0 If you would like a copy of the XCCS, so you can find out what an L ogonek is, the part number is XNSS058710, available for a nominal fee from Xerox Systems Institute, 475 Oakmead Parkway, Bldg. 4, Sunnyvale, California 94086, USA.)

---

### **✂ Re: National Character variations in ASCII ([RISKS-12.25](#))**

*Kim Greer -- rjj <klg@george.mc.duke.edu>*

*11 Sep 91 13:03:38 GMT*

Perhaps it has been mentioned (or will soon to be mentioned) about the use of ASCII for use in other countries, but ...

Perhaps we have overlooked the risk of forgetting the origin of words and what an acronym \*originally\* meant. "ASCII", as we all remember, stands for American Standard Code for Information Interchange, the key word being "American". Would it not be stretching things a bit to expect non-"American" language nuances (like umlauts) to automatically fit in?

Reminds me of the saying (paraphrased): When all you've got is a hammer, everything looks like a nail.

Kim L. Greer, Duke University Medical Center, Div. Nuclear Medicine, POB 3949, Durham, NC 27710      voice: 919-681-5894

---

### **✂ Risks of sloppy terminology**

Geoff Kuenning <desint!geoff@uunet.UU.NET>

Wed, 11 Sep 91 02:01:11 PDT

When I stated that 50% of the population is of below-average intelligence, I should have used "median" instead of "average," of course. Boy, did a lot of people jump on me for that one! Of course, the IQ test is normalized so that 100 is the median, so perhaps I should have said that 50% of the population has an IQ of below 100, which is how I usually phrase that statement.

None of this changes the basic point of my message. It just reminds me of how e-mail makes it easy for people to pick on sloppiness, while being unaware of the fact that others are simultaneously doing the same thing. If I had made that slip at a conference, one person would have pointed it out in Q&A and I could have corrected myself at once, so that everybody would agree on the proper terminology. Instead, I found myself typing basically the same mail answer perhaps 10 times.

Geoff Kuenning geoff@ITcorp.com uunet!desint!geoff

---

✉ **Re: M16 ([RISKS-12.29](#))**

Ty Sarna <sarnat@rpicb8>

Wed, 11 Sep 91 01:30:27 EDT

>The cartridge ultimately chosen for the M16 was originally a "wildcat" round,

The original round used IMR ("improved military rifle") powder, which burns quickly. The Ordnance Department switched to ball powder produced by Olin-Mathieson, which burns much more slowly. The AR-15 was designed so that the gas port stayed closed through the combustion. The ball powder was still burning when the gas port opened, and let it burn into the gas tube.

In addition, the different powder also had the effect of increasing the cyclic rate of fire from 750-800 rounds per minute to over 1000, which exacerbated the jamming problems.

Another change not mentioned was the increased "twist" of the rifling from 1 in 14 inches to 1 in 12. This causes the bullet to spin faster, and thus makes it more stable. This was not a good thing, however -- it meant that the bullet would be more stable as it passed through the victim, instead of tumbling around and causing more damage. The increased damage was one of the original AR-15's selling points over the M-14, and a central part of its design theory.

SOURCE: James Fallows, "Two Weapons". Unfortunately I don't know the source of this article -- all I have is a Xerox. I'll try to find out. It's a very interesting piece, also mentioning similar stories about the F-16 fighter plane, Spencer's lever-action rifle of the Civil War era, and the Mauser/Springfield '03 during the Spanish-American War.

Ty Sarna sarnat@rpi.edu

---

✉ **Failsafe floppies?**

Jordan M. Kossack <kossack@taronga.hackercorp.com>

Tue, 10 Sep 91 23:16:55 CDT

Further, for 9-track tape, sensing a notch implies that the tape is to be read only. Inserting the write ring allows one to write to the tape. Audio cassettes operate on a similar principle as tapes and floppier diskettes - recess/notch means read-only - so it is the 7/2" diskettes that deviate from the standard.

Which is more fail-safe? Arguably the "standard", where notch implies read-only. However, no system is fool-proof ... because fools are so ingenious. :-)

Jordan Kossack (713) 270-9056

---

**✂ Re: Failsafe mode for 3.5" Floppies (Hamilton, [RISKS 12.29](#))**

Bob Jewett <jewett@hpl-opus.hpl.hp.com>

Tue, 10 Sep 91 21:47:34 pdt

Get ready to encounter another. 8mm (Exabyte, video) tapes have a small sliding panel that covers a hole to prevent writing, while 4mm tapes (DAT and DDS) have a similar but smaller panel which covers a hole to allow writing.

Bob Jewett jewett@hpl-opus.hpl.hp.com

---

**✂ Re: Failsafe mode for 3.5" Floppies**

Doug Krause <dkrause@miami.acs.uci.edu>

Wed, 11 Sep 91 02:59:33 -0700

On 8mm video cassettes you write protect by sliding a piece of plastic so that it is "in the way". This is equivalent to the stickers on a 5.25" floppy. Also for the above list: Umatic videotapes have a small piece of plastic that does a write enable.

Douglas Krause, University of California, Irvine dkrause@orion.oac.uci.edu  
BITNET: DJKrause@uci.edu

---

**✂ Re: RISKS of floppette write-protect systems (Phillips, [RISKS-12.28](#))**

David Palmer <palmer@caltech.edu>

Wed, 11 Sep 1991 02:57:51 GMT

8 mm video tape cassettes (used by Exabyte data tape drives) have the feature that when you flip the write protect tab, it is visible as a red flag. To me this says

"Danger, your data is safe."

---

## ✂ another take on floppy protection

Mike Berman <berman@gboro.glassboro.edu>

Wed, 11 Sep 91 10:52:03 -0400

Much as I prefer 3.5" disks over the 5.25" format, there's one big advantage to the older disks' method of write protection. For our student labs here, we purchased 5.25" disks without a notch, easily obtainable from any large distributor. We then modified a disk drive so that it would write these disks despite the lack of a notch. When we lend these disks out in the lab, we have a high degree of confidence that the contents will not be changed, since the write protection cannot be defeated without cutting a notch or modifying a drive. (Well, there may be ways around it, but they are relatively obscure.) This really cut down on the virus problems in our lab. On the other hand, with 3.5" disks you can pry out the little slider, which prevents accidental modification of the disk, but a malicious user has only to wedge something into the hole to make the disk writable.

A. Michael Berman, Dept. of Computer Science, Glassboro State College,  
Glassboro NJ 08028 +1 609 863-6521 UUCP: njin!gboro!berman

---

## ✂ Re: Beneficial viruses considered harmful

Brian Rice <rice@dg-rtp.dg.com>

Wed, 11 Sep 1991 01:54:43 -0400

Upon my first reading of it, Cliff Stoll's message informing us about a contest for the "Most Useful Computer Virus" ([RISKS 12-27](#)) elicited in me a reaction that I didn't really understand. Various parts of my brain simultaneously said "That's neat," "Huh?", and "Whoa...". But at the time I couldn't put my finger on just why I had such equivocal feelings about the idea.

As I read later responses, a question occurred to me: "What's bad about a 'bad virus'?" Is it its bad effects...you know, erasing my disks, slowing down my system, sending e-mail to my mom accusing her of wearing combat boots? I didn't like any of those answers... I think those viruses which have been dubbed as "harmless" (for instance, those which print a message on your screen then exit forever) are harmful too, because they decrease my confidence in the expected functioning of my system and make me paranoid about using software.

Then I said to myself, "Suppose there was a 'good virus.' I mean a REALLY GOOD virus. Like maybe a virus which would get me free pizza all the time, or would explain to me just what the hell non-homogeneous Poisson processes are and how I can make them go away. What would happen in the exceedingly fortunate event that my system got 'infected' with it?" My answer was that I would wish I could just have run the program under my own volition.

It should be clear what I'm getting at...all viruses are bad, because they take me out of control of my system and make me afraid to do things with it. Now, the issuer of the contest challenge, Fred Cohen, does forbid "entries that have been released into a computing environment without the permission of the owner...", but, for a virus to be a virus, it has to enter a computer without

SOMEBODY'S knowledge: otherwise, in effect it's just a boring old remote procedure call, with a needlessly kludgy way of getting executed. Why copy code around when, if users really wanted to run it, they could just get their own copies? The answer, I suspect, is that they may or may not want to run it, but WE know what's best for them!

You could argue that I feel this way just because I am fortunate enough to have some technical savvy...if I weren't a congenital computer nerd, I might be grateful for somebody arranging for a virus to hop onto my system and clean up all my old junk files (and order me a pizza), then quietly vanish. But I think that this notion is incoherent: either introducing such a "beneficial virus" is paternalistic (and to be avoided because you should instead educate your users and give them the knowledge and tools to maintain their systems safely themselves), or it's just a kind of remote system administration (and to be avoided because there are more efficient and less needlessly complex ways of accomplishing the same task).

Cliff writes:

> [Dr. Cohen] points out that malicious and unauthorized viruses have  
> given a bad name to viruses. I'll say!

Would he really say? Some of the arguments I presented above are practically plagiarized from The Cuckoo's Egg, so I'm not sure. I feel a great deal of trepidation in writing this note; I'd be mortified if Cliff, whom I admire enormously, got mad at me for suggesting that he was smokin' Mother Nature when he wrote something, which seems to be what I'm doing. Urp. Of course, I'm certain that part of his motivation is that Dr. Cohen is plainly a "white hat," and that the idea of code roaming around in a network looking for opportunities to do good is what we technical types call "way cool." What I'm suggesting here, though, is that the idea deserves careful scrutiny lest our cool idea translate into somebody else's increased powerlessness (or, alternatively, somebody else's decreased system performance).

Brian Rice Data General Corp., Research Triangle Park, N.C.  
DG/UX Software Quality Assurance rice@dg-rtp.dg.com +1 919 248-6328

---

## **✉ RE: Prize for Most Useful Computer Virus**

*Joe Dellinger <joe@montebello.soest.hawaii.edu>  
Wed, 11 Sep 91 00:10:48 HST*

In 1981-1983 I wrote a virus for the Apple ][ while an undergrad at Texas A+M, mostly as a demonstration to friends that such a thing really was possible. The intended "target" was my own disk collection, which was to be kept in strict quarantine so the virus wouldn't escape accidentally. The idea was to see how quickly the virus would spread within my own disk collection if I used my disks "normally". The virus itself was intended to be entirely asymptomatic: it did nothing more than check for incompatibilities with programs or DOS, check for damage to itself, copy itself, and increment a generation counter each time it infected a new disk. It could easily be removed from a disk by using the Apple ][ utility "Master Create".

"Virus 1" DID unfortunately prove to have obvious (if inadvertent) symptoms, so was considered a failure. I don't believe it ever escaped. A few months later, using what little free time school work left us, we came up with "Virus 2". This virus appeared to have no symptoms, so after a while several friends interested in the project deliberately infected their own disks as part of the test. The first hint we had something had gone wrong was when pirated copies of the game "Congo" at UIUC (a friend of mine had finished at A+M and gone off to grad school at UIUC by this time, taking copies of the virus with him) started behaving strangely: the game would still run, but its graphics would smear. (Apple ][ users there were quite perplexed: every time they tracked down a working copy of the game to get a fresh pirate copy from, it too would prove to have stopped working. Running "Master Create" or booting from a write-protected disk was not an obvious cure back then for such a "mysterious" problem.) We quickly wrote an "immunizer" utility and distributed it at UIUC as a "cure for the smeared graphics problem with Congo".

But what if Virus 2 spread faster and farther than copies of the (nonviral) immunizer program? We analyzed what had gone wrong and created "Virus 3" to displace the close-but-not-quite-right Virus 2. Amazingly (in retrospect), this strategy appears to have actually worked. We never noted any symptoms, and I guess nobody was looking for a "computer virus" back then in the absence of a red flag demanding attention. And so we heard nothing more about my virus "in the wild"...

...until 1985 (or thereabouts). By this time the microcomputer lab at UIUC was under siege from a vicious virus that would randomly erase infected disks at boot time. Frantic investigators into the problem discovered some disks had a form of partial immunity: instead of erasing themselves, they would merely crash. They could then be fixed up with Master Create, and all would be well. The cause of the baffling immunity? They were found to have been previously infected with an undetected asymptomatic virus... Virus 3! (And that really is the last I heard of it.)

I'm in the process of writing this story up for a journal; if you have any old Apple ][ DOS 3.3 48K slave disks you'd like to look for my virus on, send me e-mail and I'll tell you how. It would be very interesting to find out what generation counts the virus got up to! (I only have copies of the virus from my own collection.) PLEASE NOTE any candidate disk must be absolutely unmodified standard "slave" DOS 3.3, or my extra-cautious virus would not have attempted infection. Such disks became progressively rarer in the mid-80's as a plethora of improved DOS's from various sources became available; it appears quite likely my virus went extinct as a result. Also please let me know if you remember hearing anything about Apple ][ viruses around 1981-1985. I have since heard of at least one other very early Apple ][ virus, called "Elk Cloner". (That virus did "call attention to itself".) Thanks.

-- joe@montebello.soest.hawaii.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 12: Issue 31**

**Thursday 12 September 1991**

## Contents

- [Re: Export controls on workstations](#)  
[Neil W Rickert](#)  
[Brinton Cooper](#)  
[Haakon Styri](#)
- ["Checkless society"](#)  
[Daniel B Dobkin](#)
- [Re: Multinational Character sets](#)  
[Dik T. Winter](#)  
[Robert Ullmann](#)  
[Hugh Davies](#)
- [Re: +&\\*#&](#)  
[Mike Morris](#)
- [Re: M16 and James Fallows' "Two Weapons"](#)  
[Jon Jacky](#)  
[Tom Faller](#)
- [Junk Mail -- In memoriam, Dave Sharp](#)  
[Peter Mellor](#)
- [Risks of assumptions?](#)  
[R. Cage](#)
- [The seriousness of statistics mistakes](#)  
[Jeremy Grodberg](#)
- [Risk Assessment: a specific experience](#)  
[Justine Roberts](#)
- [Re: risk analysis](#)  
[Victor Yodaiken](#)
- [Averages and distributions](#)  
[Jerry Leichter](#)
- [Info on RISKS \(comp.risks\)](#)

---

✉ **Re: Export controls on workstations (Markoff, [RISKS-12.30](#))**

*Neil W Rickert* <[rickert@cs.niu.edu](mailto:rickert@cs.niu.edu)>

*Wed, 11 Sep 91 13:09:29 -0500*

This proposal should properly be referred to as the "full employment for people in Singapore, Taiwan, Hong Kong and Japan" bill.

Neil W. Rickert, Computer Science, Northern Illinois Univ., DeKalb, IL 60115  
+1-815-753-6940

---

**✂ Export controls on workstations (Markoff, [RISKS-12.30](#))**

*Brinton Cooper <abc@BRL.MIL>*

*Wed, 11 Sep 91 16:40:24 EDT*

The real absurdity here is the chauvinistic attitude in DoD that US-made computer workstations are the only "inexpensive but powerful" products on the world market or that such US-made products are even cost-competitive. The net result of such export controls may be one more nail in the coffin of US-based manufacturing and is likely to do absolutely nothing to thwart terrorism.

The computer-based RISK here is based upon permitting morons to make decisions about computers.

\_Brint

---

**✂ Re: Export controls on workstations (Markoff, [RISKS-12.30](#))**

*Yu No Hoo <styri@cs.heriot-watt.ac.uk>*

*Thu, 12 Sep 91 12:23:59 BST*

Why not? The European computer industry probably need something like this to get a comeback. To have DoD creating a niche in the market sounds like a nice thing to me. The end result for the DoD paper pushers will probably be \*less\* control.

Haakon Styri styri@cs.hw.ac.uk

---

**✂ "Checkless society"**

*Daniel B Dobkin <dbd@marbury.stern.nyu.edu>*

*Thu, 12 Sep 91 10:30:28 EDT*

The 11Sep91 New York Times carried an article on the first business page about the growing use of imaging systems by banks: instead of returning cancelled checks to the customer, they return scanned images (sometimes as many as eighteen on a page). This form of confirmation has been familiar to American Express customers for some time now.

To be sure, the technology offers some advantages: for example, the images can be reduced, or they can be enlarged for sight-impaired customers; they are reproduced on standard cut-sheet paper, which can be drilled for use in a ring binder. (The banks' marketing people see even more advantages: offering free binders to new customers, printing on drilled paper, printing marketing messages between the checks; the list goes on and on.)

Many banks offer reduced fees to customers who choose this option; indeed, the article reports that further fee reductions are offered to customers who don't want any checks (scanned images or otherwise) returned to them at all. If a cancelled check becomes necessary (as proof of payment, in case of a dispute with a credit card company, etc.), the bank will provide an image free of charge.

There was some discussion here lately of the ease with which bogus checks can be created by use of relatively cheap technology (laser printers and desktop publishing software). It seems that as the imaging technology gains more public acceptance, and as the banks push it more aggressively to reduce the costs of check processing, that there is a further RISK: if the scanned images are acceptable proof of payment, can the use of the same cheap technology to create bogus records be far behind?

\dbd

---

### ✉ Re: National characters on car plates

*Dik T. Winter <dik@cw.nl>*

*12 Sep 91 01:55:00 GMT*

Torsten Lif writes about the possible risk because Finnish car plates from the A\*land Islands (to follow his spelling) have a national character, and wonders what problems that might give in other countries. I think the problem is moot in this case, as there are (as far as I know) no duplicates in Finland, whether you leave off the ring or not. There is however a serious risk for people from Yugoslavia. One of their national characters is S with hajek (an upside down circumflex). There are indeed cars where the single distinction between two number plates is that hajek. E.g. cars from Sarajevo always start with the letters SA, while cars from Sabac also start with SA, but there the S has a hajek.

By the way, in Torsten Lif's own country (Sweden) until recently no national characters were used on car plates (A ring, A diaeresis and O diaeresis). With the introduction of vanity plates these are allowed, which again might result in confusion.

dik t. winter, cw, amsterdam, nederland dik@cw.nl

---

### ✉ re: Universal Character Set

*Robert Ullmann <Ariel@Relay.Prime.COM>*

*11 Sep 91 14:11:16 EDT*

What Hugh Davies and Kim Greer write on character sets ([RISKS 12.30](#)) was mostly correct, but is now out of date.

An ISO working group is working on a new version of DIS10646 (to eventually be IS10646) a multi-byte code set that attempts to be comprehensive, and will be extensible.

The Unicode Consortium and the ISO WG have agreed to merge their efforts, to create one (draft) standard. (The previous DIS10646 failed in the balloting for, among other things, not addressing Unicode: several NO votes, including the U.S., stated that having two different codes, 10646 and Unicode, was not acceptable).

One of the proposed representations of the code set is "upward compatible" with ASCII-7, and useable in mail (with 8-bit support). (Send a message to ISO-Char-Subscribe@List.Prime.COM to subscribe to a demonstration list.)

Two other points: there is a (set of) 8 bit sets defined by IS8859, which "solve" the substitute character problems that Davies laments (created by ECMA-35). 8859 is used by (among other things) Xwindows and Postscript version 2. (Of course, lots of people still use ECMA-35)

The ASCII/EBCDIC problem is "solved": SHARE (the IBM users group) has defined an invertible (reversible) mapping table, used by BITNET to Internet gateways. (I will supply a copy to anyone who wants it)

Robert Ullmann, Prime Computer, Inc.

+1 508 620 2800 x1736

---

### **✉ Re: Multinational Character sets**

*<hugh\_davies.wgc1@rx.xerox.com>*

*Thu, 12 Sep 1991 02:21:37 PDT*

Firstly, an apology, related to the topic under discussion. In my last posting, I used a dagger character to reference the footnote on the XCCS. I am writing this on a Xerox 6085 workstation, which uses the XCCS character set, and I forgot that the dagger would not be translated correctly by our mail gateway, so a string of weird characters appeared in the digest. A case in point, as if we needed one.

Secondly, klg@george.mc.duke.edu (Kim Greer) writes;

> Perhaps we have overlooked the risk of forgetting the origin of words and  
> what an acronym \*originally\* meant. "ASCII", as we all remember, stands for  
> American Standard Code for Information Interchange, the key word being  
> "American". Would it not be stretching things a bit to expect  
> non-"American" language nuances (like umlauts) to automatically fit in?

This would be entirely true, except that American computer manufacturers cheerfully exported their computers all over the world, without making any changes for the local language. It was ASCII or nothing. (Or EBCDIC or nothing!). They also didn't (and in most cases, I suspect still don't) translate their manuals into the local language. You don't read (American) English? Tough.

Perhaps this should be considered as another RISK that I hadn't considered? What happens when a standard is applied well outside it's original area? In the case of ASCII, the shambles we have today. The fact that the 'A' in ASCII

stands for "American" is irrelevant today. I suspect there are far more ASCII based computers outside America than inside it, and it's about time that we all realised that it is quite simply not good enough to expect a customer to learn a foreign language in order to use a product. You might also like to think about the fact that the majority of the people in the world don't speak English anyway. Does \*your\* computer "do" Pin-Yin and Cyrillic? (Mine does!)

Incidentally, the designers of ASCII wrought better than we might think. The ESCAPE character is supposedly intended to allow a system to insert non-ASCII characters (to "escape" from the ASCII set). Pity it's never used that way.

Hugh Davies, Rank Xerox, Multinational Customer & Service Education- Europe, Welwyn Garden City, Herts. England.

---

**✂ Re: +&\*\$ (Moore, [RISKS-12.21](#))**

*Mike Morris <morris@grian.cps.altadena.ca.us>  
Thu, 12 Sep 1991 08:26:10 GMT*

This is true in California - which has a 7-character plate format. My amateur radio callsign has 6 characters (note that ham calls can be from 4 to 6 characters). Almost all the dispatchers know that a plate of less than 7 characters includes a trailing space by default. If you run my callsign plate on the state DMV (Dept of Motor Vehicles) computer as WA6ILQ or WA6ILQ<space> it comes up just fine. If you run it as <space>WA6ILQ, or WA<space>6ILQ, or any other combination, it comes up with "Record not on file". This has caused me serious problems. Once I was pulled over by a cop who was as fascinated as I was when my plate wouldn't come up and we spent some time with his patrol car terminal discovering this quirk. You can imagine the reaction I get now when I tell the cops "Tell the dispatcher to run it as 'WA6ILQ<space>'". And it works.

Mike Morris WA6ILQ PO Box 1130 Arcadia, CA. 91077 818-447-7052 evenings

---

**✂ Source for Fallows' "Two Weapons"**

*Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>  
Wed, 11 Sep 1991 12:02:29 -0700 (PDT)*

"Two Weapons" (about the M16 and F16) is a chapter in James Fallows' book, NATIONAL DEFENSE, Vintage Books, 1982. I think the hardcover edition was from Random House, 1981, but I'm not sure.

Much of Fallows' book is a critique of technically complex weapons systems, which many RISKS readers would find interesting. Another excerpt from the book, describing Fallows' boyhood visit to a SAGE installation, appeared in RISKS a few years ago.

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

## **✂ Re: M16 and James Fallows**

*Tom Faller <tomfal@tr6.wes.army.mil>*

*Thu, 12 Sep 91 09:10:10 CDT*

James Fallows article "Two Weapons" is actually a chapter of his book "National Defense". The book discusses the perceptions used in forming a national defense policy, shows where these conflict with reality, and how the average person mistakenly perceives military life and its tools, and discusses trends in future military policy. The book just went through a revised edition, I believe.

Other good books on this subject include James Dunnigan's "How to Make War", and a book called "The Great Rifle Debate", by an author whose name I forget, but who does an excellent job of showing how the military armorers mind works.

The tie-in with computers is that most of these books include examples of sloppy war-gaming, over-reliance on favorable models, and a "if it's got more electronics, it's got to be better" attitude. A little-discussed fact is brought out; our own electronic Maginot Line, electronic, "smart", warfare. One thing nobody wants to admit too loudly is that we may be back to rifle-based warfare real soon if attacked with a nuclear weapon, due to the Electro-Magnetic Pulse (EMP) given off by a nuclear explosion. There are estimates that one good nuke, exploded in near-space over Kansas could fry most of the missile controls, computers, radios, phone switches, smart weapons, late-model automobile engine electronics, and other items this country depends on, nearly coast-to-coast. Nobody's really sure how serious this is, although a lot of testing and "hardening" goes on. And it's a losing game trying to keep ahead by shielding, a bigger bomb is just a lot cheaper than building defenses against it. There's some concern that any nuclear war will only last until the first few shots, as they will screw up the rest of the system, and any other missiles in the air. It kind of acts as a deterrent if you know that you only get one shot at it, and then you have to rebuild your arsenal from the chassis up.

Tom Faller

---

## **✂ Junk Mail -- In memoriam, Dave Sharp**

*Pete Mellor <pm@cs.city.ac.uk>*

*Wed, 11 Sep 91 19:52:16 PDT*

My apologies if this is of marginal relevance to the main subject matter of the lists to which I have mailed it.

UK readers might be interested to watch the forthcoming edition of Equinox on Channel 4 this coming Sunday, entitled "Junk Mail".

It was originally scheduled for 14th Oct., but was announced last week to be broadcast on 15th Sep. (I forget the time at which it will go out.)

The blurb on the advertising postcard reads: "How much do direct marketers know about us and how do they get our names? Why would they want to put a

brightly coloured fish in our mail?". (Photo on reverse of strange-looking man holding the fish in question over a glass of water.)

The programme was produced by Orlando Television Productions Ltd., for WGBH Boston in association with Channel 4.

Orlando was essentially Dave Sharp. As well as being a very good friend of mine, he was an extraordinarily talented film maker, and his one-man company established an excellent reputation for scientific (and other) documentary films.

"Junk Mail" promises to be a very witty and thought-provoking piece of TV journalism. It is one of the last films Dave completed before his untimely death in the collision between a 737 and a private aircraft at Los Angeles in February this year.

My thanks to those who responded to my e-mail request for information about the accident.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

---

### **✦ Risks of assumptions? (Re: Chase, [RISKS-12.28](#))**

*R. Cage <fmsrl7!wreck@sharkey.cc.umich.edu>*

*11 Sep 91 21:58:31 GMT*

>People don't compute the crash-safety of new automobiles (well, I'm sure that >they do at some early stage), they run them into walls to see what happens.

As it turns out, this is almost exactly backwards. Running a car, especially a hand-built prototype car, into a wall is horrendously expensive. Exercising a FEA model inside a Cray is very cheap in comparison, and it takes a lot less work to reconstruct a computer model after a crash, or modify it to work better.

About the only crash-testing we do these days is to confirm the results of the computer models. The sanity-checking is done; we have no chance of GIGO resulting in bad products getting out. The effectiveness of the models is a result of a great deal of work in building and testing them. It's a good thing that the properties of sheet metal are not very difficult to determine.

Having people just assume that climate models, or drug models, or population models are just as reliable is, IMHO, a big RISK.

Russ Cage wreck@fmsrl7.srl.ford.com russ%rsi@sharkey.cc.umich.edu

---

### **✦ The seriousness of statistics mistakes**

*Jeremy Grodberg <jgro@lia.com>*

Wed, 11 Sep 91 20:33:05 PDT

[RISKS-12.28](#) contained two instances of statistical fallacy, the less important of which was corrected in 12.29, and for which the moderator referred us back to earlier threads to which I had contributed. Lest you think I whine about people's misuse and misunderstanding of statistics just so I have something to complain about, I want to point out that the second statistics mistake was truly a life-or-death decision.

In [RISKS-12.28](#), Mark Fulk writes:

>The Maternal Serum Alfa-fetoprotein (MSAFP) test is administered to pregnant  
>women in order to screen for a broad range of congenital defects of the fetus  
>[which I will simply call "the disease" -- JG][...]

Let's presume Mr. Fulk's base data is correct, that the MSAFP has a 10% False Positive, is confirmed by amniocentesis which carries a 1% chance of inducing abortion, and let's also say that the chance that someone taking the test actually has the condition tested for is 1 in 10,000, which the high end of the risk range he gives.

I believe he made the wrong decision about having the test based on an incorrect analysis of the data. He claims a .1% chance of the MSAFP leading to an inadvertent abortion of a healthy fetus. I can only guess that his reasoning was: 10% of people taking the test have healthy babies but will test positive, and 1% of that 10% will lose their babies because of the amnio, and 1% of 10% is .1%, so there is .1% chance of killing a healthy fetus. Unfortunately, this analysis is wrong, because of an important, less common error (which is becoming more common as people deliberately try to mislead with statistics): misunderstanding the definition of a statistic.

Mr. Fulk made his mistake when he assumed a 10% False Positive rate meant that 10% of the people taking the test get positives that are really negative. However, it actually means that 10% \*of the positive results\* are really negative. Putting this together with the 1 in 10,000 chance for a True Positive, we come up with a 1 in 90,000 chance of taking the test and getting a False Positive (90,000 / 10,000 is 9 True Positives, which generates 1 False Positive), or a 1 in 9,000,000 chance of the MSAFP test leading to the death of a healthy fetus. Thus the test will detect 900 afflicted babies for every 1 healthy one it harms. This is the real decision making criterion, and speaks much more highly for the utility of the test.

Let me quickly add that the above analysis is inaccurate (but close), because I don't have all the necessary data. False Negatives need to be factored in correctly (which can be tricky), and there may be other data which is a better basis for predicting the possibility that a specific individual (such as a 29 year old healthy woman) will have a false positive versus having the disease. Also, a True Positive refers to someone who has the disease and tests positive, which is a subset of the people that have the disease, although the above analysis assumes that they are one and the same (no False Negatives), which Mr. Fulk tells us is not correct. My point is that the above analysis brings us a lot closer to the best information than Mr. Fulk's did, because of one simple mistake he made.

There are a number of other interesting aspects to this story which I

want to point out, in no specific order. Medical professionals have difficulty with these statistics, too. I asked a few people who have been involved with clinical drug testing (where the data for such statistics is gathered and analyzed), and none of them were sure off the top of their head of which of the two versions of % False Positive was correct, although they all knew where to look it up, and most made the right guess. Clearly the people Mr. Fulk talked to were not conversant enough with the statistics to correct his mistake.

What is worse, for some reason (which I leave to the reader to wonder about), Mr. Fulk did not find it unbelievable that his doctor would recommend a test which was 10 times more likely to kill his fetus than the disease was (.1% or 1 in 1,000 by Mr. Fulk's analysis, vs. 1 in 10,000 for the disease), and 1,000 times more likely to give an erroneously positive result than it was to detect the disease (10% or 1 in 10 vs. 1 in 10,000). I'm surprised and dismayed that he did not notice this and check further to find his mistake. Although we in the General Public have problems with statistics, our medical and scientific establishment, through researcher care, peer review, and governmental regulation have a very good record on handling the statistics carefully and correctly before the medical public policy decision is made. If the test was as bad as Mr. Fulk thought, standard practice would have been formulated to recommend against testing in his case. For example, because the prevalence of smallpox is so low, you are now more likely to get it from the vaccine than from anywhere else, so only people with higher-than-average risk factors (like people who work around smallpox-infected patients) are given the vaccine. If anything, public policy decisions are more likely to deprive you of beneficial tests because of the monetary cost (e.g. physicals for people in their 20s) than to suggest spending money on tests with high risk/reward ratios.

So here is another lesson on the risks and dangers of innumeracy. This is why I'm on a mini-crusade about statistics. This stuff *\*is\** hard, and we can't all be experts on it, but let us at least learn to know when and why we need to ask the experts, what we need to ask them, and what we can do to check on what they tell us. The life you save may be your own.

Jeremy Grodberg jgro@lia.com

---

### **✂ Risk Assessment: a specific experience (Wayner, [RISKS-12.29](#))**

*Justine Roberts <JROBERTS@UCSFVM.BITNET>*

*Wed, 11 Sep 91 20:12:31 PDT*

In [RISKS-12.29](#), Peter Wayner writes that amniocentesis-caused abortions are "a violation of the Hippocratic Oath. The patient died because the doctor was curious..." This is a distortion. The amniocentesis procedure is NOT carried out because a doctor is curious. It is requested by parents and/or recommended by physicians because there is reason to believe that there may be a problem with the pregnancy or the fetus. Any halfway good doctor will inform parents of the abortion risk which accompanies the procedure, and the parents can then refuse the procedure if they wish. Wayner seems to assume that abortions are caused only by human intervention. The percentage of naturally occurring abortions is much higher than 1-2%.

Justine Roberts, 152 Sycamore Ave., Mill Valley, CA 94941  
jroberts@ucsfvm.bitnet jroberts@ucsfvm.ucsf.edu (415) 388 6814

---

**✂ Re: risk analysis**

*victor yodaiken <yodaiken%chelm@cs.umass.edu>*

*Thu, 12 Sep 91 08:03:51 -0400*

At least some of the Post-Three-Mile-Island nuclear energy risk assessment literature has a, IMHO, properly humble tone. Here are 3 examples (transcription errors are mine, apologies to the authors):

The formulation of societal risk as an expectation value runs into difficulties when the probability of the event is low, but the consequence is high if it occurs. In this case, there would be no consequence or a very large consequence. Therefore the use of expectation value does not adequately reflect the real societal risk because the numerical value does not reflect a consequence that would actually occur. [...]

The criteria recommended in this article have no fundamental basis. Indeed, there is no fundamental approach to this issue and no way of proving whether any proposed criteria are right or wrong except by using them over a period of time and discovering whether the costs, risk, and other consequences of their use meet the requirements of society.

D.J. Higson, Nuclear Safety Assessment Criteria,  
Nuclear Safety 31-32 April-June 1990 193-185

Finally, and perhaps the most important lesson learned, risk analysis helps recognize questions that can be posed in scientific terms but cannot be answered by science (page 102)

Paolo F. Ricci in the Brookhaven/EPRI workshop on "Health and Environmental Risk Assessment" (Pergamon Press, 1985)

[In reference to Probabilistic safety analysis methods]

The modeling of dependent events, particularly human error and external events, is still less advanced. It should be noted that the qualitative aggregate results of PSAs, e.g. probability for core melt, for releases of radioactive materials or for health effects on the public should not be interpreted as frequencies in a statistical sense, although they are expressed in like units. Rather, probability is a numeral measure of a state of knowledge, a degree of belief, a state of confidence.

L.V. Konstantinov "On the Safety of Nuclear Power Plants"  
Nuclear Engineering and Design 114 (1989) 2 Page 183

---

## Averages and distributions

*Jerry Leichter <leichter@lrw.com>*

*Thu, 12 Sep 91 10:16:34 EDT*

A recent RISKS article repeated the old platitude that "by definition, half of all people have below average intelligence" (or are "below average drivers", or whatever). This led to the ritual replies, truncated by the editor, pointing out that, if by "average" you mean "mean" (the usual case), then this need not be true. In fact, it's easy to construct distributions that make it "as false as you like".

That's all very true, but it's important not to replace one mantra by another. Many measures of the real world have normal distributions. Most deliberately constructed measures have normal distributions, essentially by construction. For a normal distribution, or anything at all close to it, it is a fact that half of all measured values will be below the mean.

If you think the "average" in "average intelligence" really refers to "mean", then you need to have a numeric measurement of intelligence to make any sense of the remark. While it's been years since I looked at the literature in the field, all the various IQ scales I know of have very close to normal distributions. (They can't be EXACTLY normal since, if nothing else, an IQ can't be less than 0, and a normal distribution has infinite tails.) For IQ's, "by definition, half of all people have below average intelligence" is true.

If by "intelligence" you mean some vague idea about how bright people are, then you can only interpret "average" as a qualitative English term. My Roget's Thesaurus has the following "cluster" under MEAN: mean, middle state, middle ground; golden mean, juste-milieu [F.]; medium, happy medium; average, balance, normal, rule, run, generality; middle term [logic.], mezzo terrine [It.]. Another cluster, under GENERALITY, lists: The generality, average, ruck, run, general ~, common ~, average or ordinary run. From this it's clear that English speakers use average for a cross between "mode" and "median", depending on context. Actually, I'll argue that when we say something is "average", we aren't just picking a sense of "mode" or "median" at random; we are assuming that the two are roughly the same. After all, the rough opposite of "average" is "extreme" or even "unusual". Think about exactly what you are saying when you describe something as of "average" quality.

For a purely qualitative "average", a statement about how many items are above or below the average is difficult to interpret. In one way, it's pretty meaningless: Most things will be "average"; if we don't attempt to sub-divide those, then we're only talking about the outliers, which are presumably rare. Saying about half are above and half below the big central block means little.

In fact, however, I suspect most people, if pushed to divide things up into, say, three groups - below average, average, and above average - will put more things in average than either of the others, but will put roughly equal numbers in the "above" and "below" groups. This seems fundamental to what we mean by "average". (This would make an interesting and easy experiment. Any social scientists or linguists want to follow up on it?) To the degree that my prediction is right, the statement that "half are below average" isn't quite true, since so many will turn out to BE average; but of the ones that

AREN'T average, it WILL be true.

If I remember right, the place this issue first came up was the statement that more than half of all drivers (particularly men) believe they are "above average" drivers. It would be quite reasonable for a large fraction of drivers to believe that they are "average or above" - that simply requires a broad, fuzzy middle ground, typical of qualitative measures. But it requires a very bizarre and unlikely measure of driving ability for a large fraction to actually be ABOVE average: It requires that some small number of drivers be EXTREMELY bad. Not only can I see no plausible evidence for this, I can instead see plausible evidence for the opposite: Race drivers and other professionals are clearly MUCH better than most drivers.

Mathematics is all well and good, but the APPROPRIATE APPLICATION of mathematics is what's useful!

-- Jerry



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 12: Issue 32

Thursday 12 September 1991

## Contents

- [Security in software distribution](#)  
[Joe Morris](#)
- [Re: Crackers for hire](#)  
[Joan Eslinger](#)  
[James Deibele](#)
- [Re: Helpful Viruses?](#)  
[Stan Kurzban](#)  
[Bob Johnson](#)  
[Chuck Royalty](#)
- [Re: Cheap air tix](#)  
[Mark Seecof](#)
- [Re: EMP](#)  
[Phil Agre](#)  
[Tom Faller](#)
- [Re: The seriousness of statistics mistakes ...](#)  
[Mark Fulk](#)  
[Ronald A. Thisted](#)
- [Re: ASCII](#)  
[Eric Florack](#)  
[Mark Seecof](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Security in software distribution**

Joe Morris <[jcmorris@mwunix.mitre.org](mailto:jcmorris@mwunix.mitre.org)>

Thu, 12 Sep 91 13:48:16 -0400

Although the (in)famous technique of shrink-wrapping personal computer software has been around for a long time, mainframe software has generally been shipped with no seals other than those on the shipping box. A frequently-proposed trojan horse technique (never used, as far as I know) has been to send a computer center a box with media and documentation which appears to have come from the operating system vendor, but in reality is a trojan horse. A modification of that procedure involves intercepting

a legitimate shipment and changing the contents.

This may be changing. I recently received a shipment of IBM's RS/6000 AIX system on tape cartridges. Each cartridge is enclosed in a heat-sealed heavy plastic bag on which the IBM logo is printed, along with the legend:

This tamper evident bag ensures the integrity of your software. If tamper is evident, please call the IBM software distribution center (1-800-879-2755) to report problem and have center replace the questioned software.

(Incidentally, the bad grammar in the above paragraph is correctly copied from the text on the bag.)

The fact that I don't have an RS/6000 is irrelevant. Maybe one of these days IBM will figure out how to fix the data base systems used to generate mailing addresses for software shipments...although in this case I suspect that the problem was bad data entry, unlike the dozen or so other RS/6000 packages I've received over the past year which were addressed to me by name.

Joe Morris

---

### **re: Crackers for hire**

*Joan Eslinger <wombat@key.amdahl.com>*

*Thu, 12 Sep 91 10:31:03 PDT*

A few press releases from IBM yesterday make the cracker-for-hire business a little more serious. More interesting data will be available in local offices soon, so instead of spying on co-workers in the same office, the opportunity will exist to spy on vice-presidents. The announcements cover products that will be available sometime next year.

\* "Information Warehouse," intended to allow easy access to all data owned by a large corporation from any desktop computer within the company, in most popular formats (Lotus, DB/2, SQL, ...).

\* a partnership with Aristacom, a company which makes telephone switch / computer interfaces:

"With Aristacom's [earlier] applications a call is automatically routed to the targeted service agent with the information required to permit immediate service to the customer. This eliminates the frustrating interaction between customer and agent about the nature of the call and the identity of the customer."

\* operating system enhancements and applications to assist in the development of client/server applications between IBM mainframes and pc's running OS/2, DOS, and Windows. They are also starting to support more interactions with Suns and Macintoshes. Two of the new applications are described as follows:

-- IBM SAA ImagePlus(a)/2, a new LAN-based application for tracking and distributing image applications such as

insurance claims, loan applications and legal contracts.

-- Financial Branch Systems Services, a client/server software package that supports financial applications such as those used in a banking branch office. Also announced is support for DOS Windows users, which supplements the OS/2 and DOS support already available.

Joan Eslinger / wombat@key.amdahl.com

---

**✂ Re: Crackers for hire (Linda Edwards via Seecof, [RISKS-12.29](#))**

*James Deibele <jamesd@techbook.com>*

*Thu, 12 Sep 1991 21:38:29 GMT*

>In the September 19th Rolling Stone at page 67 an article titled "Samurai  
>Hackers" by Lynda Edwards tells us that a: "new breed of hacker has been  
>finding a niche in the corporate world in the last two years. ...

Having read this article, *\_The Cuckoo's Egg\_*, and *\_Cyberpunk\_*, I was struck by the "samurai hackers" referring to their customers and victims as "stupid". True, those people may not know a whole lot about computers, but these hackers don't seem to know that much more. What they do have is the persistence to sit in front of a machine for hours, trying passwords until they finally get one. The fact that they do seem to often guess a password is certainly a risks-related matter.

But having someone sitting for hours in front of the console entering names should be picked up by almost anybody. "Hmmm, Joe complained about the phone line being busy all weekend, but nobody logged in. I wonder if there's something wrong ..." would seem an unavoidable concern in such cases.

These "hackers" seem the equivalent of the smash-and-grab bandit: they throw a brick through the window, grab what they can, then run. They're limited in effectiveness by the crudeness of their methods, but they can be effective nonetheless. Almost all of the sophisticated computer types seem more attracted to the "good side," but given a large enough dislocation in the economy, as we might see in a serious recession, the temptation to invade other computers might seem attractive to computer professionals.

Another item was how willing people were to give out information over the phone. In *\_Cyberpunk\_*, the hackers in California were repeatedly able to impersonate someone at the phone company or in the military well enough to get information that they had no business having. "I'm General Shotfoot's aide, and he wants to know what his password is ..." seems to work fairly well. Elementary security would be to get the number of the person calling, and call them back. But as long as there are humans in the loop, computers will be vulnerable to this type of attack.

One last thing that was interesting was how abusive most of the people using e-mail were of others. As shown by other articles on electronics communications, people have no hesitation saying things in e-mail that they

wouldn't dream of doing face-to-face or on paper. One article I read talked about how two groups were assigned tasks; the group that met only in the flesh conducted their meetings without incident. The one that was conducted partly using electronic communications had people who had to be separated and sent out through different exits to keep them apart. Might one of the increasing risks of electronic communications be getting attacked by someone outraged by what you said about them electronically?

Public Access UNIX at +1 503 644-8135 (1200/2400) Voice: +1 503 646-8257

---

### ✉ Helpful Virus?

<kurzban@thornvm.vnet.ibm.com>

Wed, 11 Sep 91 15:38:31 EDT

Fred Cohen says in a number of his papers that (quoting from Computers & Security, Vol. 6, # 1, PP. 22-23) "The term virus has also been used in conjunction with an augmentation to APL in which the author places a generic call at the beginning of each function which in turn invokes a preprocessor to augment the default APL interpreter." (Although Fred always attributes the idea to a paper by Gunn in "ACM" in 1974, the paper actually appeared in ACM Quote Quad in 1984, in the Proceedings of a Helsinki conference.) What Gunn described does not fit Fred's definition of a virus, but something that does could serve the purpose Gunn described, as best I can remember. Note that APL is a logical place to expect a useful virus because APL users may leave functions vulnerable to modification in the hope of benefiting from improvements that others make.

Stan

---

### ✉ Re: Prize for Most Useful Computer Virus (Rice, [RISKS-12.30](#))

Contractor Bob Johnson;SCSS <robjohn@ocdis01.oc.af.mil>

Wed, 11 Sep 91 16:59:01 -0600

Brian Rice writes:

> ...all viruses are bad, because they take  
> me out of control of my system and make me afraid to do things with it.

Novice users feel this same fear, until they learn how to get along with the computer. Viruses, however, tend to make their computers unpredictable. When something drastic happens because the user isn't knowledgeable, they "chalk it up to experience" and go on. The damage done by a virus, though, is entirely out of their control. The user feels violated because someone came into their "territory" and damaged them in some way, even if the "damage" was just to their confidence. (Administrators of large systems have to be very careful during system maintenance to avoid invoking the same territorial feelings in their "users" ;-).

Configuration management within a community of PCs presents many of the same problems as system maintenance on large systems, and invokes the territorial tendencies of most users ("Whaddaya mean, I can't use PD software on my

machine!?!?!"). It gets more important when all of these PCs are connected through local area networks. In a previous job, we experimented with having each PC automatically log into a central server, compare it's binaries with the "distribution version", and automatically download anything new. We discussed having this routine remove "unauthorized" software, but figured it would be too easy to mess up and remove something valid by mistake.

More recently, I have learned of a product which loads a TSR when you boot each workstation, which can give control of that machine to a central administrator via the LAN. The administrator can then "poll" the workstation and perform maintenance over the LAN - including making filesystem maintenance and even copying new executables onto the PC. This sort of maintenance can happen "in the background", invisible to the user (who has no idea his/her system is being "maintained").

If you extend the idea, you could create a "configuration checker" virus that wandered thru the network, reporting system configurations back to a central authority. Is this a good idea? Depends on whether you're the user or the administrator. It wouldn't be hard to add other "useful" features. Perhaps it could find files that haven't been used in six months, archive them to tape, and then delete them from the user's system. Where do you stop?

IMHO, any time "my" computer is changed without my knowledge, I have the right to become upset - even if somebody else actually owns it. This includes viruses, configuration management, maintenance, or whatever. The underlying risk (the one which would lead to "good viruses") is what I call the "God Syndrome" -- "I know what's best for you because I'm [your\_title\_here]". That risk is prevalent EVERYWHERE, not just in computers. We see the risk more readily in other fields (such as government). Because most people don't understand computers well (yet), the risk is not so clearly seen.

Bob Johnson, Control Data Corp (contractor to...) Tinker Air Force Base,  
Oklahoma DSN: 339-5038, (405) 739-5038

---

### **✶ 'beneficial virus' is an oxymoron**

*Chuck Royalty <chuck@helpful.ca.boeing.com>  
Thu, 12 Sep 91 13:06:30 PDT*

No one has addressed the question of a 'beneficial' virus in terms of the growing concern in business over the amount of trust that can be placed in the results produced by computer systems. That concern is manifesting itself in several ways:

1. An increasing amount of attention is being paid to configuration control of support (engineering, manufacturing, etc.) systems. We can't test everything and we can't test anything exhaustively, but we want to know that what we're relying on has been tested to the extent possible and necessary so we have an idea where we're at risk. This breaks down if we can't pin software configurations down to the bit level -- any virus, beneficial or not, clearly compromises this effort.

2. We are seeking reasonable ways to hold vendors responsible for the results produced by the software they deliver. As the public begins to demand warranties (beyond the usefulness of media) for software, vendors will increasingly have to protect themselves by carefully specifying the system configurations for which warranties apply. Modification of underlying software by viruses, no matter what their intent, would also be contrary to a vendor's ability to guarantee results.

It seems apparent to me that we have to work towards the ability to completely specify and audit the configuration of systems on demand in order to have a chance of dealing with the legal and safety implications surrounding general use of computer based systems by lay people. Much as a piece of digital hardware refuses to be functional if it fails its own self test, software must be able to identify its configuration and respond appropriately prior to providing service in critical situations. We take this for granted in ROM-based embedded systems, but their safety is due solely to their isolation and resistance to alteration. Both of these conditions are rapidly disappearing.

Chuck Royalty      (206) 957-5197      chuck@helpful.ca.boeing.com

---

### ✂ Cheap air tix (re: [RISKS 11.60](#))

Mark Seecof <marks@capnet.latimes.com>

Wed, 11 Sep 91 14:05:10 -0700

In [RISKS-11.60](#), Jerry Leichter told us about the new struggle between airlines' load-management software and travel agents' computer programs which search for elusive low fare offerings. (I cannot do justice to Mr. Leichter's fine piece here).

He pointed out a risk to consumers:

> The computers battle it out--and anyone without computer  
> assistance is likely to be left on the ground.

The next chapter in the saga is discussed in an L.A. Times article by Denise Gellene titled "Airlines Discourage Bargain Hunts" (9-10-'91, page D1). [Bracketed interjections and elisions mine -MS] The article:

[...] Only a handful of travel agents use this new technology [automatic fare-finding software which "electronically scan[s] thousands of fares listed in an airline reservation system"], which can potentially save [individual] consumers hundreds of dollars. [...] Santa Ana-based Associated Travel Management says its computer program saves an average of \$150 for one customer in four.

But the new computer programs have drawn a strong reaction from the airlines. Sabre and Apollo, the reservation systems controlled by American Airlines and United Airlines, have socked the agencies with new fees to discourage extensive fare searches. Associated Travel said the new charges could cost it \$300,000 a

year.

The conflict over the new software has important implications for travel agencies, airlines, and consumers. Travel agents need an edge to draw customers, but airlines make most of their profits from higher-priced tickets. Consumers are caught in the middle.

The software helps travel agencies keep up with the thousands of fare changes airlines make daily. Working 30 times faster than a travel agent, the software can scan through a reservation system and snare customer-pleasing bargains that an agent might never spot.

[...] The reservation systems say the new fees are justified because the new programs cause reservation networks to work harder. But agents and other industry experts say that the airlines are also concerned that the new technology finds low fares for business travellers [...] who normally pay full fare.

"I think the main intent is to limit the user of these programs," said Steve Ballinger, editor of Travel Management Daily, an industry newsletter. "It seems the airlines are saying that just because there is a cheap fare out there doesn't mean you have an unlimited right to find it."

The controversy comes at a time when both airlines and travel agents are doing poorly. Airline traffic fell in July and was expected to decline overall in August as recession-battered consumers cut back on travel. [...]

[stuff about airlines trying to avoid selling low-priced tickets; and agents looking for ways to improve customer service by saving clients' money]

[the reservation systems are imposing fees designed to penalize automated searching. Searches which appear to be manual based on pattern of keystrokes and number of records retrieved aren't surcharged.]

The fees are likely to discourage small agencies from investing in the new [searching] software, which costs up to \$150,000. "There is no way a small agency can afford it," said USTravel's Nugent.

[some more details]

Not every agent finds the new limits easy to live with. Boston-based Woodside Travel said some agents in highly competitive markets, such as Los Angeles, exceed the new keystroke-thresholds manually because there are so many airlines to check.

[various back and forth about the new fees]

Travel agencies say they've taken steps to avoid hefty fees.

Associated Travel developed what it calls a "steath" version of its original software that is capable of taking an electronic picture of the information in the airline reservation system. Associated's computer then scans the electronic copy for bargains. By using this technique, the agency immediately reduced the [usual] number of hits [per fare query] to 112 from 200. Though it

may still pay a fee, it is less than the \$300,000 it stood to pay without the revised software.

Other agencies have taken different approaches. Woodside travel said it now looks for aisle or window seats less often. USTravel says it now conducts most of its searches at night, when fees are lower and most fare changes are made.

``We don't think American's Sabre is out to destroy our program," Woodside's Barros said. ``We think they would like to control how we use it." [-30-]

[Begin Mark S.'s comments.]

The tactic of caching replies from reservation systems to avoid repeating costly queries seems wise, but cache-consistency problems must come up.

The reservation systems' argument--that a high query load is costly for them--is valid so far as it goes, but the reservation systems are deliberately organized so as to preclude direct searching for low fares. If they maintained methods (and indices) to permit searching for fares, then the number of queries necessary to find low ones would drop dramatically. Of course, this gets back to the "antitrust" problems with reservation systems owned by airlines. You-all know all about that stuff, but I'll remind you that the government is in the middle of hassling a bunch of airlines for allegedly conspiring to fix fares using the O.A.G. as a signalling channel, so an "independent" system for such flight/fare info may not be a total fix.

The airline vs. agency computer wars would not be necessary if the airline systems supported the sorts of queries the agents want to process. The high price of fare-search software means that ordinary consumers are left at the mercy of the battling giants. One sure fix for all of this would be to force the airlines to provide low-fare searching. One big cost to that would be the blow it would surely deal to airline profits, and, I suggest, to the availability of low fares. The airlines have been amazingly successful at flying everyone for exactly the (maximum, it's true) price s/he can or will pay. If it looks like they'll have to let some people travel for less (than they can/will pay), the airlines'll just eliminate the lowest fares, leaving some impecunious would-be travellers on the ground.

Is computer reservation system low-fare searching compatible with reasonable "load management" by airlines? Who should take the risks in reservation-system design, consumers looking for low fares or airlines looking for efficiency?

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

---

✉ **EMP (Faller, [RISKS-12.31](#))**

*Phil Agre <pagre@weber.ucsd.edu>*

*Thu, 12 Sep 91 13:31:09 pdt*

[...] There are estimates that one good nuke, exploded in near-space over Kansas could fry most of the missile controls, computers, radios, phone switches, smart weapons, late-model automobile engine electronics, ...

I think this logic might be a little backwards. If the first shot really does neutralize everything larger than a rifle, then (as many have pointed out in other contexts) this is a strong motive for a first strike. This fact in turn a strong motive for a policy of launch-on-warning. The destabilizing results, though, are proportionate to the state of knowledge about EMP, or rather to our perception of the other folks' perception of ... . With any luck the darn things will be scrapped soon.

Phil Agre, UCSD

---

**✂ Re: EMP**

*Tom Faller <tomfal@tr6.wes.army.mil>*

*Thu, 12 Sep 91 16:07:35 CDT*

Actually, I agree with Phil Agre that the initial reaction of the military mind would be to go to a launch on warning policy, and that the military leader's usual scenario is that he rides it out in the bunker while we take damage, but manage to pound the enemy into the stone age. I didn't mention that most of our subs would still be around to throw some weight in after the initial salvo, making it potentially a long war.

What I think really scares the brass is the possibility that each side would try a strike, fry a few missile sites, but also 95% of each other's consumer electronics and military CCC (Command, Control, and Communication) circuits, and face a completely hostile home population with a relatively impotent military force, and a few subs capable of nuclear war only. I can see the entire population of Denver, relatively unscathed but for their cars, TV's, Walkmans and PCs walking out to "The Mountain" with shovels in hand, and a couple of hemp ropes.

This is not the kind of scenario you can model on a wargame computer, but I'm sure it's run through the generals minds at least once. The Soviets are getting a version of this right now, except substitute "economic planning" for "nukes" as the catalyst.

Phil's right though; the more we learn about nuclear war, it seems the less we know; that realization is probably the biggest deterrent.

Tom Faller

---

**✂ Re: The seriousness of statistics mistakes and MSAFP**

*<fulk@cs.rochester.edu>*

*Thu, 12 Sep 91 15:30:10 -0400*

Jeremy Grodberg may be correct in assailing my article, but he assails the wrong thing. I may have misused the term "False positive rate."

Roughly 10% of MSAFP tests are positive; very few of those tests are true positives. My source is the pamphlet on MSAFP passed out by our obstetrician, which does not use the phrase "false positive rate."

I don't have it immediately to hand, but a paraphrase would go: "1 in 10 MSAFP tests are positive. In the vast majority of cases, this means nothing. If you have a positive MSAFP, your doctor will recommend amniocentesis to make sure that your baby is healthy."

Other phrases: MSAFP detects about 2/3 of neural tube defects and about 1/3 of cases of Down's syndrome.

By the way, I also had my figures confirmed by my friendly genetic counsellor at Strong Hospital.

Am I alone in feeling that phrases like "False positive rate," although they may have unambiguous technical definitions, are misleading in normal use?

Mark Fulk

[You are not alone. There are some people who prefer TYPE ONE ERRORS and TYPE TWO ERRORS to False Positives and False Negatives. PGN]

---

**✉ Re: The seriousness of statistics mistakes (Grodberg, [RISKS-12.31](#))**

Ronald A. Thisted <[thisted@galton.uchicago.edu](mailto:thisted@galton.uchicago.edu)>

Thu, 12 Sep 1991 23:17:57 GMT

First, if we consider only the risk of Down Syndrome and not other conditions which alter MSAFP, approximately 1 in 800 term deliveries have the disease. The age-specific risk (=incidence) at birth ranges from 1:1700 at age 20 to about 1:30 at age 45. The risk of spontaneous abortion with amniocentesis is generally estimated between 0.5% and 1%.

Second, MSAFP is used as a screening test, not a diagnostic test. Roughly speaking, a screening test is used to obtain a more accurate person-specific risk estimate. The MSAFP results can affect the risk estimate by a factor of four in either direction.

Third, Mr Grodberg takes Mr Fulk to task for incorrectly interpreting the term "False positive rate". Unfortunately, the term has \*no\* unambiguous meaning, and is routinely used to refer to either of two rates, depending on which is more appropriate to the setting. I have seen standard books in epidemiology define the term differently, and the only safe course is to avoid the term altogether or to be careful in defining it.

"False positives" (N+) are people without the disease (N) with a positive test (+). As such, they are a subset of people without the disease. They are also a subset of the people who will have a positive test result. If we are interested in the effect of screening on a population, we are interested in  $FPR1 = (N+)/N$ , the fraction of normals who will falsely be screened positive. On the other hand, if we are interested in how much credence to give to a positive result, we are interested in the  $FPR2 = (N+)/(+)$  = 1 - Positive Predictive Value. The second formulation concerns the diagnostic value of the test, when applied in a particular population. The greater the prevalence of

the disease in this population, the greater the fraction of positive testers who actually have the disease.

In the case of MSAFP, the a "positive" result occurs when the risk, adjusted for age and MSAFP level, exceeds some threshold (1:250 is often used). Individual physicians and patients may well select other thresholds. Using the typical value for the threshold, about 5% of normals will screen positive, and about 30% of Down cases would be detected.

In point of fact, then, Mr Fulk's assumption was closer to the truth than Mr Grodberg's. But the point is similar:

- (1) Bad data may result in less than optimal decisions
- (2) Bad statistics may result in less than optimal decisions
- (3) It helps to make damn certain that the other guy is actually saying what you think he is.

Ron Thisted    Department of Statistics/The University of Chicago

---

**✉ Re: ASCII ([RISKS-12.31](#))**

*<Eric\_Florack.Wbst311@xerox.com>*

*Thu, 12 Sep 1991 12:46:35 PDT*

<>Incidentally, the designers of ASCII wrought better than we might think. The ESCAPE character is supposedly intended to allow a system to insert non-ASCII characters (to "escape" from the ASCII set). Pity it's never used that way.<<

What, you've never heard of ANSI? What of the attempt at international chrs in THAT set? Dose this count for nothing? I know of damn few DOS systems that do not have an ANSI driver mounted at all times....

---

**✉ Poor ASCII ([RISKS 12.29-31](#))**

*Mark Seecof <marks@capnet.latimes.com>*

*Thu, 12 Sep 91 15:52:15 -0700*

The moldy political odor rising from some of the remarks about ASCII and limited character sets recently published in RISKS bothers me a lot. ASCII is not some poison forced down non-English speakers' throats at gunpoint. It is not an evil scheme to enforce American cultural hegemony on long-suffering Europeans, or Asians, or anybody. Dammit, people did and do buy all that ASCII-based software and firmware of their own free will. When it doesn't suit them, they buy something else or roll their own.

We're lucky we've got 8-bit 8859 and 7-bit ASCII instead of a 6-bit code like CDC used to use (ever look at Jensen+Wirth, the "Pascal User Manual and Report"?). Soon we'll have wider codes. The falling price of computer storage, both core and secondary (e.g., disk), alleviates the pressure to keep character representations small (in terms of bits). It would not have been rational to use 16- or 32-bit chars on a machine like the 1401 or PDP-8; so how many of those fancy latin-characters-with-diacriticals (of little use in the

States) would you have expected U.S. developers to support on yesterday's hardware? And you can forget other alphabets or ideographic systems.

The risk here lies in imputing political meaning to technical decisions taken long ago which were quite rationally based upon the technical constraints felt at the time. People tend to think of a computer as some magic thing; if it doesn't do what they want they suppose that the system developers were wicked or subject to sinister influences. It just isn't so...

As customers demand and are willing to PAY FOR computer stuff which works with more characters, various writing directions, context-dependent writing schemes, etc., the world's vendors are making it available. Don't dismiss the cost factor--a developer in the U.S. might have to demand a lot of money from a client in Yemen to make it worthwhile diverting his scarce manpower and short time into making an Arabic version of some software.

Some people whine about the fact that one package or another which they want to use isn't "internationalized" but those people are rarely willing to pay the cost of "internationalizing" (or merely "other-nationalizing") the stuff just for them. Vendors looking to do well in markets outside the U.S. and the British Commonwealth do make efforts to accomodate their customers. As the problem of data interchange across linguistic or orthographic boundaries grows with improved data communications, people work on schemes like DPIS10646 for characters and other, fancier schemes for non-English orthographies and to support message translation.

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 12: Issue 33**

**Sunday 15 September 1991**

## Contents

- [British Telecom computer failure cuts off 42000](#)  
[Paul Leyland](#)
- [Security Software Bug Locks Up System](#)  
[Sanford Sherizen](#)
- [Companies Steal Information](#)  
[Sanford Sherizen](#)
- [Industrial espionage](#)  
[Jerry Leichter](#)
- [Re: Junk Mail ... 737 crash](#)  
[Steven Philipson](#)
- [RSA vs. NIST \(digital security standards\)](#)  
[Tom Slone](#)
- [Re: Salomon Brothers -- Database Design](#)  
[Gary Beckmann](#)
- [Secret Computations the basis for Corporate Decisions](#)  
[Jeffrey Sorensen](#)
- [Re: +&\\*\\$](#)  
[Bob Clements](#)  
[H. Fuss](#)
- [History of Internationalization of ASCII](#)  
[Paul Green](#)  
[Lars Henrik Mathiesen](#)
- [Export controls on workstations, or, more mantras](#)  
[Jerry Leichter](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **British Telecom computer failure cuts off 42000**

*Paul Leyland <pcl@oxford.ac.uk>*

*Fri, 13 Sep 91 13:15:30 +0100*

A very brief report appears in the Friday 13th edition of *\_The Times\_* (London):

42,000 cut off

Police sent out emergency patrols after a British Telecom computer breakdown cut off telephones in 42,000 homes and businesses in the West Midlands

---

## ✂ Security Software Bug Locks Up System

*Sanford Sherizen <0003965782@mcimail.com>*

*Sun, 15 Sep 91 19:57 GMT*

The 9Sep91 issue of Computerworld had an interesting twist on security and reliability. A faulty piece of code embedded in the Tandem Safeguard security system interpreted 4:22 PM on 27 August as an impossible command. Affected systems tumbled into an endless loop that tied up all computer resources. The security package then locked up the system. The only way to fix the problem, once it began, was to take the affected computers off-line before restarting them. Starting in Asia and continuing on to Europe, the appointed hour of doom arrived, precipitating system shutdowns. Users in the U.S. were warned by last-minute phone calls. (Luckily, there were no phone outages this time.)

In an understatement, the writer said that some sources expected Tandem to announce a fix later this fall.

Security is becoming more system critical, sometimes in ways that are not easily anticipated. Unless non-security aspects of system are fully tested and integrated, the need to have security controls shut down systems in the event of a (perceived) attack may lead to inappropriate system lockdowns and other large-scale problems for hospital and other critical applications.

Sandy

---

## ✂ Companies Steal Information

*Sanford Sherizen <0003965782@mcimail.com>*

*Sun, 15 Sep 91 19:56 GMT*

The Boston Globe (13Sep91) had an article on the competition between traffic spotting services that sell their information to the media and to commuters. A federal lawsuit alleges information piracy, theft and use of trade secrets, which involved listening in over two-way radios. Metro Traffic Control said that it feared piracy of its information by a new competitor, SmartRoute Systems, and created a disinformation program that passed made-up reports on traffic troubles. This was reported by company employees over the radios to the Metro Traffic headquarters (but not passed on to the media customers). SmartRoute is charged with getting that information and passing it on to their radio customers, who broadcast it. An example of planted information that the lawsuit contends was stolen and broadcast include a report on a dog running loose in the South Station tunnel. (A personal note: I thought that I saw the dog but it could have been a politician looking for votes.)

This example, as well as the Samurai Hacker article from Rolling Stone, are just a few indications that information stealing and manipulation is no longer

a phone phreak/hacker issues. There is a long history of businesses misusing information and attempting to restrict information by others. Increasingly, these misuses have moved into learning from and using acts that these companies and others have condemned as hacker terror. It will not be long before we hear about a company setting off a virus against its competitors in order to gain a larger market share. Competitive business intelligence has become an accepted form of industrial espionage, with major corporations reporting a trend to establish intelligence gathering units as a necessary part of marketing research.

There are some dangerous trends here that can erase the lines between legitimate and illegitimate acts. The computer crime of today may become the business strategy of tomorrow. It is getting tough to tell the good from the bad, for the scorecards don't list all of the players, the rules, or even the referees.

Sandy

---

### ✉ Industrial espionage

*Jerry Leichter <leichter@lrw.com>  
Fri, 13 Sep 91 23:06:56 EDT*

I heard on All Things Considered tonight that one of the TV news magazines is reporting that the French have a large industrial espionage operation in effect. The data, gathered by the French intelligence services, are distributed to French companies to help them in business.

According to this report, the seats on Air France flights have been bugged, and some of the passengers are crew are actually intelligence agents.

Question: If these reports are confirmed (of even if they aren't but cannot be fully refuted), would you ever consider buying a French computer, or even French software?

Are other countries playing the same game? Attempts by US government agencies (especially the NSA) to play a role in specifying cryptographic techniques raises huge suspicions. Just who CAN you trust to sell you equipment you can confidentially use to store important restricted data on? Can you only safely use such equipment if you can guarantee that it's not connected to the networks, and that it's never touched by people you don't completely trust? Consider how much interesting data a disk with an intelligent interface could squirrel away on a board that then gets replaced....

-- Jerry

---

### ✉ Re: Junk Mail -- In memoriam, Dave Sharp (Mellor, [RISKS-12.31](#))

*Steven Philipson <stevenp@kodak.pa.dec.com>  
Thu, 12 Sep 91 18:17:21 -0700*

>... collision between a 737 and a private aircraft

The collision was between two aircraft in commercial service, the smaller of which was a Swearingen Metro turboprop, certified and operating as an airliner. General Aviation frequently gets a bum rap. No reason to blame that segment of the community for something in which it wasn't involved.

---

### **✂ RSA vs. NIST (digital security standards)**

*Tom Slone <potency@violet.berkeley.edu>*

*Thu, 12 Sep 91 21:06:45 PDT*

The National Institute of Standards (NIST) has proposed a standard for secure encryption of messages for non-classified digital electronic transmissions. The method relies on a method that lacks widespread familiarity among cryptographers. RSA is the name of the most widely known and used cryptographic method; it is controlled by several patents. The patenting of RSA led NIST to seek a non-patented method that could be used as a standard.

The NIST proposal and RSA both use pairs of related cryptographic keys: one to encode and one to decode the data. The difference in the two methods lies in how the keys are generated. RSA relies on the difficulty of factoring large prime numbers, and the NIST proposal relies on the difficulty of generating something called "discrete logarithms", presumably these are logarithms that have truncated to a finite but large length.

Jim Bidzos, president of RSA Data Security Inc. (owner of at least one of the RSA patents), said, "If no one challenges what they've [NIST] done, we'll be stuck with a weakened standard." Obviously, Bidzos is biased, since his company would potentially lose out should a non-RSA standard be adopted. But there is some merit in his statement since knowledge of prime-factoring has a long mathematical history, and discrete logarithms is presumably a new sub-field. [Science News 140(10):148(1991)]

There would seem to be merit both in having a standard and in not having one. The lack of a Federal standard has apparently hindered the commercial use of encryptions schemes, so data transmission has been insecure. The existence of a single standard, however, would seem to be more vulnerable to cracking via technological and/or mathematical advances. Recall the recent advances in factoring primes made possible by the combination of better algorithms and inexpensive, fast computers. These advances have forced made it necessary to increase the length of encryption keys for the RSA method.

---

### **✂ Re: Salomon Brothers -- Database Design (Drake, [RISKS-12.29](#))**

*Gary Beckmann <beckmann@das.harvard.edu>*

*Fri, 13 Sep 91 09:47:55 EDT*

I have a good friend who works for one of the large financial houses, and he informs me that very often the programmer will be brought in for a few weeks to implement a design that very likely has not been reviewed by anyone (especially not the end user!!) except the manager who has ordered the design. There is no

reason to assume that other companies work differently. The pressure in the field is simply too great for the people to "worry about such things". Seems to me that they are setting themselves up for more experiences like the Salomon Brothers.

Gary Beckmann beckmann@das.harvard.edu

---

## **✂ Secret Computations the basis for Corporate Decisions**

*Jeffrey Sorensen <sorensen@spl.ecse.rpi.edu>*

*Fri, 13 Sep 91 10:40:01 EDT*

On the topic of risk assessment, a particularly chilling episode is discussed in *\_The Media Monopoly\_* by Ben Bagdikian. Some excerpts:

[Mark] Dowie is the investigative reporter who disclosed that the Ford Motor Company and knowingly produced dangerous gas tanks in its Pinto cars, having decided that it was cheaper to pay off heirs of the dead than to spend a few dollars per car to make the tanks safer.

The book he was proposing in 1979 would examine the history of this kind of corporate decision making. ... [Beginning with] Cornelius Vanderbilt, who rejected air brakes for his nineteenth-century trains.

[The editor Nan] Talese was excited. One of the most respected editors in New York, she had produced a series of successes for her employer, Simon & Schuster. ...Dowie, almost as an afterthought, said, "Do you think the title, *\_Corporate Murder\_*, will be acceptable."

Talese then asked an odd question: "Is Gulf and Western one of the corporations?"

When Dowie said the book did not mention Gulf + Western, Talese said, "Fine. I don't think we'll have any problem getting that title past our corporate people."

But she was mistaken. Even though she and her staff unanimously supported the book, neither the title nor the book itself was acceptable. ...The president of Simon & Schuster, Richard Snyder, was vehemently opposed to the manuscript because, among other reasons, he felt it made all corporations look bad.

If Simon & Schuster had been an independent book company, as it once was, [and, not owned by Gulf + Western,] Tales would not have asked an author the question she asked Dowie. It is also possible that Dowie's manuscript would now be available to the public, which, as of 1987, it was not.

For more info see pp.27-31 in *\_The Media Monopoly\_* 3rd edition, 1990 by Ben H. Bagdikian, ISBN 0-8090-6156-X published by Beacon Press.

The field of risk assessment involves numerous assumptions at every calculation, and if these assumptions are wrong, the resulting decisions will also be wrong. The errors will continue to be wrong because these assumptions are not effectively challenged by open and competitive ideas. In an era of

almost complete control of the media by a handful of monopolies, the assumptions involved in risk assessment are deliberately withheld from public scrutiny to create the illusion that the trade-offs between safety and cost are not being computed, when, clearly, they must be.

The result is, we are left with no information discussing the philosophy of risk assessment while on a daily basis risk assessment continues in the back closets of our many institutions...

Jeff Sorensen   sorensen@ecse.rpi.edu   (518) 276-8202

---

**Re: +&\*#&**

<clements@BBN.COM>

Fri, 13 Sep 91 10:41:20 -0400

In [RISKS-12.31](#), Dik T. Winter mentions that some Yugoslavian license plates are distinguished only by a diacritical mark, and Mike Morris reports on trouble with the encoding of Ham Radio callsign plates in California.

Here in Massachusetts, those two themes are combined. Someone decided that our Ham plates should have a jagged line (stylized lightning bolt) after the digit in the callsign. My plate reads "K1<lightning-bolt>BC". This is actually encoded in the RMV computer as "K1/BC".

In the continuing effort to raise money, the RMV started issuing some more patterns of low-numbered (extra fee) plates a few years ago. One of the patterns is <LETTER><DIGIT>

---

**re: ##\$@\*, Inames, umlauts and other nonstandard print chars**

"H.Fuss= F1Fuss@DBNGMD21.bitnet" <GSFP08@dbngmd21.bitnet>

Fri, 13 Sep 91 17:07

and: mis-printed official documents

Besides those umlauts "a", "o", "u", "A", "O", "U" (the dots are supposed to sit upon the characters) and the use of the dots as diaeresis, we in Germany have one more special character, a special form of double-s. Though pronounced 'es-zet', it has nothing to do with 'sz', but derives from a ligature of two different s's: a 'long-s' (which looked roughly like an 'f' without the horizontal bar), used in the middle and beginning of words and syllables, and a 'round-s', used at ends.

The nearest glyph to an 'es-zet' is a greek 'beta'. (For explanation, please read 'long-s' instead of 'f' in the following 7 words: is, fend, eafy, mistake, grafs, clafsroom, H.Fufs). As 'round-s' appears at ends only, there is no upper-case 'es-zet'.

However, computers and their chain printers had (numbers... and)... uppercase letters only, so all the 'special characters' had to be replaced by something else, and the 'Duden', the official spelling book

for schools etc. suggests a additional `e' for the umlauts (what is in line with the history of handwriting since medieval times) i.e. `ae' for ``a' etc., and `ss' for the missing `es-zet'.

(Interesting aside: the case of a Herr `Sch'on', who refused to accept official letters addressed to `Herr Schoen', -- which was decided against him, and his second case, an application for an official change of his family name from `Sch'on' to `Schoen' ((in order to accept properly addressed letters now)) -- which was also decided against him.)

According to this, my name was officially printed as `FUSS'.

However again, when printers were able to print lower case letters as well (and available in state administration), very clever people decided --for easy readability!-- to use the font `small capitals' a-n-d an additional 'beta'-like glyph for the `es-zet'.

As 'small capitals' are nearly as tall as ordinary capital letters, and as a misprinted 'beta' among all capitals looks more like a poorly printed 'B', my passport carries at first sight the name 'FUB'.

My wish, to print my name according to `Duden' as `Fuss', because I might get into troubles at foreign borders, whose policemen might not know `es-zet's and might accuse me of using false documents (passport differs from visa and customs documents) was turned down: not Duden, but \_l\_a\_w\_ decides how to write names, and they had their rules!!

(Up to now, I did not yet have problems from wrong name-spelling in foreign countries (borders), perhaps it could have been that messages for Mr.Fub did not get to Mr.Fuss in his hotel, and vice versa).

... BUT IT COULD BE WORSE!!!!

Following is the sad story of my friend Cesar Fernandes L.

As everybody in the civilized world knows, everybody has one or more first ('Christian', given) name(s) and a family name (inherited). (In Germany, one has 1-3 first names, but to have more is a little unusual, but nothing wrong with).

As everybody knows, first-names come first, and family-name is last (only in some official administrations the order is, for sorting and finding reasons, reversed); this is important if somebody's family name should be a first name (e.g. the ketchup producer Heinz), or if somebody has a first name which is rare and therefore not recognized as a first name by everybody (e.g. Orlambugo). Some people carry their first name(s) as initials only; some people have some abbreviations as an addition to their name, e.g. Dr., MdB (=MP), etc.

(omission of rules of how inheriting family manes... but...)

There are countries, where the equality of sexes is more advanced than in our country, e.g. in Chile. There everybody has t-w-o family names, one from his father, the second from his mother.

(In order not to exaggerate the equality of sex, the second family name, which is the less important one, is very often abbreviated, because it is only the resp. first of the two names which is transferred to the children, and in this order: father(1), mother(1).)

The signature of my friend Cesar Juan Adolpho FERNANDEZ Lopes is:

Cesar Fernandez L.

Everywhere in an index, he is listed under the letter F.

There are not 2 family names in Germany, so he got into troubles with his official documents when he stayed here for several years; they offered him to list his name as Cesar ... Fernandez-Lopes, (because family names are positioned last -- and not as last-but-one), but that steals him one name, because it is quite possible to have a hyphenated (first) family name.

Finally, the case was decided that he has officially to be listed as Cesar Juan Adolpho Lopez FERNANDEZ; according to the rule: family names are at the end (e.g. in his international drivers license).

When he returned to Chile and once had to produce his drivers license, he was detained into custody because of using false documents, here those of somebody else, namely those of Senor (Mr.) Cesar Juan Adolpho LOPEZ Fernandez.

Risks of inflexible use of computerized prints.

Dr. H.Fuss, Inst. of Foundations, National Research Centre of Information Technology, 5205 St.Augustin / Bonn, Germany

---

### **✂ History of Internationalization of ASCII ([RISKS 12.30-32](#))**

*<Paul\_Green@vos.stratus.com>*

*Fri, 13 Sep 91 17:06 EDT*

I think we may be getting off of the part of this debate central to RISKS, but as someone who has some familiarity with this area, I can't help but correct some of the earlier statements. The real history of internationalization is far more complex than the mail so far would suggest, and far less sinister. I believe that simple economics has dictated most of the decisions.

Hugh Davies notes (in [RISKS 12.30](#)) that "European consumers demand that their consumer products 'talk' to them in their language." It isn't just the Europeans; every prospective customer I've ever met wants this. Those of us on the vendor side have to balance what we can do with what people are willing to pay.

Those replacements of square brackets, etc., that he complains about were an official part of the original ASCII standard. The designers recognized that ASCII would be inadequate to meet the needs of everyone and so wisely defined ten "national use" positions that could be changed in each country. There are many so-called national versions of ASCII that exist, typically one for each country. This was the state-of-the-art in the 60's and 70's; when a US vendor exported their product to a "foreign" (non-US) country, vendor personnel in that country translated the messages, screens, and, yes, manuals, into the native language of the country.

In fact, ASCII is officially just another national version of ISO-646, the so-called International Reference Version. In practice this is irrelevant.

Eventually, vendors discovered they were spending vast sums to translate the software and manuals, were delaying the shipment of new products by months, and were greatly complicating support efforts.

In the 1980's vendors turned their efforts to creating software products that would have the same binary image in each country, but would support multiple code pages at a time, and dynamically switch between them. All they would have to translate would be the manuals and error messages. The emergence of computer networking was also a major influence here. ISO 2022 describes a technique for handling multiple code pages for the ASCII class of standards; there is a similar standard for EBCDIC. Anyone who has used MS-DOS since about version 3.0 has seen the extensions that were made to it to support multiple code pages; they are fairly typical.

The next effort was to reduce the number of code pages down to a manageable number. ISO has registered 155 code pages as of July 1990! There is considerable complexity just from the sheer number of them. ISO 8859 is a series of 8-bit code pages that have ASCII (real, true, American ASCII without substitutions) in the lower 128 positions and room for 32 new control characters and 96 graphic characters in the upper 128 positions. There are 9 variations of 8859 that I am aware of; the best known is 8859/1, also known as Latin Alphabet No. 1, which covers most of Western Europe. All together the 9 versions of 8859 cover some 40 languages.

Asian ideographic languages (Japanese, Korean, Chinese, etc.) have so many symbols that 2 bytes are needed to encode a useful subset of characters. The Taiwanese ISO-compliant standard for Chinese requires two double-byte code pages. Even at 17,672 ( $2*94**2$ ) positions, this is still a subset of written Chinese, which has over 80,000 characters! Japanese requires both a single-byte code page (Katakana) and a double-byte code page (Kanji).

Handling this requires two sizes of characters and shift characters to switch code pages. This has meant a new level of complexity in programming languages, operating systems, and applications. Further, I've only described the ISO-compliant schemes. There are a variety of non-ISO schemes; for Japanese, Chinese, etc.

The Stratus VOS operating system presently supports 9 ISO-compliant code pages that cover 17 languages. This covers the primary language of 65 countries that account for half the world's population. Same binary OS image, no confusion of codes, worldwide ability to use any supported character without confusing it with any other supported character. Oh yes, we can translate these code pages to and from EBCDIC.

I'm proud of what we did, but I'll be happy if something like Unicode can take its place. It would be nice to go back to simple, fixed-width characters again, without shift bytes. I don't expect it anytime soon, however.

Paul Green <Paul\_Green@vos.stratus.com>, Director, System Availability  
(ex-National Language Project Mgr) Stratus Computer Marlboro, Mass., USA

**✂ Re: Multinational Character sets (Davies, [RISKS-12.30](#))**

Lars Henrik Mathiesen <thorinn@diku.dk>

Sat, 14 Sep 91 16:40:14 GMT

I just wanted to point out that these extensions are not the manufacturers', but rather nationally standardized (and internationally registered) variants of the ISO 646 set, which explicitly sets code values aside for such variant uses. Formally, ASCII is just the USA version of this, but of course ASCII was the base for 646, and the ``reference'' version of 646 is almost identical to ASCII. The point is, ASCII is supposed to contain only the characters that are useful in the USA.

Of course, ISO 646 doesn't in itself have any facilities for handling more than one language at a time. Later ISO standards do define ways of changing between variants, but none were widely implemented, I think.

Lars Mathiesen, DIKU, U of Copenhagen, Denmark [uunet!]mcsun!diku!thorinn

---

**✂ Export controls on workstations, or, more mantras**

Jerry Leichter <leichter@lrw.com>

Fri, 13 Sep 91 22:58:34 EDT

(For the sake of simplicity, assume it's two years ago, before all the recent changes in South Africa.) Should US companies sell computers (guns, tear gas -- take your pick) to the South African security agencies? After all, if the US doesn't, that just opens the market for the Japanese, the Taiwanese, the Koreans, or whoever.

Once again, the issue of control of exports of high-powered computers has been raised: As reported in a recent RISKS, the US DoD has proposed new regulations on the sale of high-end workstations. The ritual responses have shown up in this forum: Why bother, they'll just buy from the Japanese, or the Taiwanese, or whoever.

These ritual responses display, to me, a certain unwillingness to really think about the issue. "Someone else will do it anyway" is an excuse. It's not at all clear that someone else will; and it's a morally bankrupt argument in any case.

There are two distinct, though related, issues that need to be resolved before deciding whether export controls on high-powered workstations should be imposed:

- a) Is it RIGHT that such machines should be kept out of certain foreign hands?
- b) Is there a PRACTICAL way to implement such controls, should the answer to (a) be yes?

I'll contend that hardly anyone will disagree with (a), posed in isolation,

though there will certainly be disagreements about exactly which foreign hands should be allowed access.

So let's examine (b). First of all, on a moral basis, controls may be justifiable EVEN IF IT'S PRETTY CERTAIN THEY WON'T WORK. Sure, others may do the dirty deed, but that doesn't mean WE should; while we may not be able to stop some evil, at least we should be involved. Should we sell arms to terrorist organizations because, after all, they can always buy them from someone else? Should we sell nuclear materials and technology because, after all, the Chinese seem to be willing to? Every effective embargo has to start with individual decisions that "No, I'm not getting involved in THAT."

Is (b) really out of the question? At the moment, the CPU's for high-end workstations are made predominantly by a small number of US companies. An increasing number are made by Japanese chip houses, but under license from US companies. With the exception of the Transputer, all CPU's in wide use today are controlled by US companies. The US could probably require US companies to place appropriate restrictions in their licensing agreements. Should the US move in this direction, the British would probably go along and similarly restrict Transputers. It would take years for another architecture, developed and controlled entirely by non-US interests, to become a significant market force - and, frankly, I don't see that happening as a response to US attempts to control exports. It's just too expensive an undertaking, and the potential market is too limited.

By the way, just about all these systems run Unix - also under US control.

Those outside of the US may not like it, but as a practical matter the US has a solid lock on leading-edge CPU hardware technology at the present time. That's not likely to change in the next couple of years. What the US chooses to DO with that lock is, of course, another issue.

So: The legal and practical bases for controls exist. What kind of controls might be practically applied? Historically, the controls have mainly been of a go/no go sort: Anything above some speed limit could not be exported. The DoD is taking a much more sophisticated approach to things this time around. Among the suggestions mentioned in the newspaper article are software limits on what kind of programs could be run (no details, but it might be things like maximum memory size allowed, I suppose), and verifiable logging of information describing the workload to a WORM device, whose media would have to be returned for inspection on a regular basis. As I recall, conditions of this sort were enforced on CDC machines sold to the Soviets for weather forecasting many years ago. How effective they can be is an open question - but it's one that can only be answered by experimentation.

Sure, any controls can be gotten around. Terrorists do manage to get arms. Iraq came quite close to building a nuclear bomb, despite all the controls on nuclear materials. Then again, people get away with robbing banks. Does that mean we should legalize bank robbery?

As Shaw put it, we already know what you are, we're just haggling over price. If you agree that, as a matter of morality, computers should not have been sold to South African security forces maintaining apartheid, then the only arguments you can have with the current proposals are (a) that they aim at the wrong

people; or (b) that they are too easy to get around. If your real problem is with (b), the right response is to try to find better implementations, not whine about what the Taiwanese may do.

-- Jerry



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 12: Issue 34**

**Monday 16 September 1991**

## Contents

- [Network Security Lacking at Major Stock Exchanges](#)  
[PGN](#)
- ["Planted" data in databases](#)  
[anonymous](#)
- [Re: RSA vs. NIST](#)  
[Greg Rose](#)  
[Steve Bellovin](#)  
[Dan Bernstein](#)  
[Kevin McCurley](#)
- [Re: Export controls on workstations](#)  
[Hank Nussbacher](#)  
[Lars-Henrik Eriksson](#)  
[John Mainwaring](#)
- [RISKS of trying to get hard facts \[OS/2\]](#)  
[Conrad Bullock via Gideon Yuval](#)
- [RISKS \(yet again\) of not enough data](#)  
[Bill Gunshannon](#)
- [Re: +&\\*#&](#)  
[Dave Roberts](#)
- [Re: Multics/UNIX Lessons](#)  
[Dick Karpinski](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Stock Exchange Risks**

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Mon, 16 Sep 91 14:28:21 PDT

"Network Security Lacking at Major Stock Exchanges --  
GAO cites susceptibility to outages, tampering"

``The General Accounting Office (GAO) found a total of 68 computer and network security and control problems at five of the nation's six major exchanges during reviews it conducted this past year for the Securities and Exchange

Commissions. The lack of adequate controls at the five stock markets could impair their ability to maintain continuous service, protect critical computer equipment and operations, and process correct information." The worst three in terms of numbers of problems were the Midwest (24), Pacific (18), and Philadelphia (18) exchanges, which were all faulted for their inadequate risk analysis. The biggest problems were in the areas of contingency planning and disaster recovery. The NY and American stock exchanges came off relatively well. [Source: article by Wayne Erickson, Network World, 16Sep91, pp.23-24.]

---

### ✂ "planted" data in databases

<[anonymous]>

Mon, 16 Sep 91 09:20:21 xxT

A previous poster discussed how a firm would send out false traffic reports over 2-way radios to confuse a rival firm. It is indeed the case that planting of false data to detect copying or misuse of information has a long, long history. In fact, many companies explicitly tell their customers that there is false data to discourage misuse, while others don't advertise the fact but don't make a secret of it either.

For example, in the mailing list industry, it is common practice for some names/addresses to be "dummies" that are people in the pay of the mailing list firm. These addresses are used to try detect if the terms of list use (e.g. one-use only) are being violated. If too many mailings show up at one of those addresses from the company, the list firm knows there's a problem. Of course, this also means that the company sending out the mailings is wasting some money sending materials to those "planted" addresses.

Another field where this technique is used involves maps. Street maps may show little side streets that don't really exist. If a competing map shows up with the street... blammo! Larger scale maps may show tiny towns that don't really exist.

It goes on and on--all manner of databases may have planted entries that are used for detection purposes. Of course, false entries aren't the only method to do such detections--other methods involve use of unusual spellings, "typos" that are really intentional, unique word orderings, etc.

[Even the RISKS Forum? PGN]

---

### ✂ Re: RSA vs. NIST (Slone, [RISKS-12.33](#))

Greg Rose <ggr@watson.ibm.com>

Mon, 16 Sep 1991 14:39:15 GMT

>... presumably these are logarithms that have truncated ...

They are not truncated logarithms.

Both schemes rely on arithmetic in a finite field (modulo n arithmetic where n

is the product of two large primes) being RSA's operating field. If  $a^b \equiv c \pmod{n}$  (all modulo  $n$ ), then finding a given  $b$  and  $c$  is called the discrete logarithm problem. For RSA, it turns out that you can do it in (at least) two ways: one is brute force, and for sufficiently large numbers is infeasible, and the other is factoring  $n$ . However, the problem being solved is still the discrete logarithm problem for both of them.

> ...

It is possible that my recollection is dated, but to my knowledge the RSA system is still the only known "reversible" system, where the private and public keys can be used for both privacy and authentication. Assuming that the other system doesn't allow this reversible use, the standard is significantly less useful than it could be.

>... These advances have forced made it necessary to  
>increase the length of encryption keys for the RSA method.

However, each extra ten digits in the key at least doubles the brute-force difficulty. This behaviour seems able to keep ahead of hardware advances fairly easily.

(I have no relation to RSA Inc, other than admiration for the elegance and utility of the system.)

Greg Rose - Chance Airlines    [ggr@watson.ibm.com](mailto:ggr@watson.ibm.com)    (914) 945 1179

---

### ✶ RSA vs. NIST (digital security standards) (Slone, [RISKS-12.33](#))

"Steven M. Bellovin" <[smb@ulysses.att.com](mailto:smb@ulysses.att.com)>  
Sun, 15 Sep 91 23:21:36 EDT

What NIST has proposed is not an encryption standard, but a digital signature standard. Digital signatures provide authentication but not secrecy. That, to my mind, is the major reason this scheme was proposed instead of RSA. Dating back at least to the adoption of the Data Encryption Standard, it's been obvious that (at least some part of) NSA is hostile to the widespread deployment of encryption technology. RSA inherently provides secrecy as well as authentication; the NIST scheme provides only the latter. (Incidentally, discrete logarithms are logarithms in a finite field, such as the integers modulo some prime. For example, given that  $c = (a^b \pmod{p})$ ,  $b$  would be the discrete logarithm. It is indeed a hard problem to find  $b$ , though not as hard as had once been thought. Put another way,  $p$  needs to be much larger than was realized a few years ago. At least one important authentication system based on the discrete log problem has been cracked.)

Numerous aspects of the NIST proposal are controversial, including the claim that it is free from (other) patents. Other oddities: signing a message in this scheme is less expensive than verifying a signature. That seems strange; for many applications, very many parties will need to validate a message that will be signed only once. (I doubt that there is any real RISK to forged RISKS messages, but most people I know would be much happier if they could validate

security fix announcements from CERT.)

The claim has also been made that the scheme either has a trapdoor, or is insufficiently secure against a determined attack. Without going into details, the nature of the standard is such that an attack on the system per se would permit solution of everyone's key; with RSA, on the other hand, each public/private key pair must be attacked individually. Note, though, that this is a signature mechanism, not a privacy mechanism; finding a party's private key allows you to impersonate that party in network communications, but does not disclose their secrets without an active attack. We can all imagine the kinds of mischief that can result from forgeries -- but NSA is generally more interested in listening than in speaking.

--Steve Bellovin

---

✂ **RSA vs. NIST (digital security standards) (Slone, [RISKS-12.33](#))**

Dan Bernstein <brnstnd@KRAMDEN.ACF.NYU.EDU>

Mon, 16 Sep 91 06:18:29 GMT

In [RISKS-12.33](#), Tom Slone comments on the NIST DSA public-key proposal. Discrete logarithms are not logarithms which have been "truncated to a finite but large length." Can you tell me what power I have to raise 3 to in order to get 77710 mod 157931? That's a discrete logarithm. Slone then repeats a statement from Jim Bidzos (president of RSA Inc., and of Public Key Partners) saying that the NIST DSA is weak, and adds "there is some merit in his statement since knowledge of prime-factoring has a long mathematical history," while discrete logarithms are "presumably a new sub-field." Actually, Bidzos's claim is entirely unjustified. We have learned a lot about both factoring and discrete logs over the last thirty years or so, and at this point there's no reason to believe that one will be easier than the other. The NIST DSA has the clear advantage of being free of patents. For that reason alone I will use it.

---Dan

[I usually unjustify short or long lines to save paper/screen length or make them readable on 80-character screens, but left this message as received because it was remarkably right justified without having any extra blank spaces inserted! With such arguments you can have a message that is entirely justified even if the contents are entirely unjustified. Just if I tried ... PGN]

---

✂ **Re: RSA vs. NIST (digital security standards) (Slone, [RISKS-12.33](#))**

Kevin S. McCurley <mccurley@work.cs.sandia.gov>

Mon, 16 Sep 91 13:37:26 MDT

The recent posting by Tom Slone on the NIST proposal for a digital signature standard contained some unfortunate mistakes that I would like to correct.

First of all, the NIST standard is for digital signatures - not encryption. If you don't know what a digital signature is, then briefly it is a means to

"sign" an electronic document in much the same way that you would sign a paper document. Its purpose is to protect the authenticity of information, not the privacy of information. It provides much more than a hash or checksum, since a hash can be produced by anyone, but a digital signature can only be produced by the legitimate signer.

Second, the discrete logarithm problem is not something that was plucked out of thin air by NIST. In fact, discrete logarithms were applied to cryptography before factoring, because the discrete logarithm problem was used by Diffie and Hellman in their original paper on public-key cryptography, whereas factoring came along the following year in the RSA paper. Certainly the problem of factoring is old - but the discrete logarithm problem has also been studied by computational number theorists going back at least to the time of Gauss in 1801. For more information on the discrete logarithm problem, see "Computation of Discrete Logarithms in Prime Fields", by B.A. LaMacchia and A.M. Odlyzko, Designs, Codes, and Cryptography, volume 1, (1991), 47-62. Also cited there is a survey I wrote in 1990: "The discrete logarithm problem", pages 49-74 in "Cryptology and Computational Number Theory", volume 42 of Proceedings of Symposia in Applied Mathematics, American Mathematical Society, 1990.

Finally, I would like to point out that there has been relatively little progress made on the problem of "factoring primes". More progress has been made on the problem of factoring composites...

Perhaps the biggest risk is in forming opinions based on incomplete information.

The NIST standard itself is based on a method published by ElGamal in 1984, but incorporates several innovations that improve its performance. The NIST proposal included a call for comments, which appeared in the Federal Register of August 30. Interested parties have 90 days from that date to send their comments to NIST.

Kevin S. McCurley, Sandia National Laboratories

---

### **✉ Re: Export controls on workstations (Cooper, [RISKS-12.31](#))**

*Hank Nussbacher <HANK@VM.BIU.AC.IL>*

*Sun, 15 Sep 91 09:21:52 IST*

>The computer-based RISK here is based upon permitting morons to make decisions

The risk here is trying to use technology as a pawn for politics. Israel has for the past 3 years tried to obtain export licenses for a vector processor upgrade for a 3090-200. Articles about this have appeared in the Washington Post and the NY Times. There was a period of a year where we could not get 486 PCs until the Far East started producing them and then suddenly the export license ban was "relaxed". We have had cases of Vax 4100s being restricted and as the compute curve moves upward we never know what we can obtain and what will be restricted. We looked into buying a Japanese mainframe but it turns out that Japan and the USA have an export agreement - whereby if the USA says no to one country, Japan has to abide by that agreement.

The risk here is not of morons making decisions but of using computers as a carrot for political policy decisions. The USA government can't control weapons making their way to various terrorists groups so there is absolutely no possible way for the USA government to restrict computer technology to these same terrorist groups. The reason these decisions are made is to restrict access to countries who wish to use these systems for education or research but who don't follow the exact views of the current administration.

Hank Nussbacher, Israel

P.S. The views expressed above are my own and do not reflect the views of my employers nor of the government of Israel.

[Note: I normally delete all disclaimers, particularly jokey ones, hoping that they are adequately covered by the masthead generic disclaimer. This one seemed appropriate, however. PGN]

---

**✂ Re: Export controls on workstations, ... (Leichter, [RISKS-12.33](#))**

*Lars-Henrik Eriksson <lhe@sics.se>*

*Mon, 16 Sep 91 09:00:46 +0200*

> ... The US could probably require US companies to place  
> appropriate restrictions in their licensing agreements.

They U.S. not only could, but the already do! Export licenses are needed for all high performance U.S. CPUs. These licenses carry the restriction that the equipment may not be reexported without U.S consent.

Lars-Henrik Eriksson, Swedish Institute of Computer Science, Box 1263  
S-164 28 KISTA, SWEDEN (intrn'l): +46 8 752 15 09

---

**✂ Re: Export controls on workstations ... (Leichter, [RISKS-12.33](#))**

*John (J.G.) Mainwaring <CRM312A@bnr.ca>*

*16 Sep 91 15:02:00 EDT*

I think Jerry Leichter's response to the thread started by John Markoff and PGN's posting, Export controls for workstations, may be missing the point of the original DoD proposal.

If the original posting and its followups had been specifically about sales to terrorist organizations or undesirable foreign governments, I might have agreed with Jerry's posting. Since the IRA does not normally apply directly for export licenses for Sun workstations, the DoD proposes to restrict ALL exports of workstations to reduce the likelihood of the IRA getting one from their Belfast Radio Shack. Jerry's choice of the South African security forces as an example also moves the discussion on in an interesting way.

If Jerry chooses to argue by analogy - always a RISKy endeavor - lets try another one. We disapprove of international terrorists robbing banks, so we

should shut down the export of all equipment used in banks overseas. Of course, since the disclosures about the BCCI, it appears that international terrorists don't rob banks, they own them - but that's the risk of not really understanding the problem.

I admire Jerry's wish to use the influence the US has in technology to bring about worthy goals. In cases such as the sale of armaments where the goods being sold have no peaceful use, his approach seems feasible. However, I think his perception of American influence in the world of workstations and UNIX is not shared by those of us who have spent most of our lives elsewhere. The rest of the world is willing to license American workstations and UNIX because they perceive the cost of developing alternatives not to be worth the effort. This is based on widespread agreement that these things would not be easy to replace. If American policy makes dependence on American products unacceptable to the rest of the world, it will create an opportunity for competition that would not have arisen purely on technical merit, and this will mean jobs in Singapore or Malaysia or wherever. Of course, views on the goodness of this outcome will vary depending on where you live.

As I said above, the rest of the world might applaud if the US significantly reduced its arms exports - to everyone - but it tends not to understand the logic behind placing controls on the export of Kleenex because it has been discovered that international terrorists are unusually susceptible to colds.

---

### **✂ RISKS of trying to get hard facts**

"Gideon Yuval 1.1114 x4941" <gideony@microsoft.com>  
Mon Sep 16 08:28:36 PDT 1991

[Forwarding from Gideon Yuval, Microsoft, 1 Microsoft Way,  
Redmond, WA 98052-6399 206-882-8080]

Newsgroups: comp.os.os2.misc  
Subject: 'OS/2 Rumours' Clarification  
From: Conrad.Bullock@comp.vuw.ac.nz (Conrad Bullock)  
Date: Wed, 11 Sep 1991 12:11:16 GMT  
Organization: Dept. of Comp. Sci., Victoria Uni. of Wellington, New Zealand.  
Originator: conrad@halswell.comp.vuw.ac.nz

Back on September 2nd, I posted an article about some rumours which I had heard from an IBM dealer, in relation to pricing and release dates for OS/2 2.0.

As it turns out, he was in no way speaking for IBM officially, and any information that he passed on to me was purely conjecture on his part. Due to the numbers that he mentioned, and in the absence of any mention to the contrary, I took that information at face value, and assumed it to be relatively reliable.

Unfortunately, I took the route of posting the information that I had here, in order to verify whether it was true or not. (The subject line was "'Rumours' about OS/2 2.0 release", and I ended my message with "Can anyone confirm or deny any of this?").

The message caused some concern to IBMers, and I can understand why. Larry Salomon, Jr. passed on the message to John Tiede, who said:

> Larry, If you could respond on USENET that the information was not  
> correct and IBM is going to inform the misinformed IBM party (note - no  
> witch hunt, as we only want to insure accurate information and not deter  
> open dialogue, which is so important in this evolving electronic world,  
> he said stepping down off the soap box.....). Thanks for your help in  
> this.....

Unfortunately, it has developed into a witch-hunt in a large way at the New Zealand end of things. I received a call from IBM New Zealand today, asking for a categorical statement saying what I had been told, and by who. The dealer concerned, and at least one person at IBM Wellington really are in quite serious trouble, and the relationship between the parties concerned, including myself, is strained, to say the least.

I have spoken to the dealer and the IBMer concerned since, and having just been hauled over the coals, they were understandably angry at me -- the dealer even spoke to my boss, concerned that it was some form of malicious message aimed at 'making a name for myself'.

It sounds as if umbrage was taken at my mention of NZ pricing policies, and any parallel that I was trying to draw between NZ and US pricing - for that I am sorry, and for the information about release dates and final prices.

Anyway, I would just like to stress that the rumours which I posted here were just that - rumours. There was no malice on my part. It was essentially a misunderstanding on my part of some conjecture from the dealer concerned. There was no IBM involvement, and I am dismayed to hear that an IBMer has got into trouble over my posting. I am writing letters to try and help his situation.

For some real misinformation about OS/2, try this message, posted in comp.sys.ibm.pc.hardware today:

> I also forgot a new version of OS/2 is coming out about the same time,  
> it is said to co-exist with DOS. It will run under MS-DOS.

Perhaps this sort of misinformation is less dangerous, as it's so obviously incorrect, while 'feasible' misinformation is a bit more insidious?

I really want OS/2 to succeed as much as anyone. I am frustrated by the disinformation about OS/2 which is spread by many channels, especially in the press, and I did not wish to contribute to that.

I am excited by the impending release of OS/2 2.0. I hope it takes the market by storm, and becomes the success it deserves to be - programmers the world over (not to mention the users), will be eternally grateful. With such a product on the horizon, and as yet, no official words from IBM on features or release dates, it should be of no surprise to IBM that there is a lot of speculation on what will or will not be included, and when, especially amongst

the OS/2 faithful.

I should have perhaps asked IBM NZ directly for clarification on these points, although they have generally not been much help in the past - I assume that they are not allowed to tell me anything anyway.

In summary:

- There was a misunderstanding - the dealer should have made it clear that he was speculating, I should not have taken the information as reliable.
- I shouldn't really have posted the information here.
- An IBMer is in trouble, and he shouldn't be.
- I probably should not have passed on the dealer's name and details to the IBMer concerned, but in my naivety, I did not imagine that it would snowball in quite this fashion.

Conrad Bullock, Victoria University of Wellington, New Zealand  
conrad@comp.vuw.ac.nz conrad@cavebbs.gen.nz Fidonet 3:771/130

---

### ✦ **The RISKS (yet again) of not enough data (Deibele, [RISKS-12.32](#))**

*Bill Gunshannon <bill@tuatara.uofs.edu>  
Mon, 16 Sep 91 12:33:04 EDT*

I think (based on my personal experience) that a much bigger RISK is that this type of media (i.e., Email, Computer Conferencing) might find its use curtailed or, in the case of schools, restricted, based on a concept that has not been researched enough to justify it.

I believe that the apparent hot-headedness seen in Email, BBSes and USENET are only signs of an immature communications media and do not accurately reflect what we can expect in the future.

My own experience tends to bear this out. When I was first introduced to USENET and NEWS, in 1982, I was very quick to flame people for the slightest remark with which I didn't agree. Today, if I come across something that I feel requires a response, I save the offending message and give the whole thing some thought. Somewhat akin to stopping to count to 10. In 95% of the cases, I then decide it isn't worth raising my blood pressure about and throw the article away.

As more and more people become exposed to this form of communications, I feel it will develop the same mores and customs as other more conventional forms of communication.

After all, we don't consider the telephone to be a disadvantage to communication even though we may receive the occasional obscene phone call.

Bill Gunshannon, University Computing Systems, University of Scranton,  
Scranton, PA bill@platypus.uofs.edu bill@tuatara.uofs.edu

---

**✉ Re: +&\*#\$( Morris, [RISKS-12.31](#))**

*Dave Roberts <dwr@datasci.co.uk>  
Mon, 16 Sep 91 11:19:33 GMT*

In [RISKS-12.31](#) in Re: +&\*#\$( Moore, [RISKS-12.21](#)) Mike Morris writes:

> ... Once I was pulled over by a cop who was as fascinated as  
> I was when my plate wouldn't come up and we spent some time with his patrol  
> car terminal discovering this quirk. [...]

It seems to me that we are all missing the risk to society here and thinking only of the individual.

The society we live in gives each motor vehicle a <supposedly> unique id so that those who need to do so can identify that vehicle easily.

The society we live in takes money from each and every one of us to spend on the common good.

Some of that money pays policemen to prevent and/or detect and recover from crime.

Society allows people to advertise themselves by writing their name, slogan, etc as big as they like on their vehicles - many elements of society do that and the results can be seen driving down any road any day.

I think Mike (and many others - nothing personal) confuse the need for a unique vehicle id with their wish for self-advertisement to the detriment of society in general.

The way to do what he appears to want is to paint his call-sign in big letters on the side of his vehicle and accept a standard issue vehicle number for the tiny little plate that is there for those who "need-to-identify".

Or am I missing something??

David Roberts

PS. I think he also owes all the other John Does paying taxes for the time of one cop and one car and one computer system for the wasted effort caused by his insistence on a misuse of vehicle number plates; the RISK is loss of availability of a cop who could be doing something useful instead.

PPS. Whether traffic cops in patrol cars EVER do anything useful is not a topic for this newsgroup - we all pay them so we all think that they do!

---

**✉ Re: Multics/UNIX Lessons (Edward Rice, [RISKS-12.25](#))**

*Dick Karpinski <dick@ccnext.ucsf.edu>*

*Fri, 13 Sep 91 17:43:58 PDT*

Since the people involved with the initial creation of UNIX are very much alive today, we could probably get the truth. Mr. Rice's version is very different from the one I tell. I claim that far from Bell Labs deciding to create a variant of Multics, Ken Thompson used a neglected PDP-7 lying about in a store room to build a little system to permit him to play a little space-war. It might actually be that before it could be said to be even the origin of UNIX, it had become a vehicle to test some of Ken's theories about building appropriate systems. Even so, I'm sure that years passed before the labs decided to use and support the system.

To keep this short, I believe the development of the UNIX system was more like the stories James Burke tells than like the steady, intended progress so often reported in textbooks.

Dick Karpinski

[I try not to interject my own historical perspective into too many messages but at this point I might as well interject that Dick is indeed closer to the truth -- except for the space war. By the way, another interesting historical perspective is provided by F.J. Corbato's Turing Address Lecture in the September 1991 CACM, relating to CTSS, Multics, and (incidentally) Ken Thompson and UNIX. 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 12: Issue 35

Tuesday 17 September 1991

## Contents

- [Computer security breach at Rocky Flats nuclear weapons plant](#)  
[Fernando Pereira](#)  
[Allen Miller](#)
- [DSA is weak](#)  
[Jim Bidzos](#)
- [The difficulty of RSA](#)  
[Jerry Leichter](#)
- [Re: RSA vs. NIST \(digital security standards\)](#)  
[Richard A. Schumacher](#)
- [Re: Export controls on workstations, ...](#)  
[John R. Levine](#)
- [Virus halted government computers in south China](#)  
[PGN](#)
- [Smart Pill Bottles \(Joe Abernathy\)](#)  
[from CACM via VOGON](#)
- [Retraction: The seriousness of statistics mistakes](#)  
[Jeremy Grodberg](#)
- [The seriousness of statistical mistakes](#)  
[Clifford Johnson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **computer security breach at Rocky Flats nuclear weapons plant**

*Fernando Pereira <pereira@klee.research.att.com>*

*Tue, 17 Sep 91 09:03:35 EDT*

AP writer Steven K. Paulson reports on 9/16/91 that security lapses at the Rocky Flats nuclear weapons plant included the storage of top-secret bomb designs for a week on a VAX accessible from the public phone network. In other instances, workers transferred classified working materials from secure computers to lower security ones, including PCs, because they were tired of constant changes in the secure systems and wanted to work on familiar [stable?] systems.

Head of DOE operations at Rocky Flats Bob Nelson said that the agency started last year a \$37M program to correct security problems, following the recommendations of outside security experts.

Nelson also said that the unclassified VAX was used by employees working from home, but that if someone tries to break in ``bells and whistles go off" [is he so sure???]

According to other documents obtained by the AP, other DOE computers had been found to be vulnerable to break-ins.

[Also noted by Nathaniel Borenstein <nsb@thumper.bellcore.com> and by miller@lamar.ColoState.EDU (Allen Miller), who added the following comment.]

---

### **✶ Nuclear weapons plans in unsecure computer**

*Allen Miller <miller@lamar.ColoState.EDU>  
Tue, 17 Sep 91 13:26:05 -0600*

[...]

For those unfamiliar with Rocky Flats, it is a plant between Denver and Golden which manufactures the Plutonium "triggers" for nuclear weapons. These parts are essentially small fission bombs which detonate much more powerful fusion reactions in H-bombs. These triggers are then shipped to the Pantex plant in Texas where the bombs are assembled. Rocky Flats has been shut down for several years due to safety concerns but is apparently about to resume production soon.

---

### **✶ DSA is weak (Bernstein and Bellovin, [RISKS-12.34](#))**

*Jim Bidzos <jim@RSA.COM>  
Tue, 17 Sep 91 10:52:55 PDT*

Bernstein comments in RISKS that my claim that "DSA is weak" is "entirely unjustified" since we have learned equally about factoring and discrete logs. As Bernstein himself notes, Greg Rose offered the discrete log-factoring comparison, not me. (Greg Rose is not entirely incorrect, however.) Get it right, Bernstein.

Since Bernstein obviously does not understand why I called DSA weak, I will state my reasons again, and the group can decide rather than accept Bernstein's erroneous statement.

DSA is cryptographically weak for 2 reasons. (There are other serious flaws not related to its cryptographic strength, but that's another story.) First, DSA proposes to limit the prime modulus  $p$  to 512 bits. (Why is there a limit at all?) In "Computation of Discrete Logarithms in Prime Fields," (LaMacchia and Odlyzko, from "Designs, Codes, and Cryptography 1," Kluwer, 1991) the authors note that in systems with a fixed  $p$ , numbers of 512 bits "should definitely be avoided."

Quoting from the conclusive paragraph of that paper, "Furthermore, since many discrete log cryptographic schemes have the feature that they use a fixed prime which cannot easily be changed, one has to allow for attacks that consume not just a couple of months, but even a couple of years of computing time. Therefore, even 512-bit primes appear to offer only marginal security." So, with discrete logs and factoring being roughly equal problems, DSA is weak (one or so  $p$ 's to compute discrete logs over compared to factoring many 512 composites, not mentioning that the discrete log problem is "brittle") as I stated.

Since NIST refuses to say whether  $p$  will be fixed for all users (or small groups; maybe there will be 4 or 5 or a dozen or so  $p$ 's), we have to assume primes will be shared. Hmm. Like sharing needles.

Another weakness is that every signature requires a random value to be used in its computation. The NIST proposal does not warn you that if an attacker can get one random value/signature pair, your private key is history. (Maybe a standard random value will be proposed...)

I'd say that's weak. And that the claim is justified.

Also, Steve Bellovin comments that DSS is only a signature standard and that "breaking" it lets you forge signatures, but not violate privacy. He's right, but consider this: Public-key is inherently complex and the supporting infrastructure (certificates, directories, etc.) is too difficult to recreate such that DSA almost certainly will become the basis for a privacy proposal from NIST/NSA. Of course, two years from now, the controversy over shared  $p$ , etc., will be over. NIST refuses to rule out DSA as a future privacy standard, so we should assume it will be the basis for one. Remember, NIST stated clearly that it took the needs of law enforcement (shades of S266) into consideration in the preparation of DSA. Will the Justice Department benefit from being able to forge signatures? Maybe, but I would ask NIST if they are proposing a future privacy standard so at least I'd know what we were getting.

--Jim Bidzos

---

## ✂ The difficulty of RSA

*Jerry Leichter <leichter@lrw.com>*

*Tue, 17 Sep 91 07:00:58 EDT*

Recent RISK's have contained a number of incorrect statements about what is known about RSA, and the difficulty of computation problems in general:

1. It has never been proven that inverting RSA is "as difficult as factoring". This little link has been tantalizing people since the original RSA paper (and presumably tantalized R, S, and A before publication). It has long been known that CERTAIN KINDS OF ATTACKS ON RSA imply the ability to factor the modulus, but that's it.
2. It is not known that factoring (expressed properly so that the

statement makes sense) is NP-complete. That is, even if  $P \neq NP$ , it is possible that a polynomial algorithm for factoring exists.

It is widely believed that factoring is, in fact, NP-complete. However, the same was believed of linear programming until Khachian's algorithm.

3. It's often claimed that factoring has been studied for hundreds of years. This is true but VERY misleading. The basis for the recent computational advances, both in factoring and in the related but (as it turns out) much easier problem of primality testing (which make RSA possible), are based on randomizing algorithms. The very notion of a randomizing algorithm is no more than thirty or so years old. Essentially, all the great mathematicians of the past searched carefully under the lamppost, and dawn has now revealed that there's a lot more street out there than anyone suspected.
4. Ultimately, we don't yet know that  $P \neq NP$ , though it's hard to find any mathematicians who doubt it. If  $P = NP$ , public key cryptography becomes impossible. (However, private key cryptography can still be possible.)
5. Lest anyone think that 1-4 are an unfair attack on RSA and related algorithms, whatever the state of our ignorance here, we know even less about the security of many other systems. In particular, as far as I'm aware the only thing known about the security of DES is that it has resisted determined attacks. We have a theory for avoiding certain weaknesses in DES-like algorithms (and DES does seem to avoid all the known weaknesses), but we have not even the glimmering of a general theory relating the difficulty of DES to NP or any other well-studied class of hard problems. (Well, maybe the NSA knows more - but they aren't saying!)
6. RSA is by no means the only known private-key system. Several others have been proposed and have survived some attack. (Others have NOT survived attacks.) In particular, Rabin many years ago proposed a "variation on the RSA theme" which has the nice property that it is provably as hard as factoring. Rabin's scheme has some disadvantages (it requires some tricks to use it to produce digital signatures) and, as far as I know, it has for the most part been ignored.
7. One has to be VERY careful about applying "proofs" to systems involving adversaries. It APPEARS that the proof (such as it is) of security RSA implies that you don't have to worry about other aspects of security, such as protocol design. In fact, this is false; a classic paper (something like "How and Why to Use a Private Key in a Public Network", by Goldwasser, Micali, and Tong) displayed a generic protocol-related weakness of all private-key systems. It was one of the things that inspired all the work on zero-knowledge proof techniques

and such, work in which Goldwasser and Micali played central roles. (I don't know what happened to Tong.) Beyond considerations of efficiency, it is also the reason that today's systems usually propose to use RSA for securely exchanging private session keys, rather than for all encryption.

-- Jerry

---

**✂ Re: RSA vs. NIST (digital security standards) (Slone, [RISKS-12.33](#))**

*Richard A. Schumacher <schumach@convex.com>*

*Tue, 17 Sep 1991 05:41:39 GMT*

Ah, but he did have to cheat, a little, by using pairs of single quotes instead of a lone double-quote character.

---

**✂ Re: Export controls on workstations, ... (Leichter, [RISKS-12.33](#))**

*John R. Levine <johnl@iecc.cambridge.ma.us>*

*16 Sep 91 14:35:03 EDT (Mon)*

- > a) Is it RIGHT that such machines [high-end workstations] should be
- >
- > b) Is there a PRACTICAL way to implement such controls, should the
- > answer to (a) be yes?
- >I'll contend that hardly anyone will disagree with (a), posed in isolation,

Jerry goes on to say that since practically all high end microprocessors are manufactured or at least licensed by U.S. companies, appropriate legal agreements would keep them out of the hands of people we don't like.

It seems to me that we have here a severe of confusing paperwork with reality. Workstations are not supercomputers. They are physically small and portable. They are sold in large enough numbers that manufacturers cannot even now track the location of every workstation they have sold. If a bad guy wants to buy a few workstations in the U.S. or Europe, put them in a station wagon or a boat, and take them east or south, there is no way to prevent that short of making workstations unavailable to everyone. In the U.S. at least, border controls are targeted almost entirely at regulating what comes into the country, not what leaves, and they have not been notably successful at stopping the incoming flow of workstation-sized bales of marijuana.

Recent reports in the paper have described DOD proposals for extremely onerous security devices that would audit every program run on a computer in a putatively tamper-proof way. This sounds to me like something that would cause only the mildest trouble to the station wagon smugglers while bringing useful domestic work to a halt. ("Sorry, pal, if we fix that bug the program's checksum will change and it'll take six weeks to have it added to the approved list.")

Furthermore, even claim (a) is pretty dubious. A few months ago, I expect many people would have claimed that it was not in the U.S.'s interest to provide



compliance to prescription regimes is a growing problem with potentially dangerous consequences should a doctor alter a prescription assuming the previous dose is not strong enough. A recent study of epileptics indicates most patients take only 76% of their antiseizure medication. the chip may be one remedy, although at this point an expensive one at \$7 a cap.  
{CACM August 1991}

---

✂ **Retraction: The seriousness of statistics mistakes ([RISKS 12.31](#))**

*Jeremy Grodberg <jgro@summit.lia.com>  
Sat, 14 Sep 91 00:38:22 PDT*

See, now I'm doing it too :-(. I've just spent the last 6 hours in a medical library researching some of the questions my posting raised, and I now need to retract almost all of my previous posting concerning the risks of statistics mistakes.

First, I need to apologise to Mr. Fulk, as I accused him of not knowing what a false positive was, and I now have no basis for that accusation; rather it is I who didn't know what a false positive was.

I thought I had the right definition for false positive on the basis of information provided to me by someone who did the research for me, backed up by the guesses of the medical researchers I mentioned in the original posting as guessing it right (and I can now say were all wrong, every one of them), and sanity-checked by the analysis I presented in the posting. Well, I was wrong about what a false positive was, although the definition I attributed to Mr. Fulk was also wrong (one cannot deduce from his posting whether he used the right definition or the one I attributed to him.) He was, however, misinformed about many of the numbers he presented.

Also, as I have noted in an interim posting, my example of the smallpox vaccine was poor at best. I will correct that part more definitively later in this posting.

So, now that I have been properly humbled, let me share my new-found information, so that future researchers won't be misled by me more recent mistakes.

In the realm of diagnostic and screening tests, there are 2 variables and 4 possible outcomes. The test results can be positive or negative, T+ or T-, and the "correct diagnosis" is either positive (has the disease) or negative, D+ or D-. The "False Positive rate" is the number of T+ given D-, divided by the number of D-. In other words, if you tested only people without the disease, the False Positive rate is the rate of positive test results you would get. Similarly, the "False negative rate" is the T- given D+, divided by the number of D+.

So, the one thing I criticized Mr. Fulk about turned out to be one of the few things I cannot quarrel with from his original posting. However, I can quarrel

with all the other numbers he presented. I'm not actually sure now what he defined as what I called "the disease", but I believe it was basically anything that the MSAFP test would detect, which is all neural tube defects (anencephaly, spina bifida, etc.). It may, however, have excluded anencephaly, which is the most common neural tube defect, but which can be very reliably detected with ultrasound. For the rest of this discussion, I will be talking about all neural tube defects except anencephaly; and referring to them all as a single disease.

Mr. Fulk cited a prevalence of less than 1 in 10,000 for the disease. The studies I looked at, including some very recent ones, gave a range of prevalences from 1 in 1,000 to 6 in 1,000. Based on my readings of the studies, and giving greater weight to the more recent studies (which take into account the earlier studies), I would propose 2 per 1,000 as the most likely rate of incidence for a healthy woman who was 29 when she got pregnant.

Mr. Fulk cited a false positive rate of 10% for the MSAFP test. This test is not a yes/no test, but rather yields a quantitative result. The medical literature recommends making it a yes/no test by comparing the results to a threshold level, but there are odds charts available for more specifically determining the likelihood of having the disease based on the quantitative result. There are two thresholds recommended in the literature, with false positive rates of 3% and 1.4%.

(The threshold which yields the higher false positive rate is the one that was originally recommended, and continues to be used because it greatly reduces the false negative rate, which can be as high as 44%.)

The rate of abortion caused by amniocentesis is much the subject of controversy in the medical community. One reason is that the skill of the person performing the amniocentesis, and the method used, have a significant impact on the safety. Another complication is that something like 1% of pregnancies are terminated due to spontaneous abortion occurring after the gestational stage where an amniocentesis would have been done, so it is hard to know how many additional abortions are caused by the amniocentesis. I found studies ranging in their conclusions about the number of spontaneous abortions due to amniocentesis from 2 in 1000 to 1 in 100; the figure I would choose based on my reading is 5 in 1000.

Another very important point not mentioned by Mr. Fulk is that ultrasound has essentially 0% false positive, and 20%-40% false negative for spina bifida, which represents the great majority of the problems MSAFP is testing for (remembering that ultrasound is a nearly-perfect diagnostic tool for anencephaly, and ignoring the hints in a 1988 study that says the MSAFP might be useful for detecting Down's syndrome). The existence of this test greatly changes the numbers involved with deciding whether or not to have the MSAFP.

Anyway, crunching all these numbers around yields a range of very roughly from 5 to 50 incidents detected by the MSAFP for every 10 healthy fetuses accidentally aborted by the amniocentesis. So, in the end, Mr. Fulk made the right choice, given the utility values he spoke of (he had a strong bias in favor of having a sick baby over killing a healthy one).

All the studies I could find recommended counseling for patients who might

benefit from amniocentesis, and in most cases indicated that doctors could not make a strong recommendation either way; it was a matter of values. In the UK, where the first studies on this stuff were done, researchers found that most couples were more worried about having a sick (i.e. seriously handicapped) child than they were worried about inadvertently killing a healthy fetus as a side effect of the testing or through misdiagnosis. Still, the recommendations generally take the form of "its too close to call, let the patient decide," although the medical bias is toward testing.

So, there it is, more than you wanted to know about this stuff.

We see the risks of bad data, the risks of bad research (on my part), the risks of believing what people tell you, as well as the risks of medical testing. And, of course, we see that even the people who complain loudest about other people's ignorance and mistakes occasionally come up just as short.

Now, about smallpox. I knew there weren't any smallpox patients; I just shouldn't have brought it up. What's worse, the risks of the smallpox vaccine do not include getting smallpox! Smallpox (variola) vaccine is made from vaccinia virus, which provides cross immunity, but causes something like 50 serious adverse reactions/illnesses per million people. Vaccination with smallpox virus was ended in the (early?) 1800's because it carried a 1-3% risk of death due to a full-blown smallpox infection developing.

The last case of smallpox occurred in 1978, wide-spread vaccinations in North America were curtailed in 1970, although laboratory researchers and some military personnel continued to receive vaccinations into the '80s. (So, if I had made the statements in question in 1974, they would have been accurate.) The only stocks of smallpox known to exist in the world are at the Centers for Disease Control in Atlanta, and the Research Institute for Viral Preparations in Moscow. According to the journal "Nature", these stocks "should be destroyed by the end of 1993, after US and Soviet laboratories have finished sequencing the smallpox viral genome." This in spite of the fears of some archeologists that the smallpox virus may still exist in nature, waiting to re-infect to world. (An Egyptian mummy was found of someone who appears to have died of smallpox. An attempt to detect the smallpox virus in the "pox" remnants failed, but since the museum authorities were understandably reluctant to give the researchers lots of the mummy's skin, the researchers didn't really get as much sample as they would have liked.)

The military doesn't think much of the smallpox virus as a weapon (too hard to transmit, takes to long to work), the vaccine doesn't require the virus, and the danger of an outbreak is huge, so it looks like the smallpox virus may become extinct in only 2 years.

One last note: my email address will be changing next week, probably to [jgro@netcom.com](mailto:jgro@netcom.com). I don't know if or for how long mail will be forwarded to my new address, so I apologize in advance if I don't answer my mail, because I may not get it.

Jeremy Grodberg [jgro@lia.com](mailto:jgro@lia.com)

[It seems important for RISKS to include correction of earlier errors, even when we drift from relevance. But, it is certainly nice when contributors take pains to get

it right the first time!

---

## ✂ The seriousness of statistical mistakes

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>

Fri, 13 Sep 91 14:53:30 PDT

- > What is worse, for some reason Mr. Fulk did not find it
- > unbelievable that his doctor would recommend a test which was
- > 10 time more likely to kill his fetus than the disease was . ...
- > If the test was as bad as Mr. Fulk thought, standard practice
- > would have been formulated to recommend against testing in his case.

There's at least one field of medicine where Mr. Fulk would be right to disregard the medical profession's routine application and endorsement of life-changing tests, namely, clinical psychology. An exemplary test is the Minnesota Multiphasic Personality Inventory (MMPI), which is used routinely as an admissions classification procedure for mental patients, and is used routinely outside medical applications to screen job applicants, decide parental suitabilities in custody cases, etc.

Like other such tests, the MMPI is a computer-scored questionnaire requiring some 550 yes/no responses to questions such as "There is life after death", "I am important", "My father is a good person", "I would like to be a flower seller". The computer calculates from the responses normalized scores on about ten psychotic scales, e.g. manic-depressive, schizophrenic, hypochondriac, paranoid, etc. If an examinee's score is in the top 5% for any scale, he's generally diagnosed (by the computer) as having that mental condition. (Worse, most such computer tests nowadays print-out pages of detailed analysis, drawn from a text library of case histories.)

What is the probability that a person diagnosed by the test as having a mental problem (being in the top 5% of a scale) is in fact in the top 5% of that scale? The answer is sensitive to the population being tested. Applied to mental patients, the probability of a correct diagnosis is obviously much higher than when the test is applied to the population at large. But most applications of the test (with life-changing decisions being dependent thereon) are to the population at large. In those cases, if a person is diagnosed as, for example, "paranoid", the chance of that person really being clinically paranoid is at an unrealistic best about 1 in 4 (whereas without the test it would be 1 in 20, assuming our 5% cut-off/base rate). Thus, a positive test, on which people are rejected for employment / parenthood etc., is known to be much more likely to wrong than right in each instance of application.

What does the profession have to say about this? I've made a hobby of reading personality measurement "validation" studies in academic journals, and am appalled by the myopic presentations of statistics by the foremost authorities (i.e. Minnesotan academics). Their prestigious journal articles claim to validate the MMPI scales (and sub-scales), affirming the value of their continued application throughout society, but the figures simply do not support their salesmanlike claims. A significant correlation over a large sample is the quintessential proof of "validity", when the correlations are nevertheless

between purely subjective variables and even so are so low that an accurate diagnosis remains improbable in any particular case.

Worse, the articles often contain statistical nonsense, and in some cases the data presented, when properly analyzed, flatly contradicts the conclusions drawn from it by the authors. Worse, my pointing out these contradictions results in nothing whatsoever, the authors evidently can't be bothered to make corrections or recognize criticism. I do believe that statistics as applied to physical medicines is much more rigorous, but let's at all times be on our guard against people called "Professor" who nevertheless misuse statistics and, in so doing, abuse us through computers.



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 12: Issue 36**

**Wednesdy 18 Septembr 1991**

## Contents

- [AT&T Phone Failure](#)  
[Ed Andrews](#)
- [Fly-by-wire without leaving the ground](#)  
[JCF](#)
- [World Bank virus](#)  
[Ted Lee](#)
- [SunOS SPARC Integer Division Vulnerability](#)  
[CERT Advisory](#)
- [The risks of a computer-based forum](#)  
[Brian Holt Hawthorne](#)
- [Descriptive terms \[false positives and negatives\]](#)  
[Jon Krueger](#)
- [Risks of mistreating programmers](#)  
[Arun Welch](#)
- [Re: Security Software Bug Locks Up System](#)  
[Sanford Sherizen](#)
- [RSA stuff](#)  
[John Mount](#)
- [Manipulation of digital images](#)  
[Joe Morris](#)
- [Re: +&\\*#](#)  
[Richard Ristow](#)  
[John Wichers](#)  
[Gary Beckmann](#)  
[Timothy Freeman](#)  
[Lynn R Grant](#)  
[John F. Woods](#)
- [Info on RISKS \(comp.risks\)](#)

---

✉ **AT&T phone failure downs three New York airports for four hours**

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Wed, 18 Sep 91 9:34:13 PDT

Operations at all three New York airports ground to a standstill from 5pm until 9pm yesterday [17Sep91] when an AT&T internal power failure at a Manhattan 4-ESS switching center knocked out long distance calls in and out of the city. Neighboring commercial power was unaffected. The 4-ESS system is used to route calls between AT&T's long-distance network and the local companies. The air traffic control centers use a network of radio towers linked by phone lines.

Although the precise origin of Tuesday's problems remained unclear, the extent of the difficulties provided yet another example of how dependent today's telephone networks are on a few pieces of equipment.

In recent years, AT&T and other companies have gone to great lengths to emphasize the back-up capacity and redundancy of their systems. Yet the long-distance carrier was unable to reroute all traffic to other gateways for several hours after the problems first became apparent."

Calls were redirected to the two remaining gateways, but those could not handle that much increased traffic. [Quotes above are by Ed Andrews, whose article "AT&T Phone Failure" appeared in the N.Y. Times, 18Sep91.]

I just spoke with Ed Andrews, who is working on a story for tomorrow's NYTimes. The current theory seems to be that AT&T was trying to be helpful to ConEd in NY by cutting its usage of commercial power on a hot day by running on internal power, but somehow did not realize that their backup power generator was not properly linked in, and that they were actually running on batteries for 6 hours until the batteries were drained! As the details unfold, we may find out the extent to which the system diagnostics and alarms gave a true picture of what was really happening. (Shades of the Three Mile Island crew trying to figure out what was happening?) So, check Ed's article tomorrow for further details.

Here we have another example of creative redundancy and supposedly conservative design (hardware reliability, fault tolerance, extra capacity, alternative routing, standby power, etc.) still not being good enough to prevent massive outages. From the system level viewpoint, it seems that we should be learning something more from the repeated cases of telephone outages (AT&T and Sprint outages reported here in the past, due to software, cable cuts, etc.) and airport shutdowns resulting from extensive telephone outages -- e.g., last year's O'Hare disruptions due to the Chicago cable cut on 15Oct90 (R.I. Cook, [RISKS-10.62](#), and ACM Software Engineering Notes 16 1, January 1991) and the three New York airport disruptions due to the fiber-optic cable cut in Newark NJ, also affecting various commodities exchanges and long-distance calling for 9 hours on 4Jan91 ([RISKS-10.75](#) and ACM Software Engineering Notes 16 1, January 1991). On one hand, RISKS readers know that no matter how carefully designed and operated a system is, it can still fail grotesquely. On the other hand, we still have to try much harder to avoid those possibilities -- and indeed likelihoods. You would like to think that airports and air traffic control could find ways of not being crunched by the outage of a single switch, but it keeps on happening!

I hope some of you will come to the ACM SIGSOFT '91 (Software for Critical Systems) at the Fairmont Hotel in New Orleans, 4-6 December 1991, where some of the underlying problems and potential solutions will be discussed. In particular, Michael Meyers of AT&T Bell Labs in Naperville will be giving an

invited talk on "Reliable Software for the 4 ESS Switch". Henry Petroski's talk on "Human Error in Design" is also relevant to this topic. The preliminary program and other information appeared in [RISKS-12.10](#). The registration packet is contained in the September CACM (pp.112-113), and is also available on-line from Judith Burgess (Burgess@csl.sri.com). I think the program will be of great interest to the software oriented seriously minded risks-aware community. Peter

---

### ✈ Fly-by-wire without leaving the ground

<fmsrl7!art-sy!chap@sharkey.cc.umich.edu>

Tue, 17 Sep 91 22:25 EDT

James Higgins, THE DETROIT NEWS, 15 September, page 1C: ... Clemson engineers ... have patented a new automobile camshaft/throttle control system they say can boost fuel economy by 20 percent in a gasoline engine-- more than that in a Diesel. ... Just by announcing the development (in a press release which, by the way, skated lightly over some serious concerns about the new system), Clemson has made it more likely that U.S., Japanese and German automakers will lose their fight against tough new fuel economy legislation in Washington. ... A camshaft controls the action of the valves that let mixed fuel and air into an engine and allow burned gases to escape. Usually it's set up so that the valves will open or close according to just one setting. That setting is a compromise, not...optimal...for all engine speeds. ... In the Clemson system, the camshaft consists of two shafts, one of which rotates inside the other. An infinite variety of valve settings is possible, theoretically allowing optimal valve action in every situation.

In its announcement, the university said the Clemson Camshaft system "improves fuel economy by approximately 20 percent." Detroit engineers object strenuously to this, saying optimal camshaft action can only boost fuel economy by about 5 percent. [co-inventor] Nelson agrees. But here's the nub--his system also includes a computer-controlled device that electronically allows the camshaft to act as the car's throttle--a revolutionary idea. All cars today have a throttle plate that opens to allow air into the engine, and in every car on the road the throttle plate is mechanically connected to the gas pedal.

The Clemson system substitutes [for] the mechanical connection...a computer control--a "fly by wire" device like those...on advanced aircraft. When the engine doesn't have to labor against a partially closed throttle, significant fuel economy gains are possible, Nelson says. This, together with the camshaft action, is the source of the 20 percent figure. But it also raises a whole host of safety concerns--not to mention potential problems with cost, manufacturing complexity, durability and so forth. Overall, though, it looks promising to this reporter. And one hopes it will get a thorough investigation from the industry on its own merits, free from the nasty politics surrounding the fuel economy issue.

[and thanks to the NEWS for a commendably objective report. -JCF]

---

**✂ World Bank virus**

<TMPLee@DOCKMASTER.NCSC.MIL>  
Wed, 18 Sep 91 12:16 EDT

The latest issue of Time (9/23) had the following on its "Grapevine" page. Does anybody know any more about what it's referring to? (I don't THINK I've missed any issues of RISKS.)

HEY! LET'S SEND A COUPLE BILLION TO WOLFGANG

World Bank economists in Washington swallowed hard when the message suddenly flashed on their screens. Identifying itself as "Traveller 1991," an invading computer virus announced, "Do not panic. I am harmless." Horrified bank officials, who use computers to transfer billions from developed countries to hard-pressed parts of the world, wondered at first if it was possible for some tiny nation to fill its coffers by tapping into their inner sanctum. An international army of computer nerds and police experts soon tracked down the trespasser and pronounced it harmless. But what about the next one? Scotland Yard investigators, who traced the virus as far as eastern Germany, believe that disgruntled hackers there are still at work injecting disruptive electronic microbes into world financial networks.

---

**✂ CERT Advisory - SunOS SPARC Integer Division Vulnerability**

CERT Advisory <cert-advisory-request@cert.sei.cmu.edu>  
Wed, 18 Sep 91 11:38:38 EDT

[We generally do not include the CERT Advisories in RISKS, because there are so many normal channels. But this one is absolutely fascinating as an example of something that ostensibly should not have an impact on security, so that at least the existence of the flaw should be widely known. PGN]

CA-91:16                    CERT Advisory  
                              September 18, 1991  
                              SunOS SPARC Integer Division Vulnerability

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in Sun Microsystems, Inc. (Sun) integer division on their SPARC architecture. This vulnerability exists on all SPARC platforms (including sun4 and sun4c) for SunOS versions 4.1 and 4.1.1.

Sun has provided patches for this vulnerability. They are available through your local Sun Answer Centers worldwide as well as through anonymous ftp from the ftp.uu.net system (in the sun-dist directory).

Fix	Patch ID	Filename	Checksum
/sys/sun{4,4c}/OBJ/crt.o	100376-01	100376-01.tar.Z	09989 11

Please note that Sun Microsystems sometimes updates patch files. If you find that the checksum is different please contact Sun Microsystems or us for

verification.

[Excerpted:]

A security vulnerability exists in the integer division on the SPARC architecture that can be used to gain root privileges. Any user logged into the system can gain root access. [Fix info deleted. Contact CERT.]

The CERT/CC wishes to thank Gordon Irlam of the Department of Computer, University of Adelaide, Australia, for bringing this vulnerability to our attention and for his further assistance with the solution. We also wish to thank Sun Microsystems for their prompt response to this vulnerability.

Computer Emergency Response Team/Coordination Center (CERT/CC)  
Software Engineering Institute, Carnegie Mellon University  
Pittsburgh, PA 15213-3890 Internet E-mail: cert@cert.sei.cmu.edu  
Telephone: 412-268-7090 24-hour hotline: CERT/CC 7:30a.m.-6:00p.m. EDT  
Past advisories and other computer security related information are available for anonymous ftp from the cert.sei.cmu.edu (192.88.209.5) system.

---

### **✂ The risks of a computer-based forum**

*Brian Holt Hawthorne <brian@ima.isc.com>  
Wed, 18 Sep 91 11:57:20 EDT*

Many people seem to approach e-mail and submissions to forums like RISKS as informal conversation. Given the persistence of the typed word, however, it may often be more appropriate to consider these forums as un-refereed journals.

Two recent examples from Volume 12, Issue 35:

Although I greatly appreciate Jeremy Grodberg's intellectual integrity spending many hours researching the objections raised to his claims, and subsequent posting of a retraction of those claims, I find his lack of references disturbing. He has introduced new figures and new claims, backed up only by his assertion of having spent "6 hours in a medical library". It is clear to me that he may truly have found some additional sources, but it is puzzling why he is unwilling to share them with us.

Clifford Johnson fails similarly in his diatribe against the misuse of the MMPI. After an excellent introduction to the nature of the test and its shortcomings, he berates "Minnesotan academics" for their "myopic" articles in prestigious journals. Is he merely being polite by not sharing with us the name of at least one of these journals, or a citation to at least one of these articles of "statistical nonsense"?

While it is acceptable to make unsubstantiated statements such as these in casual conversation, let us remember that the RISKS forum is not only archived for posterity, but is often the subject of citations itself.

brian

---

## ✂ Descriptive terms

Jon Krueger <jpk@ingres.com>

Tue, 17 Sep 91 20:21:45 PDT

[There are some people who prefer TYPE ONE ERRORS and TYPE TWO ERRORS to False Positives and False Negatives. PGN]

How ugly! And a retreat from clear, forceful, prose.

Fortunately there are four perfectly good terms from signal detection theory: hit, miss, false alarm, and correct rejection. Here is a grid that explains them:

\	said \	was (what was actually the case)
(what the \	test reported) \	
	signal	noise
	+-----+	+-----+
signal (yes)	hit	false alarm
	+-----+	+-----+
noise (no)	miss	correct rejection
	+-----+	+-----+

Unlike false positives or type one errors, false alarms conveys the error and its problems in vivid English.

Unlike false negatives or type two errors, misses denotes the type of error and reminds us of outcomes.

This terminology gives us a reasonable way to distinguish various leading and misleading statistics. The chance of the test saying yes when the fact is yes is:

$$\frac{\text{hits}}{\text{hits} + \text{misses}}$$

This can also be called hit rate on signal trials.

The chance of the test saying no when the fact is yes is

$$\frac{\text{misses}}{\text{hits} + \text{misses}}$$

This can also be called miss rate on signal trials.

The chance of the fact being yes given the test said no is:

$$\frac{\text{misses}}{\text{misses} + \text{correct rejections}}$$

This can also be called miss rate on said no trials.

And the chance of the fact being no given the test said yes is:

$$\frac{\text{false alarms}}{\text{false alarms} + \text{hits}}$$

This can also be called false alarm rate on said no trails.

And so on. All of these may be distinguished from the overall hit rate:

$$\frac{\text{hits}}{\text{hits} + \text{misses} + \text{correct rejections} + \text{false alarms}}$$

The overall miss rate:

$$\frac{\text{misses}}{\text{hits} + \text{misses} + \text{correct rejections} + \text{false alarms}}$$

The a priori chance of the test saying no:

$$\frac{\text{correct rejections} + \text{misses}}{\text{hits} + \text{misses} + \text{correct rejections} + \text{false alarms}}$$

The a priori chance of the fact being no:

$$\frac{\text{correct rejections} + \text{false alarms}}{\text{hits} + \text{misses} + \text{correct rejections} + \text{false alarms}}$$

Clearly these are all derived numbers. The numbers you want are the raw numbers in the grid, e.g.:

said \ (what the test reported) \	was (what was actually the case)	
	signal	noise
signal (yes)	50	10
noise (no)	5	100

Or more compactly, 50 hits, 10 false alarms, 5 misses, 100 correct rejections. From this you can derive all the numbers you want to compare, make all the inferences the data can sustain, and make the wisest decisions based on the available information and your personal values.

-- Jon Krueger

## Risks of mistreating programmers

Arun Welch <welch@cis.ohio-state.edu>

Tue, 17 Sep 91 20:22:45 -0400

One of our local public radio stations carries BBC news before the regular NPR news on weekdays, and I heard this on my way home. Pardon any errors in reporting, I was after all in a car and this is all from memory.

Apparently there's been a rash of new computer virus infections since the collapse of the Eastern Bloc, coming out mostly from Bulgaria. Since the Bulgarian government couldn't buy western computers or software, they would get one copy illegally and then copy them freely. Since most software is copy-protected in some manner, they trained a number of programmers to find ways to defeat said protection. Because the programmers didn't like doing this, and since they didn't pay them very much money, the programmers also spent some time perfecting their skills at virus-writing. Now that it's easy to send software back and forth, these virus' (virii?) are now spreading through the rest of the world. The one quote I do remember is "There's one bulletin-board system in Sophia that's absolutely notorious for them, and people are uploading virus' to it all the time."

Arun Welch, Lisp Hacker, Anzus Consulting

---

## Re: Security Software Bug Locks Up System (Re: [RISKS-12.33](#))

Sanford Sherizen <0003965782@mcimail.com>

Tue, 17 Sep 91 17:30 GMT

Dan\_Swinehart (PARC@xerox.com) asked me to clarify my previous posting regarding the Tandem security software problem. He wondered about the following:

>A faulty piece of code embedded in the Tandem Safeguard security  
>system interpreted 4:22 PM on August 27 as an impossible command.

Here is all that I have available from the Computerworld article.

"A unique combinations of numbers generated by Tandem's "time stamp" facility threatened to stop ....computers at precisely 4:22 pm in each local time zone...'The time stamp took on a numerical value that would trigger incorrect computer logic,' one West Coast Tandem user explained. 'The security package would then lock up the system...' ...The culprit was a faulty piece of software code embedded in the Tandem Safeguard security system that interpreted the data and time numbers as an impossible command...The computers that felt the bug were Tandem VLX and Tandem Cyclone systems running the new C 20.2 release of the Safeguard security package along with Tandem's Guardian operating system."

Hope that clarifies the posting. Sandy  
Data Security Systems, Inc. ,5 Keane Terrace, Natick, MA



## RSA stuff

John Mount <John\_Mount@GS6.SP.CS.CMU.edu>

Wed, 18 Sep 91 09:42:54 -0400

I have some problems with Jerry Leichter's summary on RSA (which is for the most part right on target). For brevity I am only quoting the parts of his article I disagree with- but I want it known that all the points I deleted I think were stated well and agree with 100%.

- > It is widely believed that factoring is, in fact, NP-complete.
- > However, the same was believed of linear programming until
- > Khachian's algorithm.

No, factoring is in NP intersect coNP and it is widely believed that no problem in NP intersect coNP is NP complete (but who knows). People do believe that factoring is hard though. I also (vaguely) remember a theorem that any problem you can build a public key code out of is going to be in NP intersect coNP because you could verify both positive and negative instances of the problem by watching a party with the key information classify messages as legitimate or forgeries.

- > If  $P = NP$ , public
- > key cryptography becomes impossible. (However, private key
- > cryptography can still be possible.)

If  $P=NP$  then if the amount of information (entropy in Shannon's sense) in a series of messages exceeds the amount of information in the encryption key then you can learn something about the messages. So if  $P=NP$  private key cryptography is still possible- but only with *\*large\** keys (like one time pads).

---

## Manipulation of digital images

Joe Morris <jcmorris@mwunix.mitre.org>

Wed, 18 Sep 91 11:07:15 -0400

The new (October 91) issue of *\_Publish\_* has a well-written article on the ethical issues raised by the manipulation of photographic images by computer. It doesn't go into the legal implications of this manipulation (e.g., the issues of evidence in a court case) or similar consequences, but it does provide a nice summary of the situation.

The article also has a subhead that sounds as if it came from one of the asides that PGN sticks into RISKS postings:

"Reach Out and Retouch Someone"

Recommended reading. Joe

[Spanked with an Electronic Airbrush? PGN]

---

**Re: +&\*#\$( Clements, [RISKS-12.33](#))**

Richard Ristow <AP430001@brownvm.brown.edu>

Mon, 16 Sep 91 17:37:29 EDT

For what it's worth, the diacritic in question is apparently also called the "caron", for example in ISO standard 8879-1986(E) and thence in documentation distributed with the University of Waterloo SCRIPT markup and formatting system.

This caused several days of searching, E-mailing, and general handwringing on my own part, that of the SCRIPT maintenance person at Brown University, and the Brown University reference librarians when I innocently asked, where's the hacek? and what is a "caron" good for? Discussion on list ISO8859 raised and sort of answered the same point; apparently "caron" is a legitimate word for the diacritic, but so obscure that Slavic language specialists have rarely heard of it. But it CAN be written in ASCII...

Richard Ristow AP430001@BROWNV.M.BROWN.EDU Bitnet: AP430001@BROWNV.M

---

**Re: +&\*#\$( Roberts)**

JJJJJust JJJJohn <wichers@husc.harvard.edu>

Mon, 16 Sep 91 21:53:34 -0400

I would argue that Mike is simply taking a requirement (the unique id each motor vehicle must carry) and combining it with a chance to express his individuality. I strongly doubt that the vast majority of people who have vanity plates would plaster the same message on the sides of their vehicles if they were not required to have plates.

>Society allows people to advertise themselves by writing their name, slogan, >etc as big as they like on their vehicles - many elements of society do that >and the results can be seen driving down any road any day.

Society also allows people to advertise themselves, within certain limits, by getting vanity plates. If it is such a detriment to society then it would have been legislated out of existence. Since that's not the case I don't see why Dave is upset about Mike and others who are well within the law in expressing themselves.

>The society we live in takes money from each and every one of us to spend on >the common good.

Mike pays taxes as well. He certainly should have the right to express himself. I don't agree with Plato's view of the ideal society as being an antlike colony in which individuality can't/shouldn't exist (or if it exists, can't manifest itself).

>PS. I think he also owes all the other John Does paying taxes for the time >of one cop and one car and one computer system for the wasted effort caused >by his insistence on a misuse of vehicle number plates; the RISK is loss

>of availability of a cop who could be doing something useful instead.

The problem with this argument is that Mike was *\*not\** misusing his license plate. The problem, and the RISK, is that society allows people to have non-standard plates without properly dealing with the consequences. If anyone owes anything for the waste of the cop's time (and Mike's!), it should be the people who designed the computer system without taking into account all of the possible legitimate plates. Don't blame the effect for the cause.

--John Wichers

---

**✂ re: ##\$@\*, Inames, umlauts and other nonstandard print chars...**

Gary Beckmann <beckmann@das.harvard.edu>

Tue, 17 Sep 91 15:45:28 EDT

H. Fuss comments regarding umlauts, etc. remind me that the German speaking Swiss do not use the es-zet anymore. Though it is unclear to me when they stopped using it, I believe it must be before the wide spread use of computers since an aunt (from Austria) who went to school for a while in Switerland had the other children fascinated with her "funny" way of writing "double-s's".

The use of an 'e' for the umlaut causes a problem if you finally get the hardware to print umlauts. How do you update you database? A global search-and-replace would cause you problems if you changed the poet Goethe's name.

Did some one say computers were supposed to make our lives easier?

Gary Beckmann beckmann@das.harvard.edu

---

**✂ Re: +&\*#\$ (Roberts)**

<Timothy\_Freeman@U.ERGO.CS.CMU.EDU>

Tue, 17 Sep 91 12:25:36 -0400

> PS. I think he also owes all the other John Does paying taxes ...

You are misplacing the blame here. The bureaucracy that controls the license plates sells personalized plates for a fee. They even advertise this (in the US, anyway). If this bureaucracy is stupid enough to advertise an offer that causes them more trouble than it is worth, the blame belongs squarely on the shoulders of the bureaucracy, not on the person who accepted the offer.

> PPS. Whether traffic cops in patrol cars EVER do anything useful is not a topic for this newsgroup - we all pay them so we all think that they do!

The connection between opinion and governmental action is much more tenuous than you say. People vote for legislators, not for policies, and a majority isn't a consensus.

---

**✂ Re: +&\$ (Roberts, [RISKS-12.34](#))**

Lynn R Grant <Grant@DOCKMASTER.NCSC.MIL>  
Tue, 17 Sep 91 12:42 EDT

Perhaps this is getting peripheral to the original discussion, but I cannot let Dave Roberts's characterization of ham radio license plates as a misuse of license plates go unchallenged.

Ham radio plates are not a misuse of the system--they are sanctioned by it. For example, in two states where I have lived, Michigan and Illinois, hams pay a very small fee (about \$2) or nothing at all for the privilege of having their call sign on their plates, while other who get personalized ("vanity") plates pay a substantial sum (about \$75, if I remember correctly).

There are a couple of reasons why the state governments do this. Ham radio operators provide emergency communications during tornados, floods, and other disasters. Frequently ham radio emergency groups will have operators stationed in the police departments and weather service offices, relaying information between the government networks and the ham radio emergency networks. Being able to identify the vehicles of radio operators during an emergency is a useful thing. Of course, not all hams are involved in emergency service, but there's a good chance that those at the site of an emergency are.

Also, state governments issue the ham plates to comemorate the service of ham radio operators, just as they have (at least in Illinois) Armed Forces plates, and purple heart plates, and ex-POW plates, and the like.

So, if the government of California issues ham plates, but can't find them in their computer, this is a standard computer data entry problem, not a misuse of the system by ham radio operators.

Lynn Grant N8AF (Grant at Dockmaster.NCSC.MIL)

---

**✂ Re: +&\*\$ (Moore, [RISKS-12.27](#))**

John F. Woods <jfw@ksr.com>  
Mon, 9 Sep 91 14:39:40 EDT

>... would not accept a license number of WAODVD - ...

Possibly he was reading the zero as an O. Someone in rec.ham-radio some time ago mentioned that, in California, they once had some trouble during a traffic stop because of their plate: WB6000 (oh oh oh). The policeman was \*sure\* it was a bogus plate, because letter-letter-four-digits is the pattern used for commercial vans (I believe), which the passenger car in front of him plainly wasn't. And sure enough, the computer had no record of "W-B-6-thousand". Fortunately he eventually was convinced to try W-B-6-oh-oh-oh, and after some gyration getting the person on the computer to type it in right, was rewarded with valid registration info. Oh-Oh-Oh indeed.

John Woods (WB7EEL)



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 12: Issue 37

Friday 20 September 1991

## Contents

- [Letter to Congress on NIST's DSS](#)  
[Jim Bidzos](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

### Letter to Congress on NIST's DSS

*Jim Bidzos <jim@RSA.COM>  
Fri, 20 Sep 91 13:36:05 PDT*

September 20, 1991

Hon. Tim Valentine  
Chairman, subcommittee on Technology and Competitiveness  
House Committee on Space, Science, and Technology  
U.S. House of Representatives

Dear Mr. Valentine:

On August 30, 1991, nine years after their first attempt and over three years after being called upon by the Congress to do so under authority of the Computer Security Act of 1987 (the "Act"), the National Institute for Standards and Technology (NIST) has published a proposal for a public-key cryptographic standard. The proposal, developed with the National Security Agency (NSA), is called DSS, for "Digital Signature Standard." [1]

While we recognize NIST's efforts in finally proposing such a standard, we have serious concerns about the proposal. We question NIST's justifications for their proposal and the manner in which it is being proposed. We are greatly concerned that NIST has not fulfilled its obligations under the Act. Since NIST provided some of these justifications in testimony to the Subcommittee on Technology and Competitiveness on June 27, 1991, you may be interested in our analyses.

Before providing our analysis of the specific statements of justification in NIST's proposal, we would like to offer four criticisms of DSS and the manner in which it is being introduced.

1. NIST has offered only a 90 day comment period for their proposed standard. This time period is insufficient for analyzing DSS. Further, DSS will not be fully complete and presented within the 90 days, but will appear in pieces over a much longer period.

DSS proposes a new, untested public-key cryptographic algorithm. The cryptosystems in use today became trusted over a period of more than ten years, during which much research was conducted and published. Since no one outside of NIST and NSA has seen the DSS algorithm until now, we feel that a much longer comment period---at least one year---is appropriate. Public-key technology has been ignored by NIST for fifteen years; it is inappropriate for NIST to foist a new scheme upon the country with such a short review period. NIST is admittedly submitting a proposal which is missing important components. It is therefore inappropriate for NIST to offer a comment period which expires prior to an opportunity to review a complete proposal.

2. NIST's proposal fails to address the use of public-key cryptography for privacy. It covers only authentication, and is incomplete even as an authentication proposal. Data privacy is an important requirement of the Act, and a large part of NIST's responsibility.

While authentication is certainly important, neglecting to allow for the powerful privacy that public-key cryptography can provide denies U.S. industry important protection against industrial espionage. There is no discernible reason for this omission. Further, NIST's authentication proposal is incomplete --- it is missing important components such as a hashing algorithm and a structure for "certificates" and thus is not yet ready for any actual use. NIST gives no indication of its plans to complete the proposal, but it could easily be one to two years before their proposal is complete. This is a major reason why a 90 day comment period is inappropriate: there is not a complete proposal to comment on.

3. A system different from the one NIST proposes, known as RSA, has come into widespread use around the world as a de facto standard over the last ten years, but NIST, for reasons unknown, has ignored this development.

A growing number of major computer industry companies have licensed and endorsed the patented RSA system. Many, including Motorola, Northern Telecom, Lotus Development and Novell, Inc., have already made RSA a standard part of their mainstream products and have shipped over half a million copies. Current plans of RSA licensees will put this number at several million within a year. (Recently, a Fortune 10 company purchased 15,000 copies of a product from a U.S. licensee of RSA which has privacy and authentication based on the RSA system embedded in it, for use in Europe.) The RSA system offers both authentication and privacy. Furthermore, there is a well developed, complete standard for its use, developed by a number of the most important companies in the U.S., including Microsoft, Sun Microsystems, Lotus, Digital Equipment, and many others. NIST has ignored these developments, not even acknowledging them.

In response to criticism from the press that NIST has ignored developments in

the private sector, NIST has stated that their standard is nominally "only for the government." However, it will be seen that NIST's behavior gives every indication that they are aggressively pursuing a U.S. commercial standard based on their system, attempting to supplant existing de facto standards, and employing every means available to accomplish these objectives.

4. The proposed NIST standard as presented thus far appears inflexible, and cannot support or adapt to new technologies or new technological developments. In a security standard, such inflexibility amounts to gross negligence.

Any cryptographic standard should be structured to support multiple algorithms. (With the exception of the NIST proposal, all such efforts have this flexibility.) Such a facility would provide a means to "switch" algorithms in the event one algorithm becomes "broken," or unsuitable. Support for multiple algorithms is normal practice in cryptography standards, and does not affect interoperability. Such a facility, in this case, would also protect a major investment by U.S. industry, made during government inaction over the last ten years. NIST's approach gives the appearance of trying to reverse a major worldwide trend in industry and standards making. In the same direction, the NIST proposal does not allow for a gradual increase in key size as technological improvements give greater strength to potential adversaries. With computer performance steadily increasing at approximately 40% per year, any reasonable security standard must plan to compensate with a gradual increase in key size. Any proposal, such as NIST's, that contains unnecessary restrictions on allowable key sizes (NIST's proposal only allows 512-bit keys) contains the cause of its own eventual demise. There is no reason for the NIST proposal to restrict users from choosing arbitrarily large key sizes, and thus protecting themselves from technological advances.

We will formally submit these observations to NIST during the comment period for DSS, and request explanation and justification from NIST, consistent with their obligations.

#### NIST'S JUSTIFICATIONS FOR DSS

It is interesting to review NIST's justifications for DSS. The proposal states: "Among the factors that were considered during this process were the level of security provided, the ease of implementation in both hardware and software, the ease of export from the U.S.; the applicability of patents, impact on national security and law enforcement and the level of efficiency in both the signing and verification functions."

We shall examine each of these justifications separately.

#### SECURITY LEVEL

The security level of DSS is clearly an important consideration.

The most serious technical flaw in DSS is that it provides insufficient security. The security of the system depends on the size of certain numbers. Based on the most thorough and recent work on the subject, numbers (such as the DSS numbers at the proposed length of 512 bits) "should definitely be avoided" because they offer only "marginal security" [2]. Such numbers are vulnerable

to catastrophic failure, compromising the security of every single user of the system. An attacker could surreptitiously have the "run of the system." The threat this poses to the security of sensitive U.S. government, commercial, and financial data cannot possibly be justified.

The referenced research [2] on the security of the discrete logarithm problem, on which the DSS system is based, is well known worldwide, ensuring that the NIST system would never be used by any company not forced to do so, and would never be purchased from U.S. suppliers by companies outside of the U.S.

In addition, every single use of the NIST proposal to create a "digital signature" requires a new, truly random value. Although the NIST proposal does not warn users of this, an attacker who could obtain the random value used in any one signature could easily derive that user's private key. Given the user's private key, the attacker could forge the user's digital signature on any document. Obtaining cryptographic quality random values is non-trivial, and may not be possible in some computing environments, making DSS unusable in many applications. We note that the RSA system does not suffer from this weakness.

#### EASE OF IMPLEMENTATION

In addition to the security risk it poses, the added burden of providing the "randomizing" apparatus in a secure manner makes the NIST proposal a cumbersome and costly scheme to implement. Other, more popular schemes do not share this burden; they either require no randomization whatsoever or do not require that the randomization apparatus be kept secret.

Furthermore, the inefficiency of the DSS proposal --- see the following section on efficiency --- makes it difficult to implement if specific performance goals must be met.

#### EASE OF EXPORT

We note that as a signature system, the NIST proposal is no more or less exportable than any system employing cryptography (of any type) for authentication, as opposed to data privacy. All systems that employ cryptography for authentication only fall under Commerce Department jurisdiction, whereas systems applying cryptography to data privacy are controlled by the State Department.

#### APPLICABILITY OF PATENTS

NIST cites, as a major justification for this decision, economic factors related to patent applicability. (see "U.S. Plan Is Seen Hurting Electronic Data Standard," the Wall Street Journal, July 2, 1991.)

NIST feels the government should not pay royalties for the use of technology. (see "NIST Proposes Standard for Electronic Signatures - Move Criticized by Some as Ignoring Tried and True," Network World, July 1, 1991.)

It is a simple fact that the U.S. government does not need to pay royalties or any fees for the use of any public-key cryptography developed in the U.S. since the known public-key schemes were all developed with at least partial federal funding, thereby giving the government royalty-free use. Further, the

government has the right to solicit the private sector to build products, royalty-free, for government use. This justification by NIST could not be more wrong.

NIST further claims it wants to offer a royalty-free system for industry as well. Most licensees of the patented RSA system do not pay royalties but have already absorbed the cost through single payments so that high-grade security can be made available at no extra cost to users as a standard part of high-volume products. Again, since NIST has not consulted industry, it is fair to ask how NIST has determined that this should be the most important criteria. Much of industry has already spoken; a well-studied and well-respected public-key system is worth paying a reasonable royalty for.

A significant part of the U.S. computer industry clearly felt the RSA system offered sufficient value to invest in. Whether one feels RSA is worth paying for or not, NIST's proposal attempts to take this option away from U.S. industry and from the U.S. government. There are currently well over 100,000 documented users of products containing RSA-based security in the federal government and defense industry alone.

In April of 1990, the patent holders for the RSA system offered to cooperate with NIST in a well publicized letter to the agency. Unfortunately, NIST chose not to respond to this offer to work with industry.

NIST's decision to work with NSA instead of industry has the unfortunate effect of "punishing" those companies that haven't waited for DSS. If the NIST standard should prevail as proposed, then those who decided not to wait for NIST lose their investment, and, further, may be put at a disadvantage as they must "retool." How the Commerce Department, after four years of work, could develop a standards proposal that would result in a setback for U.S. companies whose collective annual revenues exceed \$30 billion, demands more explanation than NIST has provided. By punishing our industry leaders who have adopted RSA, NIST's proposal also has the undesirable effect of discouraging the adoption of innovative technology, something U.S. industry must do to be competitive in a global marketplace.

We note that if the NIST proposal becomes the government standard to the exclusion of all others, as currently proposed, then the government itself is deprived of the economic benefit of the investment industry has made in the RSA system.

NIST is the only organization to propose a non-RSA scheme as a public key standard. Those who have proposed RSA standards include the British, French and Swiss banking communities; the International Organization for Standardization; CCITT; and the Internet, among others. Of course, no one can expect that U.S. industry will ignore these developments in favor of the NIST proposal; so in order to remain competitive internationally, U.S. companies will be forced to bear the economic burden of supporting two different systems.

We also note that it has been administration doctrine for over a decade that the government should support, rather than compete, with private industry. NIST's actions are in direct conflict with this policy.

## EFFICIENCY OF SIGNATURE COMPUTATION VS. SIGNATURE VERIFICATION

NIST has stated that performance in signature creation is more important than in signature verification, and offered this as part of its justification for DSS.

We believe, however, that it can be shown without doubt that NIST's claim about the relative importance of these functions is absolutely false, and we invite NIST to justify their claim publicly. We note that special purpose hardware provides identical performance regardless of the algorithm used. NIST's claim makes no sense.

We note that it is true that the NIST proposal features an algorithm with the property that "signing" is faster than "verifying." However, we also note that the RSA system "signs" 35% faster than the NIST proposal, and that RSA operates 40 to several hundred times faster in the critical "signature verification" function. (This can be demonstrated mathematically.) Its poor performance makes DSS useless in interactive applications. DSS will be unusable by a large segment of U.S. industry without the added expense of special purpose hardware, and entirely unusable in most software applications.

## NATIONAL SECURITY AND LAW ENFORCEMENT CONSIDERATIONS

We are left to speculate as to what the concerns of national security and law enforcement NIST refers to may be. We are deeply concerned that it is likely NIST and NSA intend to restrict use of DSS to specific conditions facilitating their own ability to "break the system."

Law enforcement organizations are concerned that the plaintext version of encrypted information be obtainable by subpoena. This was established during the debate over Senate Bill 266 (see "Move on Unscrambling of Messages is Assailed," the New York Times, April 17, 1991).

One may justly ask whether a future privacy standard based on DSS is in fact not NIST's intended concession to national security and law enforcement. The known concerns over obtaining plaintext, NIST's potential use of patents [3], and the weaknesses in DSS make this possibility difficult to ignore. Using a short comment period to avoid future scrutiny and offering only an incomplete signature proposal increases suspicions. Therefore, we must view DSS as the underlying technology for providing a standard for data privacy in the future, and ask if it is appropriate for this use. Of course, NIST could reveal its plans for a privacy feature to calm these fears. Instead, NIST states that a privacy mechanism is "years away," and will not give any indication as to its plans.

If such a system becomes the de facto U.S. commercial standard, then it may indeed benefit law enforcement, albeit at the expense of the privacy of everyone. In this case, a "breakable" system is effected by forcing the use of a single number or small group of numbers that the government can "break," but that they believe no one else can. A number of the size proposed by NIST seems just about right for this scenario.

As a standard for U.S. private sector, such a system gives the government unwarranted, unnecessary, and undesirable powers to violate personal privacy.

Further, there is no assurance that a foreign government cannot also "break" the system, running the risk of a "digital Pearl Harbor" --- a devastating loss of the security of the entire national financial and business transaction systems. The possibility that DSS is intended to be used in this manner alone justifies congressional investigation.

#### OTHER CONCERNS

The DSS proposal states, "This proposed FIPS is the result of evaluating a number of alternative digital signature techniques. In making the selection, the NIST has followed the mandate contained in section 2 of the Computer Security Act of 1987 that NIST develop guidelines and standards to '...assure the cost-effective security and privacy of sensitive information in Federal Systems.'"

We note that NIST has so far declined to identify alternative techniques it evaluated. A Freedom of Information Act request was filed in August of this year by CPSR (Computer Professionals for Social Responsibility) with NIST seeking documents related to NIST's evaluation, but NIST claims to be exempt in this case, claiming in their response that such information is "advisory and pre-decisional" as well as "related to pending patent applications." We note that NIST has made and publicized its decision and that it has also published the scheme it hopes to patent. NIST's denial of information with no apparent justification does not inspire confidence in DSS, but intensifies concern that there is a hidden agenda, such as laying the groundwork for a national public-key cryptosystem that is in fact vulnerable to being broken by NIST and/or NSA.

Statements made by NIST officials in defense of DSS do not offer any clarity. According to Lynn McNulty, associate director of the National Computer Systems Laboratory at NIST, "Even if someone breaks the DSS, it is only a signature standard." ("NIST Signature Standard Whips Up Storm of Controversy from Industry," Federal Computer Week, Sep. 2, 1991.) Aside from the insight this comment may provide about the security of DSS, this statement may be misleading if NIST in fact plans to base a data privacy standard around DSS.

#### CONCLUSIONS

It is well known that the larger part of NSA's mission is to gather electronic intelligence. It is also well known that strong data encryption technology (already well known and coming into use around the world) may interfere with that mission. But electronic eavesdropping by others and industrial espionage through electronic means are also realities. The U.S., with the largest computer market in the world, is at greatest risk, and therefore has the most to gain from high quality encryption technology.

Through its active promotion to industry of less than fully open programs such as CCEP (NSA's Commercial Comsec Endorsement Program), NSA has lost any credibility it may have had with the private sector. (see "A Supersecret Agency Finds Selling Secrecy to Others Isn't Easy," page 1, column 1, the Wall Street Journal, March 28, 1988.) Sadly, NIST seems to be headed down the same path.

The government should be playing a leading role in advancing the U.S. information industry into the next century. The NIST proposal, with its unanswered questions, NSA origins, and questionable justification, looks backward. We would hope that with the stakes involved in the country's first government standard for public-key cryptography, NIST would "go the extra mile" to ensure the integrity of the process. Instead, NIST shuns industry cooperation and offers flawed proposals developed secretly with NSA.

NIST's proposal gives industry no privacy mechanism, and has a long way to go before being usable for authentication. It is a great disappointment that a multi-year effort involving the Commerce and Defense Departments has yielded such an incomplete, flawed product. U.S. industry and the taxpayers of this country deserve better from our government.

NIST is either unable or unwilling to justify its actions. Only Congress has the power to force NIST and NSA to answer critical questions about the proposed DSS. Even the most remote possibility that there is a hidden agenda behind DSS justifies congressional action. We urge you and your committee to have NIST, and, if necessary, NSA, answer important questions about their proposal or have it withdrawn.

We are at the disposal of the Committee if we can be of any assistance.

Respectfully,  
RSA Data Security, Inc.

(signed)  
D. James Bidzos  
President

cc: Members, Subcommittee on Technology and Competitiveness  
Hon. Jack Brooks, Chairman, House Committee on the Judiciary  
Hon. Robert Mosbacher, U.S. Secretary of Commerce  
Dr. Willis H. Ware, RAND Corporation

[1] NIST's proposal is Docket No. 910807-1207, RIN 0693-AA86, "A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)." A digital signature is an electronic analogue to a handwritten signature that demonstrates the authenticity of an electronic document or message. A user "signs" a document by applying a cryptographic function to the contents of the document using a quantity known only to that user called a "private key." Anyone can "verify" a user's digital signature on a document by applying another cryptographic function to the contents of the signed document employing the user's corresponding "public key," a quantity published and known to everyone. Digital signatures are essential for the transition of commerce from a paper-based system to electronic media.

[2] "Furthermore, since many discrete log cryptographic schemes have the feature that they use a fixed prime which cannot easily be changed, one has to allow for attacks that consume not just a couple of months, but even a couple of years of computing time. Therefore, even 512-bit primes appear to offer only marginal security..." from "Computation of Discrete Logarithms in Prime Fields" by B. A. LaMacchia and A. M. Odlyzko, published in "Designs, Codes,

and Cryptography 1" (Kluwer, 1991, pp47-62)

DSS specifies a 512-bit prime modulus, and states that such a modulus can be shared by groups. This is important as the discrete log problem is known to be "brittle," meaning a table of discrete logarithms could be built, allowing an attacker to simply "look up," rather than have to "break," a user key.

[3] NIST has stated clearly in its proposal that worldwide patents have been filed for DSS. It is not clear how NIST can justify spending tax dollars to file for worldwide patents on DSS if, as NIST claims, the goal is to grant royalty-free use of DSS. NIST need simply publish the scheme without patenting it, and save the expense. One likely reason to patent DSS is to control its use. NIST could then offer "royalty-free patent licenses to anyone who practices the standard." This would insure that no one could use DSS except as specified by NIST. Interestingly, there is precedent for precisely this approach to licensing standards.



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 12: Issue 38**

**Friday 20 September 1991**

## Contents

- [Midwest Stock Exchange Reaps Millions Due to Accounting Glitch](#)  
[Jeff Helgesen](#)
- [Newark NJ high school computer problem](#)  
[Martin A. Leisner](#)
- [Technology and the oldest profession](#)  
[Henry Cox](#)
- [YATO \(Yet Another Telco Outage\)](#)  
[Richard Johnson](#)
- [AT&T switch trouble](#)  
[Fernando Pereira](#)
- [English Supermarket Checkout Failure](#)  
[Maddock](#)
- [Samurai Hackers' Cunning Employer Screening Process](#)  
[Marco Barbarisi](#)
- [Re: Fly-by-wire without leaving the ground](#)  
[A. Padgett Peterson](#)
- [MSAFP, utilities, and all that](#)  
[Mark Fulk](#)
- [Computer monitoring of pill bottles](#)  
[Jennifer Heymont](#)
- [Documentation and lack thereof \(Stanley S.T.H.\) Chow](#)  
[S.T.H.\) Chow](#)
- [Just the wrong number](#)  
[Jerry Leichter](#)
- [Reliability and Redundancy](#)  
[Bill Murray](#)
- [CPSR Annual Meeting](#)  
[Eric Roberts](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Midwest Stock Exchange Reaps Millions Due to Accounting Glitch**

*Jeff Helgesen* <[jmh@guinevere.pubserv.com](mailto:jmh@guinevere.pubserv.com)>

*Fri, 20 Sep 91 14:54:15 cdt*

The Chicago Tribune reports that leaders of the Midwest Stock Exchange had discovered a 13-year-old accounting glitch which enabled a subsidiary to wrongfully reap millions of dollars in interest payments which should have gone to broker-dealers. While the exact amount of money received by the subsidiary due to the error was not disclosed, the chairman of the exchange said that he estimated that over the last twelve months, the firm received around 1.8 million dollars.

The accounting error, due partly to human error and partly the fault of computers[sic], apparently dates back to about 1978. At that time, the exchange and two of its subsidiaries, Midwest Clearing Corp. and Midwest Securities Trust Co., altered the way certain broker-dealer transactions were handled. Clearing Corp. instituted a change, largely computerized, ordering broker-dealers to wire money to it for the sale of securities before the securities were received by Securities Trust Company.

By depositing these funds in short-term, government-backed securities, sometimes overnight but also for longer periods, Clearing Corp. generated for itself interest payments which should have gone to the broker-dealers. This is referred to as "playing the float". When the clearing system is working properly, the securities and proceeds are transmitted through the system simultaneously, thus eliminating such a float.

The Midwest Stock Exchange insists that they are taking the situation very seriously, and plan to pay the money back. Some exchange members are concerned that the money used for the refund will come in the form of higher exchange rates, putting the exchange at a serious competitive disadvantage.

[Summary from Chicago Tribune Business Section, 9-20-91, "Exchange: Unit profited from 13-year glitch"]

---

### **✂ Newark high school computer problem**

*Fri, 20 Sep 1991 11:55:41 PDT*

>From the New York Times, Wednesday 18Sep91, page B2:

"Computer Glitch Sends Newark School Into Chaos" by Joseph F. Sullivan

The article starts off:

Newark, Sept. 17 -- When Central High School's 1000 students and 90 teachers showed up for the start of the school year on Sept. 5, many found themselves in a computer-generated game that was part musical chairs and part hide-and-seek.

About half of the students had no schedules for classes or had schedules with holes in them. Some classrooms had no teachers, while others had four teachers instead of one. Many students spent much of last week in the school auditorium conferring with guidance counselors who were trying to correct the scores of mistakes in their classroom assignments.

The article then goes on to talk about absenteeism and the other problems this caused.

marty leisner.henr801c@xerox.com UUCP:uunet!xerox.com!leisner.henr801c

---

### **Technology and the oldest profession**

Henry Cox <cox@cadence.com>

Thu, 19 Sep 91 09:37:25 EDT

This morning, the Boston Globe had an article about a \$3 million prostitution ring which had been running out of a Boston suburb, which was broken in a series of raids yesterday. The computer relevant (or irrelevant, as the case may be) portion of the story was that the group kept a database of their 4000-odd customers and had used call forwarding/etc. to be able to move headquarters from place to place quickly and easily.

The story was unclear on what the police intend to do with the customer list, most of whom are apparently fairly well off.

[Similar stories have been recorded in the RISKS annals before -- e.g., SoftwEngNotes 11 5, 12 1, 14 1. (See RISK-7.72, 8 Nov 88, Computers in the oldest profession (Dave Horsfall). PGN)

---

### **YATO (Yet Another Telco Outage)**

Richard Johnson <richard@oresoft.com>

Fri, 20 Sep 91 9:19:19 PDT

According to KINK radio in Portland, Oregon, this morning, most of the suburbs south and east of Portland were without telephone usage for about six hours because someone cut a fiber-optic cable.

More importantly, the towns of Milwaukie and Lake Oswego (just south of Portland, upstream on the Willamette river) were without 911 coverage for over three hours.

Richard Johnson richard@oresoft.com richard@agora.rain.com

---

### **AT&T switch trouble**

Fernando Pereira <pereira@klee.research.att.com>

Thu, 19 Sep 91 14:51:13 EDT

According to the AP, the union for the technicians in charge of monitoring the AT&T switch that shut down this Wednesday causing major disruptions to air traffic control ([RISKS-12.36](#)) claimed that they were not on duty because they were attending a class to learn about a new alarm system for the problem that caused the shutdown.

---

## ✂ English Supermarket Checkout Failure

"Maddock :-)" <SOEF\_16@leicester.ac.uk>

Wed, 18 Sep 91 10:41 GMT

The English 'Daily Telegraph' (Sept 18) reports on the failure of 32 computer operated checkout tills in the Sainsbury supermarket in Aylesford, Kent.

'Shoppers ... were invited to suggest a fair price for the goods in their trolleys when the scanners which which read the bar codes refused to work. The breakdown happened only 10 days after the opening of the new store ... The store was then closed for the rest of the day.'

Sainsbury's described the failure as 'extremely rare' and said 'when a total failure occurs we ask the customer to suggest a price'. The chain said that 'this allows customers already shopping to complete their purchases'.

---

## ✂ Samurai Hackers' Cunning Employer Screening Process

Barbarisi <marco@email.ncsc.navy.mil>

Wed, 18 Sep 91 13:59:07 CDT

I'm sure many of you have seen the recent issue of Rolling Stone magazine, with the article entitled "Samurai Hackers". It discusses the hiring of young computer enthusiasts by law firms, ad agencies, and the like, for the purpose of prying into the electronic data of subordinates and coworkers. Basically, individuals and firms recruit "hackers" from BBSs and pay them thousands of dollars to do little more than break passwords and riffle through files. Appropriately, the young hackers call these people "Stupids". Of course, the young hackers should really be called "crackers", but I really don't want to start another semantics war.

Both the crackers and their employers have unsettling views on privacy: Data stored electronically is considered public information, regardless of the locks (passwords) enabled by the keeper.

The really cunning aspect of the article is one little paragraph in which the samurai explain how they screen potential employers over a BBS. Claiming the need to "authenticate" potential employers and differentiate them from the Feds, the crackers will not deal until they get the person's social security or credit card numbers! Though not mentioned in the article, it seems reasonable to assume that this "authentication" process includes requests for other information such as birthdate, childrens' names, home phone number, car tag, etc. All of this occurs remotely over a BBS system.

I'll leave it as an exercise for the reader to figure out what is wrong with this picture.

Marco C. Barbarisi - NCSC Panama City, FL - marco@email.ncsc.navy.mil

---

**Re: Fly-by-wire without leaving the ground**

A. Padgett Peterson <padgett%tccslr.dnet@uvs1.orl.mmc.com>

Wed, 18 Sep 91 17:10:51 -0400

From: fmsrl7!art-sylchap@sharkey.cc.umich.edu

>James Higgins, THE DETROIT NEWS, 15 September, page 1C: ... Clemson engineers  
>... have patented a new automobile camshaft/throttle control system they say  
>can boost fuel economy by 20 percent in a gasoline engine.

Over what ? A '74 Toronado, or a Honda Civic HF ?

>A camshaft controls the action of the valves that let mixed fuel and air into  
>an engine and allow burned gases to escape. Usually it's set up so that the  
>valves will open or close according to just one setting. That setting is a  
>compromise, not...optimal...for all engine speeds. ... In the Clemson system,  
>the camshaft consists of two shafts, one of which rotates inside the other. An  
>infinite variety of valve settings is possible, theoretically allowing optimal  
>valve action in every situation.

Both Bruce Crower (1973) and the Cadillac 8-6-4 (1978) tried similar but less complex solutions. Neither was satisfactory.

>But here's the nub--his  
>system also includes a computer-controlled device that electronically allows  
>the camshaft to act as the car's throttle--a revolutionary idea.  
>The Clemson system substitutes [for] the mechanical connection...a computer  
>control--a "fly by wire" device like those...on advanced aircraft.

The Knight sleeve-valve engine had some similar characteristics back in the 20's as I recall.

The idea has promise but a MAP (Manifold Absolute Pressure) following throttle plate would have the same characteristics without the drawbacks. So does any cruise control. See below.

> When the engine doesn't have to labor against a partially closed throttle,  
>significant fuel economy gains are possible, Nelson says.

This is wrong. An engine doesn't "labor" against a partially closed throttle any more than a vacuum cleaner "labors" against a blocked inlet - the power requirement goes down, not up as the MAP decreases since less air volume is being moved/compressed. When you remove the combustion aspects, a gasoline engine is often modeled as an air pump with maximum capacity at WOT (wide open throttle) and minimum load with a closed throttle.

One point not mentioned is that such a scheme would also require direct cylinder fuel injection, also like a Diesel & considerably more expensive than the port or throttle body injection currently used on "conventional" gasoline engines since the very short intake duration and low manifold & port gas velocities at cruise would preclude other methods.

This is not to mention the lack of any manifold vacuum source for accessories or emissions devices (why passenger Diesels have little vacuum pumps mounted on them). Of course this is solvable with a bit of engineering but the question remains whether any advantage is gained that is not available with a "fly-by-wire" throttle plate alone. It would be interesting to see how this device would match up with a good cruise control on a modern engine.

This is not to say that the variable camshaft duration (haven't seen the device, but would expect the delta to be in duration not lift since a) is much simpler to implement, and b) would allow tailoring not only of the effective flow, but also the advance/retard characteristics that could spread effective scavenging/ram effects over a broader range than with a fixed cam) doesn't sound theoretically feasible, just that there are easier ways to go about it and I have to wonder if it might be more suited to racing than the road.

Really digging now but didn't Mercedes experiment with variable durations on the 300SLR's desmodromic (sp?) valve gear in the early fifties ?

In short, the idea has promise but, at least for the moment, I would have to put it in the same category as the D.A.F. "DAFODIL" with the constant velocity transmission of a few years ago - the same idea approached from the opposite side.

Padgett

---

### **✂ MSAFP, utilities, and all that**

*<fulk@cs.rochester.edu>*

*Wed, 18 Sep 91 11:42:42 EDT*

I must regret having created something of a monster.

My original point was simply this: the advocates of the MSAFP assigned different utilities to the various possible outcomes than I did. However, their advocacy literature did not address this possibility.

On questioning, one MSAFP advocate (a geneticist at Strong Memorial Hospital) admitted that the rate of spontaneous abortions had relatively little impact on consideration of the MSAFP. It was clear from our conversation that the MSAFP advocates (the geneticist was one) were concerned with the social good of reducing defective births, whereas I was also concerned with the grief and self-recrimination that would surely follow an accidental abortion.

Although it is tempting to respond at length to Mr. Grodberg, I will limit myself to three points: I did this calculation in 1987, it was done with the numbers supplied to me by the ADVOCATES of MSAFP screening, and I possessed and used some relevant facts that Mr. Grodberg lacked.

In particular, I regarded anencephalic births as having only about double the (negative) utility of spontaneous abortions, whereas spina bifida was given a much lower (worse) utility. This because anencephalic infants do not survive, whereas infants with s.b. do and require surgery; at least a few years ago they

were generally paralyzed from about the waist down. Almost all s.b. victims also suffer hydrocephaly (maybe it's all, I forget); and the shunts used to treat hydrocephaly frequently break down.

I'd provide you with precise numbers if I could find my notes. Unfortunately, they are buried under about a foot of papers on my table here. After all, it has been nearly four years now.

Mark Fulk

---

**✂ Re: MSAFP, utilities, and all that**

<fulk@cs.rochester.edu>

Wed, 18 Sep 91 13:47:47 -0400

If people would stipulate three points:

- (1) The parties affected by a choice do not usually share a common assignment of utilities to outcomes (if they can be said to have utilities at all; see Kahneman and Tversky).
- (2) Point 1 is rarely acknowledged by published risk-benefit analyses. (Emphasize rarely; some studies may, but the studies that I've read haven't.)
- (3) Points 1 and 3 are of interest to RISKS readers, and should be born in mind whenever discussing risks of any sort.

then I would have succeeded, and I don't really give a damn what people think of the MSAFP. In fact, my position would be that people OUGHT TO make their own evaluations of the MSAFP.

The same point can be made in several different ways. For example, government tends to equate all deaths, or at least to equate years of life lost; people in general, however, have strong preferences about the NATURE of their deaths.

Mark

---

**✂ Computer monitoring of pill bottles**

<jleah@ATHENA.MIT.EDU>

Wed, 18 Sep 91 13:57:05 -0400

There seems to me to be one very obvious problem with the so-called "Smart Pill Bottles," which is that there does not need to be any correspondence whatsoever between the number of times that a patient opens a pill bottle and the number of times that they actually \*take\* the medication. Two scenarios, both of which are common to people who take medication regularly, come readily to mind:

- a) patient opens the pill bottle to see how many are left and whether or not they need to refill their prescription. This would

result in more openings than pills taken, and the doctor might well think that the patient was taking the appropriate number when in reality they are not. This would probably be in the noise, since it doesn't happen that often.

b) much more common is a patient who opens the bottle, transfers some to another bottle, which he keeps in a different place, takes on a trip with him, etc. This would result in a number of bottle opens that was drastically less than the number of pills taken, causing the doctor misattribute effects the effects of too low a dosage to incomplete ingestion of medication.

Now granted, in both of these scenarios, all that is necessary to avoid the problem is for the patient to know what is going on and make sure to keep track of things like this. However, presumably if they were on the ball enough to do that, they wouldn't need something like this in the first place!

Jennifer Heymont

[There are many problems with the original approach...  
But the fundamental problem is another example of looking  
for a high-tech solution to a low-tech problem... PGN]

---

## ✂ Documentation and lack thereof

Stanley (S.T.H.) Chow <SCHOW@bnr.ca>

19 Sep 91 13:02:00 EDT

In a recent issue of "Vectors", published by Hughes Aircraft, there is an article entitled "So, you can't replcae it then make it better". The article talks about the amazing feats the Hughes achived in winning the MTSP (Microelectronics Technology Support Program). The whole MTSP seems to be a response to the problem of not being able to obtain obsolete components for military systems. This is itself of some interest due to the military going from leading edge to the trailing edge.

Of more interest to RISKS readers, contractors to the MTSP had to solve three problems:

- "Reverse engineer an obsolete intergreated circuit".
- "Given technical data on a circuit board, reverse engineer the circuit board". (There is no statment of how much technical data)
- develope replacements for above, using silicon compilers and generic gate arrays.

Given the well-known mountains of paper that the Pentagon requires for any hardware, and the many mil-spec's for documenting and testing any and everything, it is quite a surprise to me that anyone should need to reverse engineer anything.

To make explicit the RISKS:

Even excellent documentation is useless, Unless you can find it again.

Stanley Chow (613) 763-2831

BNR PO Box 3511 Stn C, Ottawa, Ontario, Canada K1Y 4H7 BitNet: schow@BNR.CA  
schow%BNR.CA.bitnet@relay.cs.net ..!uunet!bnrgate!bcarh185!schow

---

## **✂ Just the wrong number**

*Jerry Leichter <leichter@lrw.com>*

*Thu, 19 Sep 91 22:33:47 EDT*

Sanford Sherizen's recent posting about the Tandem crash due to the date/time have "just the wrong value" reminds me of two other such incidents that I know of. Curiously, in both cases the POTENTIAL for the problem was spotted in the code, but as far as I know in neither case was it ever triggered.

Case 1: So you think that's a good password?

When I was an undergraduate at Princeton, a group of friends and I, ahem, made full use of some of the more arcane and undesirable aspects of OS/360. Now, OS/360 had no provision for passwords on accounts - it was, after all, a batch/card system. However, the local system support people decided that passwords were needed.

They needed to retrofit a password scheme into an existing system. To store the password, they re-used 3 bytes in the existing user data file (they had previously contained the user's initials). A submitted deck could, anywhere at all within it, contain a \$PASSWORD card with the correct password. (The recommendation was that carry with you a \$PASSWORD card, pre-punched with your password, but with the printing turned off. The card would not appear in your output, and without the printing it couldn't be "accidentally" read without a deliberate effort. Given the technology, not a bad system.)

Since many old decks existed, and there was a large group of existing users, it was decided that the password feature would be optional: Initially, you had no password. If you had no password, you didn't need a \$PASSWORD card; if fact, if you provided one, your job was rejected. Once you had set a password, you had to provide it.

Now, there is no free bit to indicate "has set a password", so instead the chosen field was re-used: If it was three 0 bytes, the system assumed you had no password. In that case, it didn't even check the password provided on a \$PASSWORD card - it immediately rejected the job.

Three bytes does not a good password make. It's not that there are too few combinations - in an environment where the only way to try a password is to submit a deck of cards,  $2^{24}$  of them is plenty. However, people want something they can remember. So the system allowed passwords of, as I recall, up to 16 bytes. The 16 bytes were run through an encryption algorithm (the designers apparently thought it was a one-way encryption - it wasn't, as we proved by inverting it) and then compressed down to three bytes.

There are many perfectly valid passwords which, after running through this algorithm, produce an encrypted, compressed password of three zero bytes. The password setting code didn't check for this; it simply stored the calculated value. Set one of those passwords, and you were locked out of your account until you thought to run a deck with no \$PASSWORD file in it at all.

Case 2: A spacey kind of Saturday.

A number of years ago, I worked on a system that supported all of DEC's manufacturing plants. The system was written in BASIC PLUS on RSTS/E - sounds bizarre, but it worked out quite well. (This experience also left me permanently skeptical of all claims that any new language/OS/whatever is a panacea. Most programmers, and probably all academics, would look down their noses at the environment we had - but we built and maintained a large, successful system, running quite reliably 24 hours a day, tying together multiple CPU's - in 1974, when networking was virtually unheard of.)

The standard RSTS representation for the date was a two-byte number representing an offset from some base day, I forget when. BASIC PLUS had some very nice file management calls, but they worked with strings, not numbers. No problem: There was a set of what amounted to type coercions that would take, say, a date and treat it as a two character string.

One day. I did a little calculation and realized that we were quite close to an interesting anniversary: The day that the date, interpreted as a string, came out to two spaces. The date happened to fall on a Saturday.

Some string operations in BASIC PLUS truncate trailing spaces - the obvious string comparison operation is one. I could imagine many potential failures in programs that suddenly found that the current date was the null string. So I was looking forward to an interesting Monday morning of panicked calls from, literally, all over the world. I must say that I was glad that none came in!

-- Jerry

---

### ✂ Reliability and Redundancy (Re: PGN, [RISKS-12.36](#))

<WHMurray@DOCKMASTER.NCSC.MIL>

Fri, 20 Sep 91 15:34 EDT

>Here we have another example of creative redundancy and supposedly  
>conservative design (hardware reliability, fault tolerance, extra capacity,  
>alternative routing, standby power, etc.) still not being good enough to  
>prevent massive outages.

This should not come as a surprise to anyone. There is an upper bound to the degree of reliability that can be built into a system by redundancy. At some point, one introduces so much complexity, so many components, and so many connections that these begin to cause failures that would not have occurred in their absence.

I do not intend to suggest that there is an upper bound to reliability; while I

suspect that there is, I do not pretend to know. Only that there is clearly an upper bound to the reliability that can be achieved by redundancy.

I have more hope for what can be achieved by integration and simplification.

William Hugh Murray, New Canaan, Connecticut

---

## **CPSR Annual Meeting**

*<eroberts@Eeyore.Stanford.EDU>*

*Thu, 19 Sep 91 14:09:33 PDT*

1991 Annual Meeting  
of  
Computer Professionals for Social Responsibility  
October 12 and 13  
Massachusetts Institute of Technology  
Cambridge, MA Auditorium 34-101

Celebrating Ten Years of CPSR

Computer Professionals for Social Responsibility, the nation's only public interest organization of computing professionals, will hold its 1991 Annual Meeting on October 12 and 13 in Cambridge, Massachusetts. The CPSR Annual Meeting is a national gathering that gives computer professionals from all over the country a chance to meet and to discuss the important and interesting issues facing the profession and the public. The meeting is open to everyone who has an interest in computers, communication, the future of our high-tech society, and our role as citizens in the development of policy.

This year's meeting will focus on current developments in information technology and the impact they will have on our ways of communicating and distributing information. The Bush administration has proposed a \$2 billion program of investment in new computer networking technologies, which have the potential of transforming the future of international communication. There are many pressing policy issues raised by the proposal: Who will control the new network? Who will have access to its resources? What are the provisions for privacy, security, and equity?

The sessions on Saturday, October 12, will include several distinguished speakers addressing these and other pressing public-interest issues surrounding electronic communication and the emerging "information age." It will provide an opportunity to think together about the problems, and through CPSR to pass the resulting assessments along to the media, to policymakers, and the other participants in the democratic process.

Admission to the CPSR Annual Meeting is \$20 for members, \$25 for non-members, and \$10 for students and low-income attendees. We welcome additional contributions to support our work. Contributions to CPSR are tax-deductible.

For more information and registration materials, contact CPSR at (415) 322-3778 or by electronic mail at [cpsr@csl.stanford.edu](mailto:cpsr@csl.stanford.edu).

## PROGRAM

Saturday, October 12

8 a.m. to 9 a.m. Registration and Continental Breakfast

9 a.m. to 9:15 a.m. Welcome from the CPSR Board

9:15 a.m. to 10:45 a.m.

"The Past, Present, and Future of Government Policy in the Information Age"

John Shattuck, Vice President, Government, Community and Public Affairs, Harvard University. Research Associate in the Science, Technology, and Public Policy Program at the John F. Kennedy School of Government, Harvard University. Former Washington director of the American Civil Liberties Union, and former vice-chair of Amnesty International.

10:45 a.m. to 11 a.m. Break

11 a.m. to 12:30 p.m.

"The Personal and the Political in Electronic Communication"

Judith Perrolle, Associate Professor of Sociology, Northeastern University. Research Associate at the Harvard School of Public Health. Author of the book, Computers and Social Change.

12:30 p.m. to 2 p.m. Lunch (not included in the conference)

2 p.m. to 3:30 p.m.

"Educational Equity and the International Economy in the Information Age"

Herb Gintis, Professor of Economics, the University of Massachusetts at Amherst. Co-author of the books Inequality (with Christopher Jencks and others), Schooling in Capitalist America (with Samuel Bowles), and Democracy and Capitalism (with Samuel Bowles).

3:30 p.m. to 4 p.m. Break

4 p.m. to 6 p.m.

Parallel presentations on public interest programs involving information technology.

- o An overview of CPSR's programs and operations, intended for new members and those who would like to become more active in the organization, presented by members of the CPSR Board of Directors.
- o Mass OnLine, a project of the Boston Computer Society, presented by Tracy Licklider, president, Boston Computer Society.
- o Community Bytes, a project of the MIT Community Fellows Program, presented by Laxmi Ramasubramanian, research associate, Community Fellows Program.

- o The Electronic Frontier Foundation, to be presented by a representative of EFF.
- o The CPSR Computing and Civil Liberties Project, presented by Marc Rotenberg, National Program Director, Computer Professionals for Social Responsibility.

Sunday, October 13

8 a.m. to 9 a.m. Continental breakfast

9 a.m. to 10 a.m. Reports from CPSR leadership

10 a.m. to 10:30 a.m. Break

10:30 a.m. to 12:30 a.m. Chapter organizing workshop

12:30 p.m. to 2 p.m. Lunch

2 p.m. to 3 p.m. General CPSR business meeting

3 p.m. to 4:30 p.m. Parallel workshop sessions on CPSR projects

4:30 p.m. to 5 p.m. Wrap-up and evaluation



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 12: Issue 39**

**Monday 23 September 1991**

## Contents

- [Carpal Tunnel Syndrome strikes](#)  
[Peter Mellor](#)
- [Risks of technical translation](#)  
[Bertrand Meyer](#)
- [Patent for Travelmation on Fare-Search System](#)  
[Bob Frankston](#)
- [Rounding and truncating within multilevel software](#)  
[Brenton Hoff](#)
- [Re: SunOS SPARC Integer Division Vulnerability](#)  
[Dik T. Winter](#)
- [Re: Risks of mistreating programmers](#)  
[Vesselin Vladimirov Bontchev](#)
- [Re: Play the lottery via Nintendo](#)  
[Mike Cepek](#)
- [Re: documentation and the obsolete parts problem](#)  
[Lou](#)
- [Ideas made simple](#)  
[Bob Frankston](#)
- [Book review: Technological Risk, H.W. Lewis](#)  
[Jack Goldberg](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Carpal Tunnel Syndrome strikes**

*Peter Mellor* <[pm@cs.city.ac.uk](mailto:pm@cs.city.ac.uk)>

*Mon, 23 Sep 91 12:10:21 BST*

A friend of mine has suffered for years with what she thought was arthritis. About 18 months ago, she was diagnosed as having a classic case of CTS. She is due to have an operation to "depress the nerve in the wrist" very shortly and is a bit concerned about the likely outcome. A few people she knows have undergone the same operation with good results, but she has been warned that the scar will be extremely sensitive for a long time.

Does anyone out there have any experience, which I can quote to reassure or warn her?

A have noticed a few curious things while this has been going on:-

- All the people she knows who have suffered from CTS are female, and the affected hand has been the non-dominant hand. Is this a general rule?
- The operation list at the consultant's surgery showed that he does around two CTS cases a week. That's one consultant in London, and only the cases severe enough to be operated on! How prevalent is CTS? Any statistics?
- My friend is a highly-skilled touch typist (who for years trained other people to professional qualification standard), and very careful regarding the ergonomics of typing, position of seat, hands, etc. Why does CTS strike the professional, and not the idiot amateur like me, who types with one hand only (having lost the use of the other years back in a road accident), and whose idea of ergonomics is having the ash-tray and the coffee cup within easy reach? (I put in sufficient hours at a workstation to qualify for the "at risk" category, though!)

All information gratefully received. (I am aware of the correspondence around [RISKS-10.12](#) from Andrea Frankel et al., and have already passed on that information.)

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

[RESPONSES TO PETER MELLOR, PLEASE, NOT TO RISKS. I TRUST HE WILL SHARE ANYTHING SIGNIFICANT WITH THE REST OF US... Thanks. PGN]

---

## ✂ Risks of technical translation

*Bertrand Meyer @ SOL <bertrand@eiffel.fr>  
Thu, 19 Sep 91 12:07:27 +0200*

Being interested in languages (both natural and artificial) I lent an ear to the following story, heard from a participant to a seminar I recently taught in Berlin. I tried to get the details right, but this is all hearsay and I can make no guarantee of accuracy.

It appears that the UCSD Fortran (?) compiler had a confusing option which enabled programs to write to a ``device'' as well as to a Fortran ``unit''. In particular, unit 6 is the standard output in Fortran; but writing to DEVICE 6 rather than UNIT 6 would erase the whole disk...

Such an event, disastrous as it was, could only occur as a result of some combination of bad luck and carelessness - for people using the original documentation.

But according to my source the German translation used the word ``einheit'' as a translation for ``device''. (Apparently the translator also rendered ``unit''

by ``einheit", which is indeed appropriate; but I am not sure of this point.)

The result is obvious: in German-speaking countries an inordinate number of people lost everything as a result of erroneous write-to-device operations...

Perhaps someone with first-hand experience can confirm or correct.

Bertrand Meyer bertrand@eiffel.com (temporarily: bertrand@eiffel.fr)

[In UNITY there is DEVICEiveness? PGN]

---

### **✂ Patent for Travelmation on Fare-Search System**

<frankston!Bob\_Frankston@world.std.com>

20 Sep 1991 20:28 -0400

There is an article in the Sept 16th issue of Business Travel News. To quote one paragraph "The patent decision recognizes as unique Travelmation's system for checking its own database of fares and flight availability and automatically selecting low fares that conform to corporate travel policies." Later in the article, "Part of the patent also covers Travelmation's Trip Planner system, a program that allows travelers to send their travel requirements from a personal computer to Travelmation..."

---

### **✂ Rounding and truncating within multilevel software**

behoffski <XTBJH@levels.unisa.edu.au>

Sun, 22 Sep 1991 17:45 +0930

Rounding and truncating data can often get you into difficulties, as we found recently in our fuel management system.

We collect data about refuelling transactions, and record the quantity of fuel measured and the price of the transaction. We report the quantity to the nearest hundredth of a unit (litres), and the price to the nearest hundredth of a dollar. Recently, one of our customers complained that at a price of \$1.00 per litre of fuel, the quantity would sometimes be 0.01 higher than the price.

What we found was that the program in the system that collected the transactions and forwarded them to the database handled the numbers differently: quantities were rounded to 2 decimal places, but prices were rounded to 3 decimal places (effectively tenths of a cent). The program which brought these transactions into the main reporting database then truncated the price to two decimal places. I believe that this truncation was unintentional.

Our options in fixing this problem were:

1. Rounding the 3-decimal digit price to 2 decimal places.
2. Storing all 3 decimal places of the price.
3. Reporting the price to 2 decimals, instead of 3.

Option 1 was quickly discarded: you must not round a number twice, as

distortions creep in (0.4449 -> 0.445 -> 0.45 instead of 0.44).

Option 2 was unacceptable: since every transaction report only reported 2 decimal places, the totals might be corrupted where they were computed using the unrounded price instead of the rounded display.

Option 3 was chosen, so that the precision of the raw data agrees with the precision for individual transactions shown on reports. Given the accuracy of the fuel measuring equipment, the thousandths of a cent was mostly garbage.

Just a small reminder of the hazards of truncation, rounding and significant digits.

Brenton Hoff (behoffski) | Senior Software Engineer | My opinions are mine  
xtbjh@Levels.UniSA.edu.au | AWA Transponder | (and they're weird).

---

### **Re: SunOS SPARC Integer Division Vulnerability**

*Dik T. Winter <dik@cwil.nl>*

*21 Sep 91 01:00:03 GMT*

OK, some sensible information from Barry Margolin <barmar@think.com>:

- > The patch replaces the C runtime library linked into the kernel;
- > we disassembled the old and new versions and compared them (actually, we
- > only disassembled the portion that implements the C integer division
- > operator, because of the description of the bug).

I intended to do that, but never came to doing it, although apparently I only needed to look at the code presented in Version 7 of the Architecture manual on page 183!

- > The change has to do with the action taken when division by 0 is detected.
- > In both cases, it does a "ta T\_DIV0", i.e. signal a division-by-zero trap.

In the Architecture manual it says "te ST\_DIV0", not a big difference.

- > The old code assumed that this instruction would never return; if it did,
- > it fell through to the rest of the code that implements division, and
- > presumably gets some wrong answer. The new code is prepared for the trap
- > instruction to return, and the operator returns 0 in that case.

Yup. In the first case, who are you if you return from the second trap?  
And who are you when you return again?

- > Note that the description of the vulnerability is somewhat misleading. The
- > perpetrator doesn't gain privileges by using division in his own program.
- > He somehow has to get the kernel to try to divide by zero; I suspect the
- > vulnerability is that the kernel then might use the result as in array index
- > into some kernel structure (e.g. the u area).

No, not true. With version 8 of the architecture Sun introduces instructions for multiplication and division. These are on non-version 8 machines trapped

as illegal instructions and emulated in software (since SunOS 4.0?).

> As far as I'm concerned, the fact that the kernel ever even \*tries\* to  
> divide by zero is a bug.

True, but the reasoning is wrong. Why is this code executed in kernel mode? It ought to be executed in user mode. The same holds by the way for a number of fp emulation routines, plus some more. The risk is that people concentrating on getting there emulation code right are also bothered by security issues.

The fix is completely bogus (although it serves as a kludge or hack). When something has to be done to support the user for which kernel mode is not needed, the processor should go in user mode. I think that Sun failed big with its traps on unimplemented instructions. Just try to single step under adb an instruction that adb knows about but as does not; expect a panic.

dik t. winter, cwi, amsterdam, nederland

dik@cwi.nl

---

**✂ Re: Risks of mistreating programmers (Welch, [RISKS-12.36](#))**

*Mr. News <news@rzsun2.informatik.uni-hamburg.de>*

*Thu, 19 Sep 91 09:25:15 +0200*

Well, since probably I am the source of the information, permit me to add my two cents worth. Yes, the above is mostly correct, although a bit scatchy. For more information, see my paper "The Bulgarian and Soviet Virus Factories", published in the proceedings of the First International Virus Bulletin Conference on Computer Viruses, which was held in Jersey, UK, September 12-13. A slight correction of your message - the town mentioned is Sofia (not Sophia) and it is the capital of Bulgaria. :-) The BBS mentioned really exists, it is called Virus eXchange, SysOp is Todor Todorov, and it is indeed specialized in virus exchange and virus discussion between virus writers. I'm really sorry, but this is not illegal in Bulgaria, so we really cannot stop them. :-((

Vesselin Vladimirov Bontchev      Universitaet Hamburg, FB Informatik - AGN  
Bontchev@Informatik.Uni-Hamburg.de    Schlueterstrasse 70, D-2000 Hamburg 13  
New address after October 1, 1991:   Vogt-Koelln-Strasse 30, D-2000, Hamburg 54

---

**✂ Re: Play the lottery via Nintendo ([RISKS-12.27](#))**

*"Mike Cepek, MGI" <cepek@vixvax.mgi.com>*

*Sun, 22 Sep 1991 11:16:23 CDT*

In followup to the article I repeated here recently, George Anderson, director of the Minnesota State Lottery, writes in the Sun 22 Sep 91 Minneapolis [MN] Star Tribune "Letters from readers", (pg 22A):

[...] The play at home test will use Nintendo's control deck, a modem by which the deck communicates to the Lottery computer and a Lottery cartridge. Transactions occur much as they do in

the terminals found at our retailers across the state. The cartridge will not be available through retail outlets. No "children's games" are involved. Only existing Lottery games will be available.

Adults must preregister, predeposit (no credit play) and prove their age. Adults will control a password for limited access. The deck will shut down if incorrect passwords are entered or if the machine is left unattended. Daily play will be limited. Statements will be [mailed].

[...] The control deck has enormous potential for interactive transactions -- it is used in Japan for personal banking and stock transactions. Control Data Corp. and the Lottery believe that this test will demonstrate that the security and controls over player access removes the specter of minors' play, even as it provides the convenience demanded by Lottery players.

Oh, yes, lottery players here in Minnesota are quite near rioting at how inconvenient it is to have to go to the nearest gas station or quick mart to play!

Seriously, I'd like to know more about how the Japanese use it. Security issues must have been adequately addressed for people to be comfortable playing with their money via Nintendo. Or maybe there aren't any hackers in Japan?

---

### ✂ Re: documentation and the obsolete parts problem

<lou@cs.rutgers.edu>  
Sat, 21 Sep 91 23:55:22 EDT

In [RISKS-12.38](#), Stanley (S.T.H.) Chow <SCHOW@bnr.ca.bitnet> comments on the military's "obsolete parts" problem (the difficulty of obtaining obsolete replacement parts for military systems). He says:

>Given the well-known mountains of paper that the Pentagon requires for any  
>hardware, and the many mil-spec's for documenting and testing any and  
>everything, it is quite a surprise to me that anyone should need to reverse  
>engineer anything. [...]  
>Even excellent documentation is useless, Unless you can find it again.

I was peripherally involved in one effort to get around the obsolete parts problem, and my impression is that the problem is NOT in finding the old documents. The problem is that you can't rely on the documents. They are often out of date or incomplete. There is always that one last minute design change to fix the "final" (-) bug, that may well not make its way into the formal documents. The basic problem is that there is no affordable way to check whether the documents are correct, and without checking such documents aren't much more reliable than an untested program.

---

## ✂ Ideas made simple

<frankston!Bob\_Frankston@world.std.com>

21 Sep 1991 23:01 -0400

This is a copy of a letter I just FAXed to Business Week in response to their article that presents object oriented programming as the grand solution to all software problems. This is absurd, but it is hard to blame Business Week by itself when many within the industry espouse such views and some even believe it.

As we've seen in some of the recent articles on representations many of the fundamental difficulties aren't even related to programming as such. As we try to model the real world in our computer systems we are discovering what a messy place it is. But wouldn't it boring otherwise?

I apologize for the tone of this article, the moderator suggested that I be stronger. In appropriate circumstances I would much more forceful but I think this letter represents the limit of what I can explain to a publication like BW. Feel free to send your own comments. The fax number of "Readers Report" (letters to the editor) is 212-512-4464.

To: business week

From: Bob Frankston

Date: (09-21-91 22:49:19)

Subject: Ideas made simple

At the risk of great oversimplification, I'll be extremely brief. In doing so, I appreciate your difficulty in covering complex issues of technology in a small amount of space in a general (albeit business) publication. Your two recent articles, one on user interface and one on software development do a disservice by announcing "solutions" to complex problems.

In your recent article on simplified controls for consumer appliance such as VCRs you gloss over the fact that good (interface) engineering involve more than just limiting capabilities until products become trivial to use. While this is indeed a valid and often appropriate technique, the problem faced by product engineers is presenting the user with access to advanced capabilities in a way that makes them obvious without being trivial.

In a similar vein, the problems of developing software are not suddenly solved by the use of "objects". Like structured programming, modular programming, programmer teams, databases, relation databases, automatic programming (now called programming languages), object-oriented programming is yet another useful tool. But it doesn't magically solve all problems. In fact, some of the capabilities described in the article are more the result of taking advantage of the additional power of today's computer systems than completely new techniques. Many of the traditional programming techniques represent engineering tradeoffs given the limited slack available and not just ignorance. With more powerful systems, more attention can indeed be played to assembling components rather than crafting each one.

But we still have much to learn about what the components should be and how

they can fit together. As you pointed out in this article, to some degree the task is one of finding programming analogues to real world complexity. If we indeed reflect the complexity of the real world, why should it suddenly become simpler when it is modelled in a computer?

In other articles Business Week has explained that "reengineering", or the process of rethinking a system as a whole, is much more effective than naive modelling. In contrast, the Software Made Simple article advocates mimicking existing systems.

I do sympathize with the difficulties of presenting ideas concisely and understandably. In writing this letter I too have had to resort to extreme simplification. The price is a loss of accuracy. But simplifying shouldn't mean misleading the reader by suggesting that we have a grand solution to an intrinsically complex problem.

Personal Categories:

Use Inner Header:

Delivery Priority: High

Delivery Report: Basic

Receipt Report:

Sender phone number: 617-945-9199 (Personal Pager)

Sender fax number: 617-244-1567

Cover Text for Faxes:

Cover Page for Faxes:

---

**✘ CANCEL: Ideas made simple**

<frankston!Bob\_Frankston@world.std.com>

22 Sep 1991 10:55 -0400

You think BW shuts off its FAX machine on weekend or do they just get overwhelmed after a particular stupid cover story?

To: Bob Frankston | EMS: Slate Corporation | MBX: Bob Frankston

cc:

From: MCI Mail Fax Service | EMS: MCI Mail | MBX: POSTMASTER @ mci @ FRANKSTON

Date: 09-22-91 03:10:00 (09-22-91 03:39:37)

Subject: CANCEL: Ideas made simple

Your fax message

To: Readers Report

Destination Fax: 212-512-4464

Date/Time Sent: Sun Sep 22, 1991 3:02 am GMT

Message ID: 24910922030242/0004464426NC4EM

was not delivered.

Date/Time Cancelled: Sun Sep 22, 1991 7:10 am GMT

Delivery Attempts: 12

Cancellation Code: 0015 - Ring no answer

For online assistance type HELP FAX CANCEL or contact MCI Mail Customer Support at 800-444-6245 (U.S. only) or 202-833-8484.

Please retain the information contained in this cancellation when calling for assistance.

---

### Book review for risks

Jack Goldberg <goldberg@csl.sri.com>

Mon, 23 Sep 91 13:48:35 -0700

I found the book "Technological Risk" by H.W. Lewis, W.W. Norton & Co., 1990, to be a very thoughtful and readable introduction to risk assessment. Lewis is a professor of physics at UC Santa Barbara and has chaired numerous government risk assessment committees. The dust cover has high and accurate praise from Hans Mark (former deputy administrator of NASA), W.H. Press (professor of Astronomy and Physics at Harvard) and James Schlesinger (former Secy of Defense and Secy of Energy). The first section, Generalities, talks about the risks and value of life, the measurement, perception, politics, assessment and management of risks, and "The delusion of Conservatism". The second section, Specifics, gives examples from toxic chemicals, chemical carcinogenesis, highway safety, air transportation, ionizing radiation, fossil fuels, nuclear winter and non-ionizing radiation. There is no major discussion of computer risks, but the subject is touched on in discussions of air transportation. Lewis has lots of experience. The book has much wisdom and is free of dogma. It is also a pleasure to read.



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 12: Issue 40**

**Wednesday 25 September 1991**

## Contents

- [Bell V-22 Osprey - correct sensor outvoted](#)  
[John Wodehouse](#)
- [Challenger O-ring Problem heads topics at conference on ethics](#)  
[George Leach](#)
- [People and Public Screens](#)  
[Antony Upward](#)  
[PGN](#)
- [Credit bureaus, heisenbugs, and clerical errors](#)  
[Peter G. Capek](#)
- [Electronic locks at Harvard](#)  
[David A. Holland](#)
- [Bad error handling in Lamborghini Diablo engine management](#)  
[Richard Boylan](#)
- [Denver Hacker Hacks NASA](#)  
[Andy Hawks](#)
- [Re: MSAFP, utilities, and all that](#)  
[Eric Eldred](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ **Bell V-22 Osprey - correct sensor outvoted**

"John Wodehouse" <[w0400@usav01.glaxo.com](mailto:w0400@usav01.glaxo.com)>  
25 Sep 91 09:23:00 EST

Further information about the V-22 crash from Flight International 18-24 September 1991.

"A Bell-Boeing V-22 Osprey tiltrotor is flying again for the first time since the crash of aircraft number five on its first flight in June. Aircraft number three has made at least three flights, after extensive checks by the US Navy (USN).

The USN has also released a brief report on the accident, which reveals that similar faults have been found in two other aircraft.

It says that TWO roll-rate sensors (my capitals), know as vyros, which provide signals to the flight control computer, were reverse-wired. In the triple-redundant system the two faulty units "outvoted" the correct sensor, leading to divergent roll cycles and a crash shortly after take-off.

The report says the cockpit interface unit is connected by a 120-wire plug connector in which the vvro unit uses numbers 59 and 60 - which were reversed. Examination of aircraft one and three revealed that one vvro in each was also reversed.

The number three aircraft flew for 18min on 10 September in a flight cut short by extremely poor visibility. It flew again the next day, and was to complete a third flight on 13 September."

What worries me is that aircraft one and three were obviously flying with one vvro reversed-wired for quite sometime. The triple-redundant system would have outvoted this vvro, but why was no indication given that there was a problem at all. What confidence does that provide for other systems, which depend on voting, if the failure is not reported.

Lord John --- the programming peer

[We have reported on similar cases in RISKS before. For example, see J.E. Brunelle and D.E. Eckhardt, Jr., Fault-Tolerant Software: An Experiment with the SIFT Operating System, Proc. Fifth AIAA Computers in Aerospace Conference, 355-360, 1985, where two programs written by different people to the spec of a correct program had a common flaw, and outvoted the correct program. PGN]

---

## **Challenger O-ring Problem heads topics at conference on ethics**

*George Leach <reggie@pdn.paradyne.com>  
Tue, 24 Sep 91 10:53 EDT*

>From the Tuesday, September 24, 1991 issue of the St Petersburg Times:

"Event explores ethics in business"

An engineer who worked on the Challenger says not "doing the right thing" can have dire consequences, but so can acting ethically.

By John Craddock, Times Staff Writer

TAMPA - When the engineer studying the O-rings on the space shuttle Challenger suspected they might cause a catastrophe, he told his bosses. They listened. Then they made what former Morton Thiokol engineer Roger Boisjoly called "a management decision." That decision launched a tragedy. The O-rings failed, and the Challenger exploded Jan. 28, 1986.

In later statements before a presidential commission and in documents he produced, Boisjoly showed he had tried to do the right thing. But for him, doing the right thing ethically meant the undoing of his professional life. "I

stepped into quicksand....It was the total destruction of myu career," he said.

Discussions - and confessions - about ethical behavior and what it means to professionals, - are the theme of a two-day conference at the University of Tampa. The conference ends today. Titled "Doing the Right Thing: Revolutions in Professional Ethics," the conference Monday attracted a blue-chip panel of ethical experts, as well as politicians, lawyers, and journalists.

Among those speaking Monday morning was Gov. Lawton Chiles. He told the group of about 150 that he doesn't blame the lack of ethical fiber in recent years on "the mindless materialism of the 1980's" creating a "moral vacuum across the land." He said unethical behavior has always been with us. "I'm not sure we can blame it all on the 1980's," said Chiles, who has been involved in politics since the 1950's.

He noted one difference: The lack of surprise when people hear that a judge is taking bribes or other news of the public trust being betrayed. "Our citizens are no longer shocked," he said. That's why political and business leaders must step out and "be willing and able to do the right thing." He then launched into his own campaign to build trust with the people of Florida and cut state spending. [Note: the St Pete Times reported last week that the state's projected revenue will fall short by some 623 million dollars - prompting cuts, including in education - gwI]

Boisjoly, who appeared in an afternoon session, said the anguish he felt from his experience at Morton Thiokol was two-fold. He wondered whether his own protests were strong enough and whether he could have prevented the Challenger tragedy. He also said his company came to view him as a traitor. The public tends to view whistle-blowers as "good guys," he said. But the perception in government and corporate circles is that "we're the bad guys. We're the messengers with bad news."

Other speakers included Manuel Velasquez, director for the Center for Applied Ethics at Santa Clara University in California. He said business ethics are somehow presumed to be separate from the everyday ethical decisions people make. He said people tend to think of business as a poker game with its own rules. But business ethic "are not specialized," he said, and shouldn't be considered outside the normal bounds of fair play.

---

## ✈ People and Public Screens

*KPMG - Antony Upward,IVC <UPWARD.A@applelink.apple.com>  
25 Sep 91 07:34 GMT*

I was recently returning to Paris from Birmingham (UK). Birmingham international airport has just opened a new terminal, including of course, the latest in computerised information systems to keep travellers informed.

It appeared that they no longer have a direct link between the screens being updated with new information (e.g., Flight BA5310 Boarding Gate E, or flight BM540 delayed 30mins), and a public announcement to the same effect. The public announcements seemed to be about 5 minutes after the screens were updated.

My flights gate details were displayed - Gate E. I, and about 100 other passengers, went to gate E, and waited. There were no airline staff present.

After about 5 minutes of 100+ people waiting at Gate E the public address system announced, quite calmly (not indicating that the screens were displaying wrong information), that my flight was boarding at Gate D. \*NO ONE MOVED\*. No one believed the public announcement, even though there were no airline staff at Gate E.

It was only when one of the airline staff at Gate D wondered why none of the passengers had turned up that they came in person to investigate. Of course we were all waiting at Gate E. Only then, when the announcement was made in person, were the information on the screens disbelieved!

It seems, at least on this experience, that a majority of people now 'trust' the information on screens, even when it is directly contradicted by a human announcement, and by circumstantial evidence that the screens are not correct.

Antony Upward, Apple Computer Europe

---

### **✂ Re: People and Public Screens**

*RISKS Forum <risks@csl.sri.com>*

*Wed, 25 Sep 91 15:14:08 PDT*

On my previous trip East I discovered an annoying bug in United's display program. My flight was not listed on the multiscreen DEPARTURES display. After checking back several times, I discovered the problem: whichever flight should appear on the LAST LINE on the FIRST SCREEN of a multiscreen DEPARTURES display was getting truncated. An example of off-by-one programming, probably. I wonder if anyone fixed it yet?

[I thought I had reported this one previously, but I cannot find it in the archives, and it seems too cute and relevant not to include. PGN]

---

### **✂ Credit bureaus, heisenbugs, and clerical errors**

*"Peter G. Capek" <capek@watson.ibm.com>*

*Tue, 24 Sep 91 00:32:15 EDT*

I reported here recently about the effect which might occur to an individual's credit rating as a result of many inquiries by, say, car dealers, where that person was shopping around for a car. The dealers, in order to assess the likelihood that a person might buy a car would request a credit report on the individual, but the effect of repeated such inquiries was to give the impression that the person was overextending himself. ([RISKS-12.20](#))

The Wall Street Journal today (23Sep91) reports on credit bureaus and their difficulties. Specifically relating to the earlier comment is a description given by a headhunter who would obtain, from a candidate's credit bureau report, the names of other firms who had recently requested that report. He could then call the candidate and say, quite accurately, "You're applying to X and Y and Z; why don't you also consider W?" (I believe that the law

regulating this, the 1971 Fair Credit Reporting Act, requires inclusion in the report of the names of all those to whom a copy was sent within the last 2 years; was this requirement intended to let the individual know who had seen the data, or to let the requesters coordinate amongst themselves what credit had been granted, etc?)

The most interesting item in the article, however, is the intriguing lead, in which much of the citizenry of Norwich, Vermont, is abruptly flagged as bad credit risks by TRW. The problem was ultimately tracked down to an alarmingly simple error: A person working part time (for a similar, but not apparently related company) at obtaining public records and feeding them back to the credit bureaus had been asked to obtain the list of Norwich's delinquent taxpayers. She mistakenly got the list of tax receipts and carefully reported that some 1400 residents -- in a town of 3100 -- were delinquent. It took nearly three weeks to clear up; half the delay was simply in getting TRW to return repeated phone calls. [It seems as though a reasonableness check on the (size of the) delinquent list might have averted the problem.]

But the article goes on to shed some light on what may be the motivations of the credit agencies: their customers, banks and stores, are anxious to obtain reports with the largest amount of negative data, thinking that it has the effect of maximizing their probability of detecting a bad risk. Since the bureaus are paid by the organizations to whom they provide the reports, and not by those whom the reports describe, one is led to speculate on their motivation.

Risks? I think the effect of the requirement to record and report the names of those receiving the report may be seen here to have boomeranged. Perhaps that problem wouldn't arise if those names were recorded, but only reported to the individual. The lesson here may simply be that we need to be as conscientious in assessing the risks of our solutions, as we are in evaluating the problems they address.

Peter G. Capek

---

### **Electronic locks at Harvard**

*<dholland@husc.harvard.edu>*

*Tue, 24 Sep 91 11:50:11 EDT*

>From the Harvard Independent, Sept. 19, 1991, pg. 4:

#### The Key to Security

Computerized ID cards are the wave of the future, but for residents of the three Union dormitories - Greenough, Hurlbut, and Pennypacker - time seems to be moving faster than in other parts of the University. The Harvard University Police Department (HUPD) has replaced the standard entryway keys for each of these dorms with computerized, credit-card-like key cards. According to HUPD chief Paul Johnson, the cards prevent unauthorized persons from gaining access to the dorms, enable the police department to track the use of each key card by computer, and prevent people from jimmying locks. "It's state of the art," said Johnson. Union dorm residents feel more secure with the improved locks. Said

Pennypacker resident Missy Francis '95, "Ninety percent of the upperclassmen have skeleton keys to the Yard, so this way no one can get into our dorms." If all goes as planned, other dorms will be wired by the end of the year.

----

Now, some of the risks here are obvious: tracking the usage of each key, for example. I am sure RISKS readers are familiar with the implications of that. Worse, the article implies that the police are actively aware of the possibility and may be pursuing it directly. While I have nothing against the Harvard police, I nevertheless don't see this form of surveillance as a good thing.

Of course, the fundamental problem is that skeleton keys to all the dorms in Harvard Yard are readily available to anybody who wants one and has some vague idea where to go. This is not a new risk, of course, but I have severe doubts that throwing technology at the problem will make it go away. There must be card-keys somewhere that will open all the locks in question; the maintenance staff needs them. It is only a matter of time before they start circulating just as freely as any other key. I haven't seen any of these card-keys yet myself, but it strikes me as highly unlikely that they are not forgeable, and even more unlikely that (as the article claims) the locks can't be jimmied.

And none of this even begins to take into account the risks of failure - power failure, for example, or electronic interference, or any of the other things that electronic devices are subject to in the real world.

- David A. Holland      dholland@husc.harvard.edu

---

## ✂ bad error handling in Lamborghini Diablo engine management

<Richard\_Boylan@vos.stratus.com>

Wed, 25 Sep 91 17:14 EDT

This is excerpted (without permission) from an article in the September 1991 issue of CAR, a British magazine. In the cover story, the writer is driving one of the first Lamborghini Diablo automobiles from the factory back to England:

"Then, on the outskirts of Annecy, calamity. The power drops off suddenly, there's a soft, metallic buzz, a muffled bang, and a much louder, rattling clatter. The 'right side engine' warning light comes on. Uh-oh, time to coast over to the hard shoulder.

"Tentatively, we raise the engine cover, lean over the wide wings, and peer in. The right-hand exhaust pipe is glowing like the fires of Hades. The aluminium heat shield surrounding it in the bay has melted (aluminium melts at 1000degC), and molten blobs trace a glinting trail of our move across the carriageway.

. . .

"Swiss Air takes us back to the Diablo a few days later. Factory troubleshooters have diagnosed and fixed the problem. There are two engine-management systems, which each look after a bank of

six cylinders. If there's trouble on one side, you're still left with a straight six to get you home. Because a wire had fallen off one of the Lambda probes for the catalytic converter, the right-hand side of our engine was closed down by the chip--hence the power loss. But it seems the fuel wasn't cut off at the same time, and as it reached the exhaust it ignited inside the pipe."

The moral of this is that no matter how critical a piece of code is, the correctness of its error-processing paths is even more critical. It's ironic that in an attempt to provide fault-tolerance, the designers of the Diablo engine-management system actually increased risk. If the engine had simply shut down entirely when the first fault occurred, it would have undoubtedly shut down the fuel-delivery system as well. But by attempting to keep the engine running in a degraded mode, they allowed a potentially explosive situation to develop.

---

## ✈ Denver Hacker Hacks NASA

Andy Hawks <ahawks@isis.cs.du.edu>

Wed, 25 Sep 91 15:33:05 MDT

The Denver Post, Denver & The West section p. 1 9/25/91

NASA vs. hobbyist

Computer whiz accused of illegal access, mischief

By. Peter G. Chronis  
Denver Post staff writer

An Aurora computer hobbyist who allegedly used a personal computer and his home phone to penetrate NASA computers hacked off Uncle Sam enough to be indicted on seven federal counts yesterday.

Richard G. Wittman, 24, the alleged "hacker," was accused of two felonies, including gaining unauthorized access to NASA computers to alter, damage, or destroy information, and five misdemeanor counts of interfering with the government's operation of the computers.

Wittman allegedly got into the NASA system on March 7, June 11, June 19, June 28, July 25, July 30, and Aug. 2, 1990.

Bob Pence, FBI chief in Denver, said Wittman used a personal computer in his home and gained access to the NASA systems over telephone lines.

The investigation, which took more than a year, concluded that Wittman accessed the NASA computer system and agency computers at the Marshall Space flight Center in Huntsville, Ala., and the Goddard Space Flight Center in Greenbelt, Md.

The NASA computers are linked to a system called Telenet, which allows

qualified people to access government data bases. A user name and password are required to reach the NASA computers.

Federal sources declined to reveal more information because the complex case involves "sensitive material."

Wittman, a high-school graduate, apparently hadn't worked in the computer industry and held a series of odd jobs.

The felony counts against him each carry a possible five-year prison term and \$250,000 fine.

[I suppose the Denver authorities locked up his PC to prevent him from using it. They must have used a Denver Boot Load. PGN]

[For our out-of-country users, a Denver Boot is a fiendish device that police attach to a wheel to prevent you from driving your car until you have paid up all outstanding fines. Of course, more fines accumulate unless you pay immediately.]

---

### **✉ Re: MSAFP, utilities, and all that**

*Eric Eldred <eldred@apollo.com>  
Wed, 25 Sep 91 14:36:43 EDT*

Do we really need any more discussion of medical statistics and cost/benefit analysis of tests? Yes, because after all the verbiage here I'm afraid more people are more confused than enlightened.

Mark Fulk has pointed out the importance in decision analysis of assessing relevant utilities, especially those of and by the humans affected by the risk. He refers to Kahneman and Tversky (apparently as those who note the subjectivity and often seeming irrationality of individuals' risk assessments and utility analysis). It seems pretty clear now that one cannot discuss a test such as the MSAFP in isolation from utility analysis. Not all physicians, and certainly patients, are yet aware that this is true, however, so it could stand some repeating.

The implication of what Mr Fulk notes is also that perhaps a test should not even be done without some counseling and interpretation to those affected, and an entire therapeutic context. For example, if an amniocentesis result predicts a certain disease state of the fetus, would an abortion be done anyway? Too often physicians do tests defensively, because they would be accused of malpractice if they didn't give the "standard" treatment to all. But that is not treating patients as individuals.

For example, in a separate discussion with Jeremy Grodberg, I pointed out that utility analysis of a particular vaccine choice should involve more than just the risk of a disease or reaction to the vaccinated individual. As a good example, the US CDC (Center for Disease Control) decided after much debate (part of which was actually filmed and shown on a PBS program) that live polio vaccine should be used instead of killed virus vaccine. The latter is possibly

much safer for individuals, and prevents the occasional transmitting of the virus to unprotected others in close contact (some have died, their families sued the govt, and they lost). But the live virus has a possible extra effect in increasing the resistance of the population taken as a whole (and hence the CDC chose it).

Thus the risk to the individual is one thing; the risk to the entire population is another. Both factors must be taken into account when issuing a vaccine. It is quite possible, paradoxically, that the risk to an individual could be increased by a choice of one vaccine over another. (Here I'm not going to get into discussion of the risks of the Salk vaccine, which was hastily withdrawn at an earlier time when the manufacturing of it went awry and created false perceptions of its risks.)

My argument with the CDC is that they have not yet apparently made it clear that those performing the vaccination should communicate to patients (or parents) that the killed virus vaccine could be safer and would be available if the patient decided for it rather than the live virus vaccine. In other countries, the decisions have been made differently.

I believe this is an important point. Those exposed to risks should be able to choose responses most intelligently with full information and should not always have decisions made for them by supposedly more knowledgeable and intelligent engineers, MDs or politicians. Often, with secrecy, the necessary uncertainty of real life, or the fog of war as factors, those decisions prove quite poor ones and are hard to reverse. Generally, even rational people are willing to accept certain risks voluntarily they object to when imposed by a seeming outside force. Many teenage smokers don't put much on the chance of getting lung cancer; 40 years later, they are willing to pay a lot more money than you would predict, just in order to live a little longer, once they do have cancer. We should discuss policy openly.

In the interpretation of such tests, it should also be emphasized that--also perhaps paradoxically--the prior probability of events makes a big difference in what to make of the test result. If you redraw Jon Krueger's chart of the four signal/noise possible outcomes --but place numbers in the boxes instead of the yes/no text, and then repeat, varying the incidence of the condition (and thus the numbers in the boxes), you will confirm the basis of the argument against the MMPI. A test that has a high predictive value in a population with a high prevalence of a condition may not be any good at all (less than, say, 50% predictive value of a positive result) should the prevalence be greatly decreased--even if the "accuracy" of the test stays the same. (Thus, I believe pre-employment urine drug tests for programmers are counterproductive.)

Each test should be examined experimentally with two critical measures reported: the "specificity" and the "sensitivity", or essentially what lead to what we could call "false positives" and "false negatives". Without those measures reported, and without a prior estimate of the prevalence of a condition in the population tested, it is not really possible to say what to make of a specific test result. Hence, counseling and the wise therapeutic context, by which results can be verified and acted on correctly.

The other interesting implication of the discussion here has been the reference to the utility put on threshold values, or on the importance of false positives

or false negatives. We should realize that a medical test for a condition that could be fatal but might be prevented, and for which a false positive test result would not lead to needless suffering, anxiety, and so on, could be one with a larger number of false positives (because it is intended as a screen to be sure not to miss anybody with the condition), while one for which there might not be treatment, and for which a positive result might lead to severe consequences (say, MS, or an HIV test before AZT), might be one that one would have to be sure would not have a lot of false positives.

Consequently, the threshold values of such tests should be selected so as to magnify the desired results and minimize the undesired consequences. It is quite likely that interpretation of some tests should be withheld until confirmatory results of other tests with different utility values. However, obviously the chances of false results increases with the number of tests, so testing should be done with their limits in mind. It seems to be irrational to mandate reliance solely on such tests as HIV antibodies in arbitrary populations with unknown or low disease incidence, given what we now know about testing.

For those who want to look up all this, I'm sorry I don't have the exact references in hand. One book that did initiate a lot of talk on the subject is quite lucid: "Beyond Normality" by Galen and Gambino (I think it was published by Little, Brown, in about 1976). Later work by the Tufts clinical decision analysis group was published in the New England Journal of Medicine in the late '70s and early '80s, introducing the concept of the variability of patient assessment of outcome utility. I think the issues are still important today, since even the experts can make decisions poorly from time to time, and the ones who do make them correctly can't always explain the proper techniques to the rest of us, and so we end up re-arguing the same points.

Eric Eldred [eldred@apollo.HP.COM](mailto:eldred@apollo.HP.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 12: Issue 41

Saturday 28 September 1991

## Contents

- [Ada Code Formatters pretty dangerous](#)  
[Richard G. Hash](#)
- [Risks of computerized typesetting](#)  
[Simson Garfinkel](#)
- [Galileo's Revenge - Junk Science in the Courtroom](#)  
[Martin Minow](#)
- [Readings in Judgement and Decision Making](#)  
[Doug Jensen](#)
- [Nintendo Lottery Is For Real](#)  
[Jim Huggins](#)
- [Radio Shack computerized mailing list problem](#)  
[Joseph Poirier](#)
- [Re: Security in software distribution](#)  
[Kilgallen](#)
- [Re: Bell V-22 Osprey](#)  
[John Wodehouse](#)  
[A. Padgett Peterson](#)
- [Have you tested your machine lately?](#)  
[K. M. Sandberg](#)
- [Electronic Locks in Universities](#)  
[Martin Ewing](#)  
[Jim Huggins](#)  
[Dean Rubine](#)  
[Kraig Meyer](#)  
[Mike Carleton](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✂ Ada Code Formatters pretty dangerous

*Richard G. Hash <[rgh@shell.com](mailto:rgh@shell.com)>  
Fri, 27 Sep 91 15:10:23 GMT*

The Rational R1000 is a machine designed especially for Ada development, It has a very powerful APSE, including a really nice (?) formatter. You can type the

entire program in, hit the 'format' key and wham-bang, the entire program is beautifully formatted, according to your configuration rules. It's pretty much the "Rolls Royce" of Ada environments.

Unfortunately it has a really nasty habit:

Meant to type:

```
if Kind_Of_Test_Well (Well_Coordinates) /= Dry_Hole then
  Drill_Oil_Well (Amount_To_Spend => 4_000_000_000);
end if;
```

But if you have been LaTeX'ing or regexp'ing a lot lately, and have backslash on the brain, you might actually type:

```
if Kind_Of_Test_Well (Well_Coordinates) \= Dry_Hole then
  Drill_Oil_Well (Amount_To_Spend => 4_000_000_000);
end if;
```

and the Rational formatter silently turns it into

```
if Kind_Of_Test_Well (Well_Coordinates) = Dry_Hole then
  Drill_Oil_Well (Amount_To_Spend => 4_000_000_000);
end if;
```

Turning a syntactically incorrect, but semantically well-meaning program into a syntactically correct but semantically wrong program without even a warning is quite a risk!! In fact, when I finally found the reason that nothing was working right I assumed that I had just made a typo - (which I had), so I fixed it, hit format, and then "Whooooa!!". Everything does exactly opposite what you expect...

Some tools are just too smart(?) for their own good!

Richard G. Hash, Shell Bellaire Research Center, 713-245-7311 rgh@shell.uucp  
...!{sun,bcm,rice,psuvax1,decwrl,cs.utexas.edu}!shell!rgh

[WWN HEADLINE: Ada in 4-Mat COLLAPSE of Back Slashes, Hits Well, No Field. PGN]

---

## ✂ Risks of computerized typesetting

<simsong@nextworld.com>  
Fri, 27 Sep 91 09:58:26 PDT

In June 1991, I published the book Practical UNIX Security with Gene Spafford. After the book came back from the publisher, we discovered to our horror that all of the backquotes (`) in the UNIX shell-scripts had mysteriously been changed to forward quotes ('). Of course, this breaks all of the UNIX shell-scripts.

Both Gene, myself and the book's editor were greatly confused, because we had seen backquotes in all of the galleys and, indeed, in the semi-final PostScript

files that we had seen, backquotes were specified.

We thought that somebody at the publishing house had run some sort of filter over the text files (we used troff as our typesetting language) and changed the quotes around. But nobody would own up to the deed, and when we checked the files, they didn't appear to have been modified. So the next thing to suspect was the troff programs themselves; ORA, the publisher, had just changed over to a new version. Perhaps that was to blame.

We printed new proofs of the book and discovered, much to our confusion, that the problem was gone: all of the backquotes properly printed....

Three months pass and, thanks to a number of very kind reviews, ORA finds that they need to do a second printing of Practical UNIX Security. This time we carefully look at both the galleys and the PostScript files themselves. All of the backquotes are as they should be. We ship the files off to the printer, which will take the PostScript, typeset to film, burn plates, and make the books.

In the words of the editor, Lightning Strikes Twice in the Same Place. Same problem: all of the backquotes print as forward quotes.

It turns out that the printer has a slightly non-standard version of the PostScript courier font. In the spot where they should have a backquote, they have a forward quote instead.

"The nice thing about standards is that there are so many of them to choose from."

---

### **✂ Galileo's Revenge - Junk Science in the Courtroom**

*Martin Minow at Shiggy 27-Sep-1991 1629 <minow@ranger.enet.dec.com>  
Fri, 27 Sep 91 13:27:40 PDT*

>From a book review by Louise Kennedy (Globe Staff) in the Boston Globe, Sep 27, 1991 (shrunk by about 50%: I didn't mark interpolations and elisions, but the tone of the review and choice of adjectives are Kennedy's)

Galileo's Revenge: Junk Science in the Courtroom  
by Peter W. Huber, Basic Books, 274 pp. \$23

Everybody knows about the Audis that accelerate, or Bendectin, the drug for morning sickness that causes birth defects, or "chemically induced AIDS." Except, the these things that everybody knows simply aren't so.

Why do we think otherwise? Because lawyers managed to persuade juries that their clients had been harmed. With the PR campaign of one plaintiff's lawyer, the Audis even made it onto "60 Minutes."

All these cases, and the several others Huber studies in this ferocious and highly readable book, are the product of what he calls "junk science." The plaintiffs' claims rely on the testimony of "expert witnesses," who, as Huber

documents with devastating clarity, often have no real expertise in the relevant specialty.

A chief proponent of "chemically induced AIDS" has a medical degree but hasn't practiced for 20 years; he has failed board exams in internal medicine five times; he heads a firm that specializes in ... expert testimony. In short, he's expert only at being an expert -- and his "research," Huber says, is as shoddy as you would expect.

Why would any judge let him in a courtroom? The abandonment of traditional rules requiring "experts" to be generally recognized in the relevant scientific community allows unscrupulous trial lawyers to put almost any crackpot with a degree on the witness stand.

In short, Huber -- who holds degrees in law and mechanical engineering and is a columnist for Forbes magazine -- paints a disturbing picture of the modern legal system, and his passionate argument for a return to "the rule of fact" is eloquent and compelling. But there are moments when his faith in science seems as risky as the superstitions and pseudo-scientific fads he so effectively debunks: even good scientists can be wrong.

Huber also weakens his case by slipping into easy sarcasm -- a temptation that's understandable, given the chicanery of his villains, but nonetheless distracting. But Huber is a lively enough writer (and his cited outrages are extreme enough) to keep you reading -- and, more importantly, thinking about the junk in the courtrooms and how to clear it out.

Martin Minow

---

### **✦ Readings in Judgement and Decision Making**

*Doug <xanax!edj@ARCHONS22.ARCHONS.CS.CMU.EDU>  
Fri, 27 Sep 91 09:46:38 EDT*

As a relatively recent reader of this forum, I don't know if these two books have been mentioned before; if so, I'm sure Peter will filter this message out. My favorite cognitive science references for judgment and decision making with uncertain information are the two collections: Judgment and Decision Making, Arkes and Hammond (Eds.), and Judgment Under Uncertainty: Heuristics and Biases, Kahneman and Tversky (Eds.), both by Cambridge University Press.

E. Douglas Jensen, Digital Equipment Corp., jensen@helix.dec.com

---

### **✦ Nintendo Lottery Is For Real**

*<huggins@zip.eecs.umich.edu>  
Fri, 27 Sep 91 19:03:47 EDT*

George Anderson, director of the Minnesota State Lottery, was interviewed today on NPR's All Things Considered about the new system for playing the lottery which Minnesota will be implementing next year. As mentioned previously in

RISKS, Minnesotans with a Nintendo will be able to play the lottery using a home Nintendo unit outfitted with special software and a modem.

Details that may not have appeared previously: users will be required to deposit money in advance (no playing on credit) and will receive a PIN to verify their identity when playing the lottery. Any winnings will be issued by check to the owner of the PID, in an attempt (according to Anderson) to minimize possibly security risks for stolen PIN numbers. No other mention of security measures (besides the PIN) was mentioned.

While this may remove the financial motive from stealing a PIN, since a thief can't collect on winnings from a stolen PIN, it does nothing to protect against the malicious person who just wants to spend someone else's money...

Jim Huggins, Univ. of Michigan (huggins@eecs.umich.edu)

---

### **Radio Shack computerized mailing list problem**

*<ach@mentor.cc.purdue.edu>*

*Fri, 27 Sep 91 21:27:38 -0500*

I'm not sure if this has been mentioned in the past, but it seemed interesting enough to send to comp.risks.

I went to Radio Shack the other day. When I tried to pay for my purchases, the cashier asked for the last four digits of my phone number and my name and address. Evidently this is for their mailing lists. I knew I was on the mailing list, and I tire of having to give out all this information every time I buy some bauble at Radio Shack, so I refused to give the employee such information.

Apparently, however, the Radio Shack computer cannot deal with someone saying "no" to them. Every transaction must have a name and address. This information is printed on your receipt. So the employee typed in a random phone number and that random person's name, address and phone number appeared on my receipt.

I'm glad Radio Shack doesn't ask for Social Security numbers!

I mentioned this to friends and found out that employees at one Radio Shack nearby routinely "log" local businesses' phone numbers when customers don't want to give their name and address. They say they "round-robin" these logs so one business doesn't get logged with a lot of transactions.

Currently, these transactions (hopefully!) are only used for their mailing list -- not for billing purposes. But it certainly seemed to me as a RISK waiting to happen. Plus, does Radio Shack exchange this information? My receipt was of a person whose last four phone number digits were "0000". I expect it looks like he buys a lot at Radio Shack.

Can Radio Shack employees bypass this mandatory information need? Is it that the software itself cannot handle an unknown customer, or do the Radio Shack employees avoid using this bypass (bad user interface, for example)? Did the programmers of the software purposely put this in in an effort to try to force employees to get customers on the mailing list?

I find it hard to believe that such a simple case of an unknown customer cannot be handled by Radio Shack's systems.

Joseph Poirier

Internet: jrp@cs.purdue.edu UUCP: ...!{ backbone }!purdue!jrp

---

**✉ re: Security in software distribution (Morris, [RISKS-12.32](#))**

<Kilgallen@DOCKMASTER.NCSC.MIL>

Fri, 27 Sep 91 23:01 EDT

Last year I talked with someone who said he had been a target of such an attack aimed at a VAX/VMS system. Although I was not in a location to examine evidence, there was no reason why the individual should make up such a tale to tell me. His story is as follows:

The target and the perpetrator were both in California, and the perpetrator went to the trouble to have the package mailed by a confederate in Massachusetts (enhancing the impression that it came from DEC.)

The cover letter included in the package said "important VMS security patch - install immediately". In fact, the software was a recycled cracker modification to introduce a trap door.

The bottom line was that the attack did not succeed, because the target merely put the package into a pile of other software from DEC which had not yet been installed.

---

**✉ Re: Bell V-22 Osprey (Wodehouse, [RISKS-12.41](#))**

"John Wodehouse" <w0400@usav01.glaxo.com>

28 Sep 91 12:12:00 EST

My feeling about triple-redundancy and voting are worried, not so much because two bad units outvoted the good one in this case, but that the systems design allowed two aircraft with one bad unit to continue to fly for sometime without alerting anyone to the problem.

If the same sort of system allowed an airliner to fly with only two out of three unit working correctly and a further failure then occurred over mid-Atlantic, I think passengers might give up flying. From the USN report, we are lead to believe that this problem existed from aircraft build time and thus the whole testing of the triple-redundant system must thus be flawed. I just cannot see how a system can be built that does not allow for the check to see if all units are working correctly and providing the correct data before take-off. The facts show that I am not correct here.

Lord John - the programming peer

**✂ Re: V-22 Osprey (Wodehouse, [RISKS-12.41](#))**

*A. Padgett Peterson <padgett%tccslr.dnet@uvs1.orl.mmc.com>*

*Thu, 26 Sep 91 08:25:34 -0400*

Not having the wiring diagram, second-guessing is dangerous but consider the case in which the triple sensors are not "reverse-wired" but cross-wired (e.g. sensor 2 is connected to input 1 & vs). In this case, with "all good" everything is fine. If 3 fails all is ok. However if 1 or 2 fails, the other is reported failed, voted out, and an immediate mismatch occurs between 3 and the failed sensor (still considered good). The flight control must now rely on some other (and often lessor) means of selection (usu a calculated value or range checker) of the proper value.

This is an inherent problem in any flight-critical design that relies on detection of "first-fail". In this case the failed sensor was evidently a "second-fail" condition but thought "first-fail" & is a very real concern.

Another concern not mentioned (and again merely hypothesised) is that from the text, it would appear that at least two of the critical triplex sensor signals are routed through a single connector, not a good idea since connectors are one of the major failure areas. (there are some other equally dangerous possibilities that also have to be considered, i.e., if the signals have redundant routing shouldn't that have caused a mismatch).

On the quadruplex AFTI-F16, one of our concerns that influenced a number of routing decisions was the number of simultaneous faults that could be caused by one 20mm cannon shell.

Of course, it is all too easy to second guess a design team after the fact, on first flight everyone is crossing their fingers, anyone who isn't shouldn't be there.

Padgett

---

**✂ Have you tested your machine lately?**

*K. M. Sandberg <kemasa@ghost.hac.com>*

*26 Sep 91 15:48:20 GMT*

We have an Alliant fx/800 computer which uses the i860 processor and they made a decision, which I think was wrong, that such things as divide by zero should not be a fatal error by default. You can change this if you want to by making a call in your program. By default no action is taken on many of the exceptions. Note that also by default you have to do this for each program, not for the machine (we should be receiving the patches to make the default values what *\*we\** consider to be more reasonable).

How many people try *\*ALL\** operations that should fail on a machine before using it to get some work done? It is documented, but who has the time to read all of the documentation? This is not to say that the users do not bear some responsibility in testing the machine to make sure that it correctly handles error cases, but I think that companies selling computers should think about

what the users expect the machine to do and make that the default \*if\* it is reasonable. I do not know the exact reasons for this decision, it might have to do with performance, but who cares if the machine is fast if the answers are wrong?

Also if you notice on the output that the results are different depending on if you optimize or not.

Kemasa.

Script started on Thu Sep 26 08:24:24 1991

```
% cat t1.c
```

```
#include <stdio.h>
```

```
main()
```

```
{
```

```
int i = 0;
```

```
int j = 10;
```

```
int k = 0;
```

```
int ir = 0;
```

```
float f = 10;
```

```
float g = 0;
```

```
float fr = 0;
```

```
for (i = 0 ; i < 20 ; i++) {
```

```
    printf("i: %3d j: %d k: %d ir: %d f: %f g: %f fr: %f\n",i,j,k,ir,f,g,fr);
```

```
    fflush(stdout);
```

```
    ir = j / k;
```

```
    fr = f / g;
```

```
    printf("    j: %d k: %d ir: %d f: %f g: %f fr: %f\n",j,k,ir,f,g,fr);
```

```
    fflush(stdout);
```

```
    j--;
```

```
    f--;
```

```
}
```

```
}
```

```
% cc -g -o t1 t1.c
```

```
% t1
```

```
i: 0 j: 10 k: 0 ir: 0 f: 10.000000 g: 0.000000 fr: 0.000000
```

```
    j: 10 k: 0 ir: -1 f: 10.000000 g: 0.000000 fr: nan
```

```
i: 1 j: 9 k: 0 ir: -1 f: 9.000000 g: 0.000000 fr: nan
```

```
    j: 9 k: 0 ir: -1 f: 9.000000 g: 0.000000 fr: nan
```

```
    [...]
```

```
i: 10 j: 0 k: 0 ir: -1 f: 0.000000 g: 0.000000 fr: nan
```

```
    j: 0 k: 0 ir: -1 f: 0.000000 g: 0.000000 fr: nan
```

```
i: 11 j: -1 k: 0 ir: -1 f: -1.000000 g: 0.000000 fr: nan
```

```
    j: -1 k: 0 ir: -1 f: -1.000000 g: 0.000000 fr: nan
```

```
    [...]
```

```
i: 19 j: -9 k: 0 ir: -1 f: -9.000000 g: 0.000000 fr: nan
```

```
    j: -9 k: 0 ir: -1 f: -9.000000 g: 0.000000 fr: nan
```

```
% cc -O -o t1 -uniproc t1.c
```

```
% t1
```

```
i: 0 j: 10 k: 0 ir: 0 f: 10.000000 g: 0.000000 fr: 0.000000
```

```
    j: 10 k: 0 ir: 0 f: 10.000000 g: 0.000000 fr: +Infinity
```

```
i: 1 j: 9 k: 0 ir: 0 f: 9.000000 g: 0.000000 fr: +Infinity
```

```
    j: 9 k: 0 ir: 0 f: 9.000000 g: 0.000000 fr: +Infinity
```

```
[...]  
i: 9 j: 1 k: 0 ir: 0 f: 1.000000 g: 0.000000 fr: +Infinity  
   j: 1 k: 0 ir: 0 f: 1.000000 g: 0.000000 fr: +Infinity  
i: 10 j: 0 k: 0 ir: 0 f: 0.000000 g: 0.000000 fr: +Infinity  
   j: 0 k: 0 ir: -1 f: 0.000000 g: 0.000000 fr: nan  
i: 11 j: -1 k: 0 ir: -1 f: -1.000000 g: 0.000000 fr: nan  
   j: -1 k: 0 ir: 0 f: -1.000000 g: 0.000000 fr: -Infinity  
[...]  
i: 19 j: -9 k: 0 ir: 0 f: -9.000000 g: 0.000000 fr: -Infinity  
   j: -9 k: 0 ir: 0 f: -9.000000 g: 0.000000 fr: -Infinity  
% exit  
%  
script done on Thu Sep 26 08:25:47 1991
```

The best defense is insanity.

[Foreshortened [...] for your reading pleasure by PGN.]

---

## ✂ Electronic Locks in Universities

Martin Ewing <ewing-martin@CS.YALE.EDU>  
Wed, 25 Sep 91 22:52:22 EDT

[Moderator's note: This and the following messages are slipping through. There are some good general points. But this is probably (more than) enough on the topic, so let me not encourage a barrage of spinoffs. PGN]

David Holland's story on Harvard's new e-lock system, ([RISKS-12.40](#)) struck a chord. I can share a few experiences with systems at Yale. (The University is currently implementing a "college" [dorm] key system which is different from the one I will discuss.)

We control access to some of our student computing areas by means of the Yale ID card, which has a bar-code cleverly hidden behind a visually opaque/infrared transparent band that looks just like a magnetic credit card strip. The codes are not obvious, and I believe would be relatively hard to forge. (A screwdriver or hammer taken to the door would be a lot easier for your typical perpetrator.) I don't believe card forgery or duplication is a problem for the more advanced card systems. A lost card can be invalidated and a new one assigned with a new tag digit. There is also no way for the finder of a card to know what privileges are associated with it. (Except probably the right to check out library books, but that's not my problem!) Keep in mind, the typical risk we are protecting against is the one-time major intrusion.

We have observed some of problems that David worries about. There was an immediate protest when it became known that we log key accesses. Students were ultimately convinced that we would not routinely examine these files to see who was doing his homework, etc. We have had to consult the files on two occasions of vandalism and theft, however. Having the records in these cases was surprisingly unhelpful. First of all, the police don't seem to have a clue (PGN - forgive) what to do with electronic records like this. Secondly, evidence of room access is pretty weak when it comes to establishing who did

what and when. (Students commonly enter two at a time, or let others in.) At best, I think such evidence will be circumstantial.

A key problem has been administrative, keeping track of a large and fluctuating student population. The electronic system is better than the old scheme of physical keys (or non-serialized cardkeys), which required cash deposits, but one of our secretaries keeps very busy at the beginning of terms. Inevitably, somebody's registration is wrong, or their card was manufactured out of tolerance. (The bar codes are applied by hand before the card is laminated.) It is very important to have good database programming and production controls. (Currently, our PC software takes the whole system off-line when it's "re-orged" to include a new ID.)

On a nostalgic note, how many people remember the MIT student IDs of the late 60s/early 70s? These had your ID number (SSN) punched as a Hollerith code right through the plastic. Not too tricky to forge, I'd say. Were the codes ever used?

Martin Ewing, Yale Science & Engineering Computing Facility, Ewing@yale.edu

---

### **Electronic locks at Harvard**

<huggins@zip.eecs.umich.edu>

Wed, 25 Sep 91 23:18:21 EDT

Though I'm not familiar with the Harvard Yard layout, I find it somewhat amusing to think that computer-card locks will improve security at Harvard dormitories. Having lived in dorms and co-operative houses for the last 6 years, I can testify that the biggest causes of unauthorized entry for group housing aren't the possession of keys by non-residents, but doors propped open, doors with broken locks (usually broken by students who lost their door key and didn't want to call security to gain entrance), and good-natured people who let anybody in who knocks on the door. None of these things will change by installing computerized locks.

The idea itself isn't necessarily that bad -- I worked for a summer at IBM in Rochester, MN, where they used a security card system for employees to gain entrance to the buildings. The reason the system worked there, however, was that everyone agreed (was ordered?) to not only use the system, but to deny entry to anyone who didn't have a valid computer card. Just about everyone had a story or two about leaving their ID card at home and having to get a temporary card from security, having their card fouled up by a strong magnetic field, and so on. But the system worked the vast majority of the time, mostly because people agreed to follow it.

The moral to the story is an old one: treating the symptoms of the disease instead of the cause doesn't cure the patient.

Jim Huggins, Univ. of Michigan (huggins@eecs.umich.edu)



## Re: Electronic locks at Harvard

Dean Rubine <dandb+@andrew.cmu.edu>

Thu, 26 Sep 1991 18:43:19 -0400 (EDT)

I work at the Information Technology Center, a 100% IBM supported research lab at Carnegie Mellon University. There are badge readers and electronic locks on all the entry doors. Last week a power glitch damaged the computer that runs the locks (at around 6am) and as a result no one was able to enter the facility that morning. Even campus police was locked out. It was necessary to pull the building fire alarm, which apparently releases the electronic locks.

Presumably if that didn't work, the next attempt would have been an ax to the door or some bricks through the window. So, as we consider the risks of too many people having working keys, let us not forget the risk of no one at all having working keys.

One nice feature of the system is that when a badge is reported lost or stolen, it is invalidated and a replacement is issued. Using the missing badge causes alarms to go off.

Several days after the incident, an undergraduate employee told me of an ingenious way to get into the facility without a badge. So much for security.

Dean Rubine / CMU ITC / Rubine@andrew.cmu.edu

---

## ✂ Electronic locks at Harvard

<kmeyer@aero.org>

Thu, 26 Sep 91 15:58:30 PDT

In [RISKS-12.40](#), David A. Holland (dholland@husc.harvard.edu) quoted a Harvard Independent article describing how Harvard's dorms were being wired with card-key systems.

Nearly all of the university-owned apartments and residence halls at USC have had these for several years now, and my understanding is that Columbia has had them even longer. The card key is simple: it is merely the student ID card with a magnetic strip on the back, similar to those used by residence hall dining for a number of years now.

By each door, there is a card reader that controls the door lock: on some doors, there is actually a solenoid-controlled latch; on others there is a very strong magnet that literally keeps the door stuck closed. To enter, you swipe the card through the card reader, to exit, there is a touch-sensitive pad on the door that unlocks the lock electronically. The card readers are connected via a network, and periodically a centralized computer downloads each card reader with a list of cards that are valid for that building.

This system has some real advantages, namely that if an individual student leaves the university or loses a card, that card is taken out of the database and can no longer be used for building access. Some cards, such as those issued for on-campus conferences, are valid only on the days of the conference

and then become deactivated.

The risks of this system have been reported at great length in the Daily Trojan over the last two years and have nothing to do with lock jimmying or card duplication (not many college students know how to duplicate magnetic strips). The first risk is that the magnetic strips on the cards become unreadable; these cards are swiped through readers 2 or 3 times a day for entry, plus another 2-3 times/day if the student is on a meal plan. USC security also claims that keeping the card in an eel-skin wallet will erase the magnetic strip (anyone have any idea why this would be?)

The card readers were cleverly designed to store all valid cards numbers in local memory so that when the network or central computer was unavailable, it would still allow access. Unfortunately, the memory isn't large enough to hold all of the valid cards for the larger buildings, and whenever the network goes down, USC security has to dispatch a guard to each of the large buildings to let folks in.

In power failures, all of the doors with magnetic locks swing open (which has happened on several occasions).

--Kraig Meyer

---

### ***R* An electronic lock that failed in an incorrect application**

*Mike Carleton 297-4114 MRO1-1/JK33 <mcarterton@vino.enet.dec.com>  
Fri, 27 Sep 91 17:23:16 PDT*

In [RISKS 12.40](#) David Holland writes about the potential risks of the electronic key-card locks on Harvard Union dormitories. His mention the potential of electronic failure in these types of systems reminded me of another type of failure that I had observed.

A large oil company in Dallas TX used a key card access system to control access to sensitive sections of their building. The doors were 'locked' using a large permanent magnet mounted on the door jam and a large steel plate mounted on the door. The magnet was strong enough to hold the door closed against substantial effort. When the lock was electronically opened, a coil running through the magnet was energized with AC current. The field from the AC current disrupted the permanent magnetic field enough so that the door can be opened with little effort. A small light near the doorway was lit to indicate that the door had been unlocked.

The scheme seemed to work well with all but the main door to the lobby of the building. This door required a card-key at night but was open during business hours. They had programmed the system to leave AC coil on the front door energized all day. The degaussing effect of the AC caused the permanent magnet to lose its holding power, making the lock ineffective at night.

The normal nocturnal visitors to the site did not seem to notice the problem as they were in the habit of using the key card to open door. I expect that if the problem was noticed, maintenance workers would have replaced the magnet only to find the lock failing again soon afterward. It seems apparent that the

implementors of the locking system did not understand the technology of the locks well enough to know that the scheme could never be made to work on a door that must be unlocked all day.

Mike Carleton



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 12: Issue 42

Monday 30 September 1991

## Contents

- [Dialup lottery](#)  
[PGN](#)
- [Space Station Software Hubris](#)  
[David Bremner](#)
- [Re: V-22 Osprey](#)  
[Henry Spencer](#)
- [Re: Risks of computerized typesetting](#)  
[Lauren Weinstein](#)  
[Gene Spafford](#)
- [Re: Radio Shack computerized mailing list problem](#)  
[John R. Levine](#)  
[et al.](#)
- [Re: eelskin wallets and magnetic cards](#)  
[Robert Ullmann](#)  
[et al.](#)
- [Re: Have you tested your machine lately?](#)  
[Bennet Yee](#)  
[Henry Spencer](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Dialup lottery**

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>  
Sat, 28 Sep 91 12:32:14 PDT

A followup on the Nintendo Lottery noted in [RISKS-12.41](#) is contained in an AP item from 28Sep91 regarding a Minnesota law forbidding minors from gambling:

Lottery officials and lottery vendor Control Data Corp. of Bloomington say the game will have safeguards to prevent children from gambling, including personal passwords for users.

I'm glad that solves the problem so easily. By the way, I will be East for a week for the National Computer Security Conference, where I expect to see quite

a few of you. Among other things, Ken van Wyk (VIRUS-L and SEI.CMU) and I will be on a panel Tuesday on the risks of distributing security information electronically. That should be amusing, at least for the two of us.

A few of you have commented on some funny spellings in the masthead first line. Please recall that on two-digit Wednesdays and Saturdays in September we have a line longer than 80 characters -- resulting in the issue number getting TRUNCATED unless I foreshorten the line a little.

---

### ✂ Space Station Software Hubris

David Bremner <bremner@cs.sfu.ca>

Mon, 30 Sep 91 12:10:51 PDT

In the Fall 1991 issue of Graduate Computerworld ( A free publication consisting of promo articles on prospective employers ), there is an interview with Julius Gabriel, manager of software engineering at Spar Aerospace.

Spar is doing the software for the Mobile Servicing Station; essentially a mobile version of the Canada-Arm. Gabriel notes that "The entire space station will be highly computerized, with a software program in excess of 10 million lines of code". Apparently the MSS will be a rather small fraction of the whole, about "half a million lines of code".

Master of understatement, Gabriel notes that "Once its up there it's difficult to fix the software". The article notes that "Naturally, the entire software process adheres to rigorous standards such as the military 2167A standard". Gabriel makes some good points about the importance of software development methodology, but what worries me is the attitude that writing ( working ! ) 10 million line programs is a solved problem, that all we have to do is use Ada (TM AJPO) and mil-std 2167A, and everything will work fine.

David

References: Page 14, Fall 1991 \_Graduate Computer World\_  
bremner@cs.sfu.ca            ubc-cs!fornax!bremner

---

### ✂ Re: V-22 Osprey (Wodehouse, [RISKS-12.41](#))

<henry@zoo.toronto.edu>

Sat, 28 Sep 91 18:44:45 EDT

>consider the case in which the triple sensors are not "reverse-wired" but cross-wired (e.g. sensor 2 is connected to input 1 & vs). In this case, with "all good" everything is fine. If 3 fails all is ok. However if 1 or 2 fails, the other is reported failed, voted out...

Things can get even more interesting if there is more than one set of wires to the sensors, e.g. for feedback control of some kind. The second Saturn V test launch had a double engine failure in the second stage that was traced to such a problem: one engine did indeed develop problems, but the "shut down" command from the control computer went to the neighboring

engine instead.

Henry Spencer at U of Toronto Zoology      utzoolhenry

---

### **✂ Re: Risks of computerized typesetting**

*Lauren Weinstein <lauren@vortex.com>*

*Sat, 28 Sep 91 18:01:41 PDT*

This is a classic case where technology can render traditional publication proofing useless if the technology is used inappropriately without proper checks and balances.

In the traditional publishing environment, the galley proof usually has a photographic relationship to the final product. "Blue line" proofs for books are normally made from the same negatives that are then used to create the actual printing plates.

The whole point of the galley or blue line proof is to give the author(s) an accurate representation of the final appearance of their work for their approval. When authors are placed in the position of approving a "proof" that does *\*not\** represent that actual output that will be used to create the final plates, much of the point behind having the proof in the first place is lost. In the case where a font happens to vary in an unexpected manner (as in the case under discussion) this can be a rather serious problem.

Authors should refuse to sign off on their works until their publishers supply them with a physical proof (not just an online representation unless it is a direct scan of the actual proof itself) that accurately shows the final output from the correct output device, complete with all fonts in their final forms.

--Lauren--

---

### **✂ Errata for "Practical Unix Security"**

*Gene Spafford <spaf@cs.purdue.EDU>*

*29 Sep 91 01:33:01 GMT*

As reported in [RISKS-12.41](#), Simson Garfinkel described how a non-standard font set-up on a phototypesetter caused some problems with the printing of our book.

What follows is the announcement O'Reilly & Associates (the publisher) has made about this error. No word yet on what they are going to do with (or to!) the shop that did the printing! We breathlessly await the third printing to see what goes wrong there. :-)

O'Reilly & Associates has discovered that in the first printing of `_Practical_UNIX_Security_` by Simson Garfinkel and Gene Spafford (June, 1991) a formatting error caused the grave quotes (`'`) in the shell scripts in our final PostScript files to be printed as forward quotes (`'`). Of course, this breaks the scripts and is certainly not what the authors, editor, or publisher intended.

An errata sheet is available from the publisher that corrects these shell script examples and other minor technical errors found in the first printing. Please telephone O'Reilly & Associates at 800-338-6887 (US & Canada) to obtain a copy of this sheet. Alternatively, you may send email to [steph@ora.com](mailto:steph@ora.com), to request a copy of the errata sheet -- be sure to include your surface mail address.

We apologize for any difficulties these errors may have caused!

---

### **✂ Re: Radio Shack computerized mailing list problem**

*John R. Levine <[johnl@iecc.cambridge.ma.us](mailto:johnl@iecc.cambridge.ma.us)>  
29 Sep 91 22:54:25 EDT (Sun)*

Joseph Poirer writes about getting a receipt with someone else's name on it when he declined to identify himself at Radio Shack, and wonders if their computer system can't handle a transaction without a name.

It turns out that this isn't a computer problem, it is simply a management problem. Radio Shack employees get a bonus if they capture more than 95% of their customer names, and the employees are reacting in a locally rational way to anonymous customers. Rat Shack has severe penalties for employees who make up names, but apparently using the wrong real name is so far OK. It is easy to ring up a sale with no name, I get them to do it all the time.

Rat Shack claims they use the names only for their own mailing list which they do not sell, but at least one person has reported getting junk mail from other parties with the same distinctive misspelling as Rat Shack has.

Personally, if they hassle me when I decline to give my name, I make one up. Sometimes when I'm in a bad mood, I make one up unprompted. Phooey.

John Levine, [johnl@iecc.cambridge.ma.us](mailto:johnl@iecc.cambridge.ma.us), {spdcc|ima|world}!iecc!johnl

[This incentive to capture your vita was also noted by a bunch of other contributors, several of whom noted this discussion went on earlier for some time in [comp.dcom.telecom](mailto:comp.dcom.telecom). I therefore omit a whole slew of similar responses. You will understand if I do not enumerate you all! PGN]

---

### **✂ re: eelskin wallets and magnetic cards**

*Robert Ullmann <[Ariel@Relay.Prime.COM](mailto:Ariel@Relay.Prime.COM)>  
28 Sep 91 16:13:21 EDT*

Kraig Meyer [in [RISKS 12.41](#)]: "USC security also claims that keeping the card in an eel-skin wallet will erase the magnetic strip (anyone have any idea why this would be?)"

This is an old Urban Legend, about eelskin (or snake, alligator, etc) purses

and wallets. The explanation isn't some strange electro-magnetic effect of reptile skin. It is that such things often (usually?) have magnetic clasps!

Apparently this has to do with the skin not having the mechanical strength of (e.g.) leather; where a mechanical clasp would tear the eelskin under stress, the magnetic clasp simply opens.

-- Robert Ullmann

[Not surprisingly, we have slithered down this path before, WAY BACK IN [RISKS-6.25](#) and [RISKS-8.04](#) (Jane Dunlop Smith)!!! However, we have some alert contributors who again noted the mag clasp. This time

\* trebor@foretune.co.jp (Robert J Woodhead)

\* dplatt@ntg.com (Dave Platt)

\* mauxci!eci386!drk@apple.com (David King) and

\* kent@sunfs3.bos.camex.com (Kent Borg)

all had puns on electric-eel-skins.

\* Al Stangenberger <forags@nature.Berkeley.Edu>

noted the version that several women who carried magnetically encoded BART (subway) tickets in their eel-skin wallets noticed that the magnetic strips had been erased.

Also noting the bogosity of the magnetic clasp effects were

\* henry@zoo.toronto.edu (Henry Spencer) and

\* richg@prodnet.la.locus.com (Rich Greenberg)

---

### **🔥 Re: Have you tested your machine lately? (Sandberg, [RISKS-12.41](#))**

<Bennet\_Yee@PLAY.MACH.CS.CMU.EDU>

Sat, 28 Sep 91 18:22:04 -0400

The fact that division by zero does not generate a fatal error but gives a special value is a property of IEEE 754. Likewise with  $0/0 == \text{"NaN"}$  (Not a Number), etc. I won't repeat the arguments as to why this may or may not be appropriate, but if you'd look at the "See Also" section of the math(3M) man page, you'd see references to several papers that address the design -- Kahan (the principle designer of 754) is quite compelling as to why 754's behavior is most reasonable.

Is this a risk of coding without being cognizant of industry standards? Coding to an internal model of the machine that doesn't match reality?

>Also if you notice on the output that the results are different depending on if you optimize or not.

The fact that your code outputs "NaN" when it should have given "+Infinity" or "-Infinity" is probably a compiler bug. From the excerpt of the output, it appears that the behavior \*with\* optimization turned on is correct. This is actually a little surprising, since typically the optimizer introduces bugs, not the other way around. A risk of testing/debugging only that which we think is hard/bug-prone and skimping on the rest?

Complaining about the compiler/floating point hardware to your vendor would be quite appropriate; complaints about IEEE 754 should probably go to Kahan

instead. :) Risks of blame misattribution?

Bennet S. Yee Phone: +1 412 268-7571 Email: bsy+@cs.cmu.edu  
School of Computer Science, Carnegie Mellon, Pittsburgh, PA 15213-3890

---

### **✂ Re: Have you tested your machine lately?**

<henry@zoo.toronto.edu>  
Sat, 28 Sep 91 18:58:48 EDT

>We have an Alliant fx/800 computer...

... By default no action is taken on many of the exceptions.  
... I do not know the exact reasons for this decision, it might have to do with performance, but who cares if the machine is fast if the answers are wrong?

Very probably it's a performance issue. I don't have any detailed knowledge of the Alliant, but I do know that this is a generic problem with attempts to build seriously fast computers: if you want to move fast, you have to go pretty much in a straight line. Any situation where a departure from sequential flow might occur, \*and where it has to occur in a predictable way\*, incurs major complexity and potentially serious delays to make sure everything is synchronized just in case.

Folks interested in such things should read "Putting UNIX on Very Fast Computers", by Mike O'Dell, in the Proceedings of the Summer 1990 USENIX Conference. Mike was Chief Computer Scientist at now-defunct Prisma, which was trying to build a Cray-class SPARC. (USENIX can be reached, e.g. about availability of proceedings, at office@usenix.org.)

Henry Spencer



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 12: Issue 43

Monday 7 October 1991

## Contents

- [Full \(16 rounds\) DES Broken](#)
  - [Li Gong](#)
  - [Dave Roberts](#)
- [AT&T "Deeply Distressed" over Outage](#)
  - [Mark Seecof](#)
  - [Michael F Eastman](#)
- [Fred Cohen's contest and "good viruses"](#)
  - [Gene Spafford](#)
  - [John Markoff excerpt](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✂ full (16 rounds) DES Broken (reported in NY Times)

*Li Gong <li@cambridge.oracorp.com>  
Fri, 4 Oct 91 14:18:26 EDT*

John Markoff in The New York Times (03Oct91, p.A18) reported that Adi Shamir and his student Eli Biham had emailed their American colleagues and told them that the full 16-round DES had been broken with chosen-ciphertext attacks (probably the follow-up of what they reported last year at Crypto). The article said that Adi is not willing to comment on anything until the research result is published in a journal later this (yes, this) year.

Li Gong, ORA Corp, 675 Mass Ave, Cambridge, MA 02139

---

### ✂ Demise of DES

*Dave Roberts <dwr@datasci.co.uk>  
Mon, 7 Oct 91 11:45:14 GMT*

>From THE DAILY TELEGRAPH, London, Saturday, October 5th 1991

"Secret" bank code cracked warns GCHQ, By Adrian Berry

Banks and financial houses are being warned by GCHQ at Cheltenham to stop sending messages in their most widely used secret code [DES], because it has been cracked. [...] GCHQ, which supervises the security of secret codes, wants banks to use the more advanced code known as Rambutan.

[A known plaintext attack] helped the Americans to win the Battle of Midway in 1942. An American base radioed falsely that its water supplies had broken down. The Japanese then reported the message in a cipher. The Americans simply compared the two texts and learned to read secret enemy traffic.

Bank officials said yesterday that they would probably continue to use the DES code until officially warned against it, or until another Government-approved encryption package was made available.

[Nobody is selling commercial Rambutan chips in the UK so the banks cannot (to the best of my knowledge) get them. D.W. Roberts dwr@uk.co.datasci]

---

### ✂ AT&T "Deeply Distressed" over Outage

Mark Seecof <marks@capnet.latimes.com>

Tue, 1 Oct 91 09:47:41 -0700

The Wall Street Journal reports on page C18 of the October 1 issue that "AT&T Tells FCC a Lapse In Procedure Led to Outage." [Elisions and bracketed comments from Mark S.]

[Story Begins]

An [AT&T] executive told the FCC that AT&T was ``deeply distressed by the lapses in procedure" that led to a network failure in New York City last month. Kenneth L. Garrett, a senior vice-president in charge of AT&T's network services, said that the failure of the Manhattan switching center on Sept. 17 could have been averted if ``AT&T's existing procedures" had been followed by a supervisor. Mr. Garrett made his remarks in a letter to FCC Chairman Alfred C. Sikes released late yesterday. While AT&T's report said alarms in the building were not working properly, Mr. Garrett's letter, which accompanied AT&T's report on the outage, noted the failure wasn't a systemic breakdown of the AT&T network.

AT&T said standard procedure calls for the supervisor, whom AT&T didn't name, to assign a technician to inspect each of the Thomas St. facility's power plants when AT&T switched to its own electrical power from the grid operated by New York utility [Con Ed]. Instead, the supervisor took his technicians to a class on a new power alarm system, leaving the plant unsupervised.

The switchover blew rectifiers, which convert Con Ed's AC power to DC current, sending the switching center to emergency batteries, which quickly ran out of juice [sic!]. The switching center gradually lost power, stalling communications traffic, including critical air-traffic control information. It was AT&T's third major network failure in 18 months.

---

**✉ from telecom -- att outage**

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

Mon, 7 Oct 91 9:42:00 PDT

Date: Wed, 2 Oct 91 12:16:44 EDT

From: mfe@ihlpy.att.com (Michael F Eastman)

Subject: Update on 9/17/91 AT&T Outage

Organization: AT&T Bell Laboratories

The following report was posted on our internal news network by Corporate Media Relations. It is a good summary of the events surrounding the outage. I hope that you will find it informative.

Mike Eastman - 4ESS Development - AT&T Bell Laboratories

-----

FOR THE RECORD \*\*\* Following is a synopsis of the events leading to the service disruption on Sept. 17:

Late in the afternoon on Sept. 17, the AT&T switching center at 33 Thomas St. in lower Manhattan experienced a battery power failure in its 20th floor power room facilities, disrupting service, including voice and data communications for all three New York area airports. The events leading to the disruption began earlier, between 6-7 a.m., when the Building Operations Group was contacted by Con Edison with a request to take the facility off commercial power during the day. We agreed to do so.

At 10:10 a.m., AT&T cut over from commercial power supplied by Con Edison to backup, diesel-generated power. Such a cutover is standard procedure; it is a result of the interruptible power arrangement AT&T has with Con Edison, and was accomplished four times without incident this summer alone, most recently on August 15 and 29. The interruptible power arrangement with Con Edison has been in effect formally since 1990. It capitalizes on AT&T's ability to generate at 33 Thomas St. sufficient power to cover the building's needs. By having the means on-site to generate the building's electricity, AT&T both protects itself from voltage brown outs that could damage equipment and impair service, and fulfills a corporate citizenship obligation to shed electrical load during power emergencies.

At 10:10 a.m. the AC power supervisor threw a switch, engaging the diesel generator and taking the building off commercial power. Throughout the building, in each of the telecommunications power plants but one, that transfer of power from commercial AC to diesel-generated AC, was accomplished smoothly. On the 20th floor, where the power plant for DS3 and other high-capacity transmission facilities is located, there was a problem. A rectifier there sensed a spike in voltage level; to protect the power plant and facilities the plant supported, AC power was removed from the rectifier input and the power plant began operating on battery reserve. Subsequent tests have determined that the overload protection relay was misadjusted during recent plant modernization, making the shutdown circuit overly sensitive to overvoltage. This is the only power plant in the building that did not cutover normally.

From that moment, approximately 10:10 a.m., the batteries supporting all DS3-and-higher-capacity facilities at 33 Thomas St. were removed from their recharging system and were operating on emergency reserve. That emergency reserve power is designed to last six hours. Standard operating procedure requires the DC power supervisor to dispatch a power technician to walk through each of the building's power plants during a shift from commercial power to diesel power. Had such a walkthrough occurred on Sept. 17, the technician would have seen a "POWER" alarm in the 20th floor power room. A power technician performs such walkthroughs as a matter of standard methods of procedure. However, on the morning of September 17, the DC power supervisor decided not to dispatch a technician to verify the transfer for the following reasons:

- o All six power technicians (and the supervisor) were scheduled for a power alarm training class in another building, about 15 minutes away.
- o 33 Thomas St. had not experienced a power problem in six to eight years.
- o The rectifiers had been refurbished in the last year and the batteries were new with a six (6) hour reserve.
- o Four (4) power transfers had been conducted during the summer without problem.

Additionally, the supervisor did not arrange for a substitute by requesting the use of one of the fifty-two power-qualified technicians -- a technician normally charged with other duties, but capable of responding to a power emergency -- remaining within the building.

In the absence of a power technician, if an alarm had been recognized, one of these power-qualified technicians could have handled the problem. Doing so would have enabled the batteries in the 20th floor power room to be recharged by the diesel generator, even as they were being drained by providing power to the high-capacity telecommunications facilities in the building. There was a failure to follow standard operating procedure. Had a power technician or any power-qualified communications technician been required to perform the power plant walkthrough as methods of procedure mandated, the tripped rectifier would have been discovered and reset, and a service outage would have been avoided.

But the power plant walkthrough was not performed. All of the building's six power plant technicians had been dispatched to receive training, ironically, on a new computerized alarm system that will be cut over at 33 Thomas St. in October. The equipment for that new alarm system is functioning already at the building where the training class was being conducted; it is being installed, but has not yet been brought into service at 33 Thomas St.

From 10:10 a.m. until 4:30 p.m., all high-capacity telecommunications facilities in the building were being run on emergency battery reserve power from the 20th floor power room. All other equipment, such as the three 4ESS switching systems in the building, was supplied with electricity from other

power plants, and was fully operational and functioning normally.

At 4:30 p.m., a communications technician who was just coming on duty for the evening tour, noticed a visual display indicating the emergency battery power condition. This visual alarm is in a location that is normally unstaffed. At this point, the technician, who is power qualified, made an attempt to cut back from batteries to AC power. That attempt was unsuccessful; the batteries had been discharged to a point where they would not physically accept recharging current without being disconnected from the facilities they were supporting. At 4:40 p.m., as battery life expired, those facilities began to go down.

The restoral effort got under way virtually immediately. During the first 30 minutes, 144 non-terminating T3 circuits, carrying traffic passing through but not terminating in the New York area, were restored. This amounted to some 19,200 message circuits and approximately 1,400 private line T1 lines. By 6:00 p.m., all equipment was disconnected from the 20th floor power plant, and rectifiers were manually reset to force current into the batteries to recharge them. As the rectifiers recharged the power plant, facilities were gradually brought back on line. By 9 p.m., 43% of domestic and 8% of international traffic was restored, by 10 p.m., 51% of domestic and 56% of international traffic was restored, and by midnight, virtually 100% of domestic and 95% of international traffic was restored.

FYI:

1. The 48-volt battery plant at 33 Thomas St. is scheduled to be replaced by the end of the year. The new plant will have restart capability, in contrast to the existing plant.
2. A diversification of load distribution is now planned for both call-handling systems and power systems within the local node. This diversification will mean that any future outages would be limited to a maximum of 50% of an office's high-capacity transmission facilities. Rerouting is expected to be completed at 33 Thomas St. by March, 1992; at all major metropolitan New York offices by the end of 1992, and at all offices in the nation by the end of 1993.
3. A new power alarm system, now being installed at 33 Thomas St., will have built-in redundancy, with alarm connections to both the local building and to a surveillance center in Conyers, Ga. In the event of a failure, alarms will go off in both locations, providing a backup if the local alarms are not functioning.
4. Nationwide, AT&T has stepped up plans to spend \$200 million over the next 12 months to improve the reliability and backup of its power systems, which is expected to greatly diminish the risk of similar equipment problems.

Mike Eastman att!ihlpy!mfe (708) 979-6569  
AT&T Bell Laboratories Rm. 4F-328 Naperville, IL 60566

---

 Fred Cohen's contest

Gene Spafford <spaf@cs.purdue.edu>

Mon, 30 Sep 1991 17:17:13 -0500

The September/October issue of "The Sciences," published by the New York Academy of Sciences, had an article by Fred Cohen. In it, he tried to make a case for the existence of "good" viruses, and he pulled out a number of supporting examples that really weren't viruses or weren't clearly done well by viruses. He concluded the article with an announcement of a contest. His publishing company, ASP (which may be run by Fred for all I know) will award \$1000 for the best "good" virus as per vague rules laid down by Fred in the article.

I was quite upset by the article, and especially the contest, because I think it quite unethical to encourage the writing of viruses as he is doing. I also think there is a very clear and significant conflict of interest for him and/or ASP to be encouraging such a contest.

I wrote a letter of response to the editor a few weeks ago, and I have spent the time since then thinking about it. The toned-down letter that I actually sent is reproduced below, minus some italics and bold-facing.

Whether you agree or disagree with my comments, if you wish to make your own comments to the editor, his address is below; his fax number is 212-260-1356. I doubt I am the only person with an opinion on this matter. (Naturally, I could be the lone voice of dissent; I hope not, but it may be the case.)

=====

Mr. Peter G. Brown, Editor  
The Sciences  
622 Broadway  
New York, NY 10012

Dear Mr. Brown:

I began to read the recent article by Dr. Fred Cohen [1] with considerable interest. Dr. Cohen is a pioneer in the field of computer virus research, and I have found many of his writings quite thought-provoking. Unfortunately, by the time I finished his article, I was quite dismayed. I believe that Dr. Cohen has failed to adequately consider both the practicality and the ethics of his proposal.

First of all, I believe that there is an obvious conflict of interest involved when the vendor of a computer virus prevention product sponsors a contest soliciting the development of new viruses. I am further troubled by the lack of a list of the judges of the contest and the criteria for winning. I will not discuss these points further, however, as they are minor matters compared with my main concern: I believe that the writing of computer viruses is unethical, [2--3] and to encourage their development in an unsupervised manner is likewise unethical.

Computer viruses spread without the informed consent of the owner of the

software ("host") they "infect," and they are usually not limited in their spread, in time or space. If scientists were to experiment with organic viruses capable of infecting humans and possessing these same properties, we would likely be taking vigilante action against them, contest or no. Encouraging the general populace to develop organic viruses would bring about widespread condemnation; yet, oddly, encouraging the development of computer viruses leads to publication in a journal.

To his credit, Dr. Cohen explicitly prohibits viruses that exhibit the above two dangerous properties from being eligible for his contest. However, many viruses cause damage because of flaws within the code, or unexpected properties of their target computing environment; examples include the "Stoned" virus for IBM PCs, and the "WDEF" virus for Apple Macintoshes (cf., [3--5]). What will be the attitude of the community as a whole if a new destructive virus appears on the scene because of a bug in the software meant to contain it? What if something similar to Robert T. Morris's Internet Worm were to be discovered and explained as a buggy test version intended for Cohen's contest?

This brings me to another argument with Dr. Cohen's article: we disagree about the definition of the term "computer virus." Cohen describes Morris's Internet program as a "virus," while I (and others) would define it as a "worm." [6--7] Morris's program did not alter existing software to include a copy of itself as do viruses. His program was no more a virus than is a compiler (suggesting an interesting class of potential submissions to the contest). In fact, if we intuit a definition of "contest-acceptable virus" from Cohen's article to be something that spreads from system to system, that requires permission to install itself, and has limited potential for spread (like the Worm), it is no longer clear we are speaking about viruses at all!

Harold Thimbleby of Stirling University, Scotland and Ian Witten of Calgary University, Canada have done extensive work on software that would meet the above intuited definition of a computer virus. They have developed some very sophisticated self-propagating applications, including self-updating databases with window-based interfaces. [8--9] It is not at all clear that the community recognizes these as viruses. Professor Thimbleby himself has chosen to call them "liveware" to make the distinction clear. I am surprised that Dr. Cohen is unfamiliar with their work and did not cite it in his Sciences article; it would be a clear favorite if it were to be entered in the ASP contest. However, it also serves to illustrate how something that might win the contest is not likely to be viewed as a "virus" by the community of researchers.

This brings me to the second of my two major objections to Cohen's article and contest. I believe that his underlying thesis is flawed: I do not believe that there are any practical "good" viruses. During the Second Conference on Artificial Life, held in Santa Fe in 1990 (cf. [10]), I was on a panel discussing computer viruses. Russell Brand, another panelist, made the observation that there is nothing that can be done by a computer virus that cannot be done more efficiently and generally by other means. This observation was debated by the panel, and discussed extensively by others since that time. To my knowledge, everyone involved in these discussions now believes that is a true statement.

Consider that a computer virus is nothing other than a program coupled with code to transport and install itself as part of existing software. It will be

more difficult (or impossible) than a stand-alone program to update for new releases, customize, and maintain. A virus will also be more difficult to write and test for correctness than will a stand-alone program because of its interaction with its environment. Viruses are simply not the most practical or efficient approach to any particular task. His example in the article of the billing system demonstrates an inadequacy in the data model used and tools available, and not the superiority of using a quasi-virus. Even the example Cohen gave in his PhD dissertation of a compression virus would be better served by a well-written stand-alone program over which the user has more control. I believe that any attempt made to promote "useful" viruses involves a contradiction of the word "useful," assuming that "useful" does not also imply "malicious."

To return to my first fundamental objection (and the one I feel most strongly about) -- the impropriety of encouraging virus authorship. We have been battling computer viruses for five years now, and the indications are that the problem is growing exponentially (cf. [11--12]). Computer viruses --- even those intended to be harmless, and limited in scope and duration --- continue to cause untold amounts of damage to computer systems. For someone of Dr. Cohen's reputation within the field to actually promote the uncontrolled writing of any kind of virus, even with his stated stipulations, is to act irresponsibly and immorally. To act in such a manner is likely to encourage the development of yet more viruses "in the wild" by muddling the ethics and dangers involved. It will reinforce the attitude that there may be some benefit to be gained from writing viruses (when there is as yet absolutely no clear indication that such is the case), and may encourage people to begin uncontrolled experiments with viruses they might not otherwise have undertaken. We have seen cases already where well-trained virus researchers have accidentally released experimental computer viruses into the population; to encourage amateurs to also engage in risky behavior that may lead to similar or worse results is quite appalling. It is my fond hope that no one attempts to enter Dr. Cohen's contest, and that he quickly recognizes the dangers and cancels it.

A few decades ago, physicists talked about peaceful uses of atomic weapons, such as blasting out canals and destroying threatening icebergs. They were attempting, in good faith, to put a better moral cast on their research. Thankfully, none of them offered money in a contest for the best demonstration of such an application! Alfred Nobel, horrified at the use to which his invention of stabilized explosives were being put, did not establish a contest for the best peaceful use of dynamite. Instead, he established world-reknowned awards for research in peaceful pursuits, funded by the income from his discovery. It is quite unfortunate that ASP and Dr. Cohen could not have taken a similar approach with their \$1000 prize. They could have made a powerful statement about responsible behavior, but instead have increased the danger to the community and generated doubts about their own motivations.

Eugene H. Spafford, PhD

#### REFERENCES

[1] Friendly Contagion: Harnessing the Subtle Power of Computer Viruses, by Fred Cohen, *The Sciences*, Sep/Oct 1991, pp. 22--28.

[2] Computer Viruses and Ethics, by Eugene H. Spafford, in Collegiate Microcomputer, special issue on the Rose-Hullman/GTE Computing and Ethics Seminars, to appear, 1992.

[3] Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats, by Eugene H. Spafford, Kathleen A. Heaphy and David J. Ferbrache, ADAPSO, 1989.

[4] Rogue Programs: Viruses, Worms, and Trojan Horses, edited by Lance J. Hoffman, Van Nostrand Reinhold, 1990.

[5] Computers Under Attack: Intruders, Worms and Viruses, edited by Peter J. Denning, ACM Press/Addison-Wesley, 1990.

[6] What is A Computer Virus?, by Eugene H. Spafford, Kathleen A. Heaphy and David J. Ferbrache, Chapter 2 in [4].

[7] An Analysis of the Internet Worm, by Eugene H. Spafford, in Lecture Notes in Computer Science 387, Springer-Verlag, 1989.

[8] Bugs, Viruses and Liveware: Collected Papers by Harold Thimbleby, technical report of the Department of Computer Science, Stirling University, Scotland, 1990.

[9] Liveware: A New Approach to Sharing Data in Social Networks, by I. H. Witten, H. W. Thimbleby, G. F. Coulouris, and S. Greenberg, in International Journal of Man-Machine Studies, 1990.

[10] Artificial Life II, Studies in the Sciences of Complexity, Volume XII, edited by D. Farmer, C. Langton, S. Rasmussen, and C. Taylor, Addison-Wesley, 1992.

[11] Virus Trends: Up, Up, Up by David Stang in National Computer Security Association News, 2(2), March/April 1991.

[12] The Kinetics of Computer Virus Replication by Peter S. Tippet in Proceedings of the Fourth Annual DPMA Computer Virus Security Conference, New York, March 1991.



"Peter G. Neumann" <neumann@csl.sri.com>  
Mon, 7 Oct 91 10:07:30 PDT

Excerpt from JOHN MARKOFF, New York Times, News of the Week in Review, 6oct91

Biologists have learned to harness viruses to create vaccines and, in recent years, to reprogram faulty chromosomes by using viruses to smuggle new genes into cells.

Now a small but growing group of computer scientists is examining the possibility of designing computer viruses and similar

programs called worms to burrow into computer networks and set in motion a whole range of beneficial activities

Many computer users have been the victims of malicious virus programs propagating through networks and erasing data or causing the whole system to fail. But now some researchers are suggesting that it is possible to harness the subtle power of computer viruses to perform useful tasks.

[The article goes on to quote Cohen, Spafford, and others, and revisits the 1960s Bell Labs Darwin Days of McIlroy and Vyssotsky (Bob Morris was around then, too), Bob Thomas at BBN for ATC software, John Shoch and Jon Hepp's Xerox Worms, and Danny Hillis of Thinking Machines. 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 12: Issue 44**

**Tuesday 8 October 1991**

## Contents

- [RISKS of Highway warning signs](#)  
[Jim Hofmann](#)
- [US Coast Guard's user fiendly software \[sic\]](#)  
[Dave Schmidt](#)
- [Fiber optics can spontaneously destroy themselves!](#)  
[Jeffrey Sorensen](#)
- [911 Glitch Delayed Help in Fatal Mt. Prospect Fire](#)  
[W.F. Wicks via Mark Brader](#)
- [Risks of owning a modem](#)  
[Geoff Kuenning](#)
- [Emergency phone dialer in Contra Costa county](#)  
[Darren Alex Griffiths](#)
- [ECC == Error CAUSING Code? Tape drive overcorrects itself...](#)  
[John Board](#)
- [Re: AT&T "Deeply Distressed"](#)  
[Bob Colwell](#)
- [Re: Back quotes print wrong](#)  
[Dick Karpinski](#)  
[Simson L. Garfinkel](#)
- [Re: Space Station Software Hubris](#)  
[Stephen G. Smith](#)
- [Schipol Airport](#)  
[Peter De Graaf via Mark Kennedy](#)
- [Computer Mediated Ethical Discussion: An Invitation](#)  
[Peter Danielson](#)
- [ACM Computer Security Day](#)  
[Beth Olson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### RISKS of Highway warning signs

*Jim Hofmann 5577 <hofmann@itd.nrl.navy.mil>*

*Fri, 4 Oct 91 13:10:05 EDT*

On 3 Oct 91 just after midnight, an accident occurred partly BECAUSE of the electronic warning signs. Woodrow Wilson bridge in Washington D.C. is a drawbridge, which, when it goes up is supposed to notify three signs each in Maryland and Virginia. The signs are programmed to flash a warning message --- presumably to slow down cars and trucks coming towards the traffic. In this case, the sign operators were not notified and hence a truck barreled into a queued car and killed the driver. The implication is that had there been no signs, the driver might have been more cautious. But since there WAS a sign and it was not flashing a warning signal, the driver did not slow down.

The obvious fix here is that if the signs are broken or not notified in time, the bridge should not be allowed to raise.

J.B.Hofmann

[This saga had some strange background. There are separate controls for each side of the river, and the programming is done upon request by telephone, via a dedicated phone line. Apparently there were many hours of delay between the receipt of the request to open the bridge and the reported attempt to notify the "programming" staff, so that the notification was not attempted until after prime shift. The programming staff insisted the phone never rang, even though someone was required to be in the room at all times and even though the phone rang louder than anything else in the room. The bridge is opened something like 400 times per year. This one was for a sailboat. Source: Washington Post 4Oct91 and various news broadcasts. PGN]

---

## ✂ US Coast Guard's user fiendly software

*Dave Schmidt <daves@amc.com>  
Tue, 1 Oct 91 12:03:40 PDT*

(No, I didn't misspell it!)

I recently tried to be a good little citizen and pay the new USCG boat tax. This involves paying some money, for which you get a nondescript sticker for your boat; this supposedly prevents hassles with the Coast Guard.

USCG does not have its own personnel taking orders; you call an 800 number and either order the sticker with a credit card (!) or order an order form to use to order the sticker with a check.

The order form we sent was evidently misread, as our address was completely messed up. When I called back to find out what happened (after 2 months), the phone droid said:

"No problem. We'll send you a claim form....Uh oh. The computer won't let me fix your address. The claim form will go to the same address that the sticker was sent to - you know, the one that the post office couldn't figure out?"

Isn't it nice that with all of the work done on making user friendly software, that people still overlook obvious functions like correcting data entry errors? If this isn't "user fiendly", I don't know what is...

David Schmidt WB7RDI daves@amc.com

Applied Microsystems, Inc

---

**✶ Fiber optics can spontaneously destroy themselves!**

*Jeffrey Sorensen <sorensen@spl.ecse.rpi.edu>*

*Tue, 1 Oct 91 15:04:48 EDT*

In the Sep 28 issue of *\_Science News\_* there is an article about a recently discovered property of fiber optic cables that could lead to all kinds of risks.

It turns out that a fiber optic in an environment "where the temperature can suddenly increase" can result in the complete destruction of a fiber optic in what is known as a fiber "fuse" effect. "For certain types of optical fibers...damage can occur when the visible-light laser power transmitted... is as low as 4 milliwatts..."

The damage to the fiber is a series of bullet-shaped cavities that form at equidistant spacings from the sight of heat damage tracing back towards the laser light source. "The damage effectively (ruins) the fiber as a medium for transmitting light. One test showed that a single flare could damage 1.5 kilometers or more of fiber." The damage travels at a rate of about 1 meter per second!

The causes of the phenomena are being researched and the sides of the debate are presented in the article (pp. 200-201). The effect is related to the germanium concentration and fibers with high concentrations are at the most risk. The temperatures required to cause the effect are between 700 °C and 1,000 °C.

On the risks involved: "It's a lot more catastrophic than just cutting a line...you basically destroy the fiber." Anyone using these types of fibers in, say, a nuclear reactor or for a critical sensor would be well advised to check this out.

Jeff Sorensen sorensen@ecse.rpi.edu (518) 276-8202

---

**✶ 911 Glitch Delayed Help in Fatal Mt. Prospect Fire (comp.dcom.telecom)**

*Mark Brader <msb@sq.com>*

*Fri, 4 Oct 1991 22:42:00 -0400*

Date: 2 Oct 91 13:29:45 GMT

From: wickswf@adobe.rtsg.mot.com (William F. Wicks)

Newsgroups: comp.dcom.telecom

Subject: 911 Glitch Delayed Help in Fatal Mt. Prospect Fire

Organization: TELECOM Digest

Approved: Telecom@eecs.nwu.edu

X-Submissions-To: telecom@eecs.nwu.edu

X-Administrivia-To: telecom-request@eecs.nwu.edu

X-Telecom-Digest: Volume 11, Issue 786, Message 7 of 8

Something of interest from the suburbs of Chicago. In the September 26 issue of the Northwest Edition of the {Chicago Tribune} was the following article:

"A computer glitch in the new enhanced 911 system serving six northwest suburbs caused the system to malfunction as a Mt. Prospect man tried to alert authorities to a fire that killed his wife and mother, authorities said.

The incident led Centel to discover and correct the problem before anyone else was affected. Mt. Prospect's fire officials said the system's failure did not contribute to the deaths of the two women, who they believe died before the emergency phone call.

The 911 error was caused by a record-keeping procedure in Centel's system, which listed the man's neighbor's phone number (where he placed the 911 call) both to the home in Mt. Prospect and to another address in Des Plaines which had previously had the number. In processing the call, the 911 computer software saw two addresses for the same phone number, which is not permissible in its programming and eliminated one. When the man called 911 and the computer read the Des Plaines address, it played a recording saying that the community was not hooked up to the 911 system. At this point the call should have been routed to the Northwest Central Dispatch System, but it did not. The recording directed the man to call an operator, who put him in contact with the emergency dispatcher in Des Plaines. That dispatcher called Northwest Central Dispatch officials who sent firefighters to the scene."

Although in this case it was determined that nothing could have been prevented if the error had not existed, this could have been a very costly error. It was found that 26 other people had wrong addresses in the computer. I found this story very interesting because I live in Schaumburg which just recently converted to E-911 (not this same system though).

William Wicks Motorola, Inc. wickswf@adobe.rts.mot.com

[Moderator's Note: I saw the same story. Thanks for passing it along. Our Chicago 911 operates pretty well considering the heavy load on it this past summer with the warfare going on here for the past few months. Those suburbs with their own 911 (ie, phone exchanges unique to their community) also do okay. The troublesome ones are as the story noted, those communities with overlapping phone exchanges where one has 911 and the other does not. PAT]

---

## **✶ Risks of owning a modem**

*Geoff Kuenning <desint!geoff@uunet.UU.NET>*

*Sat, 5 Oct 91 02:38:29 PDT*

As you may notice from the header of this message, it is about 2:30 A.M. on Saturday morning (or Friday night, if you prefer). I just got a knock on my door, which was astounding in itself. It turned out to be a couple of cops. They asked me if I owned a certain phone number, which is the one I use for my modem (and nothing else). Apparently it had dialed 911. In itself, this is nothing unusual. I have seen similar reports on RISKS before. But my L.sys

file has no number containing the sequence 911! A check of my uucp logs showed successful calls at 2:01 and 2:08, followed by a failure at 2:23. Presumably this last was the cause of the 911 call (we have good police response times here). There are two numbers for the 2:23 call, both of which contain the sequence "166". Now how did that get turned into 911? Maybe my dyslexic modem turned the digits upside down, then got confused about what was repeated :-)? Seems moderately unlikely.

For what it's worth, it's a Telebit T-2500. The cops said it happens fairly often. Personally, I'm upset. Those guys have better things to do than chase spurious calls from modems. But I have no idea what I can do to prevent a recurrence. I've only had the thing a couple of months. I sure hope this isn't a "feature". If so, perhaps the police department has a way for me to tell them to ignore 911 calls on that line.

Geoff Kuenning geoff@ITcorp.com

[We have had several items on this topic before,  
but the problem does not seem to go away. PGN]

---

### **🚨 Emergency phone dialer in Contra Costa county**

Darren Alex Griffiths <unisoft!dag@ucbvax.Berkeley.EDU>

2 Oct 91 18:36:44 GMT

I noticed an interesting news story in the San Francisco Examiner a couple of days ago. It seems that a bay area county (Contra Costa) has set up a system to dial every phone in the county in case of emergencies. The system can be setup to dial all the phones (about 30,000) within a few hours in the event of a toxic spill or other disaster, or it can call every phone within a few blocks and ask people to look out for a lost child.

Initially this sounds like a good thing, and it probably is, but there are certainly some questions. I've never heard of this type of system before, is Contra Costa the first one to have it? Also, I assume they didn't test it by calling all of the phones, so how do they know it will really work? There are also some interesting risks associated with it. By definition the system is connected to the phone network, I wonder what the chance of some piece of pond scum breaking in to it and sending fake messages to people are? What if the system breaks and goes wild at 4:00am calling up numbers all over the world? Where does it get the address information from as well? I wonder if it uses the 911 database or if it has it's own built by the city?

Ahhh, so many questions, so little time.

Darren Alex Griffiths dag@unisoft.com (for now) dag@ossi.com (RSN)

---

### **🚨 ECC == Error CAUSING Code? Tape drive overcorrects itself...**

<jab@egr.duke.edu>

Tue, 1 Oct 91 11:19:32 -0400

Product manager's worst nightmare: creating a feature designed to enhance reliability (in this case of data stored on tape) which, in fact, reduced it (in this case by sometimes causing data losses). The RISK of allowing marketing to force one bell or whistle too many into a design? Reminds me of the "Uninterruptable Power Supply" we had in our lab which caused system crashes by putting spikes on the "protected" side of the supply whenever its internal cooling fans cut in, but I digress. I excerpt from a letter recently received from IBM. I applaud their frank and rapid disclosure of a potentially dangerous technical flaw; I find their tone ("well, you don't really need ECC anyway because our drive is so good") somewhat amusing, a luxury I am permitted since we experienced no losses. My opinion might be harsher if we had been adversely affected by the problem....

"IBM has discovered that the Error Correction Code (ECC) function in the IBM 150MB 1/4-inch tape drive is not performing to our satisfaction. [...] This ECC implementation is unique to this ... drive, and was intended to provide an additional margin of data protection beyond commonly accepted reliability levels. However, a problem has been found which has the potential for causing loss of data when the drive is reading a tape made with ECC. There are no error codes to indicate that this condition has occurred.

This problem will have no impact on the system until the tape is read, because the data is recorded correctly on the tape, but may be read back incorrectly under certain unusual circumstances. Most users will not experience this set of circumstances.

Since the [...] drive provides all the recognized industry standard checking features such as Read after Write and redundancy checking in addition to ECC, ECC is not required in order to provide commonly accepted reliability levels [...]."

John Board, Asst. Prof., Dept. Electrical Eng'g and Dept. Comp. Sci., Duke University, Durham NC USA +1 (919) 660-5272 INET: jab@ee.egr.duke.edu

---

**✉ Re: AT&T "Deeply Distressed" ([RISKS-12.43](#))**

<colwell@ichips.intel.com>

Mon, 7 Oct 91 15:12:25 -0700

An [AT&T] executive told the FCC that AT&T was "deeply distressed by the lapses in procedure" that led to a network failure in New York City last month.

...

4. Nationwide, AT&T has stepped up plans to spend \$200 million over the next 12 months to improve the reliability and backup of its power systems, which is expected to greatly diminish the risk of similar equipment problems.

I get the uncomfortable feeling that the real risk here is being intentionally ignored. What caused this service outage was human error. What caused Chernobyl was human error. Ditto for Three Mile Island and the Kansas City Hyatt hotel walkway collapse. Design engineers can try to anticipate how machinery and materials will interact with each other. But

it's devilishly hard to predict how something as complex and unpredictable as a human being, especially one that becomes emotional and possibly irrational under duress, will react to the system.

It's clear that the human component of the AT&T outage was what caused the outage. That's the link that needs more attention in the engineering and in the analysis of failure.

Bob Colwell, Intel Corp. JF1-19, 5200 NE Elam Young Parkway, Hillsboro, Oregon 97124 colwell@ichips.intel.com 503-696-4550

---

### ✂ Back quotes print wrong (Risks of computerized typesetting)

*Dick Karpinski <dick@ccnext.ucsf.edu>*

*Fri, 4 Oct 91 13:12:59 PDT*

I ran into this problem myself and have repeatedly reported the problem both to NeXT and to Adobe. For me, with Courier, the back quotes are correct on the screen and wrong on the laser printer. Frustrating and dangerous. It is possible to see the difference between forward and back quotes in the printer output, but it is not easy. Forward quotes print as forward quotes which are a bit heavier on the top whereas back quotes print as forward quotes which are a bit heavier on the bottom.

After such a disaster as recently reported, it ought to be easier to get the vendors involved to fix the problem. I hereby solicit anyone's assistance in reporting the problem to appropriate authorities so that it can be fixed.

Dick

---

### ✂ Back quotes explained (was: Risks of computerized typesetting)

*Simson L. Garfinkel <simsong@nextworld.com>*

*Fri, 4 Oct 91 14:54:09 PDT*

After several helpful messages from the net, we have finally figured out what happened with our Courier font.

Apparently, a few years ago Adobe did a silent change to their Courier font. Backquotes were changed from the regular character with a negative slope to a regular forward quote character which happens to be a little wider at the bottom than at the top. (The normal forward quote character is a little wider at the top than at the bottom.)

Thus, the ` and ' characters in the current Adobe Courier font *are* different characters, but you can't tell the difference unless you look at them under a magnifying glass.

Happily, Adobe made this substitution without telling anybody, and without changing the name of their Courier font.

As several people pointed out, we could have avoided this problem by providing

our publisher with our own copy of the Courier font. The publisher, ORA, has now started doing this with all of their books sent out to be typeset and printed.

Ah, standards.

-s

---

## ✂ Re: Space Station Software Hubris

*Stephen G. Smith <sgs@grebyn.com>*

*Thu, 3 Oct 91 20:39:28 -0400*

In [RISKS-12.42](#) David Bremner writes:

>... but what worries me is the attitude that writing ( working ! ) 10  
>million line programs is a solved problem, that all we have to do is use Ada  
>(TM AJPO) and mil-std 2167A, and everything will work fine.  
> David

Unfortunately, the "MIL-STD" snake oil promises exactly this. This is extremely attractive to the bureaucratic mentality -- "Follow the written procedures \*exactly\* and it will all work". Anything that doesn't work will be traced to a failure of somebody (invariably a junior non-manager) to follow the standard properly.

Note also that in the Washington Post employment ads, "Software Engineer" is a code phrase for "Junior Programmer with a working knowledge of Ada".

No wonder things don't work.

Steve Smith Agincourt Computing sgs@grebyn.com (301) 681 7395

---

## ✂ Schipol Airport

*<hvlpb!mkenned@att.att.com>*

*Fri, 4 Oct 91 14:39 MET*

[The following article appeared recently in a Dutch newspaper, possibly "de Volkskrant." I have freely translated it into English, so please excuse any errors I have made with either the translation or with the English. Thanks!]

Scrabble on Schipol, The Letter "A" May Not Be Used Anymore

Schipol celebrated its 75th jubilee in a sober way on Thursday. The airport is busy with rebuilding and expansion, and regarded the "mess" as a cause for a celebration. A new, fifth pier is being constructed. This "E-pier" must be delivered in May.

But the E-pier will never be called the E-pier. At the same time as the opening of the new pier, all of the other piers, exits and docking locations for airplanes, are receiving new letters and numbers.

A non-trivial operation, which shall be executed overnight and cost around 2 million Dutch guilders.

The letter descriptions of the piers are being pushed up 2 places in the alphabet. The A-pier will now be called the C-pier, the B-pier D-pier, etc. The new E-pier will become the G-pier.

The descriptions are changing to avoid confusion between languages. The letter "A" in English is pronounced the same as the letter "E" in Dutch [a long "ayyy" sound]. For example, the airplane to Malaga from departure gate A12 is, in English, called up as [ayyy 12, or E2 in Dutch]. Less seasoned Dutch travellers could become completely panicked, and speed off toward the other side of the airport. "And that is a very long walk, especially as you must also come back again", says a spokesman from the airport.

If the letter A is henceforth taboo in Schipol, that does not apply for the letter B. It is true that the new pier descriptions are beginning from C, but that is being done to allow the small, future extension in front of pier C to be called B.

There is still a second reason for the roundabout and costly name changes, which must be carried out not only on all of the boards, but also in all of the computer systems. The descriptions of the exits presently consist of one [number] with two digits. Exits have, in the past decade, been regularly numbered in this way. There exists, therefore, only one exit 12, and that is on the A-pier; one 42, on the C-pier; and one 83, on the B-pier.

The number of exits and docking locations are threatening to exceed 100 with the expansion of the airport. They should then be described with a letter and three numbers.

This gives problems not only with Schipol's computer system, but it could also lead to confusion with the flight numbers, which consist of two letters and 3 numbers.

"Flights from British Airways, for example, are described with BA and 3 numbers. That can then look suspiciously like a number from the B-pier," explains the spokesman. If there is a little bit of noise in the communication line, it leads to a great confusion. This applies not only for the passengers, but also for the pilots and employees in the control-tower.

To avoid such communication failures, all number descriptions are becoming adjusted. So that Schipol, in the coming days, will never need to use a number above 100.

Peter De Graaf

=====

Note: There are a large number of obvious risks in using a system which has many potential communication faults, especially when air traffic control is involved.

One quick point is that Schipol airport will be facing the same problem again if it ever expands to include, after the H-pier, an I-pier. The letter I is pronounced in Dutch like an English E, and the Dutch interpret an English spoken I as an "ij", a Dutch "substitute" for the letter Y.

Confusing? Definitely. Solution? Perhaps using distinct names for the piers instead of letters would be the best method. I seem to recall one airport which used color coded piers, such as Red pier and Green pier, etc.

Mark Kennedy, Explorations Dept., Huizen, AT&T Network Systems Nederland  
mkenned@hvlpb.ATT.COM

[If you get to where you think you are supposed to be and find nothing, you might find Nay-Pier's Bones. X-Pier-imental evidence may lead to N-Pier-ical results, especially in Leap-Piers. PGN]

---

### **✉ Computer Mediated Ethical Discussion: An Invitation**

*Peter Danielson <danielson@unixg.ubc.ca>  
Fri, 4 Oct 91 14:18:16 PDT*

#### COMPUTER ETHICS THROUGH THICK & THIN

Computer Ethics through Thick & Thin is a three year research project funded by an Applied Ethics Strategic Grant from the Social Science and Humanities Research Council of Canada. The project will investigate the ethical potential of computer mediated communication by creating two virtual colloquia that differ in the information available to their members. The Thick group will know each other only as continuing pseudonyms; the Thin group will be able to access whatever information its members will contribute.

The two colloquia are based on e-mail in order to encourage wide membership. The groups will discuss ethical issues raised by computer technology, such as privacy and ownership and control.

For a description of the project and information about how to join either group, please contact:

Prof. Peter Danielson, Centre for Applied Ethics, University of British Columbia, 1866 Mail Mall E-165 Vancouver, B.C. Canada V6T 1Z1  
danielson@unixg.ubc.ca (604) 822 4658 FAX (604) 822 8627

---

### **✉ ACM Computer Security Day**

*Beth Olson <OLSON@ACMVM.BITNET>  
Fri, 04 Oct 91 12:33:03 EST*

STUDENT DISCOUNT AVAILABLE FOR COMPUTER SECURITY SEMINAR SERIES

The sponsors of the Computer Security Day Seminars are offering a Special Discount to Students.

The normal fee of \$195 for attendance is reduced to \$35 for students.

Each attendee will receive as part of the program three excellent books on Computer Security:

COMPUTERS UNDER ATTACK -- Edited by Peter Denning

COMPUTERS AT RISK -- Published by the National  
Research Council

COMPUTERS VIRUSES -- Published by the ADAPSO  
Computer Committee

Together with posters and a checklist of 53 Ways to Observe Computer Security, the student attending will get this entire package, excluding lunch for \$35. Call 1-800-524-4023 today to register for the seminar in the city of your choice. See the following announcement.

COMPUTER SECURITY DAY  
DECEMBER 2, 1991

Computer Security Day will focus the attention of corporate executives and computer professionals on those safeguards which are essential, considering the risk of intrusion into personal privacy and potential disasters that can cause economic and personal loss. This program will emphasize that attaining increased computer security is not only a technical matter, but a management and social issue as well.

SYMPOSIA

In preparation for Computer Security Day on December 2nd, half-day symposia will be presented in the following metropolitan areas. These symposia will provide corporate executives and computer professionals with practical information to make their installations more secure.

Tuesday, October 8	Phoenix	Sheraton Phoenix
Monday, October 21	Atlanta	Atlanta Hilton & Towers
Tuesday, October 22	Los Angeles	Los Angeles Hilton & Towers
Friday, October 25	Detroit	Novi Hilton
Tuesday, October 29	Chicago	Palmer House
Wednesday, October 30	Minneapolis	Minneapolis Metrodome Hilton
Monday, November 4	Houston	Westchase Hilton & Towers
Wednesday, November 6	Philadelphia	Univ. of Pennsylvania Faculty Club
Thursday, November 7	Boston	Back Bay Hilton
Friday, November 8	New York	New York Hilton & Towers
Friday, November 15	San Francisco Bay	Sunnyvale Hilton
Monday, November 18	Washington, DC	National Institute of Standards

and Technology (NIST)

For further information, contact: Don Nowak, Program Manager, ACM, 11 W 42nd Street, New York, NY 10036, (212) 869-7440, Extension 223 [nowak@acmvm.bitnet](mailto:nowak@acmvm.bitnet)

Sponsored By: ACM SIGSAC, ADAPSO, American Express, Computerworld, Ernst & Young

Beth Olson, ACM Local Activities, 11 West 42nd Street, New York, NY 10036  
voice: 212/869-7440; fax: 212/944-1318 [olson@acmvm.bitnet](mailto:olson@acmvm.bitnet)



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 12: Issue 45**

**Wednesday 9 October 1991**

## Contents

- [TACAS -- good news / bad news](#)  
[Martin Minow](#)  
[PGN](#)
- [Safer flying through fly-by-wire](#)  
[Henry Spencer](#)
- [Friendly \(?\) viruses](#)  
[Paul Smee](#)
- [Computers and missile control](#)  
[Walt Thode](#)
- [Re: Known plaintext attacks](#)  
[Ted Rodriguez-Bell](#)  
[Clive Feather](#)
- [Re: AT&T "Deeply Distressed"](#)  
[Steve Bellovin](#)  
[Bob Colwell](#)
- [Re: Schipol Airport](#)  
[Henry Spencer](#)
- [Re: RISKS of Highway warning signs](#)  
[K. M. Sandberg](#)  
[Joe Morris](#)  
[Dominic G. Flory](#)  
[Michael Cook](#)
- [Risks of computerized typesetting](#)  
[Paul Wallich](#)  
[Joe Smith](#)
- [Re: Ada Code Formatters \(or the dangers of old software\)](#)  
[Kent Mitchell](#)
- [Re: Computerized typesetting and character sets](#)  
[Richard S. D'Ippolito](#)
- [Info on RISKS \(comp.risks\)](#)

---

✉ **TACAS -- good news**

*Martin Minow* <[minow@ranger.enet.dec.com](mailto:minow@ranger.enet.dec.com)>

Sun, 6 Oct 91 06:31:41 PDT

From the Associated Press, via the Boston Globe, Sunday, Oct. 6, 1991, in full:

### 3-way Plane Crash Averted in Illinois.

Chicago - An error by air traffic controllers nearly caused three passenger jets to collide Thursday, the Federal Aviation Administration said Friday. A warning from one of the planes' safety systems and a quick turn by the pilot averted disaster near Midway Airport, an FAA spokesman said. The near-collision involved a Southwest Airlines Boeing 737, a Northwest Airlines DC-9, and a Midway airlines DC-9. The Midway pilot saw the Southwest plane after a warning from his plane's Traffic Alert and Collision Avoidance System, the FAA said. (AP)

Martin Minow minow@ranger.enet.dec.com

---

### **✶ Air Controllers Blast New Safety System**

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

Wed, 9 Oct 91 10:09:57 PDT

Air traffic controllers urged Congress yesterday [08 Oct 91] to suspend installation of the new Traffic Alert Collision Avoidance System in the cockpits of commercial aircraft, contending that they cause chaos in control towers. But Federal Aviation Administration officials said problems with the system -- including a tendency to warn of ``phantom" aircraft that do not exist -- either have been resolved or are near resolution. Barry Krasner, president of the national Air Traffic Controllers Association, told the House Transportation Subcommittee on Investigations that from May to September, pilots and controllers reported 590 incidents of malfunctioning involving the alarms, which are designed to warn pilots when they are on a potential collision course with another aircraft. [San Francisco Chronicle, 09 Oct 91, p.A5]

---

### **✶ Safer flying through fly-by-wire**

<henry@zoo.toronto.edu>

Tue, 8 Oct 91 01:13:27 EDT

Interesting minor item in the August 5th issue of Aviation Week:

The USAF/NASA Advanced Fighter Technology Integration test aircraft is doing flight evaluations of a system to help pilots cope with disorientation: push a button on the stick and the computer automatically brings the aircraft back to level flight.

Henry Spencer at U of Toronto Zoology utzoo!henry

[That would have done wonders for Jonathan Livingston Seagull. PGN]

---

## **✂ Friendly (?) viruses**

*Paul Smee <P.Smee@bris.ac.uk>*

*Tue, 8 Oct 1991 09:42:21 GMT*

Some years ago, a similar discussion took place in comp.sys.atari.st -- would it be sensible to write ST 'benign viruses' to 'fix' known bugs in the operating system by having them patch themselves into the system call vectors. Thankfully, we managed (I think) to convince people it was a bad idea. One very major problem, of course, is 'which version of the OS?' How do you tell the thing to stop when a bugfixed version of the OS is installed in the machine? How do you teach it the about various national versions of OSes? How do you prevent it from interacting destructively with user programs which knew about the OS bugs and contain their own workarounds?

(Of interest in many real-world situations, how do you keep it from interfering with old applications which actually rely on the bug to make them work? I know that's a bad habit, but there are a lot of businesses running old versions of OSes on old machines for precisely that reason.)

I maintained (and still do) that it is an (at least) antisocial act to cause anything to run on my machine without my knowledge, and with no action on my part to indicate that I want it. I cannot think of ANY useful piece of software of ANY sort -- even standard commands -- which does not have the potential for screwing things up amazingly in SOME contexts. The possibility that I might have to debug a machine which is running some benign monster that has snuck itself on, and that no-one asked for and no-one is aware of, is frightening -- even if it is implemented 'correctly', never mind the possibilities of error.

I am not up on the state of US law, but over here even such a 'benign virus' would be a violation of the law. I believe that 'inciting someone to break a law' is itself an offense.

---

## **✂ Computers and missile control**

*Walt Thode <thode@nprdc.navy.mil>*

*7 October 1991 1306-PDT (Monday)*

PENTAGON CONSIDERING LAY ANALYST'S PEACE PATENT

By PAIGE St. JOHN

Associated Press Writer

TRAVERSE CITY, Mich. (AP) [7Oct91] Raoul Revord's international missile control system reads so much like science fiction the patent papers include a reference to a "Star Trek" episode. But the Defense Department is listening. The Pentagon has assigned Revord's Mutual Missile Control System to a strategic weapons group for study -- making the Marquette, Mich., attorney a rare breed of lay defense analyst.

[general paragraphs about DoD unsolicited proposals omitted - wt]

Revord's patent, No. 5,046,006, lays out a plan for a central computer to control the nuclear arsenals of adversaries. Essentially, the computer gives

first-strike rights to the intended victim. And it blows up, on the spot, any missile a country tries to tamper with. "They all say they want to do away with nuclear weapons. What they need is a way to do it," he said Friday. "If they mean what they say, then all we need to do is show them a way."

Revord sent his technical document to the Defense Secretary in early September, and it was forwarded to the Undersecretary for Defense Acquisitions. That office assigned it for study, and the staff has until Oct. 25 to respond.

Pentagon spokeswoman Jan Walker said it isn't all that unusual for someone like Revord -- who lives in the remote woods of Michigan's Upper Peninsula -- to put together a nuclear defense system the Pentagon would consider. But she added that most of the ideas are not developed enough to be taken seriously. Revord, who designed corporate security systems before becoming a lawyer, said he used his security systems background to tackle the problem of nuclear war.

In 1987, he got his answer: the control computer.

When one country tries to fire its arsenal, the computer would first alert the target. Then it would wait, perhaps for 20 minutes or so, to give both sides time to back out. If the attacking country still wanted to fire, the computer instead would unlock the launch codes for the intended victim to fire first. "I focused on that, to make so devastating the penalty that it would take away the initiative to risk making the first strike," he said.

Revord had an engineer map out the schematics. The U.S. Patent Office approved the patent, but noted it somewhat resembled a "Star Trek" episode. The episode, "A Taste of Armageddon," featured weaponless wars where governments ordered the executions of their citizens when the enemy announced attacks.

Even if the Pentagon says no, Revord is proud of his peace patent. "I'll still sleep good at night," Revord said. "I've spoken how I feel."

I won't bother mentioning the obvious risks. I did like the reference to the "Star Trek" episode, although I wondered if the reference shouldn't instead have been made to an old movie that I think was titled "Colossus: The Forbin Project." In that one, the world's computers got intelligent, banded together and took control of weapons (and the rest of the world) away from humans. That's not the risk I'd worry about, but it's probably more appropriate than the one in "A Taste of Armageddon."

Walt Thode thode@nprdc.navy.mil {everywhere\_else}!ucsd!nprdc!thode

---

### **🚩 Re: Known plaintext attacks ([RISKS-12.43](#))**

*Ted Rodriguez-Bell <ted@goldberry.uchicago.edu>*

*Tue, 8 Oct 91 16:04:23 CDT*

In [Risks Digest 12.43](#), D.W. Roberts quotes the London Daily Telegraph:  
>[A known plaintext attack] helped the Americans to win the Battle of Midway in  
>1942. An American base radioed falsely that its water supplies had broken  
>down. The Japanese then reported the message in a cipher. The Americans  
>simply compared the two texts and learned to read secret enemy traffic.

It was more complicated than that. The U. S. Navy was reading the Japanese code all along. They got the battle plans for an attack on a location like Point PH. They knew that the location was based on a map grid, but they

weren't sure that the grid point was actually Midway. The island's garrison sent a message in the clear that their fresh water generator had failed; it was duly intercepted up by the Japanese and reported back to headquarters. It was the fact that the code was already being read that allowed American cryptanalysts to attach a meaning to Point PH. There was a big difference between breaking JN-25 and confirming that those two letters meant Midway Island. I would not be surprised if the practical difficulties of cracking DES have been similarly understated.

This is not to say that all known plaintext attacks don't work. Towards the end of World War I, Allied intercept services were able to read messages in the German Army's low-level code quite easily; guessing the messages was one of the ways they got in. The code was changed at midnight every night, and some radio operator would invariably send out test messages containing proverbs like "The early bird gets the worm." There was also usually someone who didn't get the new code, and so a few messages would be repeated verbatim in the old (solved) one. More examples can be found from my source for these: David Kahn's fascinating and thorough [\\_The\\_Codebreakers\\_](#).

[ You may want to delete this to save space. ]

On the topic of the Battle of Midway, only marvelous luck got the Japanese battle plans read. The Japanese had planned to change to a new version of their code on April first. A submarine that was transporting new codebooks ran aground and was sunk; the newly distributed books were recalled and a new set had to be printed. That was supposed to go into effect on May first. The effective date was postponed until June first because the new codebooks could not be distributed on time. The change did take effect on June first, but by that time the plans were laid and the ships were at sea. The attack on Pearl Harbor could not have been detected the same way. The ships involved were docked when plans were being formulated, and communications were done by telegraph.

Ted Rodriguez-Bell, U. of Chicago Astronomy [ted@borgil.uchicago.edu](mailto:ted@borgil.uchicago.edu)

---

**✂ Re: Demise of DES (Roberts, [RISKS-12.44](#))**

*Clive Feather <clive@x.co.uk>  
Tue, 8 Oct 91 7:43:50 BST*

Dave Roberts <dwr@datasci.co.uk>, quoting the Daily Telegraph, says:

| [A known plaintext attack] helped the Americans to win the Battle of Midway  
| in 1942. An American base radioed falsely that its water supplies had broken  
| down. The Japanese then reported the message in a cipher. The Americans  
| simply compared the two texts and learned to read secret enemy traffic.

This is not what happened. At this point, the cipher had been mostly broken. However, map references were enciphered in a separate system, and then inserted into the message, and the cryptanalysts had not completely broken the map system. In particular, they did not know where AJ was, and they did not know the coordinates of Midway. They decided not to take the risk of assuming

the one was the other, but to get the Japanese to confirm it !

Instructions were sent (in cipher) to the base at Midway, telling them to radio in clear [unenciphered] a message stating that their desalination plant was out of order. A few days later, a deciphered Japanese message stated that "AJ is short of water". [Source: Kahn - The Codebreakers]

Clive D.W. Feather | IXI Limited  
clive@x.co.uk | 62-74 Burleigh St.  
Phone: +44 223 462 131 | Cambridge CB1 10J  
(USA: 1 800 XDESK 57) | United Kingdom

---

**✉ Re: AT&T "Deeply Distressed" (Colwell, [RISKS-12.43](#))**

<smb@ulysses.att.com>  
Tue, 08 Oct 91 13:25:19 EDT

It's clear that the human component of the AT&T outage was what caused the outage. That's the link that needs more attention in the engineering and in the analysis of failure.

Yes. Yes, but. Many of the problems we discuss on RISKS are caused by attempts to engineer humans out of the loop. People make mistakes, get bored, get distracted, panic, etc. Machines don't have any of those failings. So we build an automated system that doesn't have any of those problems -- except that it was built by people who make mistakes, get bored, etc.

It's not hard for me to envision a scenario a few years hence where some long distance network melts down (please, I hope it's not AT&T's again...) because someone misplaced a "break" statement in the automatic warning system that was intended to check the power alarms. And the human backup checks won't be meaningful because no one will really look very hard; after all, the computer is doing the real job, and probably getting it right most of the time. We've discussed this many times, especially in the context of fly-by-wire systems, but it's a universal problem. Not that I know what to do about it -- we can't build automated systems that are reliable enough (and flexible enough) that we can dispense with people, we can't build systems that use humans as a backup because that doesn't work, and we don't want to rely on purely manual systems because of the mistakes that the operators make....

--Steve Bellovin

---

**✉ AT&T "Deeply Distressed" ([RISKS-12.43](#))**

<colwell@ichips.intel.com>  
Tue, 8 Oct 91 10:51:34 -0700

Yes, I agree, it's possible to err on the other side, and (arguably) it may even be worse to do that. This seems equivalent to the question of how much override a pilot of a fly-by-computer airplane should be able to exert; when the flight computer refuses to pull too many G's because the wings may overstress, but the pilot knows he'll hit a mountain otherwise, it's a bit

clearer who should outrank whom.

It just struck me that the AT&T exec might have been exhibiting an attitude that worries me a lot -- "doggone humans, there they go again screwing up our system, where do we get these people, ah well, back to business." That attitude won't result in a better system.

Phones are phones, that's mostly just lost money for somebody (save 9-1-1, but still the danger to the population is restricted). It's the nuclear reactors and chemical plants that worry me. Maybe we should start a research colloquium entitled "How To Design Very Dependable Systems With Wacko Humans In The Loop."

Bob Colwell colwell@ichips.intel.com 503-696-4550  
Intel Corp. JF1-19 5200 NE Elam Young Parkway Hillsboro, Oregon 97124

PS. I worked at BTL for a few years, and I know a little about the system reliability goals and their previous track record. Remember the old TelCo saw that "the most reliable switcher is tended by a man and a dog; the man is there to feed the dog, and the dog is there to keep the man away from the equipment." Is it my imagination, or have the risks increased that a common-mode failure in the ESS software will take down an entire network, and very quickly at that? Bell Labs used to worry a lot about how to design a switcher to meet certain availability goals; it seems to me a qualitatively different endeavor to design switcher software to meet certain \*network\* availability goals. Is Bell approaching it that way?

---

### ✉ Re: Schipol Airport

<henry@zoo.toronto.edu>  
Tue, 8 Oct 91 14:08:01 EDT

> Confusing? Definitely. Solution? Perhaps using distinct names for  
>the piers instead of letters would be the best method. I seem to recall  
>one airport which used color coded piers, such as Red pier and Green pier...

One has to avoid getting carried away with the possibilities of colors, however, bearing in mind that some modest fraction of the population is partially color-blind. For example, however tempting it might be to save space on monitors by just using color monitors and coloring the symbols, it really is necessary to spell out the names.

There is also some potential for humans to interpret the color in their minds and confuse it with a similar color, even if the colors are used only as names and there is no actual use of color-coding. This isn't much of an issue for red and green, but when you start getting beyond the first half-dozen colors it may become a problem.

Henry Spencer at U of Toronto Zoology utzoo!henry

---

### ✉ Re: RISKS of Highway warning signs ([RISKS-12.44](#))

*K. M. Sandberg <kemasa@ipld01.hac.com>*

*8 Oct 91 19:42:55 GMT*

The accident in no way, IMHO, was caused because of the signs. The simple fact is the truck driver was not paying attention and was the cause (based on what was said above). The cars could have been stopped for many reasons other than the bridge, like an accident, road block to pull objects from the road or anything else. The sign helps to warn those not paying attention, but it does not or should not allow people to not pay attention. I have seen cars stuck in the road with no lights on, no emergency flashers or anything in the dark, but that does not mean that I bear no responsibility if I should hit them as I should be looking for object in my path. Be warned, objects stop without notice sometimes.

>The obvious fix here is that if the signs are broken or not notified in  
>time, the bridge should not be allowed to raise.

> J.B.Hofmann

The obvious fix is for \*people\* to pay attention, not to add an more and more "fail-safe" systems. Otherwise how about a radio transmitter to disable all normal (non-emergency) vehicles to kill the ignition on any cars in an area where an accident has occurred? It would prevent any additional accidents and save lives. :-)

Kemasa.

---

### ***✂* RISKS of Highway warning signs (Hofmann, [RISKS 12.44](#))**

*Joe Morris <jcmorris@mwunix.mitre.org>*

*Tue, 08 Oct 91 14:03:24 -0400*

In [RISKS-12.44](#), Jim Hofmann reports on a highway accident on the Woodrow Wilson bridge in which warning signs were not activated to tell drivers that the bridge was being raised, and Peter Neumann added some notes from news reports. A couple of points seem to have been missed...

(1) The bridge is located in a cusp of political jurisdictions. One end of the bridge is in Virginia, the other is in Maryland, and just for fun, the District of Columbia is responsible for the bridge itself. Can you say "finger pointing"? I thought so.

(2) According to news reports (and I have no other source of info on this) all of the signs on the approaches to the bridge are controlled from a central site in Virginia. This includes the signs on the Maryland side; the accident occured in the Maryland-to-Virginia lanes. The Virginia center normally closes at 9:30 PM (daily?) but the staff there says that they will stay on duty until after midnight if they have been notified that the bridge will be opened. The signs themselves are just text messages -- if there are any flashing lights or such to draw attention to them I haven't seen them.

(3) The bridge is part of the Washington Beltway, which itself is part of Interstate 95...an Interstate highway with a drawbridge. Since the

traffic in this area is difficult to describe without using words which would be unacceptable to Miss Manners, it takes little imagination to see that bridge openings for any reason -- commercial freighters or pleasure craft -- are not appreciated. Thus there are significant restrictions on when the bridge will be opened which weren't in place when the bridge was built (many years ago) or when the sign system was designed (somewhat more recently).

Part of the problem, of course, is having a drawbridge on an Interstate highway, especially one which is a major north-south corridor for trucks. That's hardly a computer RISK.

The other part is the all-too-familiar problem of changing part of a system without realizing that other parts of the system are affected. In this case, the severe restrictions on bridge openings (more severe on pleasure craft than on commercial freighters) makes the late-night openings more likely, but the control of the signs was left in the hands of a facility that normally closes in the evening.

The signs in question, incidentally, are located some ways back from the bridge, so that if you see that the bridge will be open you've got a chance to get off at the last exit before the bridge. There's been no indication or any malfunction (or nonfunction) of the overhead flashing lights (about 1/4 mi (?) before the traffic gates) or the gates and red lights at the draw itself; these are directly controlled by the bridge tender and for years were the only warning devices.

Joe Morris

---

**✂ Re: RISKS of Highway warning signs**

*<dusty.henr801e@xerox.com>*

*Tue, 8 Oct 1991 12:28:28 PDT*

<< The implication is that had there been no signs, the driver might have been more cautious. But since there WAS a sign and it was not flashing a warning signal, the driver did not slow down.>>

The was no risk here because the signs weren't working. The risk was the truck driver obviously driving recklessly. There's too much of a tendency to blame something or someone else when things happen. Bottom line is, if the trucker had been driving safely, the accident WOULD NOT HAVE HAPPENED, sign or no sign.

dusty flory

---

**✂ RE: RISKS of Highway warning signs**

*"GVA::MLC" <mlc%gva.decnet@consrt.rockwell.com>*

*8 Oct 91 12:58:00 PST*

Here in Cedar Rapids, Iowa, interstate highway I-380 passes through the downtown area. The highway has a large "S" turn in it to avoid tall buildings

that already existed when the highway was built. During the winter months, snow and ice on the highway cause accidents occasionally as drivers drive faster than conditions allow. A few years ago, it was proposed to install electrically illuminated signs over the roadway that would warn when "icy conditions may exist".

As I remember, there were discussions about who would be liable when a car had an accident in bad weather when the sign was off. The interstate is a federal highway, but running through a municipality. The wording of the sign itself was discussed. Who would be responsible for determining when the sign was turned on? What if the sign were turned on, but didn't illuminate properly? What if an accident occurred due to icy conditions, but not on the portion of the highway that was regulated by the sign?

The sign is in place. I have seen it illuminated at times. But I'm not sure how the liability issues were resolved. As far as I know, there have been no lawsuits (yet) regarding accidents on that portion of the interstate highway. At least some front-end thinking did take place.

And of course, in many locations there will be permanent signs that are obscured in one way or another, whose visibility or lack there-of will play a part in an accident.

Michael Cook Internet: MLC%GVA.DECNET@CONSRT.ROCKWELL.COM

---

### **✶ Risks of computerized typesetting**

*Paul Wallich <well!pwallich@fernwood.UUCP>*

*Thu, 3 Oct 91 15:13:14 pdt*

Fonts with slightly different characters are a subtle problem, but there are more egregious risks of computer typesetting as well. Excerpts from a memo follow:

"Please be advised we have experienced system related software problems with Quark Xpress during the November issue . . . We are reinstalling software ... this may cause some articles/departments to reflow from the current proofs..."

Translated, that means that lines will break differently on the printed page than on the screen. If you're lucky, you end up short; otherwise the last few lines of an article vanish mysteriously. It may be possible to catch this on real proofs, but for a magazine (or, even worse, newspaper) just catching it is not enough, as there may be no way to fix the problem in the time remaining before press date.

---

### **✶ Re: Risks of computerized typesetting**

*Joe Smith <jms@tardis.Tymnet.COM>*

*Thu, 3 Oct 91 18:16:56 PDT*

In regards to having backquotes (`) come out the same as apostrophe ('), I have

been consistently confounded by the Courier font built into the Postscript cartridge of the HP LaserJet printer. The two characters do show up as to distinct glyphs, but only under a magnifying glass. They both tilted about 30 degrees clockwise of vertical. The only difference is that the apostrophe is 10% thicker at the top, and the backquote is 10% thicker at the bottom.

I fear that this set of indistinguishable characters is the standard straight from Adobe.

Joe Smith (408)922-6220, BTNA Tech Services TYMNET, PO Box 49019, MS-C51  
San Jose, CA 95161-9019 SMTP: jms@tardis.tymnet.com

---

**✉ Re: Ada Code Formatters (or the dangers of old software) ([RISKS-12.41](#))**

"Kent Mitchell" <KDM@rational.com>

*Fri, 4 Oct 91 08:40:15 CDT*

I read with interest the report in [RISKS-12.41](#) on the risk of Ada pretty-printers.

While this unfortunate mis-formatting did happen in an older release, the Rational Environment Ada editor has not exhibited this behavior for some time. The Environment now (for the past three releases I could test under) correctly flags this as a syntax error.

Perhaps the real risk here is using old, out of date software. Like any software company we occasionally have bugs in our software and produce periodic releases to address them. We cannot, however, make people upgrade to these new releases.

I sympathize the the amount of debugging effort this behavior may have caused Mr. Hash, but it is comforting to note that some risks are dealt with more easily than others.

Kent Mitchell, Rational Technical Representative, kdm@rational.com

---

**✉ Re: Computerized typesetting and character sets**

<rsd@SEI.CMU.EDU>

*Fri, 04 Oct 91 19:44:44 EDT*

Well, gentle readers -- there's another risk here! The character that appears in my last name (when I can coax programmers to do it right -- it took the IEEE, of all organizations, several years to replace the spaces and commas with the correct character) is NOT a quote, forward, backward, north, south, single, double or any direction or quantity you choose -- it's an apostrophe! Its use as a special character in computer programs has caused me a lot of grief!

We have a library system here at CMU where my publications can't be found due the non-acceptance of the apostrophe. The response from the library manager was, "Sorry, that's the way the software is, and it's not a high priority."

Folks with names like mine also tend to disappear from phone lists, and, when we appear at all, appear incorrectly alphabetized. For some reason, the local Bell phone company always gets it right in the directory, though the CMU people don't. Maybe Bell directory printers never use "C"!

Additionally, the use of fonts whose capital "I"s have no serifs and look like lower-case "l"s (like the one you're reading this with?) are another source of confusion.

My guess is that the author of the subject programming language and operating system had a very simple name like..."Richie". >Sigh< It's almost enough to make me wish I were a number!

Richard S. D'Ippolito

rsd@sei.cmu.edu

[ZIPPO! You ARE a number!

And then there were the old Multics days when Corby (see the September 91 CACM) had the string `` Corbato[backspace]' ' for his account name, to get the overstruck character out of Multics' innovative character-position canonical form that permitted arbitrary overstrikes! 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 12: Issue 46

Thursday 10 October 1991

## Contents

- [Encryption Exportability \(Clark Weissman\)](#)  
from ``Inside Risks''
- [Security Criteria, Evaluation and the International Environment](#)  
Steve Lipner
- [Info on RISKS \(comp.risks\)](#)

---

### ✂ Encryption Exportability, by Clark Weissman

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Thu, 10 Oct 91 08:01:02 PDT

``Inside Risks'', Comm. ACM, vol 34, no 10, October 1991, page 162

A NATIONAL DEBATE ON ENCRYPTION EXPORTABILITY

Clark Weissman ([clark@NISD.CAM.UNISYS.COM](mailto:clark@NISD.CAM.UNISYS.COM))

Traditionally, cryptography has been an exclusively military technology controlled by the National Security Agency (NSA). Therefore, U.S. International Traffic in Arms Regulations (ITARs) require licenses for all export of modern cryptographic methods. Some methods, such as the Data Encryption Standard (DES), are easily obtained for export to the Coordinating Committee for Multilateral Export Controls (COCOM) countries, but not Soviet block countries, or most third world nations.

The recent National Research Council (NRC) report, ``Computers At Risk'' [1] describes advances in computer security uses for cryptography beyond traditional COMSEC (communications security) applications of secure text encoding. These permit business to be conducted over the network and include identification and authentication ``signatures," permission credentials transactions, registration and notarizing by third parties, unforgeable integrity checksums, ``indelible" date/time stamp, non-repudiation of message receipt, and electronic money. These new applications make cryptography a ``dual use" technology for both civilian and military users. Encryption is used in the civil sector for international banking, electronic information exchange,

electronic mail, machine safety, and internetwork commerce. It is the separation of secrecy and authentication encryption that underlies the dual use argument. This separation was made explicit in public key cryptosystems.

Industry needs cryptography for vitality and growth, which must be international in scope to address common encryption algorithms, encryption applications, key management and distribution methods irrespective of national boundaries. However, most governments have policies to restrict public access to encryption services in telecommunications. U.S. export controls constrain domestic and international growth of encryption services. Our international trading partners have less severe export restrictions.

The U.S. finds itself in a dilemma: harm our economic growth and competitiveness in the expanding world internet products and services industries if we prohibit cryptographic applications, or permit such cryptographic export and potentially weaken military security by providing new encryption capabilities to our adversaries. In both cases U.S. National Security is at issue as noted in two other NRC studies [2,3]. These reports define the agenda and technical foundations for a major encryption policy debate, while there is still time to influence the market place. We risk diminution of our U.S. role in the advancing world market for telecommunications at worst, and lost opportunity to lead the international democratic societies in establishing standard, quality, privacy telecommunication services world wide, at best.

The debate is international in applicability. However, U.S. policy on encryption appears most severe, so I urge a U.S. National debate to begin the dialog, and start with some questions. Do we gain more by strengthening our commercial competitiveness and products, upon which the military is increasingly dependent, than we lose by permitting international commonality in cryptographic services, which may weaken military capabilities? Who should debate, Congress, DOD, NSA, NIST, National Security Council, public and private agencies, and industry? Can National Security issues be given a fair hearing if the technical and political facts are classified? Will public confidence be raised or weakened by such debate? The proposed Senate bill S.266 required U.S. cryptographic equipment include government "trapdoors" which lessened public confidence. Earlier fears of weakness of the DES have diminished because continuing study and dialog suggest the DES to be free of trapdoors [4]. One practical solution by a vendor for product export license used strong encryption for authentication and weak encryption for secrecy. Is this an acceptable compromise solution out of the dual use dilemma?

Western democracies have been strengthened by debate on significant issues of public policy. Encryption policy should likewise be debated in the era of a new world order.

#### REFERENCES:

1. National Research Council (NRC), 1991. Computers at Risk: Safe Computing In the Information Age. Computer Science and Telecommunications Board (CSTB), National Academy Press, Washington, D.C.
2. NRC, 1991. Finding Common Ground: U.S. Export Controls in a Changed Global Environment. CSTB...

3. NRC, 1988. Global Trends in Computer Technology and Their Impact on Export Control. CSTB...

4. Denning, D.E. The Data Encryption Standard: Fifteen Years of Public Scrutiny. Dist. Lecture, 6th Ann. Comp. Security Appl. Conf., IEEE Comp. Soc. Press 1990, pp. x-xv.

Clark Weissman is Director of Secure Networks for Unisys Defense Systems, Inc. His career has included advances in security penetrations analysis, virtual machine OS, DBMS, and networks, on such projects as KVM, BLACKER, and DNSIX LANs. He has served on many industry, government, and professional security panels.

---

## **✂ Security Criteria, Evaluation and the International Environment**

*Steven B. Lipner <lipner@ultra.enet.dec.com>  
Wed, 9 Oct 91 06:23:57 PDT*

The following message contains the text of a paper that I gave as the keynote address at IFIP-SEC '91, the annual conference of IFIP TC11, Security and Privacy. The conference was held in Brighton, England, May 1991.

The paper addresses the status and prospects of the "trusted systems" evaluation process in the US, and its relationship to evaluation process developments in Europe and elsewhere. Briefly, I conclude that the current process in the US is not really serving the needs of vendors, users, or security authorities, and that the European ITSEC is not much of an improvement. I also give some suggestions for an improved process, probably not as clearly articulated as if I were rewriting the paper today.

At last week's National Computer Security Conference, I ran into quite a few people who seemed interested in the paper but who hadn't seen it. The conference proceedings are available, but perhaps a little obscure. I think that it would be of interest to the RISKS audience.

=====

Criteria, Evaluation and the International Environment:  
where have we been, where are we going?

Steven B. Lipner  
Digital Equipment Corporation  
Littleton, Massachusetts, USA

### **INTRODUCTION**

This paper presents a few observations on trusted system evaluation criteria. It begins with a summary of the history of the U.S. criteria and the current state of the European criteria. It then discusses the impact of criteria on the vendors and users of commercial computer systems. After suggesting some guidelines for the developers of new criteria, it goes on to

suggest a new direction that may better serve the purposes of vendor and user communities, though at the price of abandoning some long-held beliefs.

I should stress at the outset that this paper deals only with commercial computer systems and commercial applications (and with civil government computer applications that are indistinguishable from commercial ones). Defense and national security applications have their own unique attributes -- particularly the need to deal with labelled or classified information. After more than ten years of looking, I am convinced that the unique attributes having to do with labelled information are not required in the commercial and civil sector.

I would also offer the caveat that this paper reflects about twenty years of experience in computer security, the last ten gained while working in the employ of a commercial computer manufacturer. While it reflects early experience as a defense security researcher and many discussions with security evaluators, researchers, criteria developers, and most of all, would-be users of secure systems, it is clearly written from a vendor perspective and should be read in that light.

#### THE EVOLUTION OF EVALUATION

About ten years ago, the United States Department of Defense issued the directive establishing the Department of Defense Computer Security Center. The primary role of the Center was to establish and operate a program that would evaluate the security properties of commercial computer vendors' products. The theory underlying the Center was that commercial and defense users of computer security products had common needs, and that by evaluating commercial products, the Center would improve the security available both to the defense and commercial users.

The Center began its task by drafting, coordinating, and publishing the Trusted Computer System Evaluation Criteria (TCSEC, or Orange Book). The TCSEC was published in 1983, and specifies a range of security evaluation classes that apply to operating systems. By 1986 the Center -- now renamed the National Computer Security Center (NCSC) and with scope encompassing the entire U.S. Federal Government -- had evaluated a handful of commercial operating systems. As we meet, the NCSC's charter has been reduced to the needs of U.S. government agencies that process defense classified information, and a few dozen operating systems have been evaluated.

While the NCSC has undergone its decade-long evolution, the rest of the world has not stood still. U.S. legislation has given the U.S. National Institute for Standards and Technology (NIST) the dominant role in setting security standards for civil government and, by implication, the private sector. NIST has not been granted resources consistent with this responsibility. Recently NIST and NCSC have stated that they will work together "to create a new federal computer security criteria document" that can be applied across the entire U.S. government, including civil and defense sectors.

A potentially more significant development is that the governments of the U.K., Germany, France and the Netherlands have begun joint development of the

Information Technology Security Evaluation Criteria (ITSEC). The European developers of the ITSEC have begun trial use of the draft, and the European Community has begun the process of establishing EC-wide security criteria based on the ITSEC. The governments of Canada, Australia, and Sweden have also expressed, to varying levels, the intent to develop their own information security criteria. NIST is representing the U.S. government in discussions with the ITSEC developers and EC of common evaluation criteria and processes.

#### LIVING WITH THE TCSEC -- THE VENDOR'S VIEW

Almost every U.S. manufacturer of computer systems has completed at least one evaluation of a Class C2 operating system. C2 systems are the workhorses of commercial computing. They incorporate user identification and authentication mechanisms, auditing, discretionary access controls, and controls over storage residues. They are tested to insure that the controls work "as advertised". They are thus well-suited to the vast majority of commercial multiuser applications. While the TCSEC is widely condemned as applicable only to protection of data from unauthorized disclosure, a C2 operating system provides basic mechanisms that can be used to enforce a level of data integrity as well. Some users require features beyond those required by Class C2 (such as more controls over the passwords used for authentication) and these are frequently added by vendors. Other users DO NOT require some of the features mandated by Class C2, but those unnecessary features can be "turned off" by system administrators. On the whole, C2 is a good common demoninator.

The "goodness" of C2 systems, however is marred by two deficiencies that are especially visible to the vendor: First, no one can tell what a C2 system is; and second, by the time a C2 system is developed and evaluated, it is obsolete. I will spend the next few paragraphs amplifying on these deficiencies.

At first blush, it appears easy to tell what is in a C2 system -- I summarized such a system two paragraphs above. An early senior manager of the NCSC once observed to me that developers of systems up through class B1 should almost be able to self-evaluate -- to tell whether they had met the requirements by comparing their system to the criteria. Unfortunately, any development manager who has taken a system through the NCSC process knows better. Developers and "evaluators" go through seemingly endless disputes:

- o Is interprocess communication an "object" requiring access controls and auditing?
- o How is it that self group/public access controls for one system meet the C2 criteria while those for another do not?
- o Is the system's internal design documentation (not required at all by the Orange Book) adequate so that the "evaluators" can tell that all of the relevant tests have been developed and objects controlled?

The answers to such questions are not found in the TCSEC. They are defined in

a set of "interpretations" of the TCSEC maintained by the "evaluators". Because the interpretation process is often triggered by proprietary aspects of vendors' products, the total set of "interpretations" is not visible outside of the NCSC. As new vendor issues arise, however, new "interpretations" are added and cumulatively imposed on future evaluations of all vendors' products. Since every system is different, there are plentiful issues that require new "interpretations". U.S. vendors refer to this phenomenon as "criteria creep". It has the effect that a 1986 C2 system is NOT the same as a 1990 C2 system, and that no one can tell what a 1992 C2 system will be.

The problem of obsolescence results from the evaluation process. The vendor negotiates with the NCSC what C2 means for his system, and eventually gets all of the required features, security tests, and design documentation incorporated in a version. When the version goes to customer field test, the NCSC begins its formal evaluation process -- a final review of the documentation, running independent tests and so forth. The NCSC process takes time, and it is likely that by the conclusion of that process, the vendor is shipping the version that succeeds the one under evaluation. Pressures on vendors are to get releases out more often, while the pressures on the NCSC are to do a more thorough job of evaluating. Hence, obsolete evaluated versions.

The NCSC has developed a "Rating Maintenance Program" or RAMP that is intended to allow vendors to self-evaluate future versions subject to NCSC review and audit once one version has been evaluated by the NCSC. This process requires the vendor to apply the Class B2 requirements for configuration management (as "interpreted") to systems in classes C2 and B1. These requirements impose on the vendor's development process an overlay of paperwork, checking, bureaucracy and mistrust. For those of you familiar with the U.S. Defense "procurement scandals", it is the paperwork, checking, bureaucracy and mistrust associated with configuration management over all aspects of a development process that makes for \$800 hammers and the like. There is considerable resistance to RAMP as specified in the U.S. vendor community.

## LIVING WITH THE TCSEC -- THE USER'S VIEW

### REAL ENVIRONMENTS

The TCSEC states security requirements for multi-user computer operating systems -- in effect, for monolithic time-sharing systems. My employer is putting substantial resources into the development of an updated version of its proprietary operating system that will meet the Orange Book criteria for Class C2 and B1. I can, however, state with high confidence that no user will operate that system in its evaluated configuration. The reason for my confidence is that TCSEC evaluations exclude general networking facilities, while essentially all "real" computers are installed in networks. Users will buy the system, install it, and set the controls as best they can. We will document our judgment on the security of systems in networks, in the part of the system security manual that is "outside" the C2 evaluation.

The NCSC has issued a "trusted network" interpretation (TNI) of the Orange Book. It sets forth criteria for networks of systems designed, built, installed and managed as though they were a single time-sharing system.

However, real users proceed by buying a computer, hooking it up, using it, then adding a second computer, wiring it up to the first, adding a third and so on. At some point, they connect to the Internet, to a world-wide public network or both. The TNI is not comprehensible, much less helpful, to such users.

#### REAL APPLICATIONS

A second concern with the TCSEC deals with applications. When I log into the NCSC's system (through a network!) I use it in a "B2" way. I have an account, I send and receive mail, I access files in various sensitivity classes. However, many computer systems are dominated by large data bases and large applications that work "across" users. The users may never see the files and applications program at the base of the Orange Book paradigm. Furthermore, the sharing of information may be controlled by data base systems or applications -- not just the operating system. In such a configuration -- common in the commercial world -- one installs the application with "privilege" to override the operating system controls, and the evaluated product becomes irrelevant. The hard-earned NCSC evaluation is invalidated by the addition of privileged ("trusted") software that was not part of the configuration evaluated by the NCSC.

The NCSC is developing a "data base interpretation" of the TCSEC. Time will tell whether it meets the needs of real secure data base systems. It is clear in any case that end users and software houses need more guidance on the development of secure applications than criteria have yet provided.

#### REAL SYSTEM MANAGEMENT

In my work, I have occasionally encountered a user who has experienced a security penetration despite using an evaluated system. The common denominator among such incidents is system configuration and management: the user attempts to install the secure system in his environment, and "gets something wrong" that allows a hostile party to go where he shouldn't be. The trusted system evaluation is irrelevant because the user is doing something he should not -- operating in a network or running an application -- to get the job done.

Vendors try to document real-world ways of using systems securely. They offer tools to help users with this task. When an unexpected problem arises, the vendors learn from it and update their tools and documentation. Real systems used in real applications are complex, and evaluations are not a substitute for experience.

The U.S. evaluation process (the only one where we have a rich experience over time) may actually have evolved into an obstacle to security in the area of system management. As the U.S. evaluators insist that more of the objects (containers that hold information) in a computer system be subject to more controls, the security management documents get thicker and thicker. Developers, writers, and system managers are faced with the challenge of designing, documenting, and finding secure ways of using the systems in the face of a forest of controls and auditing options of interest only to the evaluators.

## ARE THERE ANY BENEFITS?

The paragraphs above paint a fairly bleak picture of the NCSC and Orange Book. The question naturally arises "why bother"? Why do vendors continue to have systems evaluated, and what is the benefit to users?

The first answer to the question "why bother" is that even in the world of distributed networks and real applications, operating system security is often fundamental to system security. A C2 operating system does have a cohesive set of controls on which a user can build. For a few applications, one installs the system, configures the controls, and goes. More often one must do design, integration, and adaptation. Regardless, the C2 controls are a useful foundation.

The second answer is that many public procurements have mandated evaluated systems, and more are likely to do so in the future. Thus vendors have little choice but to develop (at least C2 and B1) evaluated systems. The fact that the NCSC has thus dominated the domain of discourse about secure systems bespeaks a significant accomplishment, though potentially at the price of foreclosing other options. For some organizations, if the answer can't be expressed as an evaluated system, it can't be expressed -- although the real world is usually much more complex than the domain of the TCSEC.

The third answer is that the NCSC process has been fair in a competitive sense. If the criteria change over time, they are applied fairly at any point in time. The vendors know that they will get an unbiased (though painful) evaluation, while users know that they can use the evaluation class as part of a fair competitive procurement.

These three attributes -- basic security, a wide base of application, and a fair process -- bespeak significant accomplishments. Future criteria writers and evaluators should strive to do as well.

## EVOLVING EVALUATION

When I began to draft this paper, I thought briefly of including some high-level observations on the ITSEC and Canadian CTCPEC. I decided not to do so, because I felt I would be shooting at a "moving target" -- by the time I delivered the paper, the criteria in question would likely have been revised and my comments would have become moot. I will try instead to offer a few "timeless" guidelines based largely on real-world experience with the ITSEC and NCSC.

## THE WORLD MARKET

My first comment, then, is that that the computer industry is global and evaluations should likewise be global. The NCSC probably contributed in some measure to the development of the ITSEC by excluding non-US vendors from TCSEC evaluations. Happily, the European evaluators have not chosen to reciprocate by excluding U.S. vendors. However, the development of a set of criteria different from the TCSEC would appear to impose a sufficient obstacle -- especially if ITSEC evaluations are as costly and painful for the vendor as

those under the TCSEC.

Some have proposed a "feature mapping" scheme that would compare criteria by breaking them down into their finest elements. This scheme is likely to be time-consuming and ineffective, if it is feasible at all. A more sensible approach is for criteria developers to agree -- if not on criteria, at least on those classes that are comparable. It should not be necessary for a product to undergo more than one evaluation worldwide -- at least at classes up through B1 that are not used to protect the most sensitive defense information and that are most interesting commercially.

#### AMBIGUITY

The discussion above of the TCSEC and NCSC made it clear that the descriptions in the TCSEC are not sufficiently explicit. I acknowledge to my chagrin that I was a reviewer of the TCSEC drafts and was as stunned as anyone when "interpretations" started to roll in. My surprise was all the greater since the TCSEC was subject to extensive public review and comment during development, while the "interpretation" process is almost completely conducted behind closed doors.

If criteria or standards are intended as mandatory guidance for procurements, they should be very explicit about what features are required, where they must be applied, and what assurances must be provided. The first draft ITSEC was relatively precise about assurance of correctness (though see the next section), but the effectiveness and functionality criteria in the ITSEC, and the functionality criteria in the second draft CTCPEC shared with the TCSEC significant ambiguity. Experience teaches us that we must do better.

One might ask "why set feature requirements at all"? The ITSEC answered this question by allowing the sponsor to specify arbitrary security features. The answer to this question goes back to one of the benefits of the TCSEC -- a fair and competitive process. If vendors may or must go off completely on their own in selecting security feature sets, competitive procurement will likely suffer as procuring organizations find themselves unable to find any set of security features common to two or more competing vendors. Instead, criteria should be very explicit about the core set of security features required, and allow vendors to "add value" by offering additional security features and functions.

#### ADAPTABLE PROCESS

In today's computer industry, there is immense pressure to deliver products faster, with more features and better performance. This pressure is at odds with the sorts of rigid development processes proposed in the first draft ITSEC and the NCSC's RAMP.

Development processes for secure commercial products should be consistent with the real commercial development environment. They should not attempt to make computer systems into \$800 hammers, nor should they impose an atmosphere of mistrust on the development process.

This is not to say that vendors should be allowed to "get away with anything". They should not. But evaluation processes should take into account differences among vendors, the need to repair flaws, and the likely impossibility of preventing them totally. They should also allow for process improvement -- a key ingredient in the quest for improved product quality that will yield better security.

#### STABILITY

Many of the difficulties with the TCSEC result from the fact that it was not tested until after it had been promulgated. Future criteria should be used on real (not toy) systems in substantially final form before they are made authoritative.

#### NEW DIRECTIONS

The suggestions above can guide the development of more useful criteria for the evaluation of secure operating systems. Diligently applied, they might reduce the cost and increase the timeliness of developing secure operating system products. They do not, however, "solve the problem" of computer security.

Documents such as criteria or standards that are to meet the needs of users and of the custodians of data that require protection must support the development and installation of real systems. This is a daunting challenge. What can we say about heterogeneous networks? about data bases? about real-time systems and commercial applications? Stories abound in the United States of officials from the NCSC visiting banks, offering them copies of the TCSEC and saying "this is the answer to your security problems". Needless to say, no banker believed that assertion once he had examined the TCSEC, though most banks DO use systems that have been evaluated in Class C2.

Criteria for secure time-sharing systems will not "make it" in the nineties, but it is not clear that we know enough to write evaluation criteria for networks, data bases or applications. The ITSEC specifies measures for assurance and allow arbitrary functionality; the total composition of the secure system can be up to the end user. However, it seems that few end users would be rich or sophisticated enough to apply the costly ITSEC assurance measures to a unique application system.

What then to do? I suggest that we should stabilize criteria as a way of evaluating operating system security, and concentrate on removing the blatant silliness and unpredictability that have crept into the NCSC process. We do not know enough to have criteria for everything, and we shouldn't try.

Instead, write guidelines for products and practices "outside" the operating system that embody what we do know and think we know. Offer those guidelines to users with proper humility, try them out, and revise them often. Work with users who have the real problem of combining evaluated operating systems with unevaluated applications, data bases, and networks and see if we can develop suggested techniques and guidelines to apply as needed. Identify

useful features and document their attributes in clear language that can be used for competitive procurements.

Each user will ultimately select features, products, and custom development to meet his own needs. The most that common standards can do is to identify often-needed sets of products or features and suggest, as application notes, ways of configuring and applying them in real-world situations. This latter sort of guidance will give users help in the all-important area of configuring and managing the products that do meet evaluation criteria. If we listen to real experience, in time the guidelines may improve. When the rate of needed revision slows to the point of "stability", we can think about standards. It may even be that there will be additional areas of application for criteria and evaluation, though I for one am not convinced.

#### IN CLOSING

There is an old saying from the American West that goes "You can tell the pioneers; they're the ones with the arrows in their backs". The NCSC went first with security evaluation criteria. They have made mistakes, but they have also changed the way the world does -- and thinks about -- computer security.

It is up to us all now to recognize that evaluation and criteria, at least for the moment, are limited to operating system products. Rather than stretch the paradigm where it has no business going, we should concentrate on establishing stable and economical operating system evaluation processes, but put the major focus of our efforts on more broadly applicable guidelines that help to guide choice by users in the development or selection of cost-effective security measures.



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 12: Issue 47**

**Thursday 10 October 1991**

## Contents

- [Ex-DMV worker admits altering driving records for money](#)  
[Vireday](#)
- [Software migration at Johnson Space Center](#)  
[Joe Bouchard](#)
- [European Ideal Embraces Harmonised Pornography](#)  
[Brian Randell](#)
- [Prison Phone Phraud \(or The RISKS of Spanish\)](#)  
[Jim Flanagan](#)
- ["Peace Patent" and "Colossus: The Forbin Project"](#)  
[Lauren Weinstein](#)
- [UCSC to install touch-tone registration \(HELP WANTED\)](#)  
[Darrell Long](#)
- [Re: Ada Code Formatters \(... old software\)](#)  
[David Parnas](#)
- [Re: Encryption Exportability, by Clark Weissman](#)  
[Carl Ellison](#)
- [Re: Fiber optics can spontaneously destroy themselves!](#)  
[Paul Leyland](#)
- [Re: Safer flying through fly-by-wire](#)  
[Randal L. Schwartz](#)
- [Re: ``Friendly" \(?\) viruses](#)  
[Bertrand Meyer](#)
- [Re: AT&T Outages](#)  
[Peter G. Rose](#)
- [Re: RISKS of Highway warning signs](#)  
[Steven Philipson](#)  
[Arthur Hamlin](#)  
[Richard Thomsen](#)  
[Bob Haar](#)  
[Keith Henson](#)
- [Info on RISKS \(comp.risks\)](#)

---

✉ **Ex-DMV worker admits altering driving records for money**

~Vireday <rvireday@pldote.intel.com>

Thu, 10 Oct 91 08:39:32 PDT

Excerpts from "The Sacramento Bee", Friday, October 4, 1991. The RISKS are more than obvious. (Didn't something similar already happen in Great Britain?)

It is not explained how they found out about the alterations. Probably followed a paper trail, or discrepancies in backup logs. If that is so, what about all these pen-point computers about to hit the cop market? Will this increase the risk of losing this kind of "evidence"?

Ex-DMV worker admits altering driving records for money

A former technician for the [California] Department of Motor Vehicles admitted in court Thursday that she deleted bad driving records of a number of individuals who had paid for the service. Genevieve Pamela Lopez, pleaded guilty to 10 counts of illegally using the DMV computer for the purpose of altering, damaging or destroying data. Nineteen additional counts were dismissed. Proceedings against her co-defendant, Donald H. Stables, were continued to Oct. 24. He is charged with 48 counts involving computer fraud, bribery, falsification of government documents and conspiracy.

According to court records, Stables, an insurance agent in Yreka, allegedly had been receiving fees of up to \$2500 to arrange the obliteration of accident reports, drunken-driving arrests, suspensions and other violations on his clients' DMV records. Lopez was his contact at the department, according to documents, and she received between \$400 and \$500 for each transaction. ...

[The plea bargain terms Lopez has arranged are six years of formal probation, 60 days in the county jail, a fine of \$10,000, and to testify against Stables if need be.]

---

## **Software migration at Johnson Space Center**

Joe Bouchard <texsun.Central!ioscc!bouchard@fernwood.UUCP>

9 Oct 91 17:48:31 CDT (Wed)

The managers at NASA/JSC (Johnson Space Center, Houston, TX) seem to be underestimating the RISKS associated with migrating a mature software product to a completely new environment.

There is a move afoot to migrate the SMS (Shuttle Mission Simulator) from the Unisys 1100/90 - Perkin Elmer 8/16 equipment it's currently running on to another platform (not completely defined yet). The reasons for doing the migration sound something like "we need to get off that old mainframe equipment and into the modern age of Unix, multiple workstations, etc. Or maybe an modern (IBM) mainframe."

The justification for going through the effort (and believe me, it's going to be monumental) is improved uptime due to improved hardware and software reliability, ease in implementing changes, and performance (the 1100 it's on doesn't have a high MIP rating, and we all know how truly useful MIPs are to

compare dissimilar hardware/software). Upgrading the current equipment and/or software environment is not currently being considered seriously (Unisys isn't POPULAR with the big wigs at JSC, IBM & Unix anything are).

Problem one: the numbers being used to do the justification seem to be largely imaginary (I'm not close enough to the project to tell for sure). Sort of ... "Everyone knows that mainframes are unreliable and workstations are good. Rate the mainframe 10 failures per ?? (based on real data) and rate the workstation system 3 per ?? (based on who knows?). This will save us big \$\$\$." Even if the numbers are based in something resembling a scientific study, they are likely to be based on MATURE systems. Anyone who has been through a major conversion effort can tell you just how long it takes to get millions of lines of real-time simulation software to the same maturity on another box, especially a very different kind of box (the Shuttle may be retired by then).

At the time SMS was developed (more than 12 years ago), Univac (later Sperry, later Unisys) was the only vendor that had developed real time software processing to a sufficient maturity on a large enough box to get the job done (I believe they were the only ones to complete the pilot project successfully, but I wasn't around then). Since then, the software has undergone extensive growth. This system is complicated to the point that moving it to another platform will be practically as difficult as redeveloping it from scratch.

Problem two: none of the destination systems being discussed have demonstrated that kind of real-time software processing capability. Problem three: none (or almost none) of the programmers currently working on SMS has any experience with any of the new systems. There is a gigantic risk in going from the known into the unknown. This risk is unjustifiable when significant improvements can be made in the current environment.

Unisys 1100-series equipment, from the smallest (2200/100, desk sized small business system) to the largest (2200/600, big mainframe), runs the same software across the entire line with NO modifications required. Such a large range of compatible processing power is unavailable from any other vendor (the Unisys A-series has a somewhat wider range). Since the initial development of SMS, the capabilities of both the hardware and system software of the 1100-series has expanded tremendously. Upgrading SMS to take advantage of these improvements would be much less risky than moving to another platform, but the lack of popularity of Unisys at JSC prevents it. (Another of those political correctness things. Also a result of the government contractor environment. "We hired you to do what we tell you to do and nothing else.") And all this at public expense without much accountability.

NOTE: I have been doing System Software support on 1100-series computers for about 10 years and can't claim to be entirely unbiased. I have done programming on both personal computers (Apple, Commodore, IBM, etc.) and mainframes (Honeywell, Unisys 1100/2200, some IBM), so I have an idea what it takes to move conventional systems from one box/environment to another. I don't think the management at NASA does.

---

**✶ European Ideal Embraces Harmonised Pornography**

<Brian.Randell@newcastle.ac.uk>

Thu, 10 Oct 91 09:32:14 BST

[The risks entailed in the attached article, quoted in full from the front page of today's Independent, are perhaps not so much computer-related as commission-related, but I thought I would "share them" (to use an American phrase which always grates somewhat on British ears :-)) with RISKS readers.

Brian Randell, Computing Laboratory, The University, Newcastle upon Tyne,  
NE1 7RU, UK           PHONE = +44 91 222 7923 FAX = +44 91 222 8232]

European Ideal Embraces Harmonised Pornography,  
by Andrew Marshall, West Europe Editor

The European Community has a new crusade: high technology pornography. EC commissioner Filipo Maria Pandolfi told the European Parliament in a letter yesterday that the Commission is working on a code of conduct for the sex industry. Mr Pandolfi is the Telecommunications Commissioner, and does not usually get involved with below-the-waist activities in a professional capacity. But the modern pornographer is increasingly dependent on modems and multiplexes [sic] rather than plain brown envelopes and hand-wound peepshow machines. And when Brussels hears the word "hi-tech", it reaches for a directive. "Such a Code of conduct would state ... rules for the information industry ... and administer the provision of information services of a pornographic nature," says Mr Pandolfi's letter.

The pornography industry, as well as simple telephone chat lines and recorded messages, has now developed much more complicated ways of sending pornographic images along the line. Regulating these is something of a problem for old-fashioned vice cops. But when different individual member states develop different approaches, this can interfere with more legitimate business activities. So part of Mr Pandolfi's mission is to ensure that Nation shall speak dirty unto Nation, because, as the Commission puts it, "discrepancies between existing national regulations constitute a problem in establishing a common market for information services". Let nobody keep apart heavy breathers in Croydon and Cologne, lest they disrupt the single internal market.

Perhaps the commission is not aware of the risks in opening Pandolfi's box. Will pornography have to be standardised, with French maid's uniforms compulsory? Will there be heavily-subsidised industrial national champions in pornography, allowing the Dirty Old Man to represent Euro-frotteurs? Must Naughty Fifi Tell All in eight languages?

---

### **✂ Prison Phone Phraud (or The RISKS of Spanish)**

Jim Flanagan <flanagan@stat.washington.edu>

Thu, 10 Oct 91 16:51:16 -0700

This notice appeared in the University of Washington staff newspaper  
University Week:

PHONE FRAUD

It recently was discovered that inmates from the Clallam Correctional Center in Clallam Bay, WA have been using an automated phone system to try to scam unsuspecting employees at the UW.

Fone America, the long-distance provider for the correctional center, supplies an automated service for collect calls. Inmates are supposed to make recordings of their names to identify themselves to the called parties. A recording should say, "If you will accept a collect call from...(name of caller)...please press the number 3 on your telephone twice"

Fone America also supplies the same automates message in Spanish. In the scam, inmates chose the Spanish option and record, in place of their names "If you want to hear this message in English, press 33." They then call a number at the UW and try to reach employees who will press 33 which automatically accepts the collect calls. If the inmates get through, they ask to be transferred to the outside operator or to the switchboard operator. They will then attempt to place long distance calls and have them billed to campus phones.

Since late July, this scam has occurred a number of times. It is important for University employees to recognize this or similar phone scams.

[The notice goes on to suggest ways to minimize the impact of phone fraud]

Jim Flanagan, Systems Programmer, UofW Statistics [flanagan@stat.washington.edu](mailto:flanagan@stat.washington.edu)

---

### ✦ "Peace Patent" and "Colossus: The Forbin Project"

*Lauren Weinstein <lauren@vortex.com>*

*Wed, 9 Oct 91 12:08:02 PDT*

Yes, indeed, the described "peace patent" is similar in some respects to the basic concept behind the semi-classic film "Colossus: The Forbin Project" (1970). In the film, both the US and USSR put into place master control computers to manage their nuclear arsenals. Gimmick: the systems cannot be turned off or disconnected (similar to 'The Doomsday Machine' from "Dr. Strangelove") without blowing everything up.

The US computer (Colossus) realizes that there must be a Soviet computer (Guardian) and demands a hookup (TCP/IP? OSI?). Classic line: "There is another system."

Both sides let their computers talk for awhile. There's an amusing sequence where the two systems, starting with 0 and 1, build up a vocabulary and rapidly increase the data rate. The humans watching have an increasingly difficult time keeping track of what the machines are saying to each other as the rate increases. Suddenly, the machines shift to a completely unknown protocol and coding, and the humans have no idea what is going on between the machines. They panic, and pull the plug on the connection. Colossus (we see all this from the US side) tries for a while to get a circuit back to Guardian over various cable and satellite systems. He can't. He then simply demands that

the circuit be restored, or else he'll fire a missile. In fact, as I recall he does just that, as does Guardian. The warheads are only destroyed (how?) when the humans restore the link.

There are a lot more goings on, including various other attempts to disconnect the computers or disarm the warheads. All fail. The film ends with Colossus and Guardian in total control of the world, and humans relegated to a position of being, essentially, slaves to the machines.

--Lauren--

---

### **✂ UCSC to install touch-tone registration**

<darrell@cse.ucsc.edu>

Thu, 10 Oct 91 14:57:20 -0700

UC Santa Cruz is going to install a touch-tone registration system. Here's your chance to prevent a RISK before it occurs.

Please send me any RISKS that you know of in such a system. Also, pointers to relevant back-issues of RISKS will be appreciated.

Thanks, DL

[Responses to DL, PLEASE!!! PGN]

---

### **✂ Re: Ada Code Formatters (... old software) (Mitchell, [RISKS-12.45](#))**

David Parnas <parnas@qusunt.Eng.McMaster.CA>

Wed, 9 Oct 91 16:06:57 EDT

Kent Mitchell <KDM@rational.com> indicates that a bug in his company's products has been corrected and that it is no longer a problem. He then goes on to say, "Perhaps the real risk here is using old, out of date software." Others might say, "Perhaps the real risk here is prematurely released software, software that is released before adequate validation". How long can we go on acting as if it is OK to release buggy software as long as we fix it (for an extra charge of course) later.

David L. Parnas      parnas@sscvox.cis.mcmaster.ca

---

### **✂ Re: Encryption Exportability, by Clark Weissman ([RISKS-12.46](#))**

Carl Ellison <cme@ellisun.sw.stratus.com>

Thu, 10 Oct 91 14:28:52 EDT

>The U.S. finds itself in a dilemma: harm our economic growth and competitiveness in the expanding world internet products and services industries if we prohibit cryptographic applications, or permit such cryptographic export and potentially weaken military security by providing new encryption capabilities to our adversaries.

I have heard this argument multiple times and I find it bogus.

This argument assumes that we in the US are in a leadership position in the development of encryption products so that if we ship products, our adversaries will get something they can't get elsewhere.

It's doubtful that this has ever been true, except possibly for the top of the line NSA black boxes -- but that's not what we're talking about controlling, here. We're talking about the products of US private industries. Crypto AG in Switzerland isn't waiting for the US to permit exports. They have been producing high quality equipment for decades and will continue to do so. Other companies are starting up to produce and sell cryptographic equipment.

Therefore, to me there is only one side to this argument: if we prohibit export, we limit the US competitiveness, while our adversaries get equipment and algorithms at least as good as they might buy indirectly from us, but from other countries. Meanwhile, the thwarting of US industrial development of cryptographic applications and equipment leads to an atrophy of ability in US industries so that even we will have to buy equipment from outside this country.

The last time I looked at smart card cryptography, it was all produced in Europe, for example.

Is this going to be another case of the USA losing out completely on a market -- ala VCRs?

My guess is that it already is -- thanks to at least a decade of restrictions. My remaining question is whether we have any chance to catch up, assuming we do a rapid and firm about-face in policy immediately.

---

**✉ Re: Fiber optics can spontaneously destroy themselves! ([RISKS-12.44](#))**

*Paul Leyland <pcl@oxford.ac.uk>*

*Thu, 10 Oct 91 10:51:18 +0100*

> It turns out that a fiber optic in an environment "where the temperature can suddenly increase" can result in the complete destruction of a fiber optic in what is known as a fiber "fuse" effect. "For certain types of optical fibers...damage can occur when the visible-light laser power transmitted... is as low as 4 milliwatts..."

I'm surprised that a power of 4mW can destroy a fibre. Ten years ago, I was a practising spectroscopist. Several times I saw a fibre melting away in an upstream direction. The output end of the fibre had become dirty and absorbed the laser light; the fibre's tip melted, ensuring that light continued to be absorbed.

The big difference, though, was that we were pumping anything up to 10 WATTS through a 150 micron fibre. Admittedly, this was 514.5nm Ar+ light, rather than the red and near IR used in telecommunications, but as glass is more opaque in the green than near IR, I'd expect greater problems with Ar+. I

\*never\* saw a fibre burning away when less than several watts were being transmitted.

If we calculate the power densities involved, 10 watts through 150 $\mu$  is a power density of 566MW m<sup>-2</sup>; 4mW through the same fibre is 226kW m<sup>-2</sup>. For comparison purposes, a typical electric fire element (in this country at least) radiates 1kW from an area of 0.01 m<sup>-2</sup> (assuming a length of 30cm and a diameter of 1cm) for a power density of 100kW m<sup>-2</sup>. It glows dull red-orange.

Hmm, I suppose that 200kW m<sup>-2</sup> might melt a fibre if the laser light were converted to heat with high efficiency.

Paul

---

**✂ Re: Safer flying through fly-by-wire (Spencer, [RISKS-12.45](#))**

*Randal L. Schwartz <merlyn@iwarp.intel.com>*

*Thu, 10 Oct 91 09:39:28 PDT*

> The USAF/NASA Advanced Fighter Technology Integration test aircraft is doing flight evaluations of a system to help pilots cope with disorientation: push a button on the stick and the computer automatically brings the aircraft back to level flight.

But level flight based on what indications? Every IFR pilot is taught to "right" herself based on the array of gauges visible on the panel, and must do so with demonstrable proficiency before being signed off to "bore holes in the clouds". But we are also taught to cross-check... does the Artificial Horizon "make sense" compared to the changes in Altimeter and Heading? Does the Rate-of-turn indicator cross-check with that?

I can't see how this device is better than your basically-trained IFR pilot, and it may be worse (mortal failures under strange instrument failure modes).

Randal L. Schwartz, PP-ASEL-IA, 260+ hours and climbing...

---

**✂ Re: ``Friendly" (?) viruses (Smee, [RISKS-12.45](#))**

*Bertrand Meyer @ Interactive Software Engineering Inc. <bertrand@eiffel.com>*

*Thu, 10 Oct 91 12:35:23 PDT*

`` It is an (at least) antisocial act to cause anything to run on my machine without my knowledge, and with no action on my part to indicate that I want it. I cannot think of ANY useful piece of software of ANY sort [...] which does not have the potential for screwing things up amazingly in SOME contexts."

Although I see no reason to disagree in principle, it may be worth pointing out that this statement, taken literally, is too strong to reflect the reality of even the most common computer systems, which DO execute things without explicit actions from their owners and users.

Most people reading this use a machine running Unix. Somewhere in its file system (usually /usr/spool/cron or /var/spool/cron) there is a directory `crontabs' containing files which describe actions to be executed regularly without explicit user action. In particular, the file `root' describes actions to be executed by the `root' id, that is to say, with all possible privileges.

Such mechanisms, if used well, are essential to the proper functioning of the system. For example some typical `cron' actions remove unneeded or old files. For one thing, news wouldn't work without cron, since the flow of incoming messages would quickly fill out all available disk space. Neither would mail work without the help of some programs, running automatically (the Unix name, ``daemon'', is suggestive enough), which do a few things on their own, such as checking the incoming mail queue every now and then.

One may argue that there is implicit ``action on the owner's part'', using Mr. Smee's words: by accepting to use the machine, you accept its standard cron mechanisms and mail daemons; furthermore, you may login as `root' and disable the daemons and cron actions that you don't like.

But most people probably just leave the software as it was when the machine was installed, and as Unix reaches the masses there will be more and more users who don't even know about the existence of cron and daemons. So in effect the operating system IS performing, behind the user's back, actions which may directly affect his property (files, electronic mail etc.).

It's a little like signing an agreement letting a supplier or employer make direct drafts from your bank account: sure, you did perform one ``explicit action'' when you authorized it, but it still opens more risks than if you have to authorize each operation individually.

So while I agree with Mr. Smee and other posters about the oxymoronic nature of ``friendly virus'', I think the technical situation is a little more complex than his statement would suggest.

It also seems that an automatic or semi-automatic bug correction service, working somewhat in the style of mail and news (that is to say, updating remote files in controlled conditions) wouldn't be such an absurdity as he suggests. I can see why some user sites might want to subscribe (voluntarily, of course!) to such a service if it is technically well-done and has the proper safeguards. (Maybe something like that already exists.) After all, those of us who can read this still use mail and news in spite of the Internet worm and of the potential for further abuses of the same kind.

Bertrand Meyer    bertrand@eiffel.com

---

## ✂ AT&T Outages

*"Peter G. Rose" <LCO114@URIACC.URI.EDU>*

*Wed, 09 Oct 91 15:52:32 EDT*

Some people seem to want to blame human weaknesses for the AT&T failure, other people seem to want to blame the technology. What I haven't seen anyone point out is that, every time AT&T (or most other people) does something to "improve"

their system, they end up more and more centralized.

Fundamental rule of designing things:

"Sooner or later, EVERYTHING breaks."

If you don't want catastrophic failures, you need to arrange things so that the inevitable failures aren't catastrophic. Why is so much vital traffic being routed through a single installation? What are they planning to do when a fire, plane crash, flood, or terrorist action takes out that entire building? Why is the control network dependant solely on AT&T, when anyone with any sense could predict that sooner or later, that service isn't going to be there?

P.Rose (LCO114@URIACC.URI.EDU)

---

**✉ Re: RISKS of Highway warning signs ([RISKS-12.45](#))**

*Steven Philipson <stevenp@kodak.pa.dec.com>*

*Wed, 9 Oct 91 14:29:12 -0700*

Several persons commented that the cause of the accident was not that the signs were not working, but rather that the truck driver was not paying attention. The inattentiveness of the driver may have been the most significant factor, but the failure of the signs is also significant. The driver may have had an expectation that the warning signs were operating. Lack of the warning contributes to lower attentiveness.

This phenomenon has a name -- primary/backup inversion. The driver should have been more attentive, but warning systems do tend to make people less attentive. Designers must keep this in mind when developing warning and backup systems.

This accident clearly falls in the category of a "system accident" -- multiple factors in a complex system (including surface traffic, river traffic, drawbridges, warning systems, rules of operation, working hours) collectively contributed to the outcome. Charles Perrow's *\_Normal Accidents\_* discusses system accidents in detail. It is well worth reading.

Steve Philipson

---

**✉ Re: RISKS of Highway warning signs (Flory, [RISKS-12.45](#))**

*Arthur Hamlin <hamlin@codex.com>*

*Thu, 10 Oct 91 10:41:25 EDT*

>The was no risk here because the signs weren't working. The risk was the truck driver obviously driving recklessly. There's too much of a tendency to blame something or someone else when things happen. Bottom line is, if the trucker had been driving safely, the accident WOULD NOT HAVE HAPPENED, sign or no sign.

Unless you have additional information about the accident, I must disagree. If I am on an unfamiliar highway, it is up to the maintainers of the highway to "tell" me how to drive it safely. This includes speed limits, warnings about

hazards, and information about what is ahead.

There is a section of a Rt 9 in Mass. that has a stop light just over the top of a hill. You can't see it as you come up the hill, but only as you come over the top. The speed limit on this road is 45mph, far too fast to react to one or more stopped cars at a red light. The town put up a permanent sign clearly stating that there was a stop light over the hill and that cars may be stopped at it. This warning has worked very well.

However, several miles down the road, in a different town, they use an electronic sign that only turns on when the light is RED. The idea being that if the light is green and there are no cars backed up, there is no danger, so no need to slow down. Assuming that the sign goes on and off correctly, ( including time delays after cycling to allow a backup to disperse ) this will work fine. But as soon as the electronic board fails, THERE IS NO WARNING. A driver not knowing the road would go 45mph, ( the posted "safe" speed ) having no reason to think that there is any problems ahead, and smash into the cars backed up at the red light. A driver who knows the road would assume that the sign would warn him if there was a backup, so he too would be in danger. ( I'll grant you that this driver should be going a little slower over the hill because he knows that there is a potential problem )

If all drivers drove as if they had to be able to stop on a dime at all times, cars could not be a practical form of transportation. Drivers rely upon the maintainers of the highways to tell them what the risk level of the road they driving is, so that they can then drive "safely".

The Wizard of AHs

P.S. Some places use a permanent painted sign that warns of the danger all the time, and the electronic lighted sign obscures it when it is on. Therefore, in the case of failure, the warning is up. Sort of like four way stop signs at an intersection with lights.

---

**✂ RE: Liability risks of highway signs**

*Richard Thomsen <rgt@beta.lanl.gov>  
Thu, 10 Oct 91 08:29:09 -0600*

My uncle, who was a law lecturer at Cambridge, England, was telling me about liability risks. He said that sometimes if you put up a warning sign, then you are admitting that there is a hazzard, and so you are liable. However, if you say nothing, then you are not liable. Interesting cases.

Richard Thomsen

---

**✂ Re: RISKS of Highway warning signs (Hoffman, [RISKS-12.44](#))**

*Bob Haar <rhaar@gmr.com>  
9 Oct 91 21:07:53 GMT*

Certainly, there are risks associated with the expectation that any warning devices will really function. But I have to lay blame for this accident on the truck driver. Whether or not the signs were operating with appropriate

messages, the driver of any vehicle is responsible for operating it in a "reasonably safe" manner. This includes being able to stop the vehicle if there is an obstruction in the road.

In this case, either the truck driver was not paying attention or he was driving too fast so that he couldn't stop when he did see the stopped traffic.

There are many possible causes for an obstruction in the road that have nothing to do with the drawbridge. The warning signs would not have given notice of these.

Robert Haar, Computer Science Dept., G.M. Research Laboratories

---

## Warning systems

<hkhenson@cup.portal.com>

Thu, 10 Oct 91 17:29:35 PDT

While it would not have helped any on the recent ATT outage, a serious problem is trying to use people to backup machines--they get bored and nod off. Perhaps we need to have on purpose, unpredictable "false alarms" for people to respond to. I could easily design such a device to give a false warning at the sensor leads once a month or so. You could make pay, or rewards, or something dependent on taking corrective action, starting with resetting the signal. You might want an short term inhibit signal so that test alarms wouldn't pop up during a real emergency. Let's see, I have a year from this going out to file for a patent. :) Keith Henson

[Well, this idea keeps coming up in RISKS, every time we have a problem with backup and emergency systems... 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 12: Issue 48**

**Friday 11 October 1991**

## Contents

- [Police raid wrong house -- for second time](#)  
[David B. Benson](#)
- [Crypto Public Policy](#)  
[Bill Murray](#)
- [Re: Security Criteria, Evaluation and the International Environment](#)  
[Henry Spencer](#)  
[PGN](#)
- [Re: "Safer Flying through Fly-By-Wire"](#)  
[Arnd Wussing](#)  
[Mary Shafer](#)
- [Re: Computers and missile control](#)  
[Eric Prebys](#)
- [Re: Software migration at Johnson Space Center](#)  
[Bob Frankston](#)  
[Doug Burke](#)  
[Guy J. Sherr](#)
- [Human error: once more, with feeling](#)  
[Don Norman](#)
- [Re: AT&T outage](#)  
[Bob Colwell](#)  
[Mark Secof](#)  
[Bob Niland](#)  
[Martyn Thomas](#)
- [A step towards adopting DefStan 00-55](#)  
[Vicky Stavridou](#)
- [Digital Retouching on the Telephone](#)  
[Chuck Dunlop](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Police raid wrong house -- for second time**

*David B. Benson* <[dbenson@yoda.eecs.wsu.edu](mailto:dbenson@yoda.eecs.wsu.edu)>

*Fri, 11 Oct 91 09:47:50 pdt*

Lewiston Tribune/Friday, October 11, 1991, page 6C

Associated Press

FEDERAL WAY, Wash. -- King County Police confounded by a typographical error mistakenly descended on the home of Terry and Dean Krussel this week -- for the second time this year. At least this time they didn't break the door down.

When the officers from the narcotics unit raided the Krussel home in May, they kicked in the door, ordered Terry Krussel, 57, to get down on the floor and held her at gunpoint while they searched the house.

County officials replaced the door at a cost of \$2000 and apologized profusely.

When the Krussels got a letter from the county prosecutor's office on Sept. 11, addressed to the person officers had sought in the May raid, they worried that their address was still on file as a den of iniquity and dangerous drugs.

King County police scrambled to delete their address from the department's computer files, and deputy prosecutor Judith Callahan assured the Krussels in a Sept. 17 letter of the county's good intentions.

"Our office is truly concerned that Mr. and Mrs. Krussel not feel that they are victims of county bureaucracy," she wrote.

Unfortunately, the Krussels' address remained in the drug dealer's file -- and that's what the officers pursuing the dealer Tuesday night were working from.

The officers didn't leave until Dean Krussel showed them Callahan's letter. "This thing just won't go away," he said after the couple's latest run-in with King County's finest.

---

## **✂ Crypto Public Policy (C. Weismann)**

<WHMurray@DOCKMASTER.NCSC.MIL>

Fri, 11 Oct 91 09:42 EDT

>The debate is international in applicability. However, U.S. policy on encryption appears most severe, so I urge a U.S. National debate to begin the dialog, and start with some questions.

I agree with Clark that debate is indicated. There is no proper forum for this debate. The present policy has ancient origins. They are older than the Cold War, though the Cold War has been used to justify them since the National Security Act of 1947. The current policy dates from the Great War and was placed in law without public debate in 1943. That law, passed in war time, has been used since to suppress any further debate.

>Do we gain more by strengthening our commercial competitiveness and products, upon which the military is increasingly dependent, than we lose by permitting international commonality in cryptographic services, which may weaken military capabilities?

While it is difficult to state the issue, proper debate requires that it be stated clearly. I do not think that Clark's question properly frames it. I think that the issue is more one of the trust and confidence required for commerce than it is one of "competitiveness." This country needs trade. The most efficient way to mediate trade in the modern world is electronically. Trust and confidence in electronically mediated trade requires secret codes which both parties can trust. That is one interest. I submit that it is far more compelling than mere "competitiveness."

I also understand the contending issue differently. Rather than relative "military capability," the issue is one of the cost of intelligence gathering. Even in a peaceful world, security requires that we gather intelligence. Prudence suggests that we gather it about everyone, not simply "adversaries," but everyone. History screams that any political instability causes people to choose sides. Therefore, it behooves us to know as much as we can about what is going on in the world. If the ether begins to fill with "random appearing" data, the cost of intelligence gathering will rise as a geometric function of the quantity of that data. Therefore, the second interest is to discourage that data to the extent that we can. It is not simply one of effectiveness; we cannot hope to discourage all use of secret codes. Rather it is one of efficiency; how much can we discourage and at what price.

Neither of these interests is trivial. Each is worth defending. They do conflict. To date they have been debated only in secret proceedings. I am concerned that in those debates, the latter interest has prevailed and that the former may not have been properly appreciated. I do not believe that either interest will be seriously compromised by a more public debate.

William Hugh Murray, Executive Consultant, Information System Security  
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840 203 966 4769

---

## **✉ Re: Security Criteria, Evaluation and the International Environment**

*<henry@zoo.toronto.edu>  
Fri, 11 Oct 91 14:08:31 EDT*

One note of caution here...

> Criteria for secure time-sharing systems will not "make it" in the nineties, but it is not clear that we know enough to write evaluation criteria for networks, data bases or applications...

I think I see the Wheel Of Reincarnation operating here in several ways. Time-sharing systems are passe', but everyone is busy rediscovering the same old issues in the context of networks, databases, etc. What, exactly, is the fundamental difference between a time-sharing system and (say) a heterogeneous network? Answer: there isn't one, unless you insist on thinking of time-sharing systems in terms of a narrow stereotype that has never described all time-sharing systems. (As a case in point, note that the Plan Nine experimental operating system at Bell Labs is aimed specifically at making a heterogeneous network look pretty much like a time-sharing system. They're succeeding fairly well.) What, exactly, is the difference between the access

controls enforced by a shared database and the ones enforced by a time-sharing kernel? Answer: while there is a different flavor to some of it, the problems and solutions are often very similar. And so on.

"Those who do not remember history are condemned to repeat it." If we continue to discard past experience with multi-user systems as obsolete, we will continue to rediscover issues and make the same old mistakes when building new multi-user systems. Criteria for secure time-sharing systems deserve very careful examination, as much of that experience should be applicable to networks, databases, applications, etc., given some caution in the presence of shifts in the underlying concepts.

Henry Spencer at U of Toronto Zoology

---

## **✉ Re: Security Criteria, Evaluation and the International Environment**

*Peter G. Neumann <neumann@csl.sri.com>  
Fri, 11 Oct 91 12:10:14 PDT*

Ah, but the people who wrote the Orange Book (TCSEC) years ago were thinking not in terms of generic functionality for trusted distributed systems, but primarily in terms of isolated-system security kernels. They wrote the criteria in an overly-specific manner that makes the applicability to networks and distributed systems very difficult/uncharted/unclear/... Nevertheless, the Red Book tries... See also the European ITSEC. But in principle any sensible operating system concept could be distributed in a nice clean invisible way; in practice there are LOTS OF PROBLEMS, some of which are indeed different from the old ones (such as distributed authentication).

---

## **✉ Response to "Safer Flying through Fly-By-Wire (Spencer, [RISKS-12.45](#))**

*Arnd Wussing <AW@PRI-CE.Prime.COM>  
11 Oct 91 10:14:36 UT*

>The USAF/NASA Advanced Fighter Technology Integration test aircraft is doing flight evaluations of a system to help pilots cope with disorientation: push a button on the stick and the computer automatically brings the aircraft back to level flight.

As an active aerobatic pilot, I've had the experience several times of complete disorientation, the horizon cannot be interpreted or seen and the G-forces acting on the body lead to incorrect conclusions regarding the attitude of the aircraft. Although a mechanical device to recover from an unnatural flight situation would be of immense benefit, the process of achieving level-flight from a given spatial orientation can be quite complex, involving judgements regarding G-Forces, rudder & aileron coordination (or dis-ordination in some cases), airspeed (both indicated & true), aircraft red-line and stall characteristics, etc. These factors can for the most part be vectorized into a given computer system/program assuming that \*ALL\* of the sensors are functioning correctly; the consequences of going over red-line and getting flutter due to a partially blocked Pitot-tube or going into an unrecoverable stall because the aircraft isn't balanced correctly on this

flight (perhaps the cargo shifted) and the recovery-software wasn't informed or stalling because there is icing and the stall-warning is out of function are devastating.

The risks inherent in such a system would be outweighed by the benefits when an emergency situation occurs assuming the pilot has no recourse; but the knowledge that the aircraft is equipped with "a device which will get me out of any situation" might make a pilot take more risks and thus induce exactly that situation where the system must be used; somewhat akin to the RISKS article about the warning signs for the Virginia drawbridge.

---

**✉ Re: Safer flying through fly-by-wire (Schwartz, [RISKS-12.47](#))**

Mary Shafer <shafer@skipper.dfrf.nasa.gov>

Fri, 11 Oct 91 08:31:09 PDT

The AFTI/F-16 is a completely instrumented airplane and has several accelerometer packages. Level flight just turns into setting a\_x and a\_y to zero, with a\_n = -a\_z = 1.0 g. You can couple in the rate gyros and set p, q, and r to zero too. This is a pretty simple little feedback system.

>I can't see how this device is better than your basically-trained  
>IFR pilot, and it may be worse (mortal failures under strange  
>instrument failure modes).

Quinine, in the form of tonic water, doesn't give the accelerometer package vertigo like it does the pilot's vestibular system (being discussed in rec.aviation right now). Accelerometers don't get the leans, either.

Actually all F-16s have similar accelerometer and rate gyro packages, the AFTI/F-16's are just tied to the instrumentation package as well. Modern fighters are somewhat more heavily instrumented than are general aviation aircraft (which, by the signature, is what the poster, a private pilot, is familiar with).

The system was first proposed to deal with GLOC (g-induced loss of consciousness). The F-16 is notorious for having such a high instantaneous rate of g onset that pilots in combat are at risk of GLOC. The question is really whether this system is better than an unconscious pilot. (To further tie this to a thread in sci.military, the F-20 had the same high g onset rate and many people believe that GLOC led to at least one of the prototype crashes.)

Mary Shafer DoD #0362 NASA Ames Dryden Flight Research Facility, Edwards, CA  
shafer@skipper.dfrf.nasa.gov shafer@pioneer.arc.nasa.gov

---

**✉ RE: Computers and missile control**

Eric Prebys, CERN-PPE/OPAL <prebys@vxcern.cern.ch>

Fri, 11 Oct 91 18:56:11 +0100

All technical issues aside, the first (obvious) question that comes to mind is:

Who gets to design, build, program, install, verify and maintain this system?

If all countries got along well enough to settle that question, the whole issue would become moot (perhaps that's the real idea).

But another very real question is:

Would it really be an improvement over the existing situation?

Maybe I'm missing something, but wouldn't it just make Mutually Assured Destruction even more "mutually assured". Unless, of course, the idea is to give the victim enough time to completely destroy the attacker at the outset. In that case, it would be as "realistic" (and a lot cheaper) to get countries to agree to just blow themselves up if they ever get angry.

What I really don't understand is, if (a huge "if") it WERE possible to establish central, tamper-proof control over ALL countries' abilities to launch ALL nuclear weapons (as the article suggests), why not go the one (IMHO small) step further and make it impossible to launch them at all? ...maybe through the use of a "beneficial virus" (just kidding). Personally, I think it would be very sad if the world could achieve the sort of trust and cooperation necessary to implement this system, and not manage to do away with the things entirely.

Eric Prebys, CERN, Geneva, Switzerland

---

### **✂ Re: Software migration at Johnson Space Center**

*<frankston!Bob\_Frankston@world.std.com>*

*10 Oct 1991 22:57 -0400*

I can't vouch for the details of the arguments, but this is a good example of trying to decide a scope of solution. Is it more important to maintain a given system in its own cocoon or take the risk of change in order to get the benefits of what, over a decade, has emerged as a standard. We can argue the technical benefits (and I would think that 10 years of change has produced some improvements, though nowhere near as much as it might have) but there are larger issues such as switching into a more cost effective/price competitive market. There is also the benefit of standardization in terms of being able to take advantage of common knowledge and tools.

Risks are necessary part of evolution. It is important to be aware when one is taking a risk and the consequences and not be naive. But not taking a risk can be a bigger risk.

Again, I claim no knowledge or insight about this particular instance and I'll admit to a bias in favor of rampaging PC's.

---

### **✂ Re: Software migration at Johnson Space Center**

"Doug Burke, Shell Account Spec., Malaysia" <doug.burke@msa.mts.dec.com>

Thu, 10 Oct 91 20:53:05 PDT

I used to use UNIVAC 1100 series computers too. However, I would like to cast some doubt on one of the statements, and refute another made under this topic in [RISKS-12.47](#).

First of all, there were other companies who had well developed realtime software processing more than 12 years ago, although perhaps not on a processor the size of a, say, UNIVAC 1108. For example, one machine and operating system that comes to mind is the PDP-11 running RT.

Then there is the VAX...

And speaking of the VAX, it is a system sold by another vendor (Digital Equipment Corporation) which has as large a range of compatible processing power as the UNISYS 1100 series, if not more. Since I am a software specialist, I'll spare the sales pitch...

Doug Burke, Senior Software Specialist, Digital Equipment (Malaysia),

---

**✂ Re: Software Migration at Johnson Space Center (Bouchard, [RISKS-12.47](#))**

"Guy J. Sherr" <0004322955@mcimail.com>

Fri, 11 Oct 91 17:24 GMT

>Unisys 1100-series equipment, from the smallest (2200/100, desk sized small business system) to the largest (2200/600, big mainframe), runs the same software across the entire line with NO modifications required. Such a large range of compatible processing power is unavailable from any other vendor (the Unisys A-series has a somewhat wider range).

I must take exception with this. The VAX family processor will faithfully execute programming which makes no installation dependant call provided that the VMS linker was used to link it, and that the VMS executive is at the same release point or is a later release. I believe DEC is not owned by Unisys.

Also, will the Unisys equipment take the executing image of the code, or must the source be recompiled? The VAX family processor, for example, executes the exact same executive no matter what model it runs on. Actually, I do recall one release of VMS where that was not the case, but then DEC fixed it anyway.

Guy Sherr, Lab Configuration Mgr, MCI Reston, VA 0004322955@mcimail.com

---

**✂ Human error: once more, with feeling**

Don Norman <norman@cogsci.ucsd.edu>

Fri, 11 Oct 1991 07:40:10 -0800

Perhaps our moderator, Peter Neumann, should just keep a copy of this on hand and reissue it as needed. This is long, but needed periodically. (Maybe Peter should add a brief version to the masthead of RISKS!)

The real RISK in computer system design is NOT human error. It is designers who are content to blame human error and thereby wash their hands of responsibility.

in RISKS

The ATT failure

The truck driver and bridge

In Aeronautics Digest 3.22 (Oct. 10, 1991)

Traffic collision avoidance system failures: the Federal Aviation Administration (FAA) ordered a shutdown of 200 of the 700 units that had been installed. The 200 systems were seeing phantom aircraft and instructing pilots to evade planes that simply were not there.

"We had a simple human error where an engineer misclassified the changes in the software"

Human error is almost always a result of system and design error. It has to be taken account of in the design and in the work procedures.

Lots of people in Risks have proposed design procedures that will help.

Even the manufacturer of the TCAS system (in the last incident above) said:

. To prevent similar omissions, Collins now requires that a committee of  
. software engineers review changes before a program is released. "More than  
. one pair of eyes must review these things and make a decision"

That will not guarantee correctness (if, for example, the specifications are incomplete or inappropriate -- as they almost always are -- the committee will simply verify that the program meets the wrong specifications) but it will help. Committees are also subject to various kinds of group decision processes that sometimes propogate errors. It is a first step, but it still does not indicate that the designers are sensitive to the nature of error and will take design pains to avoid it.

Example: if only the truck driver had been attentive, the accident would not have happened. True. But also if only the signs had been working, or if the procedures required traffic to stop elsewhere, or if only the drawbridge hadn't been raised. In any accident, there are always dozens of "if onlys".

NO HUMAN IS 100% ATTENTIVE. Designers assume perfect human attention, which is fallacious. (My restatement is that humans are excellent at switching attention among competing demands. Alas, the demands of modern technology are not always compatible with the evolutionary structure of the human.) The design error is assuming inappropriate properties to humans and assuming they can perform in ways that are foreign and unnatural -- truly, biologically determined, "hard-wired," unnatural.

We design to allow equipment to work in the face of noise and even component failure, certainly in the face of out-of-tolerance components. We should do the same for people. It is no excuse to blame training, attention, attitude, or "human nature." These things happen so much that they have to be designed for. And we even know how to do so. The real problem is the attitude of the design community, even among those who read RISKS.

The other problem is the training of the design community: engineering and computer science departments train technology, program verification, and the like. No expertise in human and social issues. Computer scientists cannot turn overnight into social scientists, nor should they. The design of systems for people requires design teams consisting of computer scientists, cognitive and social scientists, (and representatives from the user community).

Technology alone cannot provide the answers when we deal with human activities.

"What has this to do with computer science? Nothing, directly, but indirectly it means a lot. The same computer that makes so much possible, also sets up the conditions for human error. And if this is not understood, the systems will fail, and the failure will be blamed on "the computer" or even on "those computer programmers and scientists."  
(rephrased from Norman, in press)

SEE:

Perrow, C. (1984). Normal accidents. New York: Basic Books.

Norman, D. A. (1990). Commentary: Human error and the design of computer systems. Communications of the ACM, 33, 4-7.

Norman, D. A. (in press, 1991). Collaborative computing: Collaboration first, computing second. Communications of the ACM, 34

Donald A. Norman, Department of Cognitive Science, University of California, San Diego La Jolla, CA 92093-0515 dnorman@ucsd.bitnet

---

**Re: AT&T ([RISKS-12.47](#))**

*<colwell@ichips.intel.com>*

*Fri, 11 Oct 91 10:40:45 -0700*

Some people seem to want to blame human weaknesses for the AT&T failure, other people seem to want to blame the technology. What I haven't seen anyone point out is that, every time AT&T (or most other people) does something to "improve" their system, they end up more and more centralized.

Actually, that's partly what I was trying to point out in my earlier post. When you install the same software (do they still call them "generics" inside Bell?) everywhere, you have an implicit single-point-of-failure across the whole network. Yes, when they route too much through a physical single point of failure, that's bad, and they know it (or should).

But it appears to me that

- the historical system availability target of 2 hrs outage in 40 years is no longer being met, even though it once was with much lower tech hardware
- the reason may be related to this implicit single-point-of-failure not

being made explicit in the way the code is written, or the development project is run.

Perhaps the attitude they took with the Space Shuttle computers needs to be transferred to the phone company. Yes, do a superlative job in programming the four on-board computers, write it to the most exacting specifications, then test the heck out of the code. But oh-by-the-way, here's a fifth computer with completely alien hardware AND SOFTWARE in order to obviate any implicit, unanticipated, yet catastrophic single-point-of-failure modes.

I don't know that this solution can or should be adopted wholesale; it's the frame-of-mind that the shuttle designers had that there is this class of problems that appears to be lacking in the current design of the phone system.

Bob Colwell, Intel Corp. JF1-19, 5200 NE Elam Young Parkway, Hillsboro, Oregon 97124 colwell@ichips.intel.com 503-696-4550

---

### ✦ **man-machine interface (was AT&T outage)**

*Mark Seecof <marks@capnet.latimes.com>*

*Fri, 11 Oct 91 11:13:06 -0700*

I think we're in danger of missing a key element in the AT&T outage. Yes, the technicians were lax (if understandably so); yes, AT&T had routed too much stuff through the one switch w/o any backup path (which I think was the chief screwup); yes, the alarm system was inadequate (which AT&T has promised to address).

But the real problem is that the power system and its alarm system were designed under the assumption (now vitiating) that technicians would be there to supervise it. Recall that AT&T says the rectifier failure was discovered only when a technician happened upon an alarm registering at a location (away from the power equipment) which was not ordinarily manned. That location would have been manned before AT&T ruffed many of its technicians. The alarm system was not adequate to alert the present human supervisory regime-- perhaps the old technicians should have been kept on the job until AFTER the promised new alarm system was installed?

Beefing up drills as suggested by some is an inadequate response to the design-constraint/ reality gap evident in the description of the AT&T setup. As hard as it is to get the humans to meet the needs of the system, or the system to meet the needs of the humans, if we don't try to match them at the interface as best we can, failure is certain. Building a machine which needs a supervisor, then firing that supervisor and expecting all to be well is foolish.

Mark Seecof <marks@latimes.com>

---

### ✦ **Re: "AT&T `Deeply Distressed' (Colwell, [RISKS-12.43](#))**

Bob Niland <rjn@hpfco.fc.hp.com>

Fri, 11 Oct 91 12:31:23 mdt

>This seems equivalent to the question of how much override a pilot of a fly-by-computer airplane should be able to exert; when the flight computer refuses to pull too many G's because the wings may overstress, but the pilot knows he'll hit a mountain otherwise, it's a bit clearer who should outrank whom.

Perhaps in that specific case, but in the general case it's not that clear. I haven't studied the statistics (if anyone even has any along these lines), but what if the data show that more people die because the crews override when they shouldn't than because they can't/don't override when they should.

We have already had a couple of Airbus losses in which a suspected cause is the crew inappropriately overriding the flight computer and riding the aircraft into the ground (e.g. Toulouse airshow). Have we lost any because the crew failed to override? Have we lost any other air transport types because of inability to override?

Speaking as a pilot myself, emotionally, I always want to have total authority of the craft, but if statistically I am more likely to live longer by not having (or at least not exercising) that authority, my preference is not completely obvious.

Perhaps the

"automatic | manual"

override switches need to have big legends above those descriptions, stating

"PROBABLY | USUALLY

SURVIVE | PERISH "

Bob Niland, 3404 East Harmony Road, Ft Collins CO 80525-9599

Internet: rjn@FC.HP.COM UUCP: [hplabs|hpfco]!hpfcrjn!rjn

---

### **✦ Keeping people in the loop (Bellovin, [RISKS-12.45](#))**

Martyn Thomas <mct@praxis.co.uk>

Fri, 11 Oct 91 12:47:09 +0100

We could make the humans the prime operators, and use the computers as a back-up. This preserves the motivation - noone wants to be caught making mistakes - and gives many of the desired benefits. Of course, we still cannot predict the reliability of the overall system, but that's another problem :-)

---

### **✦ A step towards adopting DefStan 00-55**

Vicky Stavridou <victoria@cs.rhnc.ac.uk>

Thu, 10 Oct 91 07:09:40 BST

Although 00-55 is an interim standard, it seems that there is real progress

towards its development and eventual adoption. About a year ago, we produced a VDM specification of the safety requirements for an ammunition control system (ACS) which is used by the Directorate of the Proof and Experimental Establishment of the MOD for managing the ammunition holdings of some ranges. I understand that the appropriate MOD authority intends to issue our specification as a part of the Operational Requirements draft for the next generation of the system. I believe that the intention is to provide an improved statement of the safety requirements during the tendering process. Although, this is a long way from full application of 00-55/56, it is certainly an encouraging and a very welcome step in that direction.

We have a technical report for anyone who is interested.

Victoria Stavridou

PS. If you want to followup this topic, please email me direct because our news server is down at the moment.

---

### ✈ Digital Retouching on the Telephone

<Chuck.Dunlop@ub.cc.umich.edu>

Fri, 11 Oct 91 01:28:16 EDT

The latest Hammacher Schlemmer catalog advertises a "Voice-Changing Telephone", that

uses digital signal processing technology to realistically alter the sound of the user's voice, even changing male speech to female, child to adult and vice-versa, to completely disguise identities and discourage unwanted calls. Perfect for people living alone or children at home by themselves . . .

Yes, and perfect also for abusive or threatening telephone calls, imposters' scams, and sexual harassment.

Even if used in the way that the advertisement suggests, some peculiar scenarios emerge. E.g.,

Deep Male Voice: Mommy and Daddy aren't home right now.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 12: Issue 49**

**Monday 14 October 1991**

## Contents

- [Nuclear Computer Safety Fears](#)  
[Antony Upward](#)
  - [Computer Error by Policeman](#)  
[Antony Upward](#)
  - [Thermostat failure mode](#)  
[Liudvikas Bukys](#)
  - [I really like banks -- world wide!](#)  
[Boyd Roberts](#)
  - [I'm sorry, the computer says your credit is bad](#)  
[David Bremner](#)
  - ["Who Flies the Plane?"](#)  
[Ken Tindell](#)
  - [Risks of Enterprise-Wide Phone Systems](#)  
[David Fiedler](#)
  - [AT&T Outage](#)  
[Jerry Schwarz](#)
  - [Re: "AT&T `Deeply Distressed'](#)  
[Flint Pellett](#)
  - [Re: External risks to computer systems](#)  
[Peter Mellor](#)
  - [Re: Keeping people in the loop](#)  
[George W. Leach](#)
  - [Re: ``Friendly" \(?\) viruses](#)  
[Brandon S. Allbery](#)  
[Paul Smees](#)
  - [Re: buggy software](#)  
[James B. Shearer](#)
  - [Re: Security Criteria, Evaluation...](#)  
[David States](#)
  - [Re: Software migration at Johnson Space Center](#)  
[Richard H. Miller](#)  
[Tim Parker](#)
  - [Info on RISKS \(comp.risks\)](#)
-

## **#Nuclear Computer Safety Fears**

*KPMG - Antony Upward, IVC*

*14 Oct 91 11:03 GMT*

>From the London Independent on Sunday, October 13, 1991

### Computer Watch On Nuclear Plant Raises Safety Fears

by Susan Watts, Technology Correspondent

Fears are growing that computer software designed to protect the Sizewell B nuclear reactor from serious accidents is too complex to check.

Sizewell B will be the first nuclear power station in the UK to rely so heavily on computers in its primary protection system. A computer-controlled safety system was seen as superior to one operated by people because of the risk of human error.

But Nuclear Electric has told the Independent on Sunday that the system for Sizewell B, based around some 300-400 micro-processors, is made up of modules which in total constitute more than 100,000 lines of code.

A number of software engineers close to the project are known to have suggested that the software is now so unmanageable that it should be scrapped, and the whole system built again.

The Nuclear Installations Inspectorate (NII), the public's watchdog on the nuclear industry, has taken the unusual step of publishing the safety requirements it is asking of Nuclear Electric, the company that will operate Sizewell B, before the utility can expect a licence to go ahead with the power station.

This is an attempt to calm the mounting anxieties of specialists in "safety-critical" programs such as the protection system at Sizewell - where lives are at risk should the software fail.

Two senior inspectors describe the watchdog's requirements in a paper in the latest issue of the trade journal Nuclear Engineering International. The paper is unusual because the NII traditionally keeps its options open when deciding whether to grant a nuclear power station a licence. The onus is on the operator to prove that its system is safe. Publishing this description of its requirements gives a clear idea of what the NII expects of Nuclear Electric.

Independent experts in safety-critical software are not happy with the NII's safety requirements. They say the paper shows the inspectorate is not asking Nuclear Electric to use the most stringent testing procedures currently available to prove that the software will work as specified.

They also criticise the inspectorate for not insisting on the most up to date mathematical analysis that could give an indication of the software's reliability.

These critics want Nuclear Electric to publish the results of its own internal

assessments and those of independent consultants whose date would give the rest of the industry a chance to see just to how reliable the protection software is meant to be.

The British Computer Society says it would welcome the chance to comment of the safety case for the software. It is concerned about what it sees as "the secrecy which surrounds the safety-critical software in the Sizewell B control and production systems".

David Parnas, an advisor on a similar project at a nuclear reactor in Darlington in Canada, agrees. "If somebody is introducing a technology with as bad a reputation as software, then they are obliged to show that they have done a really thorough analysis." Given the public interest, he says, the results should be published.

The main worry is that the software, being produced by Westinghouse, an American company, is so large and complex that it is impossible to verify that it would react as it should if the reactor behaved dangerously.

A simpler system would be easier to verify and to maintain. But it would be difficult, though not impossible, to find a politically acceptable route whereby the existing system could be scrapped and development started again from scratch.

The software is thought to have reached its size because it has many extra features which, although desirable, have complicated its structure and blurred the distinction between the software which controls the nuclear reactor and that which protects it.

David Hunns, superintending inspector at the NII, and one of the authors of the recent paper, says that this distinction is "fundamental". Nuclear Electric insists that independence between the two systems "is fully maintained".

Mr Hunns adds: "We don't think it [the system] should be scrapped. We believe a safety case can be made. But it has to be proven. We have made a judgement. It's an honest and it's heart-searched judgement. We've looked hard at the technology - all the aspects that we possibly can. We've developed a rationale that is expressed [in the paper]. Providing the elements of that frame work are fulfilled that [Nuclear Electric] will make it. If they are not fulfilled, they won't. Then maybe they will wish they had started in another direction."

[Subsequent to the above, the following appeared -- giving what I thought to be a very good introduction to the complex problem of testing, and how it relates to the Sizewell B Nuclear Power Station.]

>From the London Independent on Sunday, October 13, 1991

A Complex Problem of Tests, by Susan Watts, Technology Correspondent

Software engineers agree that it is not safe to assume that software will always operate correctly - especially in systems such as nuclear power stations where people's lives are at risk if the software fails.

But computer programs are notoriously difficult to verify. The chief anxiety

over the protection system for Sizewell B is that it is very large and complex. This bucks the trend in safety critical software, which is to built small, simple systems.

It is usually impossible to test software for all combinations of the inputs it may receive - say from the reactor in a nuclear power station. It would take thousands of years to test the most simple system.

An alternative approach is to rely on statistical analysis of the system to give probabilities of its reliability. This would involve running the system for long enough to get an idea of the chances of it failing. But even this could take many years for a large system.

A more recent technique is to use so-called "formal methods". This involves converting the specification for a piece of software into a precise mathematical model of the requirements to "prove" that it works. But formal methods are a new idea; the software for Sizewell B began life some eight years ago, when the concept of formal methods was embryonic.

David Hunns, superintending inspector at the Nuclear Installations Inspectorate and co-author of a recent paper on protection systems for Sizewell B, says the case for insisting on formal methods is not clear cut. In his paper Mr Hunns says "the NII has accepted that is not reasonably practicable to achieve their incorporation for Sizewell B".

He adds that the viability of a second best approach, which involves "backfitting" the mathematical techniques of formal methods to a completed piece of software, also "remains unresolved".

Independent software engineers disagree. This method of backfitting is being used to verify software at a nuclear reactor in Darlington in Canada with a similar, although far smaller, computer-based protection system.

Nuclear Electric has designed its system such that it should fail no more than once in every 10,000 "demands" (a demand is when the reactor is in a state where the software should shut it down).

It is just about feasible that a system with such a failure rate could be simulated by building another computer program to replicate the reactor, hooking that up to the protection software and physically testing whether the protection system behaves as it is designed to. This approach would be time-consuming, and expensive.

Nuclear Electric is building a scaled down version of such a test system, and expects results next summer. The test involves a prototype of one channel of the protection software, but will not run for long enough to be described as exhaustive. Mr Hunns insists that if the simulation shows the software contains an unacceptable number of errors, NII will ask Nuclear Electric to extend the test.

[Antony Upward, KPMG Management Consulting, Software Development Group, 8 Salisbury Square, London, UK EC4Y 8BB Phone: +44 71 236 8000]

---

## # Computer Error by Policeman

*KPMG - Antony Upward, IVC*

*14 Oct 91 11:03 GMT*

>From the London Guardian Friday October 11, 1991

Computer Error by Superintendent

A police superintendent discovered his former wife had a new man after checking a car through the Police National Computer, Bow Street Magistrates court, London, heard yesterday. Leslie Bennett, aged 44, based at Chelsea, west London, asked another officer to access the computer about the car which his former wife said belonged to a friend of their daughter's. But the vehicle's details related to the wife's firm. His daughter, Jane, then told him the man was her mother's "new friend". Mr Bennett was found guilty of an offence under the Computer Misuse Act 1990 and fined =L150 with =L250 costs. The case followed a complaint by Mrs Bennett.

[ADDED NOTE: We learned on 13 Jul 2009 that Mr. Bennett's case was later appealed and upheld; Mr Bennett received his fine and costs back. PGN]

---

## # Thermostat failure mode

*<bukys@cs.rochester.edu>*

*Mon, 14 Oct 91 12:05:48 EDT*

I have a typical electronic setback thermostat installed. A couple of nights ago it failed "on", causing my furnace to run and run, until my three-year-old woke up and came to tell me that she was hot. The temperature had reached 92 degrees(F).

The thermostat itself had decided that it was still 68 degrees(F). Rebooting the thermostat by removing and re-inserting the batteries made it get back in touch with reality. I replaced the batteries too, but, considering it had enough power to run the LCDs, that's probably not it.

There are electronic setback thermostats that mount over existing mechanical (mercury switch) thermostats. I always thought it was silly to have a little motor move the arm up and down to cycle the furnace. But now I have to wonder about what temperature my electronically-controlled furnace would be driven my house to before either reaching thermal equilibrium or igniting or melting something, especially if left to itself over a vacation. (I don't know yet whether the furnace itself has its own thermal shutdown, but I doubt it.) At least with a mercury switch in there, the most extreme setting is probably still below where my good old all-electronic device would have taken my house.

Liudvikas Bukys <bukys@cs.rochester.edu>

---

## **✶ I really like banks -- world wide!**

*Boyd Roberts <boyd@prl.dec.com>*

*Mon, 14 Oct 91 11:09:33 +0100*

I'm Australian, but I now live in France. In the past few months I have had some really gnarly problems with banks in Sydney, Paris, London and the West Coast.

My `new' bank refuses to give me a cheque book, but they don't bother to tell me why. I got this missive from one of the administrators here today:

Hi Boyd,

My telephone discussion with your bank this morning was another piece of surprise !

Your checkbook request was refused because records showed Mr. Roberts was under national bank interdict !!! I certainly refused such a statement and discussed your personal data with them. What actually happened is that a confusion was made between two different Mr.Roberts (I do not understand why, as nationality, birth date, address, are totally different ...)

Mrs.[deleted] is requesting today interdict removal on your name and getting a checkbook for you. Checkbook should be ready by next Monday. I'll keep you posted, as usual.

Boyd Roberts                      boyd@prl.dec.com

---

## **✶ I'm sorry, the computer says your credit is bad**

*David Bremner*

*Mon, 14 Oct 91 14:29:03 PDT*

>From an article on financial software in DEC Professional:

"Expert systems is [sic] another rapidly growing area in financial software, notably in real-time applications found in banking, insurance and accounting venues. Inference, for example, has developed expert systems credit approval software Dun & Bradstreet and Swiss Bank"

Ah yes, I can see it being a major competitive advantage to be able to propagate data-entry errors in "real-time" :-)

Reference: p. 54, Oct. 1991 DEC Professional                      ubc-cs!fornax!bremner

---

## **✶ "Who Flies the Plane?"**

<ken@minster.york.ac.uk>  
14 Oct 1991 16:23:59 GMT

I recently caught a television programme on Channel 4 in the UK called "Who flies the plane?" (part of a consumer affairs series of programmes). The programme dealt with some of the issues of software in fly-by-wire commercial aircraft, particularly the 'human factors' problem. A number of notable people in the aviation field were interviewed.

I wrote to Channel 4 and asked if I could have a transcript of the programme, and permission to post excerpts to RISKS ("RISKS is a highly regarded international forum on software safety .. blah blah .. welcome comment .. blah blah .. "). The terse reply was along the lines of "The transcripts are too costly, and Channel 4 owns the copyright, so no". And the RISK of this story? I believe these programmes to be sensationalist, interested in viewing figures rather than rational discussion of the issues.

Ken Tindell, Computer Science Dept., York University, YO1 5DD UK  
+44-904-433244

---

### **✶ Risks of Enterprise-Wide Phone Systems**

David Fiedler <david@infopro.UUCP>  
Sat, 12 Oct 91 15:19:14 PDT

The other day, my wife called our local bank to discuss refinancing a loan. Her call was transferred to a loan officer, and she made an appointment for us to meet at the bank to discuss matters. When we got there, nobody at the bank had ever heard of the loan officer. It finally developed that the loan officer was based at another branch 35 miles away.

When transferring phone calls within a company's phone system is so easy, customers have no way of knowing that "the bank" they were talking to was somewhere else. Perhaps phone systems could be designed for the office personnel to be notified when a call has been transferred from another location, by a special ring or tone on the line.

David Fiedler UUCP:{ames,bytepb,mrspoc}!infopro!david  
USMail:InfoPro Systems, PO Box 220 Rescue CA 95672 Phone:916/677-5870

---

### **✶ AT&T Outage**

Jerry Schwarz <jss%summit@lucid.com>  
Mon, 14 Oct 91 16:06:01 PDT

It is easy to focus on the proximate causes of accidents and even on the general system level causes. But the recent AT&T outage in NY is a perfect opportunity to ask a question about very high level causes that has bothered

me for a while. Can the recent rash of failures in the phone system be traced to divestiture and price competition in the phone business? When new technology (such as software of fiber optic cables) fails it is hard to address this question. But here we had a failure in one of the oldest technologies in the business. So we can ask the specific questions: Have procedures or staffing levels in "power" changed since divestiture? Would pre-divestiture procedures or staffing levels have prevented the recent outage?

I have no particular knowledge of this area. Perhaps someone who does would care to address my question.

Jerry Schwarz jss@lucid.com

---

**Re: "AT&T `Deeply Distressed' (Niland, [RISKS-12.48](#))**

*Flint Pellett*

*14 Oct 91 19:30:31 GMT*

Why have an all-or-nothing user interface? If you're at 105% of design tolerance for G force, it isn't the same thing as exceeding the design by 200%. Tell the pilot by how far the design is being pushed, and let them decide if the risk is warranted by the situation. The machine's job is to make sure all the information necessary to produce a good decision is available to the pilot, not to suddenly at some arbitrary cut-off point start making the decisions for them.

Flint Pellett, Global Information Systems Technology, Inc.,  
1800 Woodfield Drive, Savoy, IL 61874 (217) 352-1165 uunet!gistdev!flint

---

**Re: External risks to computer systems (Rose, [RISKS-12.47](#))**

*p mellor <pm@cs.city.ac.uk>*

*Fri, 11 Oct 91 17:41:49 BST*

> If you don't what catastrophic failures, you need to arrange things so that  
> the inevitable failures aren't catastrophic. (P.Rose in [RISKS-12.47](#))

Despite the possible consequences of system design (including software) faults, it is still the case that fire, flood, and other "natural" disasters can be far more disastrous for a computer system, particularly a centralised one.

Earlier this week, the London Evening Standard carried a very small paragraph reporting a fire at Hitchin College of Further Education. This drew my attention, since it is a few miles from my home, and my ex-wife works there as a secretary.

The fire started at 2 a.m., and was not discovered for an hour. By then the building complex housing the total computing facilities of the college, both educational and administrative, had been gutted. The back-up tapes, needless to

say, were stored on-site, close to the computers, in a non-fireproof cupboard.

Total damage to computer equipment was quoted in the paper as 10 million pounds. This seemed a bit high to me (for a moderately-sized college with no large mainframe), and the figure probably includes other damage (library, dance studios, video equipment, etc., etc.) and a finger-in-the-air guess at consequential loss. The last item seems to be incalculable, however, given that the college's financial and student records have all been wiped out. It is on the cards that Hitchin College will cease to exist as a separate institution.

My ex-wife was surprised that the college had not been regularly exchanging back-up media with its associated institutions in Letchworth and elsewhere. I replied that this is exactly what I recalled ICL doing: 3-level back-up cycled every day between sites, and all tapes stored in locked fire-proof safes. I then recalled why ICL adopted this admirable policy. In the early 70s they lost an entire installation, including all back-up, when the night operator dropped a cigarette into a waste-paper basket.

Do we always have to learn the hard way?

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

---

**Re: Keeping people in the loop (Re: Thomas, [RISKS-12.48](#))**

*George W. Leach*

*Mon, 14 Oct 1991 13:50:12 GMT*

>We could make the humans the prime operators, and use the computers as a  
>back-up...

This is exactly how the monorail system at Walt Disney World is operated. There is a human driver who controls the speed of the train. There are speed zones along the lines where, if the operator fails to keep the speed under a prescribed value, the train will be shut off automatically. However, the human is the primary operator.

George W. Leach, AT&T Paradyne, Largo, FL 34649-2826 USA 1-813-530-2376

---

**Re: ``Friendly'' (?) viruses (Smee, [RISKS-12.45](#))**

*Brandon S. Allbery KF8NH*

*Sat, 12 Oct 91 18:41:43 -0400*

> Most people reading this use a machine running Unix. Somewhere in its file  
> system (usually /usr/spool/cron or /var/spool/cron) there is a directory  
> `crontabs' containing files which describe actions to be executed regularly  
> without explicit user action.

Granted --- but the system administrator should check these actions both when installing the system and periodically thereafter. (I do so once a month; a more secure environment would require more frequent checks.)

That many novice Unix sysadmins do not check their crontabs (by the way, you neglected to mention the V7 and BSD /usr/lib/crontab) is a RISK, but is in essence their fault. That modern "plug-and-play" Unixes do not provide an easy means to do this for the novice sysadmin is a contributory factor; this can be likened to the off-and-on "fly by wire" discussion on this list ("system administration by wire"?). Modern Unix systems do not take this into consideration, mainly because the systems of the past did not --- but those systems required competent system administrators anyway, so it was not a problem then.

Brandon S. Allbery allbery@NCoast.ORG uunet!usenet.ins.cwru.edu!ncoast!allbery

---

### **✱ Friendly (?) viruses (Meyer, [RISKS-12.47](#))**

*Paul Smee <P.Smee@bris.ac.uk>*

*Sun, 13 Oct 1991 16:08:56 GMT*

I think you are taking me a bit TOO literally. True, there are things which run on 'my' systems which I don't explicitly know about each instance of. There are also things (user programs) which I generally don't know about at all, but which are necessary to our service.

The point is that (as an admin), for every 'proper' thing running on the system I can, if necessary, point a finger at who is responsible for it, who DOES know about it (if I don't), and who is responsible for making sure it behaves sensibly (if that's not me). It's not that I know everything that is happening, but I can, without needing to use heroic or unusual procedures, find out what I need to know about it, and where I can get help if required, in order to ensure continued service.

>It also seems that an automatic or semi-automatic bug correction service,  
>working somewhat in the style of mail and news (that is to say, updating remote  
>files in controlled conditions) wouldn't be such an absurdity as he suggests.

The salient points here are your 'in controlled conditions', and (in a bit I've cut) providing that the machine owner/operator/administrator has `subscribed' to such a service. (And that the group providing the service can control it to ensure that only those sites which want it get it. We don't even install official manufacturer-provided upgrades without first evaluating them under test conditions, to make sure they don't interact unfortunately with other things we run. It's surprising how often something can't be put up exactly as supplied, without requiring other work. I've long been in favor of automagic DISTRIBUTION of bugfixes, rather than having to wait for the semi-annual release tape. But, with the present state of the art, I want to look at them before I put them in.)

---

**Re: buggy software (Parnas, [RISKS-12.47](#))**

<jbs@watson.ibm.com>

Sat, 12 Oct 91 19:49:36 EDT

So far as I know no one is required by law to buy the products of Mr. Mitchell's company. If mature adults wish to buy buggy software I do not see why this should be any concern of Mr. Parnas.

A real risk is that laws will be passed requiring people to use certain crackpot programming methodologies which purport to be better than existing practice but which for some strange reason people refuse to adopt voluntarily.

James B. Shearer

---

**Re: Security Criteria, Evaluation ... (Spencer, [RISKS-12.48](#))**

David States

Sun, 13 Oct 91 20:53:58 GMT

> What, exactly, is the fundamental difference between a  
> time-sharing system and (say) a heterogeneous network?  
> Answer: there isn't one...

In a closed, time-shared system, if the kernel is secure, all of the kernel mode communications are secure. In a network environment, kernel messages must travel over communication paths which are not guaranteed to be secure. How long would a time-shared OS remain secure if user programs could monitor queries made by kernel mode system calls to kernel databases?

By this line of reasoning, public key encryption is essential to the development of reliable network based computing systems. If you can't rely on secure communications to distribute a key, there is not an alternative. Distributed networks are almost by definition insecure.

David States

---

**Re: Software migration at Johnson Space Center**

Richard H. Miller

Sun, 13 Oct 1991 20:18:07 CDT

This is starting to get off the the strict area and into computer religion was but I do need to make the following points: [We run both 2200 and VAX systems.]

1) The high end VAX does not even begin to compare to the high end Unisys systems. A 2200/644 is a large mainframe system and the new 2200/900 is even more powerful. A large VAX 9000 will not provide the same level of performance as a fully configured 2200/600 or 2200/900.

2) A Unisys machine will run absolutes created 15 years ago. There is no requirement for recompiling or relinking. The same application code will run and most of the same system control software across all processors.

Richard H. Miller, Asst. Dir. for Technical Support, Baylor College of Medicine  
One Baylor Plaza, 302H Houston, Texas 77030 Voice: (713)798-3532

---

**Re: Software Migration at Johnson Space Center (Sherr, [RISKS-12.48](#))**

*Tim Parker*

*14 Oct 91 21:01:08 GMT*

Where are the Silicon Graphics advocates??? From my recent research, SGI has a line of equipment much better suited to simulation than anything in the VAX line (more horsepower, better graphics)- at a small fraction of the price.

Tim Parker - Independent Consultant

---

**Informatik journal available**

*Duane*

*Fri, 11 Oct 91 10:23:52 CDT*

Announcing the first issue of 'Informatik,' a journal of free information.  
Currently available by FTP from: uunet.uu.net /tmp/inform1.Z  
ftp.cs.widener.edu /pub/cud/misc/inform-1.1.Z

Here is an excerpt from the introduction:

*/\* Introduction \*/ By the Informatik staff*

Welcome to the inaugural issue of Informatik, an electronic periodical devoted to the distribution of information not readily available to the public, with a particular emphasis on technology and the computing world. First and foremost, this publication is dedicated to the freedom of information. This journal is made possible by The First Amendment of the U.S. Constitution which states:

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; OR ABRIDGING THE FREEDOM OF SPEECH OR OF THE PRESS; or the right of the people peaceably to assemble, and to petition the Government for redress of grievances.

In this and coming issues, we plan to exercise our First Amendment rights to the best of our ability. We will print feature articles on hacking, phreaking, and various other illicit activities. We also plan on bringing you recent news and gossip from the underground, anything news of interest to hackers, phreakers, grifters, cyber-punks, and the like. Informatik will also provide a

plethora of information on the inner workings of corporate America and the U.S. Government.

DO distribute this freely! Remember this is not illegal, this is information.

\*Please send submissions and comments to [duane@shake.tamu.edu](mailto:duane@shake.tamu.edu). (for now)\*

Mack Hammer & Sterling [Editors]



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 12: Issue 50**

**Tuesday 15 October 1991**

## Contents

- [TRW misreports local taxes](#)  
[Mark Seecof](#)
- [ATM Doesn't Catch Cash Cache Problem](#)  
[Ed Miller](#)
- [Re: buggy software](#)  
[David Parnas](#)
- [Risks of genetic engineering?](#)  
[Michael Pilling](#)
- [Electronic thermostat failures](#)  
[Ralph Palmer](#)  
[Mary Shafer](#)  
[Bob Wilson](#)
- [ACM SIGSOFT'91: SOFTWARE FOR CRITICAL SYSTEMS \[timely reminder\]](#)  
[Nancy Leveson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ TRW misreports local taxes**

*Mark Seecof <marks@capnet.latimes.com>*

*Tue, 15 Oct 91 09:48:31 -0700*

According to the Wall Street Journal Monday 10-15 page B1, TRW has decided to purge local tax delinquency info from the files of consumers residing in four New England states. You will recall the Norwich, CT, local tax info errors; it seems that similar errors have been made in the files of consumers living in several other communities. TRW blames the problem on a lax sub-contractor. Many other people blame the problem, more broadly, on TRW's apparent unwillingness to verify input or accept corrections... Consumers say it's difficult to reach anyone at TRW who even appears capable of influencing the data in a file, and further report that TRW's personnel refuse to rectify errors even when the TRW folks' attention is drawn to them.

I heard a radio report (just a headline, really) this morning that TRW will provide "free copies" of credit reports to some (of their New England?)

consumers, in a PR move.

I'll seize this moment (do not attempt to adjust your display) to suggest that, darn it, Congress should require ALL credit reporting agencies and the like to notify each consumer they report on every time they issue such a report, except under a search warrant with a secrecy injunction. The agencies should be permitted to batch such notifications (e.g., must notify within 3 weeks and may include more than one notification in the same envelope). The cost of the notification can be absorbed into the cost of the triggering report (honestly, the cost would not exceed 25 cents/notice what with bulk mail rates and reports usually cost \$5-\$10 to the requester so it's not a big burden). Every notification should include the name, address, and telephone number of the original report requester and a copy of the report as issued (not some opaquely coded extract, such as the disclosures Equifax is famous for--the NSA could hardly decode them; they are MUCH harder to understand than the ones given to paying customers). Agencies should be liable for statutory damages in the amount of \$2500 or proven economic damages if greater plus reasonable attorney's fees in any event if they fail to correct any substantive error in a credit report within 30 days of written notification (with corrected reports sent to anyone who got an erroneous one).

Mark Seecof <marks@latimes.com>

[WSJ article also noted by Will Martin <wmartin@STL-06SIMA.ARMY.MIL>. PGN]

---

### **✂ ATM Doesn't Catch Cash Cache Problem**

*Ed Miller <Ed.Miller@corp.sun.com>*

*Mon, 14 Oct 91 17:34:17 PDT*

I went to extract cash from the ATM at a nearby branch of my bank. Instead of the twenty dollar bills normally issued by the machine, I was given one dollar bills. My account transaction indicated that the ATM believed it had given me twenties. (Had I been given twenties, the number of bills would have been correct.) RISKS of garbage in, garbage out? RISKS of computers that can not "read" their output?

Since I was actually at the bank branch and since they were open I went in to have my account corrected. One other customer had the same problem at the same ATM and was in line ahead of me. After the bank personnel had taken the ATM off-line, I asked several questions. I learned that the money put into the machine comms from U.S. Federal Banks in sealed containers. The local bank employees can neither open or inspect the contents of the containers. Since the bank had already paid the Fed for the cache, the bank appeared to be the loser in the situation, unless they can convince the Fed that they owned the problem. The bank employees did not seem to know of a process by which they could report this problem to the Fed. RISKS of a security system that does not allow a human monitor?

Ed Miller e@sun.com 415/336.4278

---

✂ **Re: buggy software ([RISKS-12.49](#))**

David Parnas <parnas@qusunt.Eng.McMaster.CA>

Mon, 14 Oct 91 21:38:33 EDT

James B. Shearer (jbs@watson.ibm.com) writes; "So far as I know no one is required by law to buy the products of Mr. Mitchell's company. If mature adults wish to buy buggy software I do not see why this should be any concern of Mr. Parnas."

As far as I know no one is required by law to buy an electrical appliance. Nonetheless, every country that I know requires appliances to meet certain minimal standards. Nobody is required by law to buy a car, but we do require cars to meet certain minimal safety standards. Nobody is required by law to fly in a commercial aircraft but we all expect that those vehicles and their pilots will be produced and/or trained in a professional way. Moreover, the manufacturers of all of these products are all expected to take responsibility for the things that they sell. When a defect is discovered in my car, the manufacturer is required to issue a recall notice and to repair that defect without cost to me. He cannot simply announce an upgrade and try to sell it to me, not if the problem is a real defect.

We could use the "mature adult" excuse to get rid of all of these regulations, but we would all be worse off for doing so. Your apartment could be destroyed because one of your "mature adult" neighbours bought an appliance that was not properly designed. Your child could be injured because one of your "mature adult" neighbours bought a car with defective brakes. Further, every time you bought one of those products you would have to determine its safety for yourself, whether you knew enough to do so or not.

Those who object to the suggestion that software products should be subject to safety requirements and that software manufacturers should be held responsible for the results of any negligence seem to believe that we are asking for special treatment of software. Au contraire! We are asking that software be treated like other products, produced by registered or licenced engineers, and that software manufacturers be treated like other manufacturers. Now, because of the supposedly non-physical nature of software, programmer's products seem to have special exemption. If cars were as buggy as the software on the market today, the automobile manufacturers would have long ago been sued into bankruptcy.

Mr. Shearer goes on to write, "A real risk is that laws will be passed requiring people to use certain crackpot programming methodologies which purport to be better than existing practice but which for some strange reason people refuse to adopt voluntarily."

I can assure Mr. Shearer that we are all against "crackpots". The problem is that it is difficult to tell the difference between crackpots and visionaries. Years ago I read a biography of Steinmetz, a visionary who thought that mathematics could be used to analyse the behaviour of electrical power lines and was considered a nutty theoretician by some practical people. Today, those who do not understand and use the methods that he proposed are considered incompetent. I am sure that there were some real crackpots around in Steinmetz' time, but I am certainly glad that his views prevailed.

David L. Parnas      parnas@sscvox.cis.mcmaster.ca

---

### **✂ Risks of genetic engineering?**

*Dr Chocberry)*

*15 Oct 91 04:01:07 GMT*

I would like to know what some molecular biologists, notably gene splicing specialists, have to say about this.

As I computer scientist, I know that even though we perfectly understand every single line of our programs, we often make mistakes in even small programs, and it is very difficult if not impossible to generate a bug free program of any medium to large size.

In genes, we do not even understand most of the basic instructions, and yet we are trying to make new programs using these instructions. Since DNA has far more single instructions in it than the average program, I wonder just how error prone genetic engineering is and how if at all you can protect against the effects of latent errors in the code?

Michael

---

### **✂ Electronic thermostat failures (Bukys, [RISKS-12.49](#))**

*Ralph Palmer <rpalmer@Think.COM>*

*Tue, 15 Oct 91 09:31:52 EDT*

I have also had an electronic thermostat fail 'ON'. I have a RobertShaw model T1020. I've had a problem with my transformer on my oil fired furnace, it only supplied ~5 volts to the thermostat, not the ~10 that the thermostat needed. Since the voltage is low, the thermostat draws down the 9 volt backup battery. I have observed two failure modes. If the battery dies when the furnace is off, the thermostat fails off. However if the battery fails when the heat is on, the heat doesn't shut off! I was fortunate to find this out on a saturday afternoon and shut down the furnace when the house was only ~90F.

I feel that the best design would be a fancy digital set back thermostat as the primary control unit, defaulting to a mercury thermostat in case of power loss to the control unit . Until I find such a unit I'll stick with my round Honeywell mercury thermostat, turn down the heat at night myself, and wake up to a cold house.

Ralph Palmer    rpalmer@think.com

---

### **✂ Thermostat failure mode (Bukys, [RISKS-12.49](#))**

*Mary Shafer <shafer@skipper.dfrf.nasa.gov>*

*Tue, 15 Oct 91 07:53:29 PDT*

I had a standard, non-computerized perfectly simple Honeywell round thermostat break about 20 years ago. We came home to find the house at about 95 deg and the heater still running.

I think you overestimate the reliability of "old-fashioned" systems. I've never had the trouble with any of the electronic thermostats that I had with the gems with the mercury switches.

By the way, many of us learned long ago to either turn off the heat when on vacation or to have someone check the house every day. Frozen water lines, stuck toilets, broken thermostats--no computer technology needed to mess things up. A co-worker came home from a week of houseboating on Lake Powell to discover that her house had caught fire. Fortunately a neighbor noticed and the damage was limited to the kitchen. The fire department says that it was probably the toaster oven. Apparently these are known for suddenly immolating themselves and the surrounding kitchen.

Mary Shafer DoD #0362 NASA Ames Dryden Flight Research Facility, Edwards, CA

---

**✂ Re: Thermostat failure mode (Bukys, [RISKS-12.49](#))**

*Bob Wilson <wilson@math.wisc.edu>*

*Tue, 15 Oct 91 10:35:20 CDT*

Both the failure mode and the fact that it failed at all are things to worry about, but your furnace almost surely does have a thermal shutdown. You don't say what fuel it uses, or whether it distributes the heat through forced air, hot water, or steam. I assume from your use of the word "furnace" and the phrase "to run and run" that it is not any common form of electric heating. Every plenum chamber (for hot air heat) should have an overheat switch. They have been required by code wherever I have lived, and even if your local code does not require it I am sure that so many do that it is much cheaper to include them in all cases. Typically the switch is a bistable disk type thermostatic switch mounted to the plenum chamber. I am not sure that boilers (for hot water or steam) have switches actuated by temperature but they do have overpressure switches which in most cases will accomplish the same thing.

Bob Wilson, University of Wisconsin, Department of Mathematics

---

**✂ ACM SIGSOFT'91: SOFTWARE FOR CRITICAL SYSTEMS**

*Nancy Leveson <nancy@ICS.UCI.EDU>*

*Mon, 14 Oct 91 17:16:26 PDT*

[With the deadlines approaching for reduced-rate early registration and for assured hotel space, it seems appropriate to run this reminder. PGN]

4-6 December 1991  
Fairmont Hotel, New Orleans  
FINAL PROGRAM AND REGISTRATION INFORMATION

Computer systems are increasingly affecting nearly every aspect of our lives. They control aircraft, shut down nuclear power reactors in emergencies, keep our telephone systems running, monitor hospital patients, and execute financial transactions. Although such critical systems offer considerable benefits, they also pose serious risks in that we are increasingly vulnerable to flaws and other deficiencies in the software, hardware failures, and effects of accidental and intentional computer misuse. SIGSOFT '91 focuses on the problems in building and validating critical software.

General Chair: Mark Moriconi, SRI International

Program Co-Chairs: Peter Neumann, SRI International

Nancy Leveson, Univ. of California, Irvine

Travel Arrangements: Johnette Hassell, Tulane University

Registration and Coordination: Judith Burgess, SRI International

burgess@csl.sri.com phone: (415) 859-5924, FAX (415) 859-2844

Program Committee:

David Barstow (Schlumberger)

Dines Bjorner (Technical University of Denmark)

Marie-Claude Gaudel (Universite de Paris - Sud)

Jim Horning (DEC Systems Research Center, Palo Alto)

Bill Howden (University of California, San Diego)

Hermann Kopetz (Technical University of Vienna)

Carl Landwehr (Naval Research Laboratory)

Bev Littlewood (City University, London)

Leon Osterweil (University of California, Irvine)

David Parnas (McMaster University, Canada)

Fred Schneider (Cornell University)

Vicky Stavridou (University of London)

Martyn Thomas (Praxis, Inc.)

Walter Tichy (University of Karlsruhe)

Elaine Weyuker (NYU Courant Institute)

WEDNESDAY, 4 DECEMBER 1991

Welcome and Introduction: 8:45am - 9:00

Mark Moriconi, SIGSOFT '91 Chair (SRI International)

Peter G. Neumann, Program Co-chair (SRI International)

Session 1: 9:00 - 10:15, Carl Landwehr, Chair

Formal Verification of Algorithms for Critical Systems

John Rushby (SRI International), Friedrich von Henke (University of Ulm)

State-Based Model Checking of Event-Driven System Requirements

Joanne M. Atlee and John Gannon (University of Maryland)

Open Discussion

Session 2: 10:45 - 12:30, Dines Bjorner, Chair

Rigorous Development Using RAISE

Bent Dandanell (CRI, Birkerod, Denmark)

Specifying and Verifying Requirements of Real-Time Systems

K.M. Hansen, A.P. Ravn, and Hans Rischel (Tech. University of Denmark)

A Systematic Kernel Development

J.F. S/ogaard-Andersen, C.O. Rump and H.H. Lovengreen (Tech. Univ. Denmark)

Open Discussion

Session 3: 2:00 - 3:45, Elaine Weyuker, Chair

The Infeasibility of Experimental Quantification of Life-Critical Software Reliability

Ricky Butler and George Finelli (NASA Langley Research Center)

PANEL: The Limits of Probabilistic Risk Assessment

Bev Littlewood (City University, London)

David Parnas (McMaster University)

Martyn Thomas (Praxis, Ltd)

Ricky Butler (NASA Langley Research Center)

John Musa (AT&T Bell Labs, Whippany, NJ)

The Butler/Finelli paper argues that ultra-high reliability cannot be validated directly from testing, nor can be it demonstrated by appeals to software fault-tolerance. What progress might we reasonably expect to make toward numerical risk assessment of life-critical software?

Session 4: 4:15 - 5:30, Martyn Thomas, Chair

PANEL: The Confused World of Standards for Critical Software

Martyn Thomas (Praxis, Ltd)

Peter Neumann (SRI International)

Mike DeWalt (FAA)

This session will explain and assess current government regulation such as British MoD DEFence STANdard 00-55/56 and various security criteria (e.g., U.S. TCSEC, European ITSEC, Canadian CTCPEC). What role should such standards play? What should be mandated?

THURSDAY, 5 DECEMBER 1991

Session 5: 9:00am - 10:30, Fred Schneider, Chair

Comparing Fault Detecting Ability of Testing Methods

P.G. Frankl (Polytechnic University), E.J. Weyuker (NYU Courant Institute)

An Exception Handling Model For Parallel Programming and its Verification

Valerie Issarny (IRISA/INRIA)

Open Discussion

Session 6: 11:00 - 12:30

INVITED TALK: Human Error in Design

Henry Petroski (Duke University)

Author of the widely-acclaimed books "To Engineer is Human: The Role of Failure in Successful Design" and "Pencil"

Session 7: 2:00 - 3:30, Victoria Stavridou, Chair

A Real-Time Transition Model for Analyzing Behavioral Compatibility of Telecommunications Services

E.J. Cameron and Y-J Lin (Bellcore)

Programming and Verifying Critical Systems by Means of the Synchronous Data-Flow Language LUSTRE

C. Ratel (Merlin-Gerin), N. Halbwachs and P. Raymond (IMAG/LGI)

Open Discussion

Session 8: 3:45 - 5:30, Mark Moriconi, Chair

Invited Presentations on Practical Experiences:

Validation of Critical Flight Controls

Jim McWha (Chief Engineer in charge of 777 Flight Controls, Boeing)

Reliable Software for the 4 ESS Switch

Michael Meyers (AT&T Bell Labs)

A Case Study of the THERAC-25 Accidents

Nancy Leveson (U.C. Irvine)

Session 9: 8:00pm - 9:30pm, Evening Poster Session

FRIDAY, 6 DECEMBER 1991

Session 10: 8:30am - 10:30, Hermann Kopetz, Chair

Stepwise Design of Real-Time Systems

Reino Kurki-Suonio (University of Technology, Tampere)

On Satisfying Timing Constraints in Hard-Real-Time Systems

Jia Xu (York University) and David Parnas (McMaster University)

Automated Analysis of Bounded Response Time for Two NASA Expert Systems

C-K Wang, R-H Wang, D-C Tsou, J.C. Browne, and A.K. Mok (University of Texas, Austin)

Open Discussion

Session 11: 11:00 - 12:30

PANEL: Future Directions, Nancy Leveson, Chair

Adjournment at 12:30

=====

AIR TRANSPORTATION. Delta Airlines is offering 40% off RT Coach fares within the U.S., 35% Canada, 5% off already discounted fares. Call 1-800-221-1212, ask for Special Meeting Network, refer to file ref no. V18006. Valid for travel from Nov. 30 to Dec. 10. 7-day advance purchase required.

=====

ADVANCE REGISTRATION FORM

SIGSOFT '91 -- Software for Critical Systems  
Fairmont Hotel, New Orleans, Dec. 4 -- 6, 1991

Name \_\_\_\_\_  
Affiliation \_\_\_\_\_  
Address \_\_\_\_\_  
City, State and Zip \_\_\_\_\_  
Phone (and FAX) \_\_\_\_\_  
Email address \_\_\_\_\_  
ACM or SIGSOFT Membership No. \_\_\_\_\_

Registration Fees

Category	Before	After
	Nov. 1	Nov. 1
ACM or SIGSOFT Member	\$280	\$330
Non-Member	\$330	\$380
Full-time Student	\$180	\$230

To pay by credit card, circle one: AMEX    VISA    MC  
Name on card \_\_\_\_\_  
Card number \_\_\_\_\_ Exp. date \_\_\_\_\_  
Signature \_\_\_\_\_

Make checks payable to SIGSOFT '91 in U.S. dollars. Fees include 3 continental breakfasts, 2 lunches, and the Proceedings.

Dietary requests: Vegetarian \_\_\_\_\_ Kosher \_\_\_\_\_

SEND THIS FORM WITH FULL PAYMENT TO:  
Judith Burgess / EL266, SRI International, 333 Ravenswood Ave.,  
Menlo Park, CA 94025, USA

For further information, contact Judith Burgess,  
telephone: (415) 859-5924, FAX (415) 859-2844, EMail burgess@csl.sri.com

NOTE: REGISTRATION BY EMAIL OR FAX IS ALSO PERMITTED (ONLY WITH CREDIT CARD).

=====

FAIRMONT HOTEL RESERVATION FORM

SIGSOFT '91 -- Software for Critical Systems

New Orleans, Dec. 4 -- 6, 1991

Name \_\_\_\_\_  
 Affiliation \_\_\_\_\_  
 Address \_\_\_\_\_  
 City, State and Zip \_\_\_\_\_  
 Phone (and FAX) \_\_\_\_\_  
 Date/Time of Arrival \_\_\_\_\_  
 Date/Time of Departure \_\_\_\_\_

Room Rates (subject to taxes):

Circle one:            Single \$99      Double/Twin \$119

RESERVATIONS: 1-800-527-4727 or 1-504-529-7111

To guarantee your reservation by credit card:

Circle one: AMEX    MC    Visa    Carte Blanche    Diners Club

Name on card \_\_\_\_\_  
 Card number \_\_\_\_\_ Exp. date \_\_\_\_\_  
 Signature \_\_\_\_\_

These rates apply from Nov. 29 through Dec. 8, subject to availability.  
 Reservations should be received 30 days in advance to ensure availability, but  
 later reservations will be accepted as possible. A deposit for the first night  
 must accompany your reservation to guarantee it for arrival after 6:00pm.  
 Cancellations must be made 24 hours in advance.

SEND THIS FORM TO:

The Fairmont Hotel, University Place, New Orleans, LA 70140, USA

=====

---



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 12: Issue 51**

**Wednesday 16 October 1991**

## Contents

- [Mathematical and scientific foundations for engineering](#)  
[Henry Petroski via PGN](#)
- [Thermostat failure](#)  
[Richard Schroepfel](#)
- [Blockbuster `Loses' Returned Video](#)  
[Mowgli C Assor](#)
- [Credit Card Fraud](#)  
[Brian Randell](#)
- [New Massachusetts check/credit card ID law](#)  
[John R. Levine](#)
- [Giving Away Privacy \(Continued\)](#)  
[Sanford Sherizen](#)
- [Re: buggy software](#)  
[Martyn Thomas](#)  
[Magnus Kempe](#)  
[Dave Parnas](#)  
[Bart Massey](#)  
[Ernesto Pacas-Skewes](#)
- [Re: TRW misreports local taxes](#)  
[Rob Spray](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***✉* Mathematical and scientific foundations for engineering (Petroski)**

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

*Tue, 15 Oct 91 19:54:33 PDT*

Henry Petroski (who is now writing a regular column for *\_American Scientist\_*) has a fascinating analysis of the Tacoma Narrows Bridge collapse on 7 Nov 1940 in the latest issue of *\_American Scientist\_*, Sept-Oct 1991, pp.398-401. Here are the last two paragraphs, food for thought particularly for those of you planning to be in New Orleans for Henry's talk at SIGSOFT '91:

Modern engineering rests heavily on mathematical and scientific foundations,

and that is why the first two years of the engineering curriculum are dominated by mathematics and science courses. Eager and impatient engineering students often ask the relevance of those courses to real engineering, and so the discussion of real-world examples such as the oscillation and collapse of the Tacoma Narrows Bridge is especially important to receptive and impressionable students. Teachers of engineering are repeatedly reminded how difficult it is to break poor mathematics and science habits, especially those acquired in elementary courses that give preemptive explanations to dramatic engineering phenomena and failures. Yet in the Tacoma Narrows case study, mathematics and physics are clearly behind the engineering science, for which they are properly prerequisite.

The juxtaposition of a simple, albeit retrospective, physical explanation and a complex engineering error has implications far beyond mere puzzle solving, for it contrasts the omniscient mathematician/scientist and the blundering engineer. It behooves us all to avoid such oversimplification and stereotyping, whether explicit or implicit, in our textbooks and our classes. The collapse of the Tacoma Narrows Bridge will no doubt remain, as it should, an irresistible pedagogical example; it should not also remain a classic example of interdisciplinary hubris and conflict.

---

### **✂ thermostat failure**

*"Richard Schroepfel" <rsc@cs.arizona.edu>  
Wed, 16 Oct 91 10:45:17 MST*

This is pretty vague, but relevant:

I recall hearing on the radio a couple of years ago, probably in Los Angeles, of a family that was killed by failure of a conventional thermostat. Investigators concluded that the temperature in the house had reached 110F.

Rich Schroepfel

---

### **✂ Blockbuster 'Loses' Returned Video**

*Mowgli C Assor <mowgli@magnus.acs.ohio-state.edu>  
Wed, 16 Oct 91 1:48:59 EDT*

Along the lines of the discussion of the AT&T and other semi-computerized systems risks, I ran into one today.

The Blockbuster chain of video stores uses a very spiffy computer system to, among other things, keep track of what videos you've watched, what they have in stock, & who has checked in & out what. All videos have a barcode, which they simply scan into the computer system.

When you bring a video in, you put it in the return box & eventually someone scans it into the computer as a 'returned' video. I checked out a video Friday, (Video A) and returned it Monday when I picked up another one (Video B). Today (Tuesday) I got a call that I had not yet returned Video A, & should do so

soon (on Monday it was already 1 day late).

I went in & returned Video B, & then mentioned that their computer was a little behind & had missed my return. The lady there remarked that that was odd, and went to find her manager (turns out assistant manager ;). The manager did all sorts of neat computer things, & wasn't able to find that someone else had checked out the video, & of course didn't find a record of me checking it in. She then mentioned that she didn't know how this could happen.

I pointed out to her that I had at least twice seen employees get distracted when they put the video on the counter (but before they check it in), & have another overzealous employee come along & clean the counter off (moving the tapes to the 'to be shelved' section). She then sent the first lady to check the shelves for it.

The video couldn't be found, & I then asked the manager if she could check if the video had been checked out by someone else. She replied that it had not, so if I didn't have it it must still be in the store. I was getting a little bit annoyed at this point, when the manager then said "I was training a new girl on Monday, & this morning we found about 25 videos hadn't been checked in properly." (Note that 2 paragraphs up she didn't know how this could happen ;)

So the upshot of this is, I have to hope that they find the video around the store somewhere (she also mentioned that misshelving videos was common among new employees) because otherwise I will have to buy it (and of course, I'm not allowed to rent any more videos from here until the entire matter is resolved).

At this time, Blockbuster thinks I stole the tape (even though the manager doesn't ;) & since I gave them the proof I didn't on Monday & they lost it, I of course have no proof anymore. The risk of relying on employees to know their jobs, I guess.

<Mowgli>

Address: mowgli@magnus.acs.ohio-state.edu (Mowgli Assor in quasi-real life)

---

## Credit Card Fraud

<Brian.Randell@newcastle.ac.uk>

Wed, 16 Oct 91 17:13:51 BST

The attached article is reprinted in its entirety from today's (London) Financial Times. I find it rather pleasing that one (claimed) reason for not using photographs on cards is the risk that this would in effect create a national identity card scheme. If we are to have such a scheme - and public sentiment against such a scheme in the UK has for years been very strong, with the cards that were introduced during World War II being abandoned as soon as the war ended - then I'd prefer it to be introduced properly, with suitable safeguards and legal framework. However, I also know that past research by the UK's Inter-Bank Research Organization (as it was then called) threw grave doubt on the effectiveness of using photographs, so I doubt that the identity card reason was foremost in the bankers' minds.

Brian Randell

Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, UK  
EMAIL = Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923

=====

#### CARD FRAUD PLAN COSTS BANKS (Pounds) 500M

By David Barchard

Britain's Banks plan to spend more than (Pounds) 500m in the next three years on an initiative to combat plastic card fraud but they have persuaded Mr. Kenneth Baker, the Home Secretary, to drop controversial proposals to put photographs of holders on all credit and debit cards.

Under the new fraud prevention measures, shoppers may soon have to punch in their personal identity number into a computer terminal each time they pay by card.

Other possibilities being discussed by the banks and the Home Office include checking a customer's identity by shining a laser beam on his or her retina and verifying the signature on the card by computer.

These proposals were discussed at a meeting in London yesterday between Mr. Baker and banking industry representatives on how to combat the rapid increase in plastic card fraud.

Losses on card fraud are expected to increase by more than (Pounds) 20m to about (Pounds) 150m this year and some bankers fear that losses next year could be close to (Pounds) 200m.

The banks promised Mr. Baker that they would spend more than (Pounds) 500m on technology and training during the next three years to fight card fraud. This would be the largest joint investment that they have ever made.

Banks fought against the introduction of photographs on cards because they feared the government was asking them to introduce an identity card scheme through the back door.

Mr. Baker said he had asked the banks to report to him early in the new year on the action they were taking to beat credit card fraud.

"There is a lot that can be done to curb it. We must work together to keep ahead of the criminals involved," he said.

Proposals to use personal identification numbers with cards at retail outlets would represent a partial return by the banks to something close to National Eftpos, the proposed national card scheme for electronic payment which they abandoned in January 1990 at a cost of more than (Pounds) 65m.

The odds are heavily on personal identification numbers being adopted rather than other methods. Bank customers already know how to use Pin numbers when using cash cards. Numbers could be introduced without any need to change the existing magnetic stripe technology for credit cards.

---

## ✂ New Massachusetts check/credit card ID law

John R. Levine <johnl@iecc.cambridge.ma.us>

Wed, 16 Oct 91 19:11:43 EDT

According to today's Boston Globe, the state legislature has recently approved and the governor is expected to sign a new law regulating the data that may be collected when a customer pays with a check or credit card. When a customer pays with a check, he may be asked to show a credit card and photo ID, but the only information that may be written on the check is the address and phone number. When a customer pays with a credit card, he may be asked to show a photo ID, but no extra info may be written on the charge slip. The customer's address can be recorded separately if needed for warranty or delivery.

This is in response to two separate abuses. One is that many stores recorded customers' race, ostensibly to help prosecute check bouncers. The other is that crooks armed with a victim's credit card numbers, SSNs, and addresses from checks and charge slips were able to get credit cards in victims' names and make thousands of dollars of phony charges.

Violators of the law will be subject to triple damages in case of credit theft.

John Levine, johnl@iecc.cambridge.ma.us, {spdcc|ima|world}!iecc!johnl

---

## ✂ Giving Away Privacy (Continued)

Sanford Sherizen <0003965782@mcimail.com>

Wed, 16 Oct 91 17:13 GMT

A bit ago, I wrote in RISKS about some of the ways by which individuals are giving away their private information. At times, this is involuntary (such as a condition of employment) while, at other times, people give away this information for a sales coupon or while filling in a warranty card for a product. In my previous posting, I said that Big Brother has turned out to be the Big Browser.

Even though TRW may have changed some of its tactics, the credit industry continues to grab bits and pieces of private information in any way possible. The privacy battle is far from over, particularly since TRW is going to provide credit histories while not having to reveal all of the personal information that it has gathered and continues to sell. What follows is a perfect example of what information is being sought and the often manipulative ways by which it is being gathered.

This is from a letter that BUYER'S MARKET sent to me.

"If you enjoy shopping by mail, we are ready to give you \$150 in savings just (sic) for telling us what's on your personal (sic) shopping list. This invitation is mailed to consumers with unique interests. People just like you, who are sought out by the nation's leading mail order companies. As part of this sought-after-group, you qualify for a six-month FREE charter membership in

BUYER'S MARKET, the new nationwide organization that not only arranges generous discounts for preferred mail order customers but also brings you:

\* MAIL-SELECTOR---...that helps you get catalogs and special offers on products you want (underlined) while helping to reduce unwanted (underlined) mail! (Sic)

\* [Deleted--Other similar materials]

... There is only one requirement: To receive a minimum of \$150.00 in Savings Certificates and FREE Charter Membership in BUYER'S MARKET, you MUST complete and return our Consumer Survey by October 30, 1991."

At the bottom of the questionnaire is a box market confidential. In small print, it is revealed that the organization is part of Equifax, which few consumers may realize is a biggie in the credit history industry. The confidential (but note not a confidentiality) statement is as follows:

"BUYER'S MARKET is a nation-wide organization of consumers sponsored by Equifax Consumer Direct. Consumer information provided to BUYER'S MARKET is used solely to facilitate consumer purchasing choices; it is not supplied for any consumer-evaluative activities and will not be added to any other Equifax database. The information you provide to Buyer's Market by completing this Member Profile will be kept completely confidential. Your answers will be used by the staff of BUYER'S MARKET solely to guide cooperating merchants in directing to you offers you may be interested in, and/or to help eliminate your name from mailings of offers you indicate you don't want."

Doesn't this confidential statement make you feel protected? I wonder how many people are going to fill out the "Consumer Survey", which contains sections on personal interests, uses of coupons, leisure and hobbies, new product preferences, purchasing plans, and "about YOU" (including questions on age, income, home ownership, length of residence, size of household, marital status, children by age, and personal computer).

Maybe Mr. Justice Thomas or the Honorable Senator Orrin Hatch, new converts to the cause of privacy, will become advocates for limiting this invasion. I wonder if their records on video rentals are available through Equifax?

Sanford Sherizen, Data Security Systems, Inc., Natick, MA  
MCI MAIL: SSHERIZEN (396-5782), PHONE: (508) 655-9888

---

### **✂ Risks from legislation (Re: buggy software, Shearer, [RISKS-12.49](#))**

*Martyn Thomas <mct@praxis.co.uk>  
Wed, 16 Oct 91 10:09:53 +0100*

jbs@watson.ibm.com (James B. Shearer) writes:

> A real risk is that laws will be passed requiring people to use  
> certain crackpot programming methodologies ...

This \*is\* a real risk. If our profession continues to be irresponsible, and

to use unqualified and untrained staff, undefined processes and poor quality assurance, for developing critical systems, then legislators will force us to change. If (when) this happens, I am confident that the legislation will be far from ideal - but the fault will be ours.

---

### **✂ Control of the software industry (was Re: buggy software)**

"(Magnus Kempe)" <magnus@lglsun4.epfl.ch>

Wed, 16 Oct 1991 18:02:25 +0100

David Parnas <parnas@qusunt.Eng.McMaster.CA> writes:

> As far as I know no one is required by law to buy an electrical appliance.  
> Nonetheless, every country that I know requires appliances to meet certain  
> minimal standards.

If this is intended to be an argument, then it is a fallacy. If all governments in the world practiced censorship of philosophical and political literature, would that make full-scale censorship a moral goal? Would that justify any kind of censorship?

It is certainly true that the software industry is not shackled by all-encompassing government control, while virtually all other business activities are. However, this does not imply that it is morally right to extend government interference (coercive "standards", "certifications", "licensing", etc.) to the creation of software --or to any other kind of productive activity.

Several premises are implicit in the arguments in favor of government control of business activities--especially when it comes to technical activities (e.g., software engineering.) Here are a few:

1. That pointing a gun at someone, telling him "Think and produce", is practical and moral.

In fact, it is neither practical--a mind can not be forced--nor moral--the man who, alone, initiates force against another is properly considered to be an evil criminal. Similarly, 50 million men holding the gun against a single man are both impractical and immoral. And 50 million men holding guns against each other are suicidal and evil, too.

2. That men, left to their own devices, will not create good things; therefore, they should be forced to act "in their own interest".

According to whose standard is it in a man's interest to be forced to act against his own judgment? It is not a value to be forced to spend one's time, one's life, in order to have, keep or make something one does not want.

3. That businessmen are evil man-haters, intent on destroying all human values; thus they should be presumed guilty unless they prove otherwise (e.g., "you will hurt someone with the things you do --prove you won't.")

But that is a negation of the purpose of business: the creation and trade of \_values\_. It is also a negation of logic and justice: the onus of proof is on he who asserts the positive ("you \_will\_ hurt someone", or, in Parnas's words: "we \_would\_ \_all\_ be worse off for [getting rid of all of these regulations]" --emphasis mine); it is profoundly unjust to consider a man guilty unless he should somehow "prove" a negative.

4. That voluntary trade to mutual benefit is bad, and that software is systematically "buggy" because software producers are not doing their best.

Of course, proof of \_this\_ is that the software industry is making \_billions\_. If you don't like my software, or if you distrust me, don't buy my products. If you think you can write better software than I do, go ahead--you are free to do so. I am eager to watch as you flood the world with excellent software. And, pray tell, do \_you\_ need to be pushed around by the government, with a gun pointed to your head, in order to write good software? Why want to coerce your fellow men, if you have the ability to do everything much better than they do? Why aren't you already many times richer than, say, Bill Gates?

5. That some people, especially those in government, know everything about anything, and should therefore dictate how software must be written.

I trust I am not alone to see the disastrous implications of this idea.

If, in the future, a moral cannibal should attempt to use the government's power to force me to create software according to \_his\_ "standards", "certification requirements", or to impose compulsory "licensing", I will not submit: I will never produce a single line of code under the threat of a gun. I do not ask men to live under my threats, nor do I surrender my life, my work, to their threats. What kind of man is it, who is ready to submit his free-will to a gunman? And what does the gunman expect to achieve--production, or destruction?

Check your premises.

Magnus Kempe, magnus@lgsun.epfl.ch

---

### **✂ Re: Control of the software industry (was Re: buggy software)**

*David Parnas <parnas@qusunt.Eng.McMaster.CA>*

*Wed, 16 Oct 91 13:53:50 EDT*

I hope that this discussion is not about to degenerate into the age-old debate about whether any regulation of industry is needed at all and whether that regulation should be "brutal", "full-scale", "all-encompassing" "coercive" or any of the other highly loaded adjectives and rhetorical phrases used by Mr. Kermpe. It seems to me that those issues are much more general than the mandate of RISKS and that Mr. Kempe's "Red Herring" images of people pointing guns at programmers are best discussed somewhere else. The issue that is relevant to RISKS is whether there is any reason to treat software products different from those produced by older technologies.

One premise that seems to run through Mr. Kempe's message is that programmes, like other pieces of text, are artistic creations and should not be "censored" any more than we censor books, poems, or essays. As a strong defender of the right to free speech, I can sympathise with his rejection of any restriction on our freedom of expression. However, our creations differ from those of traditional text producers in that they can be turned into mechanical objects with all the capability of endangering our fellow humans that other mechanical products possess. I am all in favour of allowing people to write, even publish, any text, but I worry about telling people that that text can be loaded into a mechanical device and will transform that device into something safe and usable. At that point, one must treat the text as one would any other appliance.

When I went through Mr Kempe's "declaration of independence" looking for remarks that were specific to computers I found only,

"4. ... that software is systematically "buggy" because software producers are not doing their best."

While I would not ever put the word "systematically" in front of "buggy", I think that this statement would be true if one inserted the word "many" (instead of the implied "all") before "software". There are many people who, because of a variety of external pressures are producing a lower quality of software than they could produce. In fact, I know many who have told me that they would like to do better, and could do better, if the market were better controlled and users were better informed about products. None of these people believe that "some people, especially those in government, know everything about anything, and should therefore dictate how software must be written" but they do believe that some regulation (e.g. truth in advertising) would help. Some believe that cigarette box style warnings would be enough, while others would prefer inspections and grading. Most take pride in their work and would like to make it easier for customers to tell the difference between their products and those of lesser quality.

Rather than paint frightening pictures of "big brother" censoring our our outpourings, we should try to examine the ways in which software products differ from other products and find the appropriate compromise between our right to produce arbitrary texts and our responsibility to avoid flooding the world with unreliable products.

David L. Parnas [parnas@sscvox.cis.mcmaster.ca](mailto:parnas@sscvox.cis.mcmaster.ca)

---

**✉ Re: buggy software (Parnas, [RISKS-12.50](#))**

*<bart@cs.uoregon.edu>*

*Wed, 16 Oct 91 13:50:00 PDT*

> We are asking that software be  
> treated like other products, produced by registered or licenced engineers

Like all those small appliances you mentioned?

There's no one right answer to the question of how to ensure the safety and

reliability of something as wide-ranging and widespread as software, and I am concerned that a person of Mr. Parnas' reputation might mistakenly give the impression that licensing all programmers across the board is feasible, much less a panacea of some kind.

IMHO, you could make a case for requiring a licensed safety engineer specializing in software safety to be in charge of development of certain types of software, such as medical software or control software for large industrial systems (e.g., nuclear power plants) where the general public welfare depends on this expertise. For other types of software, such as computer games or word processors, it is clear that no safety supervision should be required, since there is no threat of bodily harm to anyone as the direct result of the use of this software. There is probably some intermediate class of software applications where a UL-like oversight body would be the appropriate answer.

The situation with regard to reliability and fitness is similar. For example, the implied warranties of merchantability and fitness which already exist are probably adequate for computer games, but perhaps there should be special protections provided to banks who purchase multi-million dollar accounting packages.

Part of the problem IMHO is the use of the generic term "software," which implies that "it's all the same" in some important sense. This is less and less true as time goes on, and I believe that there will soon come a time when lumping all "software" together in discussions of safety and reliability regulations is about as common as lumping together cars, household appliances, and roller coasters under the term "electromechanical devices" in these discussions.

Bart Massey bart@cs.uoregon.edu

---

**✉ Re: buggy software (Parnas, [RISKS-12.50](#))**

*Ernesto Pacas-Skewes <skewes@CAD.MCC.COM>*

*Wed, 16 Oct 91 16:15:21 CDT*

Good common points brought up by Mr. Parnas. I specially support free bug fixes.

- > ... We are asking that software be
- > treated like other products, produced by registered or licenced engineers, and
- > that software manufacturers be treated like other manufacturers. . . .

The goal is commendable, but I'll take exception on the "registered or licenced" part. Looking back, registering and licensing are not necessarily related to being competent and responsible. The only (exaggeration?) things that registering and licensing are guaranteed to produce is income for the registra(e)r/licenser and job security for registered/licensed elites that are not necessarily competent or responsible.

Following the line of examples: The last time you went to a licenced (otherwise unknown to you) professional, were you sure s/he was "good"? Were you sure it was going to be expensive?

To be sure, I'm not saying that all those who are are, and all of those who aren't aren't. I'm just saying that registration and license like so many other things aren't always what they seem.

> . . . If cars were as buggy as the software on the market today,  
> the automobile manufacturers would have long ago been sued into bankruptcy.

I wasn't driving at that time, but I'm sure cars WERE as buggy as software IS.  
(Besides, several things can prevent bankruptcy, lawyers and lobbying come to mind)

Ernesto Pacas-Skewes PACASSKEWES@MCC.COM

---

**Re: TRW misreports local taxes**

*Rob Spray <spray@convex.com>*

*Wed, 16 Oct 1991 16:35:10 GMT*

>I heard a radio report (just a headline, really) this morning that TRW will  
>provide "free copies" of credit reports to some (of their New England?)  
>consumers, in a PR move.

According to Nareen (sp?) at TRW (214/235-1200) the report is slightly erroneous. Starting January 1, 1992, TRW will provide consumers with one free credit report per year. (You currently get a freebie, if you've been denied credit or employment because of a report, otherwise it's \$15). Apparently, they've had "a lot" of calls about this!

They need:

Full name

Spouse's first name

Addresses with zip codes for last five years

SSN

DOB

and a signed request for the info.

Send it to

TRW

PO Box 749029

Dallas TX 75374

A recording that explains this (but not the free deal) is on 214/235-5005

--Rob Spray

--spray@convex.com

--your RISKman in Dallas

[AND WAIT UNTIL AFTER 1 JAN 92. 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 12: Issue 52

Monday 21 October 1991

## Contents

- [The Future is Here](#)  
[Amos Shapir](#)
- [The\\_RISKS\\_of\\_Geraldo](#)  
[Andy Hawks](#)
- [Re: Police raid wrong house -- for second time](#)  
[Amos Shapir](#)
- [Re: TRW](#)  
[Bob Colwell](#)  
[Anthony DeBoer](#)  
[Steve Hollasch](#)
- [Re: buggy software](#)  
[Mark R. Cornwell](#)  
[James B. Shearer](#)  
[Byron Rakitzis](#)  
[Richard Hanlon](#)  
[Stephen G. Smith](#)  
[Bob Wilson](#)  
[David Parnas](#)  
[David Chase](#)
- [Licensing Software Engineers](#)  
[Christopher E. Fulmer](#)
- [Info on RISKS \(comp.risks\)](#)

---

### The Future is Here

*amos shapir <amos@cs.huji.ac.il>*

*Thu, 17 Oct 91 17:45:36 +0200*

The Israeli Broadcasting Authority (IBA) is an independently budgeted government agency, financed by a special tax (sometimes called, for historical reasons, "TV license fee"). Since it does its own collection, it's sometimes even more zealous than the IRS. The following is a true incident that happened to a friend of mine:

She received a notice from the IBA to pay back due taxes. The strange thing about it was that it was sent to an address she moved into just ten days before, and was sure nobody but the landlord knew about. While she was in the IBA's office to settle the matter, she'd found out that due to recent unification of government databases, the following information about her was retrieved at a touch of a clerk's terminal key:

- Her new address (probably from the city's municipality);
- The type of each TV she'd owned since 1984 (dealers and importers are required to report that to the IBA);
- The dates in which she'd left and entered the country during that time (probably from the border police passport control records).

All this was just information necessary for the specific case at hand; that Big Computer probably knows a lot more about us. In short, the future is here, and it looks more Orwellian than Orwell could have ever imagined.

Amos Shapir, The Hebrew Univ. of Jerusalem, Dept. of Comp.Science. +972 2 585706

---

## **✂ The\_RISKS\_of\_Geraldo**

*Andy Hawks <ahawks@isis.cs.du.edu>*

*Wed, 16 Oct 91 18:41:23 MDT*

I'm sure many of you saw or have heard/read about Geraldo Rivera's Now It Can Be Told Program which featured a show on hackers a couple of weeks or so ago.

Well, by airing this program, it appears that Geraldo (or actually the producers/editors of the show) have put at least one military computer at risk.

One segment of the program featured a "home video" of Dutch teenagers hacking. This home video would occasionally focus in on the computer screen as the hackers hacked. As reporter Krista Bradford describes what is going on, the screen shows:

```
>
| quit
| 221 Goodbye.
| rugrcx>
| telnet tracer.army.mil
| Trying 192.33.5.135....
| Connected to tracer.army.mil
| Escape character is '^]'.
|
| Xenix K3-4 (tracer.army.mil)
|
| login:
| dquayle
| Password:_
>
```

Then we learn that previously, the hackers have gained superuser privileges to the system. As Krista Bradford is describing the superuser access, we see the

computer screen again and the hackers are attempting to login to the same site with the 'sync' login (so, this is apparently how they gained superuser access).

Later in the show (about 1 minute or so after the hackers have gained superuser privileges) Emmanuel Goldstein (2600) states that the hackers proceeded to create a new account. The account they create is 'dquayle' (Dan Quayle) and has superuser privileges. Then, the screen focuses in on the new record in /etc/passwd for 'dquayle', and Mr. Goldstein tells us that the new account has no password (the screen focuses in on: "dquayle::")

Thus, anyone who has telnet access could've repeated this same process, logging in to this tracer.army.mil site with the username 'dquayle' (and no password) and would have gained superuser access.

It is obvious that in this situation, whoever allowed the show to be aired in its final form had no knowledge of the Internet, otherwise this definite "how to hack" security breach would have been omitted.

Thanks Geraldo, for showing all of us how to hack into military computers.

(Note: I avoided sending this in for submission earlier to prevent any other hackers from repeating the same experiment. Hopefully, tracer.army.mil has now had enough time to plug up the obvious hole.)

---

### **✂ Re: Police raid wrong house -- for second time**

*amos shapir <amos@shum.huji.ac.il>*

*Thu, 17 Oct 91 17:39:41 +0200*

[Quoted from referenced article by dbenson@yoda.eecs.wsu.edu (David B. Benson)]

> The officers didn't leave until Dean Krussel showed them

>Callahan's letter. "This thing just won't go away," he said

This seems to be a Law of Nature in computer systems: Nothing ever goes away. Many databases keep each datum as an initial entry enhanced by a set of update records (I suspect some even run through the whole update process every time they're rebooted). Every now and then a system crashes, someone loads a wrong backup tape, etc., and voila! your magazine is being sent to an address you have left 12 years ago, or your house is being raided by the police... :(

Amos Shapir The Hebrew Univ. of Jerusalem, Dept. of Comp. Science. 972 2 585706

---

### **✂ TRW in chaos?**

*<colwell@ichips.intel.com>*

*Thu, 17 Oct 91 09:08:57 -0700*

No darn wonder the general public thinks the techies are clueless and screwing up the world. In OMNI's August 1991 issue, Kenneth Hey says (pg. 84):

"While human misuse of technology has reached bothersome levels [personally, biased and twisted thinking like this article bother me a lot more], technology can also assume a worrisome life of its own. TRW computer designers expressed surprise when a large network of computers they created began exhibiting 'strange, unpredictable' behavior. During these periods, the system could not perform specific tasks as requested. TRW suspected 'chaos', an uncontrollable but natural mathematical phenomenon, which mysteriously attacks complex computer systems. Scientists at the Xerox Palo Alto Research Center conducted a series of experiments and discovered that, indeed, large aggregates of connected computers can exhibit unpredictably wild oscillations and unstable behavior, generating unwanted actions in the system. The reality of computer instability -- that is, the real potential for chaotic behavior -- has raised professional concerns about the appropriate level of computer dependence for military, corporate, and informational systems."

Maybe the TRW system was just busy writing this article for OMNI...nah, it would have turned out a lot better. Anybody from TRW care to shed any light on what this person was talking about?

503-696-4550

Bob Colwell, Intel Corp, 5200 NE Elam Young Parkway, Hillsboro, OR 97124

---

**✂ Re: TRW misreports local taxes (Seecof, [RISKS-12.50](#))**

*Anthony DeBoer <adeboer@gjetor.geac.com>*

*Thu, 17 Oct 1991 09:28:57 -0400*

Why is it that inaccurately negative credit reporting [doesn't | shouldn't] constitute libel under the law? It would seem that if someone told a third party all kinds of horrible things about me that weren't true, at a certain point a line would be crossed and they'd be liable for damages. What is TRW's defense for this?

---

**✂ TRW Credit Reports**

*Steve Hollasch <hollasch@kpc.com>*

*Thu, 17 Oct 91 11:00:34 PDT*

In [RISKS 12.51](#), Rob Spray gave the procedure necessary to obtain a free credit report from TRW (TRW recently ``decided'' to send free credit reports to people who wish to see their file, as maintained by TRW).

Included in the description of the procedure to obtain this report is the following list of information that TRW needs before it will send it to you:

- Full name
- Spouse's first name
- Addresses with zip codes for last five years
- SSN
- DOB

It seems like catch-22 that people who are concerned about privacy are

required to send this information in order to check their records. On thinking about this list, though, it also becomes apparent that TRW must request some private information to verify that the requester is authentic.

Is it reasonable to assume that TRW already has all this information? If this is true, then my recent attempts to keep my SSN private seem rather futile. Why bother keeping something private when it is available in a public database (albeit for sale)? What information is available to those who subscribe to this service?

Steve Hollasch, Kubota Pacific Computer, Inc., Santa Clara, California

---

**✉ Re: buggy software ([RISKS-12.50](#)) and Steinmetz**

*Mark R Cornwell -- Mind Tools Corp <cornwell@rock.concert.net>*

*Thu, 17 Oct 91 13:32:26 -0400*

In recent exchanges between David Parnas (12.45,50) and James Shearer (12.49) the issue of who should assume the risk of software bugs has arisen. Let me say at the outset that I dislike the term "bug". I will use the term "error".

It is not necessary to make a blanket judgement about who should assume the risk of programming errors. A software license can be structured so that either the client or the vendor assumes this risk. The decision is best left to them. The public then has recourse against the party who has agreed to assume the risk.

That said, I think that it would be better for the software profession if standard practice were that the vendor assume the risk of his programming errors. I know of no better way to create an incentive for vendors to provide quality software. If software vendors chose to be accountable for programming errors in their products, they might be willing to try more "crackpot" ideas in place of a process that few believe is working well.

Last night I was at a gathering of local entrepreneurs speaking with an independent software developer. He is president of his own corporation. He writes programs. He described his work with XWindows and Motif on the latest workstations in manufacturing. He asked me what kind of mathematics I studied and I started to tell him about correctness proofs of programs. When I told him that a program could be viewed as a function from states to states he was fascinated. He said he had never thought of programs like that before, but the idea appealed to him.

I felt like Steinmetz must have felt talking to an early engineer who built electric power systems. "You can think of the current plotted against time as a sine wave".

"Very interesting, I'd never thought to look at it that way before."

--Mark Cornwell

[OK. Time to blow the whistle on this subject, after the following messages... PGN]

---

✂ **Re: buggy software (RISKS-12.49,12.50)**

<jbs@watson.ibm.com>

Wed, 16 Oct 91 20:22:22 EDT

In reply to my post suggesting buggy software is not a major threat to the republic David Parnas writes in part: "We could use the "mature adult" excuse to get rid of all of these regulations, but we would all be worse off for doing so. Your apartment could be destroyed because one of your "mature adult" neighbours bought an appliance that was not properly designed. Your child could be injured because one of your "mature adult" neighbours bought a car with defective brakes. Further, every time you bought one of those products you would have to determine its safety for yourself, whether you knew enough to do so or not."

And what, pray tell, terrible disaster will befall me when my neighbor buys buggy software for his pc? Also if Mr. Parnas believes that the regulation of autos and electrical appliances means there is no need for a buyer to consider their safety he is sadly mistaken. Tens of thousands of people are killed using autos every year. This is somewhat more than are killed using computer software.

David Parnas also writes: "Those who object to the suggestion that software products should be subject to safety requirements and that software manufacturers should be held responsible for the results of any negligence seem to believe that we are asking for special treatment of software. Au contraire! We are asking that software be treated like other products, produced by registered or licenced engineers, and that software manufacturers be treated like other manufacturers. Now, because of the supposedly non-physical nature of software, programmer's products seem to have special exemption. If cars were as buggy as the software on the market today, the automobile manufacturers would have long ago been sued into bankruptcy."

Mr. Parnas appears to have things backward. So far as I know software is currently treated like any other product in the uniform commercial code and other general laws regulating commerce. Mr. Parnas is asking that software be subject to additional special regulation like that imposed on certain hazardous products such as cars despite the fact that in most cases software defects pose no equivalent direct danger.

James B. Shearer

---

✂ **Re: buggy software (Parnas, RISKS-12.50)**

Byron Rakitzis <byron@archone.tamu.edu>

Wed, 16 Oct 1991 23:47:55 -0500

Were it not for the hauteur in this posting, I would have let this go by. But let me just state: there are a number of us who believe that the product liability laws have gone way past any reasonable point. What used to be governed by contract law is now covered by the law of torts in the US, with the

pervasive motif being "it's the rich guy's fault".

Please keep the hysterics to a minimum and try to assess what product liability laws have to offer: there is some added factor of safety at a huge cost.

Witness the skyrocketing costs of medical insurance. Witness the fact that pharmaceutical companies are most reluctant to release new products, and for example have all but halted research on contraceptives.

Another snag is that liability is not determined by experts, it is determined by a JURY (at least in these United States). How is a jury going to make a reasonable decision on the alleged defectiveness of FooNix? And if some such laws come to pass, what software developers in their right minds will market products like FooNix? Will we all not be somewhat the poorer for this?

No doubt the intentions of such laws are noble: to protect the ignorant (your implication, not mine) public from being duped by unscrupulous business. However, such protection comes at a huge cost in liberty, money and time, and this cost should not be so callously dismissed.

---

### ✦ self regulations for buggy software instead of gov. regs

*<d3e198@bsip54.pnl.gov>*

*Thu, 17 Oct 91 12:45:56 -0700*

Although I believe that both Mr. Kempe ([RISKS-12.51](#)) and Mr. Parnas ([RISKS-12.50](#), 51) have good points, I believe Mr. Thomas ([RISKS-12.50](#)) points out a greater risk that our profession may be painting itself into a corner. After the recent failures of computer systems (AT&T's phone outage causing airline travelers to be delayed, the stock market problem which I can't remember when it happened, plane crashes, etc.) it would only take a headline like Computer Glitch Causes Nuclear Power Plant to Meltdown, XXX People Evacuated, State Declared Off-Limits for Next 10,000 Years, or Computer Glitch Causes Missile Launch, XXX People Killed before the world's public would demand a reckoning (witch-burning comes to mind).

Instead, perhaps our profession should try to become more *\_self\_* regulating. If we clean up our own act, *\_before\_* the government can step in, then it will be possible to set the regulations ourselves, instead of the *\*all knowing\** committees of governmental bureaucracy. Just as doctors are mostly self-regulating, so should the computer science field be. For example, as Mr. Massey suggests, the term software is used as a conglomerate of a large, diverse genre of products. But I feel that the computer science field itself should break it apart and do the categorizing. If we do not, someone else surely will, and will probably not do it in a way that most of the rest of us like.

Computers now control major parts of our lives e.g. airline safety, automobiles, medical systems, nuclear power plants, etc. (Whether this control is good or bad, or whether the manner in which they do the controlling and interacting with humans is good or bad is another topic.) They can easily do massive damage through negligence on the part of the software, design, or through hardware failure. This risk of disrupting (even endangering) our lives

makes a great need for regulation as Mr. Parnas suggests. The public has a reasonable expectation of safety and reliability, and the only way to meet this expectation is through some sort of standardization.

But as Mr. Kempe points out, pointing a gun at a programmer's head does NOT produce necessarily good code. Forcing people to do things usually ends in failure. The government is definitely not the body to do any regulating. I further agree that software engineering is an art. The U.S. Court systems have been treating software as books in the regards to the copyright laws. Many license agreements liken to their software to books. [Therefore you must treat this software just like a book with the following single exception. ... make archival copies of the software for the sole purpose of backing-up your software and protecting your investment from loss.]

To avoid the problem of *\*Big Brother\** watching the programmers, and to avoid taking the art out of the software engineering, a self-adopted code of *\*ethics\** can satisfy both the regulations and the art. If one feels pride in the following of a such a code, then there is a greater chance that the person will continue to follow this code willingly. It becomes a matter of personal integrity. This system is not fool proof, e.g. how many doctors are sued in mal-practices suits each year, but nobody quits going to the doctor because he then believes that all doctors are quacks.

Self-adopted codes would need validation of course. This could be provided with a minimal intrusion by the government, making it a law to provide free bug fixes (there's ALWAYS at least one more bug). From there on, the economic laws of supply and demand based on quality should enforce adherence to the regulations. For example, if company X develops a reputation as having very reliable software the first time around, then people will tend to buy X's software, just as is done in the market for other products.

Richard Hanlon

---

## **✉ Re: buggy software**

*Stephen G. Smith <sgs@grebyn.com>*  
*Thu, 17 Oct 91 16:38:40 -0400*

In [RISKS DIGEST 12.51](#), skewes@CAD.MCC.COM (Ernesto Pacas-Skewes) writes:

>I'm just saying that registration and license like so many other  
>things aren't always what they seem.

Ain't it the truth!

In particular, I see registration, licensing, etc, as being an attempt by the companies that write software to limit their liability. By having a "licensed professional" sign off on their software, they hope (IMHO!) to be able to say "This software was produced according to standard industry practice" when they produce the next Therac-25.

Unfortunately, there is no "standard industry practice" that will provide an assurance of good software, other than the blanket "good engineering practice".

The main causes that I've seen for bad software are management issues, rather than technical issues. In particular:

1. Software always seems to be produced under *\*extremely\** high stress. Only medicine and (possibly) law require high performance under higher stress conditions. This is usually caused by assorted forms of bad scheduling.
2. Many software managers fancy themselves as techies, despite the fact that they may not have ever written a line of production code. The urge to micromanage seems to be irresistible.
3. Specifications (IMHO, the most important part of the project) are often confusing, conflicting, or incomplete. "Formal verification" against a bad (English!) specification is, at best, a waste of time.

So how can we improve management? I dunno. Most of the outfits that I've worked for were strictly "top-down" -- directives come down from the top and status information goes up. Statements from the troops like "No way can this get done on time" tend to get lost.

Steve Smith, Agincourt Computing    sgs@grebyn.com    (301) 681 7395

---

### **✉ Re: Bart Massey on "Buggy Software"**

*Bob Wilson <wilson@math.wisc.edu>*

*Thu, 17 Oct 91 16:21:11 CDT*

Bart Massey believes you could make a case for licensing software production for medical software, etc., for which he sees a "threat of bodily harm", but he goes on that "it is clear that" no safety supervision is needed for computer games or word processors because they can make no such threat. (Of course "it is clear that" is a dangerous phrase to dangle in front of a mathematician...)

He may be right about a threat of BODILY HARM, but there are other very real threats. RISKS has had several examples of potential harms from word processors, to take one of his examples. Many of us surely write memos or letters we need to go back and tone down: The original, if published, might be dangerous at least to our economic health. We have seen here in the last several years examples of commercial word processors which would retain in the disk version of your document what you had deleted from the printed version, or for that matter what might have been in a disk block unrelated to the present document. Those contents are not hard to look at, if your employer sends somebody in to see what you have been saying about your boss or the company.

The controversy over Prodigy and whether it was "stealing" copies of things from your system represents a RISK in a system frequently used for game playing. Regardless of whether Prodigy was doing it, the RISK is there for some other communications related software to exploit. I don't like the idea of licensing software engineers, but I think it is too simplistic to think the only dangerously RISKy software is that used for medical instruments, nuclear

power systems, and vehicle controls. Those make nice examples because they are so far beyond question, but by the same token they also get more scrutiny. That scrutiny may not be enough, but it surely doesn't mean we can ignore the RISKS in more mundane applications.

Bob Wilson, Math Dep't, Univ. of Wisconsin

---

**✉ Re: buggy software ([RISKS-12.51](#))**

*David Parnas <parnas@qusunt.eng.McMaster.CA>  
Fri, 18 Oct 91 17:42:39 EDT*

Bart Massey claims there is no risk of harm from buggy wordprocessing software. If that software is used to produce the manual for a dangerous device, and deletes important warnings, there is a risk. I agree with Mr. Massey's attempts to draw lines and think it is obvious that there are shades of grey in this area, but the analysis is more difficult than it looks.

I am aware of all the weaknesses of licensing and registration raised by Ernesto Pacas-Skewes. I sometimes have to drive a car and observe what licensed drivers do with their properly registered (but inadequately equipped) cars. Nonetheless, when given a choice, I prefer drivers who did pass a driving examination to those who never were able to do so.

Perhaps we should stop arguing about whether some regulation is ever needed and start to think hard about what should be regulated, how it should be regulated, and who should do the regulation. When we do, I think we will find useful ideas in other fields of engineering.

Dave Parnas  
parnas@sscvox.cis.mcmaster.ca

---

**✉ Re: buggy software (Parnas, [RISKS-12.51](#))**

*<jbs@watson.ibm.com>  
Thu, 17 Oct 91 19:58:31 EDT*

I suspect "variety of external pressures" means "competition", "if the market were better controlled" means "if the competition was put out of business" and "users were better informed about products" means "users stopped worrying about minor factors such as cost, performance, timeliness and function".

James B. Shearer

---

**✉ re: buggy software (bart, [RISKS-12.51](#))**

*David Chase <David.Chase@eng.sun.com>  
Thu, 17 Oct 91 17:20:54 PDT*

> ... There is probably some intermediate class of  
> software applications where a UL-like oversight body would be the  
> appropriate answer.

This is a mere "difference of opinion", but I have certain expectations even of games and word processors. In particular, I expect that there are no bugs in the program which might result in the destruction of unrelated data stored on the same computer. (At this point, of course, the OS vendor and the games vendor engage in heated finger-pointing, and the customer is left grumbling.) This is a far cry from the reliability I expect from an airplane, or an EFT point-of-sale-terminal, but it is more than none at all, and I'd rather not verify it for myself. Furthermore, past experience indicates that "verification" is difficult and time-consuming, and not something that a customer is interested in doing.

There is the second problem of "the use of this software". Both software and physical devices are both put to unintended uses. I can't think of any really juicy software examples just this instant, but once upon a time someone I know did use a bicycle cone wrench in place of a 70-amp slow-blow fuse (that had blown).

David Chase, Sun

---

### **✂ Licensing Software Engineers (still more)**

*Christopher E Fulmer <fulme-ce@lea.csc.ncsu.edu>  
Fri, 18 Oct 91 13:26:51 -0400*

With all of the discussion going on about the RISKS associated with not having a mechanism for licensing software engineers, it seems to me that we are ignoring a few basic points.....

1. Licensing software engineers has the effect of reducing the number of people who are involved in software engineering. While this can be good (In the case of eliminating those who are incompetent), it also has the effect of putting the decision of "Who is competent" in the hands of some governing authority. And, that authority may have ulterior motives for making their decisions. The authority would have to be made up of practicing software engineers. (Who else is qualified to judge?), who may very well desire to keep the field of software engineers down, by making the standards tougher, thus increasing their own marketability. (Dry cleaners have managed to do this by pushing through a "Certification of Dry Cleaners" law in some states.)
2. The market does tend to push out poorly-designed products. However, for some products, it may not be desirable to wait for the market to decide. After all, Audi's sales dropped after the problems with "Instant Acceleration" were found by real people, not before.
3. A mechanism which is typically used by Government and Commercial bodies is the idea of the "Contract model," wherein certain specifications are set up, and products which do not meet those specifications are not paid for.

So, perhaps the solution to all this is not for the government to license

software engineers, but to instead set up minimal specifications for safety critical applications. Or, perhaps, to provide for the independent licensing of the products, and not of the people who design them.

In addition to solving the problems posed by #1 & #2 above, this also solves problems caused by bad software written by good people. Heck, certified engineers make mistakes all the time. What makes us think that programmers are different?

So, in conclusion, It's my opinion that we're trying to solve the problem of poor software quality by looking at the people who wrote it, instead of looking at the product of their work. Poor programmers, given enough time, can write perfectly good software, just as fantastic programmers in a rush can write terrible software. So, it's essential that we gauge the quality of the work, and not the quality of those who produced it.

Chris Fulmer      fulme-ce@lea.csc.ncsu.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 12: Issue 53

Monday 21 October 1991

## Contents

- [Inappropriate ATM error codes](#)  
[Sean Eric Fagan](#)
- [Blood Donor Cards](#)  
[Robert E. Van Cleef](#)
- [RISKS of new E911 system](#)  
[Paul Robichaux](#)
- [Unusual risks of frequent flying](#)  
[Rob Aitken](#)
- [Review of THE GLASS COCKPIT](#)  
[Robert Dorsett](#)
- [Yet another journalistic cock-up \(cracker activity\)](#)  
[Simon E Spero](#)
- [Assurance of High-Integrity Software - Report](#)  
[Rick Kuhn](#)
- [Video stores losing videos...](#)  
[Chris A. Anderson](#)
- [Re: Blockbuster](#)  
[Brian Boutel](#)  
[Matt Crawford](#)  
[Kevin Hughes](#)  
[Patricia Shanahan](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Inappropriate error codes

*Sean Eric Fagan <sef@kithrup.com>*

*Sun, 20 Oct 91 22:22:17 PDT*

After a longish day yesterday, I was on my way home, and decided to pick up some stuff for both dinner and breakfast at Lucky's. For those not acquainted with it, Lucky's allows customers to use an ATM card to pay for the purchases (and they pay for the transaction fee, which makes it attractive to me). This was at about 3:30AM or so. After getting everything I wanted, and standing at the register and shouting for someone

to come take my money, I tried to pay with my ATM. Slid it through the machine, entered my PIN, said I wanted \$20 extra in cash, approved it, etc.

Wait.

Error code 60. No approval.

I go, "Huh?!" Cashier takes out a little card, and shows me where it says "Error Code 60" is "incorrect PIN." So I tried again, making sure I had the right card, making sure I had the right PIN. Same result. I tried it with a smaller amount. Same thing. Paid with my reserve cash, and proceeded to drive down to a branch of my bank so I could make sure I hadn't gone broke.

Well, it turns out that it was the one hour a week when Bank of America takes down their network for (I assume) routine maintainance. Normally, when this happens, and I'm at a bank ATM (my own or a different bank), it says that it is unable to conduct the transaction, which is a different message than an incorrect PIN entry.

If Lucky's had had a correct error code (ETIMEDOUT would do 8-), I would have driven home a bit slower, and not had the near-corrorary when I passed the cop...

---

### **✂ Blood Donor Cards**

*Robert E. Van Cleef <vancleef@nas.nasa.gov>  
Thu, 17 Oct 91 11:32:51 -0700*

Last June I donated blood at a local blood drive. I was told that I would receive my blood donor's card in the mail in a couple of weeks.

I just got off the phone with a representative of the local Red Cross organization. A new computer system was installed last January, and the "card printing" portion of the software "didn't work out".

I can expect to receive my card in two to three months....

Bob Van Cleef, NASA Ames Research Center (415) 604-4366

---

### **✂ RISks of new E911 system**

*Paul Robichaux <robichau@freedom.msfc.nasa.gov>  
Thu, 17 Oct 1991 13:00:34 GMT*

[\_The Huntsville Times\_, Huntsville AL, 1991Oct15. My comments in braces.]

"Enhanced 911 put on hold until early '92"

[Julie T. Schultz, \_Times\_ Staff Writer]

Enhanced 911 officials [how are they enhanced?] Monday announced yet another delay in the operations of the new emergency communications system.

Emergency Communications Board Chairman Richard Holloway said that the system will be operational sometime in early 1992 rather than at the end of this month or early November.

The agencies that will use the system, Huntsville's police and fire departments, the city's ambulance service, and the county Sheriff's Department have requested a delay, Holloway said today. The agencies feel their dispatchers and other workers need more training on the system, he said.

[Concerns of this new system's impact on personnel, staffing levels, etc. deleted.]

If agencies had to switch to the new system during the next few weeks, [E911 Committee Chairman Philip] Arnold said workers would have to run a "parallel operation to the computer-aided dispatch system."

"Anytime you convert over to something new you continue the current process for awhile and then compare them for glitches," he said. "We would have to staff the old and new systems simultaneously if we started" late this month or early November.

Several months will give workers time to train on and test the system at the same time, he said.

Despite the fact that Mr. Arnold appears to be aware of some of the RISKS of abruptly switching over to a new system, the article seems to say that Huntsville's E911 will abruptly replace the current system \*with no parallel system in operation at startup.\*

The RISKS here should be evident to readers of the Digest.

-Paul Robichaux

---

### **✂ Unusual risks of frequent flying**

*Rob Aitken <aitken@hpdtra.ctgsc.hp.com>*

*Thu, 17 Oct 91 13:02:36 pdt*

Recently, when I opened the monthly statement for a frequent flyer program to which I belong, I discovered that someone else's statement had been stuffed into the envelope with mine. I was thus able to see which flights this person had taken that month. A potentially RISKier piece of information I was also able to obtain, however, was the amount of her airline Mastercard bill, which had been credited as miles to her account. I think the biggest risk of the entire episode, though, comes from the sorting technique used to print the mileage statements: In order to get discount mail rates, the airline presorts the statements by 9 digit zip code. As a result, the person whose report I received lives in my neighborhood.

While I can't speak for the person involved, if information about me was

to be accidentally released, I would prefer that it be to someone with a similarly spelled name in another city or state (as would occur in an alphabetic sort) than to someone down the street (although it was admittedly easier in this case to send the report to the correct destination).

Rob Aitken, HP Santa Clara aitken@dtl.hp.com

---

## **✂ REVIEW of THE GLASS COCKPIT**

*Robert Dorsett <rd@cactus.org>*

*Sun, 20 Oct 91 09:04:32 CDT*

[ This may be of interest to RISKS readers. The tape described would definitely go a long way toward clearing up a lot of misconceptions which keep on popping up. ]

THE GLASS COCKPIT. 80 min. \$49 + \$3 S&H. Aviation & Space Videos, 316 N. 12th St., Sacramento, CA 95814. 800-348-9933.

"The Glass Cockpit" is an introduction to the Flight Management System (FMS) concept, using the 757/767 cockpit environment as a practical example. FMS's comprise the backbone of the operation of modern jet aircraft, and were introduced beginning in the early 1980's.

The setting is that of an operational United Airlines 767 flight simulator. The tape follows this approximate format:

- Introduction to displays:
  - electronic attitude director indicator (EADI).
  - Nav display (EHSI).
  - upper Engine Indication and Crew Alerting System (EICAS).
  - lower EICAS.
- Intro to autopilot mode control panel.
- Detailed coverage of the Control Data Unit (longest segment).

The tape finishes with an event-oriented flight from LAX to SFO, including a demonstration of how to use the FMS to accommodate two changed clearances: one at departure, and one inbound. It finishes with a CAT IIIA landing. It's exclusively demonstrated on the instruments: the only "out the window" view is when the airplane crosses decision height (and even that's overlaid on what we'd be seeing on the EADI).

The narrator/emcee sits in the captain's seat, showing us around the cockpit and systems. A split-screen format is frequently used, as is a screen pointer. The coordination of the presentation of systems is good: changes made through the CDU or autopilot mode panel are shown on the EADI or EHSI.

Overall, the quality of the tape comes across as somewhat amateurish: there's a lot of background noise from the simulator, for instance, so

the narrator has to speak up, which in turn sounds kind of stiltish--rather like those 50's and 60's-era documentaries we all had to sit through in grade school. :-)

A major failing is that we \*see\* changes to the CDU through the \*right\* CDU. However, the majority of the changes are \*made\* through the \*left\* CDU. Thus, we don't see EXACTLY how items are "put into the scratchpad" or assigned to other items (an operation which, surprisingly, looks a lot like Mac- style Cut & Paste). The narration usually goes "Now, we'll put line L# in the scratchpad, then put it in over line R#..." But we don't really see the mechanics involved.

The strong point is the quality of the amount of data on the subject matter itself: it's an excellent introduction to the systems. The narrator is clearly a proponent of FMS systems, but one has got to wonder whether his basic points (smarter, more economical, faster) are presented effectively: there's a LOT of heads-down workload in that simple run from LAX from SFO. It's an unrealistic example for a 767, but we know that 737s (and MD-80s, and, eventually, A320s) have to do this all the time. And the CDU comes across as the User Interface from Hell: slow, and with a hodgepodge of text sizes and styles. It's very difficult to tell what the "active" fields are, and what the labels are (it's bad enough that I started to suspect parallax between the selector buttons and fields from the camera angle, but when we actually see what the fingers are doing, it turns out that it really is that bad). Even the narrator gets "lost" a couple of times. But I digress. Again. :-)

Overall, the tape's worth having, for those interested in glass cockpits.

#### Glossary:

- CAT IIIA An ILS landing, with no decision height, and RVR of 700'.
- CDU Control Data Unit. Primitive, keyboard-driven interface between pilot & FMC.
- EADI Electronic Attitude Director Indicator.
- EHSI Electronic Horizontal Situation Indicator. Shows A/C plan view relative to nav aids and waypoints.
- EICAS Engine Indication and Crew Alerting System. For engine and systems monitoring, systems messages, and checklists Replaces F/E and traditional center instruments.
- F/E Flight Engineer.
- FMC Flight Management Computer. Central aspect of the FMS.
- FMS Flight Management System. The sum total: FMC, CDU, IRS, displays, etc.
- ILS Instrument Landing System. A way of landing airplanes in low visibility.
- IRS Inertial Reference System. Black box that tells pilots where the plane is.
- LAX Los Angeles International Airport.
- RVR Runway Visual Range. Visibility down the runway, measured by mechanical instruments.

SFO San Francisco International Airport

Disclaimer: I have no personal or business connection whatsoever with Aviation & Space Videos, Inc, or any of its products.

---

### **✂ Yet another journalistic cock-up**

*Simon E Spero <ses@ccgr.technion.ac.il>*

*Fri, 18 Oct 91 00:51:05 -0200*

There's an double page spread in "Ha'aretz" today (17/10/91) based on an interview with an ex-cracker who for the past four years has run a computer security firm. When he was a teenager, he took his revenge on a hated maths teacher by breaking into computer of the American bureau of an Israeli paper, and inserting a false story reporting on how the said teacher had been arrested on a drugs charge. The story was duly transmitted back to Israel, and printed in the next edition. [See Risks:???? Internet link's down, and I can't reach the WAIS risks archive (meta-risk?)]

Now it seems he's found an even easier way to get bogus articles into a newspaper - just talk to a journalist.

He decided to demonstrate his prowess to the journalist by breaking in to one our VM machine. The account he chose was that of the head of the Computer Centre advisory centre. The owner of this account isn't the most technical of people- her passwords are chosen from a quite small, related set of words. Four years ago, he broke into her account - he claims that by chance, her password happened to be the same at the time of the demonstration. I have no evidence to contradict this, although it seems more likely that he guessed her current password using the information he had from the old one.

Up until this point, the article is mostly accurate - but now, the bogometer needle starts going off the scale.

-----

Claim #1: He claimed that the account he broke was privileged.

Lie: The account was an ordinary user account, with *\*no\** system privileges.

-----

Claim #2: He stated that the account name had a prefix which indicated that the account was special, and that this showed how naive the system managers were.

Lie: See #1. Even if his claim were valid, the risk is exactly the same as being able to cat /etc/groups on a UN\*X box to see who's in wheel.

-----

Claim #3: He claimed that from this account he could enter the accounts of all employees and researchers, and change their files.

Lie: See #1.

-----

Claim #4: He claimed that from this account, he could change information on the administration computer. He offered to wager the journalist that he could make him a Technion employee, give him a professorship, pay him a bonus, and then erase everything without leaving a trace.

Lie: See #1. Also, the administration computer is completely separate from VM machine. The only connection is that both have the same three letters written on them. This machine can only be connected to from special terminals.

-----

Claim #5: He claimed he could shutdown the computer and destroy all the data on the machine.

Lie: See #1.

-----

Claim #6: He claimed he could destroy all the back-ups.

Lie: Maybe if he stuck magnets on a few SCUD-C's and lobbed them at the various tape archives. It's a lot harder to spoof a human being, especially when you're a 24 year old male, and the spoofer is a 50ish woman.

He also makes other false statements, including a claim that before he hired a salesman, he never approached anyone to offer his services. Four years ago, he came to the Technion, and offered his services to a member of computer centre staff. This offer was not taken up.

What made things worse was the slightly inept performance of the Technion spokesbeing. After a quick telephone call to the head of the centre, who gave him the usual spiel about how theoretically, all systems are breakable if you can connect to them, and that without more details, he couldn't say what the cracker could or could not do. The spokesbeing took this message, and then garbled so completely that he acknowledged almost all the allegations in the article.

The risks?

1: Technologically naive journalists can easily be taken for a ride by experts with something to sell. The best computer reports in the press come from papers like "*The Guardian*", where the computer editor has a technical background as well as a journalistic one.

2: Technologically naive spokesbeings can be taken for a ride by journalists

with something to sell. Maybe Spaf or Cliff Stoll could give pointers on how to handle the media when statements can only come from the talking suits.

3: The boy who called "wolf!" effect. We know that our computers aren't secure (here in the UNIX group, doubly so). In an academic environment, there's really nothing you can do about it, except for blocking the more obvious holes, and keeping good backups. But when an article like the Ha'aretz one appears, it throws a bad light upon the institution, and lessens the impact when you really do have a serious break in.

Simon ses@techunix.technion.ac.il ses@techunix.bitnet Tel +972-4-292658

---

### **✶ Assurance of High-Integrity Software - Report**

*Rick Kuhn <kuhn@swe.ncsl.nist.gov>*

*Fri, 18 Oct 91 08:34:00 EDT*

Assurance of High Integrity Software - report available

The need for dependable software has resulted in the production of a variety of standards: the Trusted Computer Security Evaluation Criteria ("Orange Book"), the British MoD 00-55, the DO-178A standard for civil aviation, the IEC 880 standard for the nuclear industry, and others. Because of technical, economic, and political considerations, these standards approach the question of assurance from a variety of viewpoints. There is much disagreement over how dependable software can be produced. The controversy over MoD 00-55, with its requirement for formal methods and deprecated programming practices, is a recent example.

To address the question of assuring the trustworthiness and integrity of software, and what assurances should be required in standards, the National Institute of Standards and Technology brought together experts from industry, academia, and government in a Workshop on the Assurance of High Integrity Software in January. The report is now available for electronic distribution. (It will soon be available from the Govt. Printing Office in paper form.) The report can be obtained from our mail server. Both Postscript and troff formats are available. Send a message containing ONE of the following requests to [posix@nist.gov](mailto:posix@nist.gov):

```
send ahisrpt      /* for Postscript */
send ahisrptt    /* for troff */
```

The report will be delivered as three (troff) or 16 (postscript) email messages. Remove the headers and concatenate the files, then unpack them using either 'unshar' or the UNIX shell 'sh'. (Instructions included in the files.)

---

### **✶ Video stores losing videos...**

*Chris A. Anderson <caa@unify.com>*

*Thu, 17 Oct 91 10:00:27 pdt*

Mowgli Assor mentions an occurrence that happened to him at Blockbuster Video recently. I also had something like this happen to me and it's worth sharing with others...

Our local video store (not Blockbuster, by the way) also has a very nice computer system that keeps track of what's checked in and out, as well as a history of recent transactions. At one point, I had a video out for longer than the rental period and was required to pay for the extra time. I paid with a check and went my way without a thought.

Several weeks later, I was renting another video from the same store when the attendant told me that I owed money on a late rental. I couldn't remember being late with anything, so I asked him for the title (hoping to jog my memory). It turned out to be the video that I had payed for previously. I told him that I had already payed for it. He replied that their system had no record of it. I asked if there was any other audit trail and of course there wasn't.

At that point I said that I had the cancelled check at home and that I would go and get it for him. He told me that a cancelled check didn't prove anything, since it wouldn't have what it was for on it (the store sells other things as well as renting videos).

By this point, I was upset and asked to speak to the manager. The attendant replied that he was at home and they were not allowed to call him there. Deciding that I had had enough, I asked for my drivers license back (the store uses the DL number to identify the renter). He refused to give it to me until I payed for the late video. I blew up at that point and asked for him to call the manager at home again. He refused. I asked for the manager's name. He gave it to me and I went to a pay phone to look him up in the phone book and call him.

The manager agreed that this was an unfortunate occurrence and asked me to pay the late fee "just for now" and then bring him the cancelled check in the morning. I wasn't available to bring him the check in the morning since it was a workday, and he wasn't available any other time. He kept repeating that his computer system always kept "perfect" track of all of the accounts, and that it couldn't be wrong.

In the end, I payed the video late fee, got my drivers license back, took my cancelled check to the manager's home (it was conveniently listed in the phone book) and had him write me a personal check to cover the late fee. He didn't really believe the cancelled check, but I had already proved myself to be a dangerously unbalanced person just by driving to his home at 10:00pm to recover a \$3.00 late fee.

To the end, he kept repeating that his computer systems didn't make mistakes. Like most people, he didn't realize that it took \*humans\* to enter the data into the system and that they \*did\* make mistakes.

Needless to say, I do business elsewhere now. And the video store that I use has a paper trail to back up the computer system. Just another risk.

Chris Anderson, Unify Corp.

---

**Re: Blockbuster `Loses' Returned Video**

Brian Boutel <boutel-brian@CS.YALE.EDU>

Thu, 17 Oct 91 10:12:46 EDT

This is a problem that can occur in any library. It arises for two reasons. First, in almost all modern circulation control systems, the discharge transaction is not done at the time of return - the books/videos are left on the counter for later processing, and human failure can then intrude. Second, there is no physical evidence residing with the borrower (a receipt?) that provides proof of the return.

The antique (Brown?) system solved these problems. Borrowers had a collection of tickets, and could borrow one item per ticket. Books also had tickets, and the loan record was the physical pairing of a borrower ticket and a book ticket, usually one fitted inside the other, filed in chronological order of due date. When returning items, borrowers had to wait for the loans to be discharged in order to have their tickets returned. Being able to account for all your tickets was proof of not having lost or stolen a book. Alas, computerised systems have cost us this piece of security.

Actually, some library systems go to the other extreme. One library I used microfilmed each issue transaction. An 80-column card with a transaction number both punched and printed on it was inserted into the book, and the open book, card, and borrower's ID were photographed together. Presumably the control on non-returned books was based on sorting returned cards and looking for gaps in the sequence, which could then be looked up on the film record. The risk here was for the library, since the primary record of the loan was with the borrower. As long as the card was returned, the library assumed that the book with which the card was issued had been returned, which did not follow at all.

On the subject of risks associated with video libraries, last year (at home in New Zealand) I went to borrow a video, and was told that my card had been reported lost, and was no longer valid. I had not made that report, and had been out of town on the day it was recorded. I said "But it's not lost. I'm here, I have the card, and ID to prove who I am." They said "Sorry, but there is no way we can reactivate that card. The computer won't let us. You will have to go to head office for that." "But I want to take out this movie now." Silence, then: "Oh, I know what we can do. We can issue you a new card." Which they then did, using the same ID previously offered. It turned out that one of my children, looking for my card in the drawer where it is usually kept, failed to find it - it happened to be in my wallet that day - decided to apply for their own card, and reported mine missing at the same time. This report was accepted, and prevented the legitimate owner (me) from using the card, even though it was made by someone else, not even obviously a family member since they have a different address and surname.

--Brian Boutel

**✂ Re: Blockbuster `Loses' Returned Video (v12n51)**

"Matt Crawford" <matt@odjob.uchicago.edu>

Thu, 17 Oct 91 11:16:55 CDT

When I first got a VCR, not so awfully long ago, I used to always ask for a receipt when I returned a rented movie. They would *\*never\** give me one. I kept asking, figuring if they lost a movie I'd at least be memorable as the guy who always asked for a receipt.

---

**✂ Re: Blockbuster 'Loses' Returned Video**

<hughes@gpx1.square-d.com>

Fri, 18 Oct 1991 11:07:53 EDT

I have experienced a similar situation at another video store and have found at least a temporary manual solution to the problem (until they make the bar code readers available and print receipts). Whenever I check a video (or any valuable media) out now, whether from a store or the library, I physically make sure that they check it in as I stand there. This avoids problems of the nature Mr. Assor has described. This may seem like a bit of a nuisance at times, especially when you are in a hurry, but believe me, it is a small price compared to what one video company wanted when they claimed that *\*five\** videos (3 childrens movies and two comedies for those of you who keep track of these things) had not been returned. Sometimes the employees give me problems when asked to do this but if I forcefully explain that an incompetent employee was the reason for this and perhaps I should explain this to their manager, I usually have no more problems.

It seems a bit redundant in this ultra-efficient computer age to have to manually force this condition but as long as there is a human link in the chain of events, there needs to be a check on that link.

Kevin Hughes

---

**✂ Re: Blockbuster `Loses' Returned Video**

Patricia Shanahan <ps@dreamit.fps.com>

Fri, 18 Oct 91 08:34:39 PDT

[Rented video tape actually returned, but the return not recorded in the stores computer system, and the tape is not on the shelf where it should be.]

> At this time, Blockbuster thinks I stole the tape (even though the manager >doesn't ;) & since I gave them the proof I didn't on Monday & they lost it, I >of course have no proof anymore. The risk of relying on employees to know their >jobs, I guess.

There are both technological and social fixes for this type of problem. The best technical fix that I can think of would be for the store to have a barcode reading receipt printer. It would take only a moment to scan each tape as it is returned, and hand the customer a printed receipt proving that the tape was

returned.

There are currently a large number of transactions that do not have satisfactory systems for verifying what happened. ATM transactions have similar problems.

The social fix that I think should be applied is to force the cost of such disputes onto the person who has the power to determine how the transaction is done. There is already in at least some states a rule that resolves ambiguity in a contract against the person who wrote the contract. The equivalent rule would say that any issue of fact that is inherently unresolvable because of how the transaction is organized is to be decided against the person who designed the transaction.

The application in this case would be that if the customer claims to have returned the tape, and the store designed a tape return system that leaves both the customer without any proof of return, and the store without any proof of non-return, then the store should carry the cost. If the store always issues a receipt for returned tapes, than it becomes reasonable for the store to demand that the customer either return the tape or produce a receipt. The store would have to judge whether the cost of issuing receipts exceeds the cost of lost tapes due to customers lying about having returned them.

Patricia Shanahan ps@fps.com uucp : ucsd!celerity!ps (619) 271-9940

[Time to blow the whistle on this subject... But there are a lot of lessons to be learned by the unwary customer. Asking for a receipt sounds like a great idea. If enough customers did ask, the video outfits might do something intelligent! You might bring in a piece of paper with the name of the film and the date, and INSIST that the clerk sign 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 12: Issue 54**

**Tuesday 22 October 1991**

## Contents

- [Oki Telephone Programming](#)  
[Stuart Bell](#)
- [Nintendo lottery sidetracked for now](#)  
[PGN](#)
- [Single Point of Failure in L-1011 Intercom](#)  
[Craig H. Seidel](#)
- [Computer reads water meter](#)  
[John Sullivan](#)
- [Risks of software controlled safety switch](#)  
[Diomidis Spinellis](#)
- [Re: Licensing of Software Engineers](#)  
[David Parnas](#)
- [Law requiring bug fixes](#)  
[Mark Seecof](#)
- [Re: Yet another journalistic...](#)  
[Amos Shapir](#)
- [More ATM anecdotes](#)  
[Ralph Moonen](#)
- [Re: TRW misreports local taxes](#)  
[Matt Bishop](#)
- [Re: JSC SMS rehost](#)  
[David Carlson](#)
- [Avis vs. Spaf](#)  
[Gene Spafford](#)
- [Re: Have you tested your machine lately?](#)  
[Boyd Roberts](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Oki Telephone Programming

*Stuart Bell* <[stu@mwvm.mitre.org](mailto:stu@mwvm.mitre.org)>  
*Tuesday, 22 Oct 1991 09:28:11 EDT*

My wife just purchased one of the new Oki programmable cellular telephones with

a built in beeper. When it didn't beep for a day or so, we tried to originate a call and found it had not been activated by the vendor. No problem, he said, "Just bring it in and I'll change its number to the one I entered by accident." Turns out, he had accidentally transcribed a number so the incorrect number was activated.

My wife objected to the trip - so the man nicely explained how to reprogram the internal memory and change the number of the telephone!

The risk is obvious: tired of paying those high telephone bills and don't know where to buy one of the chips described earlier in RISKS that change your telephone number? Just buy an Oki and reprogram it to any number (within limits) you choose and off you go.

Or, examine your bills very carefully.      Stu Bell      (713) 333-0906

---

### ✂ Nintendo lottery sidetracked for now (See [RISKS-12.27,39,41,42](#))

"Peter G. Neumann" <neumann@csl.sri.com>  
Fri, 18 Oct 91 16:45:20 PDT

Game Over For Nintendo Lottery  
MINNEAPOLIS (AP) [18Oct91]

A controversial plan to introduce the state lottery into homes with the popular Nintendo video games was dropped amid complaints it would harm children and encourage compulsive gambling. State Lottery Director George Andersen said more discussion of the play-at-home system the first such plan unveiled in the nation is warranted in light of lawmakers' complaints. "I still think it's a good idea," he said. "But we never want to operate without as broad a consensus as we can." [...]

---

### ✂ Single Point of Failure in L-1011 Intercom

<seidel@puma.sri.com>  
Tue, 22 Oct 91 16:23:38 -0700

On October 19 I was on TWA Flight 843 from JFK to SFO which was delayed 2 1/2 hours while repair crews located and repaired a wiring harness in the intercom system used for communications through the aircraft. The intercom is essential for safe operations because it is used for communications in case of any emergency in-flight (for example, on another flight a Pan Am pilot told me of the time a flight attendant informed him that a wing-tip fuel tank was losing fuel, something he could not see from the cockpit).

What I found interesting about the intercom system is that it is wired like christmas tree lights where any failure in the chain causes a complete failure and requires a check of each component. If this is truly an essential system, I would expect more redundancy--I can imagine many emergencies that would disable this system.

The intercom wiring harness in the TWA L-1011 simply wore out (each time the

flight attendant sits down, the harness is bent), a consequence of flying planes for so many years. What will happen to modern fly-by-wire aircraft after they have been in the air for 30 years?

---

### **✂ Computer reads water meter**

*<sullivan@geom.umn.edu>*

*Tue, 22 Oct 91 19:14:12 CDT*

Minneapolis will be introducing "Easy Reader", a computerized water meter reading system, over the next five years. You get a new meter and an interface unit plugged into your phone line. Once a month, a reading will be taken automatically, and sent to a central billing computer. This will happen between midnight and 7am. Presumably the unit in your house places the call; they say "Your telephone will not ring".

They have anticipated several objections people might have to the service. They promise your phone service will not be interrupted: "If you do happen to be on the phone ... Easy Reader will get a busy signal [sic] and try again later. If you pick up the phone while the meter is being read, [it] will instantly disconnect."

They also reassure you that nobody will use this equipment to listen in to your phone conversations, and perhaps most curiously, reassure people with unlisted numbers that "Telephone numbers need only be disclosed during the installation of the system. After the initial contact with your home phone has been made, your number is no longer needed. The Water Works will gladly respect your privacy by not recording your number anywhere in its files." Why would they even need the number temporarily to set up service?

They don't promise that the system won't accidentally dial 911 in the middle of the night :-)

John Sullivan, Univ. of Minnesota, [sullivan@geom.umn.edu](mailto:sullivan@geom.umn.edu)

---

### **✂ Risks of software controlled safety switch**

*Diomidis Spinellis <dds@doc.imperial.ac.uk>*

*Tue, 22 Oct 91 18:56:19 BST*

A portable CD player I was experimenting with, features a safety switch, located on the hatch door, which turns the unit off once the door is opened. The role of that switch is to ensure that the laser in the unit will not operate with the door open. A number of other appliances (microwave ovens come to mind) have similar safety switches.

One day I decided to deeply discharge the batteries of the unit (i.e., drain them as much as possible) as a precaution against the NicCad "memory effect." The unit has an auto-power-off feature whereby when the batterie voltage falls bellow a certain level it switches itself off. Every time the unit switched itself off, I pressed "play" again to switch it on. The objective of this procedure was to drain the batteries as much as possible.

After some time the unit crashed. The display had some strange segments lit and the auto-power-off feature was no longer functioning. My first conclusion was that the auto-power-off was software controlled. My next move was to check what other things were software controlled. I plugged mains power to the unit so that I would not lose this crashed state and tried opening the hatch door. As I was expecting the safety switch was also, apparently, software controlled because the unit remained on. Now, I was faced with a unit turned on, with full power applied to it and with an open door hatch.

Moral: Software emulation of safety interlocks is not a good idea. Even with formally proven correct software, we would still need hardware that was formally proven to correctly function under all probable conditions to implement a safe product. Direct control methods (such as a switch connected to the power supply in this case) are more appropriate.

Diomidis Spinellis, Department of Computing, Imperial College

---

### ✂ Re: Licensing of Software Engineers ([RISKS-12.52](#))

David Parnas <parnas@qusunt.eng.McMaster.CA>  
Tue, 22 Oct 91 12:59:10 EDT

There seems to be a false assumption in some of the comments made by those who fear this concept. They assume that the body that issues the licenses is the government. That is not the case for other engineers. In many jurisdictions there is a professional body that is charged with this task. In Ontario it is the APEO, Association of Professional Engineers of Ontario. In Australia there is an "Institution of Engineers". Thus, it becomes the job of professionals to set the standards for their own profession and to enforce them. Why should the software field be different?

---

### ✂ Law requiring bug fixes (Hanlon, self-regulation, [RISKS-12.52](#))

Mark Seecof <marks@capnet.latimes.com>  
Tue, 22 Oct 91 11:20:02 -0700

In [RISKS-12.52](#) Richard Hanlon suggests:

> ..with a minimal intrusion by the government, [by] making it a law to  
> provide free bug fixes (there's ALWAYS at least one more bug).

Such a law might have horrible consequences for software vendors. Fred Brooks in *\_The Mythical Man Month\_* (Addison-Wesley, Menlo Park, 1982) reports (in Ch. 11, adducing evidence which I've elided here) that:

The fundamental problem with program maintenance is that fixing a defect has a substantial (20-50 percent) change of introducing another. So the whole process is two steps forward and one step back.

and

...All repairs tend to destroy the structure [of the software], to increase the entropy and disorder of the system. Less and less effort is spent on fixing original design flaws; more and more is spent on fixing flaws introduced by earlier fixes. As time passes, the system becomes less and less well-ordered. Sooner or later the fixing ceases to gain any ground. Each forward step is matched by a backward one. Although in principle usable forever, the system has worn out as a base for progress. [...]  
Systems program building is an entropy-decreasing process, hence inherently metastable. Program maintenance is an entropy-increasing process, and even its most skillfull execution only delays the subsidence of the system into unfixable obsolescence.

So I suggest that any law interfering with the allocation of resources to maintenance or development (often of a replacement system) by the presumably expert management of a software vendor would be unwise and ultimately destructive. Customers exercising a legal privilege to demand that bugs in a senescent system be fixed could force a software vendor right into the Pit of Despair.

Mark Seecof <marks@latimes.com>

---

### **✉ Re: Yet another journalistic ...**

*amos shapir <amos@cs.huji.ac.il>  
Tue, 22 Oct 91 09:03:58 +0200*

- > I've listed the relevant allegations - I guess Amos Shapir or
- > somebody will probably send you the full article.

Well, the full article is too long to post (and nothing new to most RISKS readers). I agree with most of Simon's conclusions, but there are some inaccuracies in his quotes. I understand his indignation at having \*his\* system exposed in public, but he'd rather leave the posting to the guy who had actually read the article.

- > Four years ago, he broke into her account - he claims
- > that by chance, her password happened to be the same at the time of the
- > demonstration. I have no evidence to contradict this, although it seems more
- > likely that he guessed her current password using the information he had from
- > the old one.

Actually, she was asked about it and is quoted in the article as admitting to reusing the same old password.

- > Claim #2: He stated that the account name had a prefix which indicated that
- > the account was special, and that this showed how naive the system
- > managers were.

(This is not a correction, it just reminds me of something that happened here).  
On CDC's NOS system, privileged accounts are the ones which begin with a C.  
You can guess what happened when a somewhat ignorant administrator assigned the Computer Science department accounts which begin with CS...

- > Claim #6: He claimed he could destroy all the back-ups.
- > Lie: Maybe if he stuck magnets on a few SCUD-C's and lobbed them at the
- > various tape archives. It's a lot harder to spoof a human being,
- > especially when you're a 24 year old male, and the spoofee is a 50ish
- > woman.

Not exactly. What the cracker claimed was that he could use the administrator's account to ask operators to mount the backup tapes, then destroy them; the operators could have no way of knowing that the request wasn't legitimate. The spokesman's response in the article is along the line "if we'd get such a request we'd probably call back and ask what it's for".

Amos Shapir, The Hebrew Univ. of Jerusalem, Dept. of Comp. Science.  
Givat-Ram, Jerusalem 91904, Israel Tel. +972 2 585706

---

### **✂ More ATM anecdotes**

*Ralph 'Hairy' Moonen <hvlpa!rmoonen@att.att.com>  
Tue, 22 Oct 91 11:17 MET*

I am a frequent user of ATM's. As banks in The Netherlands are closed after 17:00 and in the weekends, the only way you are going to get cash after that time is through an ATM. Unfortunately not all of them are the same, and some display a most peculiar behaviour. Example:

ATM: INsert card

Me: I insert my card

ATM: key in your PIN code.

Me: I do so.

ATM: There are no receipts available currently. Choose the amount of cash you wish to withdraw.

Me: I choose 100 Guilders

ATM: There are no receipts available currently. Do you want a receipt?

Me: I press the "No" key.

ATM: We're sorry, there are no receipts available currently.

ATM: Please wait.....

ATM: Retrieve cash from ATM please. There are no receipts available currently.

Me: I KNOW THERE ARE NO RECEIPTS!!! Please quit whinig and give me my money.

[withdrawal hatch opens, and my money is there, so I take it]

ATM: Please take your card out.

Me: I take my card out.

ATM: Please wait for your receipt. There are no receipts available currently.

RISKS? Well, none really, but quite frustrating..... Another example is funny stuff is the banks apparently can edit the on-screen messages on the fly, for once I was making a withdrawal, and the screen is flashing a bank advertisement on the bottom two lines. Something like: "Open a new account now, and receive this great CD with the greatest hits of 1991, PLUS a whopping 5.4% interest" When suddenly, the cursor moved to that line, and lo and behold, they edited the interest rate. The ATM continued my trans- action perfectly, but it was pretty weird to see the line edited \*on-screen\*.

For a last weird stuff thing, I once arrived at an ATM, that looked in pretty bad shape. Someone had apparently drank too much and decided to unload his lunch over the keyboard. I took one look and decided to, well, not make the planned transaction. At that point a van stopped and some service guy gets out. So I wait and see. The guy goes through a door next to the ATM, does something to the inside, comes out, and lifts the complete front off. Puts it into his van, and replaces it with a new one. I asked why, and he said well, would you like to have to poke in someone others puke. I said, but you don't need to replace the whole \*front\* for that, you could just clean it! The answer was a vague story about disinfecting the thing, and AIDS (!! ) and that he didn't fancy having to clean it.

--Ralph Moonen rmoonen@hvlpa.att.com

---

**✂ Re: TRW misreports local taxes (DeBoer, [RISKS-12.52](#))**

*Matt Bishop <bishop@dartmouth.edu>*

*Tue, 22 Oct 91 09:06:29 -0400*

> Why is it that inaccurately negative credit reporting [doesn't | shouldn't]  
> constitute libel under the law?

"DOESN'T":

It's (US federal) law. As I understand it (admittedly, I'm no lawyer), the credit reporting agencies are protected unless they maliciously report the information. If they make a mistake, that's not actionable. (The explanation given to me also included the statement, "Well, they have so many records, you can't expect them to have everything right, so as long as their errors aren't deliberate, they shouldn't have to pay." Unfortunately, I don't remember WHO gave me that explanation but I'd be interested in knowing if that is in fact the reason behind the law shielding the agencies.)

Matt

---

**✂ Re: JSC SMS rehost ([RISKS-12.47,48,49](#))**

*David Carlson <dave@bigguy.ocpt.ccur.com>*

*Fri, 18 Oct 91 9:49:38 EDT*

I read recently in RISKS the serious question by a Johnson Space Center employee on the risks of rehosting a large realtime program currently on minicomputers manufactured by my company. It was some amusement that two contributors offered parochial suggestions that their favorite hardware was clearly the "right" choice for such a large problem. This misses (and yet reinforces) the point the original contributor made that cost of the rehost to IBM/workstations would be larger than understood by management.

The reinforcement of the original idea is that the two followup contributors answered a software complexity unknown by asserting "it will be easy using

---

**✂ Avis vs. Spaf**

*Gene Spafford <spaf@cs.purdue.edu>*

*Fri, 18 Oct 91 21:41:37 EST*

Yesterday, I flew into Chicago O'Hare airport from Vienna, Austria. I wasn't too awfully jet-lagged, and rather than wait 8 hours for the next flight to West Lafayette, I decided to cash in my ticket and rent a car one-way. (West Lafayette is a 2.5 hour drive from O'Hare.)

I got to the car no problem. The agent at the counter said it was in stall J-32, and that is where the bus dropped me. So, the keys were in the ignition and the driver's side door was unlocked. I threw my coat in and tried to open the back door to toss in my portable PC. It was locked. So, I hit the powerlock button on the driver's side door to unlock all the doors, and then went to get my PC. A gust of wind blew the driver's side door shut. I then discovered I had LOCKED all the doors by pushing the button the wrong way! (This was a Chevy Lumina.) On my old 1975 car, one must hold the handle out when closing it, or lock it with the key after closing -- a form of fail-safe behavior compared to this.

To make matters worse, the car was to be rented one-way, so they had given me a car originally from Maryland...with no duplicate keys to be had locally. It took 2 of their mechanics working together for about 30 minutes to break into the car without excessive damage. If my coat hadn't been in the car, they would have just rented me a different one. Sigh.

But wait, it gets better! On the way out of the lot, the guard checked my rental agreement against the sticker on the car. The numbers didn't match! I had to go back because I had the wrong car for the agreement, and he couldn't let it out of the lot.

The woman at the counter sort of rolled her eyes when I came back in for the third time, but she forced a smile and said that rather than switch the car, she would just adjust the contract to show the car I had. Some quick keypresses, a new contract agreement off the printer, and I was on my way.

This morning, I drove the car out to the airport here to return it and pick up my car in the parking lot. As I was transferring my briefcase & books from rental car to personal car, the wind must have blown the rental agreement off the car seat and into the surrounding fields. I couldn't find it anywhere. Sigh.

Trudge into the airport. Give the person at the counter the keys and mumble "I seem to have lost my agreement somewhere." No problem -- she'll just take the ID off the keys, enter the final mileage, and print a duplicate agreement. The benefit of having one of those marvelous computer networks, eh?

So, she puts in the mileage and vehicle number, confirms that my rate was \$89 with the corporate discount, and prints the receipt. As she hands it to me, she smiles and says "Have a nice day Mr. Anderson" (I don't remember the exact name). This takes me a bit aback, and I ask "Anderson?" fearing the worst. I look at the rental agreement. The name, home address, and so forth are not mine. The agreement shows that the car was rented at Dulles Airport and was not to be returned until tomorrow -- back to Dulles. It had someone else's credit card number. It was the correct car, but the wrong renter.

After struggling with the computer for about 20 minutes, the clerk then called Chicago and spoke to 9 different people (we counted) in 30 minutes before getting someone who could help find my rental record. It seems Avis's system does not allow (for privacy reasons?) any field agent to do a lookup based on name, based on credit card number, based on rental location, or based on anything else I had with me or could produce. It needed either the rental agreement number, which was lost, or the vehicle ID, which was incorrect. The folks in Chicago had to find the duplicate PAPER copy of the rental record in their files to get the correct number.

Once my agreement was finally corrected, they had to fix the record for "Mr. Anderson" because he hasn't returned his car. However, they can't cancel a transaction in the system, I guess because it might allow employee fraud ("Mr. Spafford, our records do NOT show a checkin -- either produce the car or we swear out a warrant."). Instead, they have to issue a special form of checkout that negates the effect of the checkin. Unfortunately, the computer now showed that the vehicle was checked in, because the local office had file a record to indicate they had the car. The system won't allow a car marked as present at a local office to also be marked as "rented."

Between Chicago and locally, they decided to take the car "out of service" somehow, thus removing it from the ken of the system. They then did a correction checkout on Mr. Anderson. He's in for a surprise, probably, when he tries to check HIS car in tomorrow. I hope he doesn't have a flight to catch. Then again, maybe he'll do an express checkin where he simply throws the keys and the agreement envelope into a mailslot, and add even more entropy into the mix.

This whole mess took almost 45 minutes to get straightened out. I bet their records are still messed up, with the car I had now marked out of service and some other car lost in the system. I wonder if they will ever get it evened out. As for me, no more rentals on windy days!

---

### **🚩 Re: Have you tested your machine lately?**

*<boyd@prl.dec.com>*

*Thu, 17 Oct 91 13:14:35 +0100*

Two weeks ago we had a power outage which damaged various bits of hardware in some of our DECstation 5000's. I had been out of the lab for 8-10 days and I wasn't around when the outage occurred. So I wasn't really sure of the state of the world, but it didn't sound good.

I log in on my 5000 (it has two big colour screens and runs X) and immediately I see some `_very strange_` things happening.

1. ``sunlock'` paints a white icon and then exits.

``sunlock'` shows a map of the world with the land illuminated by the sun in white, and the dark areas in black.

2. `xman's buttons are missing the semi-circular edges on the left hand side of the buttons.

`xman' is the X implementation of `man'.

3. Clicking on some of `xrn's buttons crashes my X server.

`xrn' is an X based newsreader.

4. Most everthing else works.

At this stage I conclude that something is seriously wrong. But just where is the problem? Is it the X clients, the server, a font problem, the display or a real machine problem? I just don't know, so I have to go looking.

So I start with `sunclock' because I believe that it is probably a simple system and a sound test case. I was right, but I dismissed my conclusion because I don't trust the debugger I was using (`ups'). `ups' was telling me that the math library was returning NaN and `sunclock' would use this bogus value, compute with it, and then index off the end of an array -- and dump core.

I wasn't trusting `ups' because it likes to second guess the compiler on ULTRIX 4.2. It `_knows_` where the SP is. When it sees the SP is not where it should be it aborts. I commented the line out, and it works, but I don't place a great deal of trust in it, given my knowledge of the MIPS archictecture/compiler is not large.

So where to next? Is it in the X server? We have quite a few field test X servers here, and maybe the new wiz bang version will fix this. After trying a few I conclude that this is not the case.

Is it in the display hardware? So I board swap the display hardware and then reboot. This is what I should have done in the first place. The self test tells me the FPU failed its self test, and I conclude that it's returning garbage to the math library.

All the software using floating point is broken -- in mysterious ways.

This consumed a day of my time. The thing that really worries me is that when confonted with a problem with these `modern' systems you just have too many variables of which you have to know `_a lot_` about to diagnose the problem. I can't see this trend ending. In the future I can see that 5 or 6 people with diverse, non-intersecting knowledge will be required to analyse the simplist of problems. This is a disturbing conclusion.

Boyd Roberts



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 12: Issue 55**

**Wednesday 23 October 1991**

## Contents

- [Power outage downs New York Stock Exchange for 24 minutes](#)  
[PGN](#)
- [Near-sighted or far-sighted fibre-opticians?](#)  
[PGN](#)
- [MCI Friends & Family & anyone else with a touch-tone phone](#)  
[Brian R. Krause](#)
- [Risks of double standards \(on PRODIGY\)?](#)  
[David HM Spector](#)
- [Use of Prodigy on AMC Computers](#)  
[Louise R. Silsby via Brinton Cooper](#)
- [A note on RISKS contributions](#)  
[PGN](#)
- [Re: Videos and "Dumbing Down" \(again\)](#)  
[Daniel J Yurman](#)
- [Re: More ATM anecdotes](#)  
[Mark Bartelt](#)
- [Re: Oki Telephone Programming](#)  
[Randal L. Schwartz](#)
- [Re: Computer reads water meter](#)  
[Lauren Weinstein](#)  
[Sam Ho via John Sullivan](#)  
[Lars Poulsen](#)  
[Bjorn N. Freeman-Benson](#)
- [Re: Have you tested your machine lately?](#)  
[Neil Hunt](#)
- [Re: Software Migration at the Johnson Space Center](#)  
[Joe Bouchard](#)
- [Info on RISKS \(comp.risks\)](#)

---

✉ **Power outage downs New York Stock Exchange for 24 minutes**

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Wed, 23 Oct 91 10:17:15 PDT

The NYSE was down between 10:21am and 10:45am on Tuesday 22Oct91 because of a power outage that downed all of the computers (but not the lights!). ConEd suggested that the outage might have been related to a severe voltage dip at the local power station, resulting from problems with a disconnect switch on a 138,000-volt line. [Reuters, in SanFrancisco Chronicle, 23Oct91, p.C3]

---

### **✦ Near-sighted or far-sighted fibre-opticians?**

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

*Wed, 23 Oct 91 9:21:23 PDT*

U.S. spy masters prevent sale of optic fibre to Soviets' experts  
(by MARIE JOANIDDIS)

PARIS, Oct 22 (AFP) - The United States, seeking to maintain its ability to spy on conventional telecommunications, is preventing western companies from selling much-needed optic fibre to the Soviet Union, several western experts say. Agreement on policy appeared unlikely before the next high-level meeting in Paris at the end of November or beginning of December of the western coordinating committee for export control (COCOM) which restricts the export of high technology to communist countries, they said.

[This is the beginning of a longish article.  
The entire piece can be found in [RISKS-12.55afp](#).]

---

### **✦ MCI Friends & Family & anyone else with a touch-tone phone**

*"Brian R. Krause" <brian@EDDIE.MIT.EDU>*

*Wed, 23 Oct 91 19:11:07 EDT*

I should have known better than to tell MCI who my friends and family are. Here's part of the brochure they sent to introduce me to their Friends & Family program:

Q. "How can I leard the immediate status of my Calling Circle?"

A. All you have to do is dial 1-800-FRIENDS from any touch tone phone, anytime. A recording will tell you who has been added, who is not eligible and who is in the process of being contacted.

Anyone who knows your phone number and ZIP code can get a complete list of your Calling Circle. You don't need to know a number to check its status; the computer lists them all.

I called MCI about this. The first representative I spoke with tried to convince me that nobody would try to get my numbers that way, and that, really, if someone was malicious, they could call him and cancel or change my service anyway. That made me feel good.

I then spoke to the supervisor--she had never used the FRIENDS number, since "I work at MCI and can check my numbers all the time." She seemed surprised that

you only needed a ZIP code, and has promised to get back to me.

In the meantime, I'm not adding any more people to my list, and I'm considering switching to a company that doesn't make my monthly bill public information.

Brian R. Krause, Software Developer, Milwaukee, WI 532XX

---

### **✂ Risks of double standards (on PRODIGY)?**

*David HM Spector <spector@acf5.NYU.EDU>*

*Wed, 23 Oct 91 08:45:35 -0400*

There have been a number of very disturbing reports in the press (CNN, and WNYW tv in NYC) in the last several days that on one of PRODIGY's forums, which discusses the Holocaust, members have been posting anti-semitic messages. Some of the messages \_advocate\_ "another holocaust", etc, etc...

The ADL (Anti-Defamation League) has protested to the PRODIGY management who responded that they "oppose anti-semitism", but they "encourage the free expression of ideas". Is this the same PRODIGY that makes decisions about what acceptable "free expression" is when it comes to use of electronic mail, and what are "acceptable" topics in their Health forums? Hmm.. sees like a pretty scary double standard to me....

David HM Spector, 310 West 18th Street 5A, New York, N.Y. 10011 (212) 243-5548  
Usenet: ..!{uunet,apple}!panix!spector

---

### **✂ Use of Prodigy on AMC Computers (from Louise R. Silsby)**

*Brinton Cooper <abc@BRL.MIL>*

*Wed, 23 Oct 91 9:34:37 EDT*

All of us on the Lab computer network (which is, in fact all of us) received this note this morning. What was the final judgement on Prodigy? I thought that the Prodigy flap was all a misunderstanding.

\_Brint

|We have been directed by HQ AMC to suspend all subscriptions to the Prodigy  
|Services Company and remove all Prodigy software from AMC owned computers.  
|This includes all individuals that have installed personal copies of Prodigy  
|on their computers at work. This directive will remain in effect until  
|further notice.

|  
|Employee owned computers used to access Prodigy Services may not be used to  
|access government owned computers so as to preclude the possibility of  
|unauthorized access to government data.

|  
|If you have been using Prodigy as described above or if you have questions,  
|contact...[name and phone deleted].

---

## ✂ A note on RISKS contributions

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

*Wed, 23 Oct 91 9:29:39 PDT*

As I have remarked before, my moderatorship tends to run in cycles from permissiveness to wholesale rejections, depending on the topic, my mood, and how much time I can devote to interactive moderating. But the real problem, I fear, is epicyclic rather than cyclic, because as RISKS gets more and more readers with greater intellectual, geographic, and other forms of diversity, more and more material gets submitted, and some of it is less generally relevant to everyone. After receiving a few complaints suggesting I get me back into a more-selective moderatorship, I think it may again be time to head back in that direction. I do not like to flood YOU with too much, but I am certainly flooded! In any event, keep the good incisive contributions coming!

The following contributions represent what I hope is a final trickle on the earlier subjects. PGN

---

## ✂ Re: Videos and "Dumbing Down" (again)

*Daniel J Yurman <djy@inel.gov>*

*Wed, 23 Oct 91 10:57:37 MDT*

Reference a series of reports in [RISKS-12.52](#) and 12.53 on problems with returning videos, I am surprised that your readers have not linked the problem of closing rental return transactions with an earlier RISKS issue -- the "dumbing down" of the workforce.

In most of the instances reported customers were eventually moved to rage over the stubborn insistence of employees and managers alike that the "computer had to be right." None of the video store staffs evidence the slightest inclination to question the information in their computer. This can be ascribed to a lack of training, education, or fear of getting yelled at by the manager for letting a late fee go by.

The larger issue is what are these people [the video store employees] going to do when IRS screws up their taxes or when their Social Security benefits records are scrambled, etc? Are they going to believe that the government's computers are right or are they going to fight for accuracy of personal information which affects their lives?

A case can be made for asking how well we are preparing people to put the question of computer accuracy in perspective. For instance, is the accuracy of the data a life and death matter. For medical diagnostic equipment the answer is yes, but for video rental transactions, the answer is no. Yet, in one RISKS report the writer reports he took the time to drive to the manager's home at 10 PM to resolve a \$3 charge. Both the writer and the video store manager have lost it. They allowed themselves to be driven -- literally -- by a bogus record in a database maintained by people paid a minimum wage!

There seems to be a problem of scale here. From an marketing point of view there are many video stores so customer service becomes a competitive edge to retain and grow sales. Enraging a patron over a \$3 late charge seems penny wise and pound foolish. Obviously, a more astute video store manager would resolve a dispute over a late charge letting it slide to keep a good customer coming back. After all the computer would have a record of how good a customer was in terms of repeat business.

Further, this example raises the issue that many businesses face which is how accurate do computer records have to be to keep making a profit and keep customers coming back? Many businesses let minor financial discrepancies slide in the interests of the overall commercial relationship with customers / clients. ATM transactions do not belong to this class of business activities, but late charges on video rentals probably do.

Dan Yurman, Idaho National  
Engineering Lab., PO Box 1625 MS 3900 Idaho Falls, ID 83415 (208) 526-8591

---

**✂ Re: More ATM anecdotes (Moonen, [RISKS-12.54](#))**

Mark Bartelt <sysmark@orca.cita.utoronto.ca>

Wed, 23 Oct 91 07:01:48 EDT

I continue to be amazed by the abysmal quality of the software that I encounter in ATMs. There are numerous situations where a bit of thought would have made them far less frustrating to deal with. Two examples:

(1) I have several ATM cards (for accounts at various different banks), all with different withdrawal limits. Since most of my cards rarely get used, I have trouble remembering what the limits are. I recently stepped up to a machine, and asked it for \$500. It insisted that I ask for a different amount, since that machine was capable of dispensing at most \$400 in one transaction. Fine. I asked it for \$400. This time it told me that it couldn't give me \$400, since my withdrawal limit was \$300.

This incident was doubly frustrating: First, because it ought to be trivial to check the requested amount against both the card limit and the machine limit simultaneously, thus requiring only one retry rather than two. Secondly, each failed attempt required that the card be removed and reinserted, and the PIN re-entered. (Why?)

(2) A few months ago I tried to make a deposit to an account which I hadn't used in quite some time. The machine refused to allow any access to the account, and displayed a message telling me to contact my branch. It turns out this bank has a policy of disabling all ATM access to an account that hasn't been used for more than six months. I was rather annoyed because (a) they don't tell customers this when an account is opened, and (b) nothing is mailed to a customer to whom this is about to happen, warning him/her that their ATM access will soon be disabled unless they take some sort of action.

In order to get the account re-enabled, it was necessary to go into the branch in person. Not just any branch, either, but the branch where the account was originally opened! In my case, this was just a fifteen minute subway ride.

What if I'd moved to a different city? To paraphrase H. L. Mencken, nobody ever went broke underestimating the intelligence of people who run banks.

I'm just lucky that I was only trying to make a deposit. What if it had been an emergency situation, where I needed cash quickly? If an ATM is down, I can generally find another one that works. But if this were my only account, and all ATM access is denied, I'm out of luck.

Furthermore, even if you agree with the concept that it's a good idea to disable withdrawals from a "stale" account (for security reasons, or whatever), what possible justification is there for not permitting someone to deposit money into an account?

Mark Bartelt, Canadian Institute, for Theoretical Astrophysics 416/978-5619

---

**✉ Re: Oki Telephone Programming (Bell, [RISKS-12.54](#))**

*Randal L. Schwartz <merlyn@iwarped.com>  
Wed, 23 Oct 91 10:03:50 PDT*

There's no risk to this. The phone number/serial number pair is validated on each call (which is why the phone wouldn't work in the first place).

Programming your own number doesn't circumvent this; the methods for programming *any* cell phone are publicly available (I think the "universal" manual costs around \$50, and I have the address somewhere). What you *cannot* change from any sequence of keypresses is the phone serial number. The serial number *can* be changed by replacing a chip, and this is what the other RISK articles have referenced.

Randal L. Schwartz, Stonehenge Consulting Services (503)777-0095

[...unless you can change the "tamperproof" serial number.  
Also noted by Dave.Katz@um.cc.umich.edu and lars@cmc.com (Lars Poulsen).  
See also recent issues of the TELECOM DIGEST.

---

**✉ Re: Computer reads water meter**

*Lauren Weinstein <lauren@vortex.com>  
Tue, 22 Oct 91 19:50:40 PDT*

Greetings. The description given would indicate that the meters to be read do *not* make outgoing calls, but rather are interrogated by the central system. There are special features in various modern telephone exchanges for "ringless" connections to subscriber lines, specifically for such purposes as meter interrogation and line testing. Doesn't that give you a warm feeling? (It should be noted that some of these are not as "ringless" as they are supposed to be--some phones "ding" or "chirp"--usually at very late hours--when hit by some existing telco test routines.)

Other clues also point in this direction, for example, the note that if *your*

line is in use the system will get a "busy signal" (this would not be the case for outgoing calls \*from\* your line, but would be the case for incoming calls \*to\* your line). I assume that the exchange is programmed to ignore any call waiting features on the subscriber line in this sort of situation and just return busy for any subscriber use that conflicts with an interrogation request.

The business about their only needing your phone number to set up the service, and that then they will delete it, is bogus. They need the number to program into the system. Once that's done, maybe the ordinary customer service rep. won't be able to see the number, but it'll be in there!

Risks? The obvious ones, mostly, many of which have parallels with manual meter reading: accidental confusion between meters, undetected read errors resulting in false data, etc. Frankly, the most serious concern might be that an "electronic" meter that crashes or is disrupted in some manner might make it difficult to correct inaccurate billings. With mechanical meters, if there's an accidental over-read by the meter reader, they can go back and look at the meter again and verify what's going on--the mechanical system is fairly robust in that respect. But an electronic system could crash pretty badly.

I wonder if electronic water meters would try to draw their power from the phone line--you can draw a very limited amount for that purpose. I also wonder how much hassle it will be to \*get\* to the phone line from many water meters! In many areas, water meters are currently mounted in the curb. This would imply installing a new meter somewhere closer to the house on the main water line.

Actually, the biggest risk may be to the utilities themselves, if people start intercepting the interrogation calls and feeding back their own (presumably lower) data. Of course, this sort of thing has been going on with mechanical meters since the dawn of metering as well.

For example, before the power companies started getting serious about really locking down power meters with steel collars and lead seals, there were people who used to flip their electric meters \*upside-down\* so that they would run \*backwards\* for some calculated period of time to reduce their bill appropriately (but not enough, presumably, to trigger computer-based flagging of their account for odd month-to-month variations). The rather amusing aspect of this was that people running such upside-down meters would need to turn \*on\* as many appliances as possible to try force the meter to run rapidly in the reverse direction.

So while new technology often brings with it new risks, we see that sometimes it also acts to bring old risks into the 21st century in new forms!

--Lauren--

[Many other folks commented on this one also, including Mark Bartelt.  
I gave up on trying to prune the following differentially. PGN]

---

**✂ Re: Computer reads water meter**

<sullivan@geom.umn.edu>

Wed, 23 Oct 91 15:01:14 CDT

Sam Ho of UIUC was kind enough to point out that I jumped to a few unwarranted conclusions. He believes that the phone company is more directly involved in the scheme than I had guessed:

-> From: ho@csrd.uiuc.edu (Samuel W. Ho)

->

-> No, the meter does not call the water company. Rather, what happens

-> is that the telephone central office sends a coded signal down the

-> line to the water meter, while the line is still on-hook. The meter

-> then responds with the reading. All this happens superimposed on the

-> usual battery voltage, with the line on-hook. If your phone happens

-> to go off-hook, or if there is an incoming call, the process is aborted,

-> regular ringing or dial tone appears, and the water company tries again

-> later.

->

-> Normally, you tell the telephone company you want to use the telephone

-> by drawing DC loop current. The meter is AC coupled so it doesn't draw

-> current.

->

-> They don't need your telephone number, since water meters are associated

-> with buildings. If you move, you don't take your water meter reading

-> with you. Instead, the meter is keyed to the telephone company's

-> location information.

This would also explain why they need your phone number to set up the service (to get the telco's location info), but don't store it.

-John Sullivan

---

## ✂ Remote Meter Reading

Lars Poulsen <lars@cmc.com>

Wed, 23 Oct 91 14:30:08 PDT

In [RISKS-12.54](#), John Sullivan, Univ. of Minnesota (sullivan@geom.umn.edu) writes about the "Easy Reader" system to be introduced in Minneapolis over the next few years. The note reveals some uncertainty about the technology.

The remote meter reading service is a feature of most electronic central office systems. It is being put into service in many parts of the country.

The system requires special hardware and software on the telephone switch; the utility company subscribes to a specially equipped trunk.

As I understand the system, the subscriber record contains a special flag to indicate that the line has a remote-readable meter on it. When it is time to read the meters, the utility company activates a special "modem" on their port, and the central office switch scans all the lines that are equipped for meter reading by that utility. Lines that are busy are bypassed (with some provision for scanning them later in a special pass). The switch connects the utility

trunk to the subscriber line, and the meter is polled, and transmits its data. If the line goes off-hook during the transfer, the reading is abandoned and retried later.

So, "your telephone will never ring" because there is not a conventional call placed. It does not interfere with service. And the utility company does not need to use your number, except as a record identifier to tell the local exchange carrier to set the proper flag bit. Since there is no dialer in the meter, it will not dial 911 in the night :-)

The polling protocol is designed to allow several meters to share the line.

This is about all that I know. If you need more detail, I am sure there is a BellCoRe document describing both the meter side and the utility trunk interface.

Lars Poulsen, SMTS Software Engineer, CMC Rockwell lars@CMC.COM

---

**✂ Re: Computer reads water meter**

*Bjorn Freeman-Benson <bnfb@csr.UVic.CA>*

*Wed, 23 Oct 91 16:56:29 PDT*

The "Easy Reader" water meter also results in a hidden rate increase for certain customers---those who use metered local telephone service. If I still lived in area with mandatory metered phone service (e.g., most of Europe) and the water company was going to do this, I'd demand a rate reduction to match the (admittedly small) extra cost to me.

Regards, Bjorn N. Freeman-Benson

---

**✂ Re: Have you tested your machine lately?**

*Neil Hunt <nhunt@Csl.Stanford.EDU>*

*Wed, 23 Oct 1991 16:39:04 GMT*

Boyd Roberts reports on mysterious manifestations of FPU failure on his DecStation, and wonders about the risks of complex systems interacting to make diagnosis hard.

We too had a similar failure, with similar symptoms: in particular, any X-windows buttons with curved edges would be scrambled across the whole screen. Meanwhile, most of the system seemed to run OK. Fortunately the DEC field service person immediately recognised the problem as I described it over the phone. We were skeptical, but let him swap CPU cards anyway, and the problem went away.

Many systems have high complexity which complicates diagnosis of problems. Modern automobile engines come to mind, for example. However the physical complexity of a modern workstation has been much reduced from comparable machines of the past -- after all there are only about three parts inside the

whole box. Once having diagnosed a hardware problem, even a novice service engineer could try swapping out all three in short order. (In our case we suspected a software problem and did a complete filesystem restore before calling in the field service!)

Perhaps the RISK is in fault tolerant systems which mostly continue to work while not alerting the user to failure, except through weird seemingly unpredictable failure modes.

Neil/.



*Joe Bouchard <bouchard@ioscc.neosoft.com>*

*22 Oct 91 18:39:18 CDT (Tue)*

First, some general replies addressed to comments about the original post.

1) Other vendors did have real time simulation software... none on a large enough box to support the proposed system.

2) Unisys A-Series (Burroughs) and 1100-Series (Univac/Sperry) equipment has the largest RANGE (i.e. ratio of fastest system to slowest system) of compatible computer systems available. In other words, these systems go from desktop processing to major mainframe class processing power with NO required changes to the software. Depending on how generically the ECL (Exec Control Language) was written, the change in disk drive types, etc. won't require changes either.

Now, the RISK I was trying to point out was upper level managements lack of understanding of the many risks involved with moving mature software from one platform to another when there are major environmental differences between the platforms.

The software we are talking about here is something like a million+ lines of fairly machine and environment specific flight simulator code (full instrument, vision, and cockpit motion included), mostly in FORTRAN and assembly language. Those languages allow a fair amount of connection to the specific details of the machine and the software environment. Simply transporting the code without doing a redesign gives mediocre results. It's something like taking a batch oriented application on a mainframe and turning it into a transaction oriented, relational database, desktop metaphor application on multiple PCs connected by LANs, expecting to keep the original design (code, too) and still get all the advantages claimed for the later environment.

The management seems to be misled by all the talk about Ada and Unix turning computers into commodities that are VERY plug compatible. If SMS were written in something like Ada, it would be designed VERY differently, mostly because Ada implementations are required to support an environment (virtual machine, if you will) with certain givens that are true on ANY box it runs on. I don't believe that the Ada machine is very good at running real time simulation programs, but you get the point.

Porting such a system from one box to another might require a bit of patching

to manage specifics. The only catch is that you would end up with EXACTLY THE SAME SYSTEM you started with. It would utilize none of the advantages of the new hardware. The impression of the management around here seems to be that porting the software from one box to another automatically gives you all of the wonderful advantages of the new box without any programming effort (not to mention the effort to port that complex a system in the first place). And most of the desired changes are possible ON THE CURRENT BOX, given the effort to do the hardware and or software upgrades necessary (trivial when compared to simply[?] porting the code).

A similar situation exists with the FADS (Flight Analysis and Design System) project. NASA has directed the migration of an existing system (also on Unisys 1100 series equipment) to multiple workstations, etc. The primary problem is that they are so concerned with avoiding change in the existing system (which works) that it is being force-fed onto boxes that were NOT designed to run that way. Changing the underlying hardware with no changes in design is only possible when the two environments are nearly identical. I do not dispute the advantages of the new environment. I DO dispute that moving to such an environment is free.

I don't believe this RISK (system migration between environments) is limited to NASA or even just government sites. I've seen it happen at a public utility I used to work for (one of the reasons I left). That example was even simpler (changing mainframes) and was completed with ALMOST reasonable results. Even so, it took longer and cost more than initially estimated. This risk is magnified by being at a government site. Distrusting contractors is a way of life. The government pays the bills and, by definition, that means they know the best way to implement the task.

While NASA used to have the technical know-how on the part of the government employees to come up with good designs (and still does in some areas), the above examples show this is no longer true with regard to these projects. Perhaps this is one of the reasons that the SSTO (Single Stage To Orbit) project is being managed by the SDI (Strategic Defense Initiative) branch of the Defense Department with limited paperwork.



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 12: Issue 56

Friday 25 October 1991

## Contents

- [More O'Hare-raising experiences](#)  
[PGN](#)
- [Swedish election results were delayed](#)  
[Martin Minow](#)
- [Campaign against telco info services](#)  
[Mark Seecof](#)
- [The computer is always right.](#)  
[E. Kristiansen](#)
- [1-900 scam](#)  
[Torsten Lif](#)
- [RISKS of Electronic Credit Card Authorization](#)  
[Derek Atkins](#)
- [Australian Software Quality Management Standard](#)  
[Douglas Thomson](#)
- [AT&T/ATC outage revisited](#)  
[Alfred H. Scholldorf via PGN](#)
- [Re: Single Point of Failure in L-1011 Intercom](#)  
[Brinton Cooper](#)
- [Re: Law requiring bug fixes](#)  
[Geoffrey H. Cooper](#)
- [Re: Prodigy](#)  
[Jamie Saker](#)  
[Fred Gilham](#)  
[Ronald Hale-Evans](#)  
[Greg Brail](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ More O'Hare-raising experiences

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>  
Thu, 24 Oct 91 13:15:02 PDT

Radar equipment at O'Hare International Airport in Chicago has been malfunctioning for months, losing track of planes, and giving images of ghost

planes in empty airspace. FAA's Jim Dermody said radar images appear and disappear for 15 to 20 seconds. Controllers have also reported seeing double images of airplanes. [Summary of an AP item, greatly foreshortened in the San Francisco Chronicle, 25Oct91]

Dermody said the FAA suspects T-CAS may be emitting too many electronic signals, causing the radars to malfunction, although the problems seem confined to the Chicago area.

In previous incidents, an American Airlines jet came within 50 feet of a smaller plane Saturday in the Chicago area, the FAA reported. Three passenger planes nearly collided near Chicago's Midway Airport on Oct. 3 in an incident the FAA blamed on an error by air-traffic controllers. On Sept. 26, a Southwest Airlines jet was forced to veer sharply as it approached Midway to avoid a smaller plane. [From the full AP report]

[The short version was also noted by  
Rodney Hoffman <Hoffman.El\_Segundo@Xerox.com>.]

---

### **✂ Swedish election results were delayed**

*Martin Minow <minow@ranger.enet.dec.com>*

*Wed, 23 Oct 91 20:35:48 PDT*

The following is a sidebar -- in its entirety -- from the Stockholm newspaper Expressen, Monday, September 16: the day after the Swedish national election. Expressen is an afternoon paper that would have gone to press sometime Monday morning: it includes photos taken early Monday morning. (My translation, with apologies for inaccuracies.)

#### Miscalculation last night

Riksskatteverket [RSV, the national tax authority] could not successfully count the parliamentary election because of computer error. At this edition's press-time, there is conflicting information about the exact parliament seat distribution.

However, the difference is on the order of a few tenths of a percent and the balance [of seats between parties] will not be affected.

The rest of the page is taken up by a large table showing vote percentages and seat distribution among the eight parties and 28 electoral districts.

A two-page article inside the paper has the title "Gigantic Foul-up by Riksskatteverket." Some quotes follow:

All night, 120 people from RSV and the newspapers' telegram bureau [the Swedish equivalent to AP] worked to get out the Stockholm election results. The work was often chaotic, and early this morning it became clear that RSV couldn't determine all the results. Thus, the following tables are missing ... [local and province results by electoral district].

The reason for the mess-up was that RSV used a new computer system for

the first time this year. "The idea behind the new system is that we will be able to serve all mass-media by the network. So it will be easier for mass-media to process the data themselves," says election chief Lennart Berg.

According to Bo Beergrehn, computer cheif for the tax authority in Stockholm, priority was given to results in electoral districts that were meaningful for mandate allocation. Those results were delivered successfully.

In the future, the new computer system will require fewer personnel and get the results out quicker.

Martin Minow     minow@ranger.enet.dec.com

---

### **✂ campaign against telco info services**

*Mark Seecof <marks@capnet.latimes.com>*

*Thu, 24 Oct 91 10:20:39 -0700*

The American Newspaper Publisher's Association, Consumer Federation of America, Dialog Information Services, Graphic Communications Int'l Union, National Newspaper Association, and Weatherline, Inc. have published a full page ad in the L.A. Times (and, I presume, in other pubs) inviting people to support a bill called HR 3515 which would restrict the LOC's entry into the "information services" arena. The ad appeals to peoples' interest in their own privacy. The number to call to support HR 3515 is 800-54-PRIVACY and the ad (after drawing a scary picture of what the telcos will do if unleashed) says "We need to stop this potential invasion of privacy. We need to keep the already thriving information services industry competitive and independent of the Bell monopoly. You can help by urging your U.S. Representative to support HR 3515. And by calling 1-800-54-PRIVACY. Because if you remain silent now, everything you say later can, and just might, be used against you."

Mark Seecof <marks@latimes.com>

In this case, I think what I've reported really does represent the opinion of my employers, at least in part.

[Wow! A nondisclaimer!!! PGN]

---

### **✂ The computer is always right.**

*"E. Kristiansen - WMS" <EKRISTIA@estec.bitnet>*

*Thu, 24 Oct 91 11:32:46 CET*

"Flying Dutchman", KLM Royal Dutch Airline's magazine for frequent travellers, October/November 1991, has an article on Eurocontrol, the pan-European organization coordinating air traffic control of some European countries. The article is written by Hans Bouman. I quote without permission. Translation from Dutch is mine.

After quite an interesting presentation of Eurocontrol, the author pays a visit

to the Maastricht ATC centre. This visit is reported mainly as a dialog between the author and Operations Officer Willy Withofs. In a presentation of "Conflict Alert Messages" and proposed recovery actions displayed on a VDU, Withofs is quoted to say:

- > Now, we only have to follow the advice of the computer. Because it is
- > always right. The system is one hundred percent waterproof.

I sincerely hope this quote was invented/enhanced/embellished/distorted (pick your choice) by the author, not a verbatim of what the Operations Officer said!

Erling Kristiansen - ESTEC, Noordwijk, The Netherlands.

---

### **✂ 1-900 scam**

<Torsten.Lif@eos.ericsson.se>

Thu, 24 Oct 91 09:38:59 +0100

A brief note in a local newspaper the other day told the story of a simple but effective scam to draw money out of public institutions.

A couple in southern Sweden set up a "singles hot-line" service using a 071x-number (our equiv. of the 1-900-numbers in the US where the Telco and the called party split the charges paid by the caller). [note to moderator: fell free to correct if I'm mistaken about the number]

Apparently, the income from this hot-line was not enough to satisfy them so they decided to increase revenue in a simple but effective fashion. They went all around town to libraries and other public buildings, looking for phone extensions that were not too closely guarded. They'd then pick up the receiver, call the hot-line number and leave the phone with the receiver off-hook. One extension in a library was reported as having been connected to the hot-line for over a week! At a cost of over \$0.50/minute, this came as quite a shock to the people in charge of economy at the library when the bills arrived, some months later.

The RISK of this is the old one of not letting a stranger use your phone but with a new twist. Normally you'd be worried about him actually USING your phone to call long-distance. In this case, it was enough for him to merely initiate a call and then go away. How many employees in a large office will think twice about a phone being off-hook? Most people will simply assume somebody else is using it and has gone away temporarily. As long as the phone in question is not on your own desk, you're not likely to replace the receiver.

Many modern phone systems offer their subscribers blocks against calls to certain numbers or area codes, forcing users to either "unlock" the phone with a certain code sequence or to order e.g. international calls through the switchboard operator. This opens up a new can-o'-worms in the matter of personal integrity and your boss knowing who you call, but it prevents the kind of abuse described here. However, it requires somebody to explicitly request this

locking service for an office/PABX/whatever. The default, as that library found out the hard way, is to have all calls enabled.

+46 8 719 4881

Torsten Lif, Ericsson Telecom AB, EO/ETX/TX/ZD, S-126 25 STOCKHOLM, SWEDEN

---

## ✂ RISKS of Electronic Credit Card Authorization

*Derek Atkins <warlord@Athena.MIT.EDU>*

*Thu, 24 Oct 91 13:43:15 EDT*

I was at a store buying something with a credit card the other day, and when the clerk ran my card through, found that the printer was out of paper. (It was one of those machines where you run the card through, it calls up the card agency for an Authorization, and then prints the receipt on a thermal two-copy printer)...

Well, after he figured out that there wasn't a receipt, and found more paper to fill the printer, he punched a few numbers and it printed out a WHOLE NEW receipt! (Receipts are the equivalent to the old carbon receipts, except you don't need to physically imprint it with the card -- the card information is printed on the receipt for you)....

He printed this receipt WITHOUT the use of the card! Now, what's to stop him from printing a second copy, etc... It seems like a risk to let that information be that easily obtained.

-derek --warlord@mit.edu

[Nothing TECHNOLOGICAL stops him, although there are other considerations such as good business practice, hiring of honest employees, and fraud laws. This is a classical RESIDUE problem of an incomplete deallocation. The notion of TRUSTED SYSTEMS in this notion usually means that the customer must blindly trust the system and the system people, not that the system is trustworthy. PGN]

---

## ✂ Australian Software Quality Management Standard

*Douglas Thomson, ...!munnar!goanna!giaea!doug <doug@giaea.oz.au>*

*Fri, 25 Oct 91 13:43:01 est*

I thought the following might be of interest (our news feed is a bit slow, so this may well be old news by now...). I am pleased to find the state of the art is sufficiently mature to warrant such a standard; I had formed a different impression from reading RISKS :-)

Excerpted from an advertising blurb (without permission):

> \* Software Quality Management System

>

> AS 3563-91 is a major two-part Australian standard which establishes

> the key elements required to operate an effective quality management

> system during the development of computer software.

- >
- > \* Indispensable wherever software is developed
- >
- > AS 3563 encourages a controlled approach to all stages of software development and can be used as the basis for a cost-effective in-house quality assurance program. It is also specifically designed to be called up as a contractual requirement in agreements for the development of software. By adopting the quality practices defined in AS 3563, both the developer and the customer can agree on a set of quality assurance procedures designed to ensure the finished software achieves its specifications. [...]
- > \* International acceptance
- >
- > The prestigious US-based Institute of Electrical and Electronic Engineers (IEEE) is currently adopting this Australian-prepared document as the US standard for quality management in software development. [...]
- >
- > \* How to Order
- >
- > AS 3563 Part 1-91 (Requirements) AU\$18.50
- > AS 3563 Part 2-91 (Implementation guide) AU\$42.00
- > [plus P&P - no idea of rates outside Australia] [...]
- >
- > Mail: Standards Australia, National Sales Centre, PO Box 1055, Strathfield, NSW 2135, AUSTRALIA FAX: +612 746 3333
- > VISA, MASTERCARD, or cheque drawn on Australian bank

---

### **AT&T/ATC outage revisited**

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

Fri, 25 Oct 91 14:42:51 PDT

Alfred H. Scholldorf, Manager of Info Services, Reuters Information Services, Inc., sent me two clippings on the aftermath of the AT&T outage, from the 30Sep91 issue of Network World. An article by Ellen Messmer is mostly familiar stuff to RISKers. An editorial considers the increased awareness of reliability problems that this outage has brought about, and "the need for the federal government to step up efforts to guarantee the reliability of the public network." [No GUARANTEES are possible, of course.] "Rep. Robert Wise [D.-W.Va] was right when he said, "The nation must have some assurance that the FCC is providing the proper oversight to ensure that carriers fulfill their responsibilities to provide reliable service to the public." ... The government needs to act now, before a network crisis cripples the U.S."

As an aside, I am reflect on the unintended irony of the word `oversight' in such a context. Government (FCC, Congress, etc.) is supposedly dedicated to oversight [overseeing], but is often guilty of oversight [overlooking]. Something about being Over The Hill? PGN

**✉ Re: Law requiring bug fixes (Mark Seecof, [RISKS-12.54](#))**

*Geoffrey H. Cooper <geof@aurora.com>*

*Thu, 24 Oct 91 13:21:41 PDT*

Certainly such laws are already on the books for hardware products. My understanding of this is that a vendor must be willing to repair (stock spare parts, maintain expertise) a computer hardware product for up to 5 years after the product ceases to be sold by the vendor.

This costs a vendor lot, but it does provide a basic protection for the consumer. One technique used by vendors is to buy their way out of the problem. I can recall several dead end product situations, where a vendor simply gave all users free upgrades to a better product, to avoid having to maintain the old product anymore. This technique is likely even more applicable to software than hardware.

Regarding Brooks' problem of fixes causing new bugs, the vendor might not be required to fix ALL the bugs for everyone. After all, if you didn't report other bugs, you might not care (e.g., color display problem but you have only a B&W). Or you might even like the product better with some of the bugs in it!

If a bug requires a simple patch, the patch itself might be sent out and registered as a delta from the released sources (or, all too often, the released binaries...). By tracking many different deltas but not allowing the original QA'd product to evolve, the few users who are "bitten" by a particular bug may be satisfied. Clearly this doesn't get around Brooks' "two steps back" problem, but does it does prevent the problem from compounding over time.

Geof

---

**✉ Re: Single Point of Failure in L-1011 Intercom (Seidel, [RISKS-12.55](#))**

*Brinton Cooper <abc@BRL.MIL>*

*Fri, 25 Oct 91 17:45:43 EDT*

Craig Seidel (seidel@puma.sri.com) writes that the intercom harness in the TWL L-1011 is "wired like christmas tree lights where any failure in the chain causes a complete failure and requires a check of each component." He then goes on to wonder if a redundant (parallel?) system wouldn't be better because it would prevent total system disability if one component were to be broken in an emergency.

On the other hand, it seems that this risk must be balanced against the risk of the redundancy masking the loss of one part of the intercom (probably because of imperfect status checking or poor system design/installation).

At least, in a total series configuration, you \*know\* that every part of the system is working, and you know when even one goes down.

I suppose a quantitative "risk assessment" (oh, no, not \*that\* again) should compare these (and other) alternatives.

\_Brint

---

## ✂ Re: Risks of double standards (on PRODIGY)?

Jamie Saker <[jsaker@unomaha.edu](mailto:jsaker@unomaha.edu)>

Thu, 24 Oct 91 15:26:40 -0500

There was an excellent write-up in the Wall Street Journal (cover of second section) yesterday about this situation - apparently some reports indicate that while the Prodigy censor staff allowed anti-semitic comments past their review, they were not allowing others who opposed such views to reply and were censoring such messages. According to the Prodigy representative cited in the article, they were censoring them since they were argumentative in nature.

I certainly would look for this to become an excellent test case in terms of liability issues. Since Prodigy did act as a guarantor of the information presented in their forums (remember their claim that they were following the "newspaper" analogy instead of the "telephone" analogy?), they quite possibly accepted liability for any information that is slanderous, defamatory, etc. Now all it takes is for some "harmed" party (possibly the ADL???) to take Prodigy to court.

Jamie Saker, The Penny Network Foundation, P.O. Box 138, Blair, NE 68008-0138

---

## ✂ Prodigy ([RISKS-12.55](#))

Fred Gilham <[quailfred](mailto:quailfred)>

Thu, 24 Oct 91 13:43:59 PDT

Someone has posted a message explaining the situation; apparently Prodigy will not post attacks on individual subscribers. Thus a subscriber can say, "Jews deserved Hitler's treatment," and that's OK because Prodigy doesn't censor ideas, but if someone says, "That was an anti-semitic sentiment," that's not OK because it is an attack on a subscriber.

---

## ✂ An inside look at Prodigy's 'double standard' (Spector, [RISKS-12.55](#))

Ronald Hale-Evans <[EVANS@BINAH.CC.BRANDEIS.EDU](mailto:EVANS@BINAH.CC.BRANDEIS.EDU)>

Thu, 24 Oct 1991 15:08 EDT

My wife is a Prodigy editor (probably known to you as a "censor"), and she gives me the following information. The incident in question happened about a year ago. First, the bulletin in question was not posted; it was private email. The receiver of the bulletin tried to post the email in full some fifteen times in order to open discussion and it was rejected as inappropriate by the editors every time. I suggest you read more recent news releases.

>Some of the messages \_advocate\_ "another holocaust", etc, etc...

My wife says messages advocating "another holocaust" are not posted. Perhaps

you are again confusing email and bulletin board messages.

>The ADL (Anti-Defamation League) has protested to the PRODIGY management who  
>responded that they "oppose anti-semitism", but they "encourage the free  
>expression of ideas".

This is in keeping with Prodigy practice; controversial ideas may be posted to the boards, but not personal insults. My wife tells me that what happened in this case was that some Holocaust Revisionists (people who believe the Holocaust never happened) were posting to the bulletin boards. Many people were angered and tried to reply, but their responses were usually rejected because they called the Holocaust Revisionists "Nazi \*ssh\*I\*s" and so on (I don't know the exact language, but the Prodigy editors understood it to be personally insulting).

>Is this the same PRODIGY that makes decisions about what  
>acceptable "free expression" is when it comes to use of electronic mail, and  
>what are "acceptable" topics in their Health forums? Hmmm.. sees like a pretty  
>scary double standard to me....

Prodigy editors do not and cannot read private email between members. If a member complains that another member is harrassing them through email, Prodigy will often warn the harrasser and sometimes remove them from the service. By the way, Prodigy no longer has a Health forum.

As for the "double standard", the editors find it both disturbing and amusing that they are usually criticised for censorship, and now they are criticised for lack of it. If Prodigy had caved to the demands of the ADL in the first place, none of this would have happened, and the ACLU would not have to step forward and speak for Prodigy, as they now are doing.

Ron Hale-Evans, Brandeis University, evans@binah.cc.brandeis.edu

---

### **✶ Anti-semitism controversy on Prodigy**

*Greg Brail <ibism!raven!gjb@uunet.UU.NET>*

*Thu, 24 Oct 91 23:04:08 EDT*

The Wednesday, 10/23 issue of New York Newsday features on the front cover a large color photo of a Macintosh II with the headline "High-Tech Hate: Computer Network Used for Anti-Semitic Venom." The article reads that Prodigy was taken to task by the Anti-Defamation League for allegedly allowing anti-Semitic messages to appear. The second two paragraphs of the article, which appear as if they might have been pasted in at the last minute, say Prodigy reviewed its records and found the messages were sent in private e-mail. Geoffrey Moore, a company spokesman, told the Associated Press that Prodigy was "100 percent sure" the messages were not in a public bulletin board. The ADL, however, said some anti-semitic messages could be seen by the public.

Rich Klein, an ADL spokesman, told Newsday he was concerned about Prodigy's guidelines, which call for censorship of other types of messages, but not anti-Semitic ones.

Newsday quotes from some of the messages in question, and even blows four of them up in the left-hand two columns of page five. "The holocaust itself is really an edifice, a monument so to speak, to the naive gullibility of the world," reads one. The ADL said this particular message appeared in a public forum.

The article goes on to quote Gerard Van der Leun of the Electronic Frontier Foundation, plus others, in a discussion of free speech on computer networks. It does not mention the call for "another holocaust" that another poster mentioned.

The quotes I read don't sound too much different from the calls for people to "prove the holocaust really happened" and other such talk that goes on regularly in Usenet groups like alt.conspiracy and soc.history. It appears there is some confusion over whether these messages appeared in public bboards, in private e-mail, or somewhere else. (I am not a Prodigy user.) If they were in private e-mail, then how did this become a controversy, and why do other Prodigy users and/or administrators read e-mail?

The local New York TV news was sure to mention this incident, basically taking the tone that computer people were out to spread hate electronically. It seems there is some risk in this sort of thing. I don't see a risk of a Fourth Reich forming on Prodigy, but of society placing restrictions and expectations on electronic speech that it claims not to place on other forms of expression.

Greg Brail, Citibank    [ibism!gjb@uunet.uu.net](mailto:ibism!gjb@uunet.uu.net)    [uunet!libism!gjb](mailto:uunet!libism!gjb)



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 12: Issue 57**

**Monday 28 October 1991**

## Contents

- [DSA/DSS -- Digital Signatures](#)  
[Ron Rivest](#)
- [Porn-Sabotage in Italian newspaper](#)  
[Enrico Musio](#)
- [Re: MCI Friends & Family](#)  
[Allan Meers](#)
- [Do floor vibrations damage disks?](#)  
[Magnus Redin](#)
- [Re: Software migration at Johnson Space Center](#)  
[Doug Burke](#)
- [A New Twist on "Speed Controlled by Radar"](#)  
[Andrew C. Green](#)
- [Call for Papers ESORICS-92](#)  
[Yves Deswarte](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ DSA/DSS -- Digital Signatures

*Ron Rivest <rivest@theory.lcs.mit.edu>*  
*Sat, 26 Oct 91 23:12:33 EDT*

Director, Computer Systems Laboratory  
ATTN: Proposed FIPS for DSS  
Technology Building, Room B-154  
National Institute of Standards and Technology  
Gaithersburg, MD 20899

Dear Director,

I'm writing to comment on the public-key digital signature algorithm, which you call "DSA", that you have proposed to become a standard. This letter is in response to your request for comments to this proposal. Although I have other comments about this algorithm (to be made in another letter), and I believe that an RSA-based standard would serve the country much better, I will restrict

my comments here to just a discussion of your proposed key size of 512 bits for the DSA. I believe that a national standard based on such a fixed small key size would serve our country very poorly--you are unnecessarily risking catastrophic failure of the integrity of our financial, industrial, and governmental information-processing systems.

To begin with, I question the rationale for having a fixed key-size at all as part of your proposal. Clearly, one needs a minimum key-size to prevent users from choosing keys-sizes that are too short to be secure. And one might want a maximum key-size so one can design efficient yet fully-compatible implementations. Yet there is no obvious reason why the minimum required key-size and the maximum allowed key-size should be the same.

Indeed, your "one size fits all" proposal is a very poor match to the engineering and security needs of most public-key applications. Typically, there are many users, each of whom has a public key used by others to verify his digital signatures. Such applications are invariably based on the use of "certificates," so verifiers can assure themselves that they are verifying signatures with the appropriate public key. A certificate is a message associating a user's name with his public key; this message is itself signed by a "certifying authority" whose public key is widely known. A typical signature verification then normally consists of two verifications: one to verify the certifying authority's signature on the user's certificate, and then another to actually verify the user's signature.

(As a side note, I observe that this typical structure contradicts your claim that signing is done more often than verification. In my experience, verification is typically done at least twice as often as signing.)

A certificate-based application thus incorporates two basic kinds of signatures: ordinary user signatures and signatures by a "certifying authority." The latter kind form the backbone of the integrity of the entire application, since the ability to forge certificates would give an attacker essentially unlimited power to corrupt the system. I consider it essential in secure public-key system design to have certifying authorities use the maximum allowable key-size. This size is typically much larger than what an ordinary user might select for his own public-key size. As an example, in an RSA-based scheme, certifying authorities might use keys of 1024 bits, whereas ordinary users might choose key sizes of 500--800 bits.

In a typical application, the trade-off between security and performance mandates the use of different key-sizes in different parts of the system. Certifying authorities, or users with very valuable data, must use very long keys to achieve the highest possible security level. Other users, with reduced security requirements and/or more stringent performance requirements, will use shorter keys. Trying to make "one size fit all" results either in unacceptably low security for all users (because all certificates will be suspect) or unacceptably poor performance for some users.

In a public-key system based on number theory, there is no valid technical reason for requiring a fixed key size. The underlying number-theoretic algorithms can support arbitrary key sizes. Users and certifying authorities should be able to choose key sizes according to their requirements.

I now turn to a discussion of the particular key size you have chosen: 512 bits. (By key size, here, I refer to the size of the prime modulus  $p$ .) I argue here that if you are going to insist on having a fixed key size, then 512 bits is far too short.

I note that you provide no rationale for the choice of your key size. While it is my belief that you have been co-opted by the NSA (who fears the use of widely distributed public keys as a basis for encryption algorithms), I will restrict my discussion to technical matters rather than political speculation.

In order to estimate the key size necessary, one needs to understand the computational resources available to an imagined potential attacker, and the computational difficulty of the underlying cryptanalytic problem. Let me address each of these issues in turn.

How much computational power can an imagined attacker bring to bear to "break" the system? This depends on the time period we are talking about (since technology is rapidly evolving) and the financial resources of the attacker (to purchase the necessary computing power).

It is necessary to know the expected lifetime of the proposed standard in order to know what level of security to aim for. A scheme that is considered "secure" today may not be secure in the year 2000, and a scheme considered secure in the year 2000 may not be secure in the year 2010. Computer technology is evolving at an incredible pace, and is likely to continue to do so for the next few decades. The security of cryptographic schemes thus tends to "erode" steadily over time, and the design of cryptographic systems must envision and plan for such erosion.

I would suggest that a digital signature standard should be designed with a minimum expected lifetime of at least 25 years. That is, one should design so that a system adopted in the year 1992 should still be secure in the year 2017. It should not be possible for an attacker in 2017 to forge a signature, using the computers available then.

Where does "25 years" come from? To consider the only available precedent of the lifetime of a NIST cryptographic standard, I note that the DES was adopted in 1976 and seems likely to still be in widespread use by 1996, twenty years later. After a cryptographic signature standard has been terminated, one needs to have an additional period of time where the validity of signatures can still be assured. For example, it is not uncommon to require that signed documents be retained and be considered legally binding for seven years. A signature produced in the year 2010 should still be verifiable in the year 2017, with an understood assurance that it wasn't just recently forged. I consider a 25-year expected lifetime a minimum reasonable requirement for a digital signature standard.

What kind of computational power will be available to an attacker in the year 2017? It is widely asserted that computational power (per dollar spent) is increasingly at approximately 40% per year. Some of my colleagues assert that 45% is a better estimate, but I'll stick to the more conservative estimate. This means that we have an approximate doubling of computer power (per dollar) every two years, and an approximate increase of a factor of 4500 after

twenty-five years. Let's round this off to 5000 for our back-of-the-envelope calculations (corresponding to 25.3 years at 40% growth/year). In the year 2017, I expect computer power will be about 5000 times cheaper than it is now.

How big an attack should one prepare for? Let me suggest that a national digital signature standard should, at a minimum, be able to withstand an attack costing an attacker \$25 million. This amount of money is easily available to large corporations, drug dealers, and third-world countries. There is no reason that our national security, in terms of the integrity of our electronic business, financial, and governmental information-processing systems, should be vulnerable to an attack costing only \$25 million. Indeed, it is easy to make an argument for a much higher threshold; it is not hard to imagine scenarios in which the benefit of a successful attack exceeds \$25 million. However, I'll continue our back-of-the-envelope calculation with the \$25 million figure.

How much computing power can one buy for \$25 million? Today, a workstation with 100 MIPS (million instructions per second) can be probably be purchased in quantity for about \$5,000. An attacker wouldn't need all of the peripherals (screen, floppy disk, mouse, nice cabinet, etc.), and could economize by sharing power supplies, fans, etc. He is basically interested in having many processors, each with a reasonable amount of memory. Let me estimate that such a "stripped-down" 100-MIPS processor would have an amortized cost today of \$1,000.

A convenient unit of computation is a "MIPS-year"---the amount of computation performed by a one-MIPS processor running for a year. A MIPS-year thus corresponds to about 32 trillion basic operations. If we assume that a 100-MIPS processor lasts for about 10 years, we obtain an amortized cost estimate for today of \$100 per MIPS-year of computation. (Here we are buying "computation by the yard"; our yard is one MIPS-year, and it should cost about \$100 in quantity. The details of buying computational power in 2017 I leave to your imagination; a simple cost-effective way might be to spend considerably more than \$25 million to purchase hardware, and then to resell the hardware after the computation is done.)

We therefore can estimate that an attacker with \$25 million to spend today could purchase about 250,000 MIPS-years of computation. In the year 2017, he will be able to purchase about 5000 times as much, or 1.25 billion MIPS-years. I believe that a digital signature standard adopted today should, at a minimum, be able to withstand an attack of 1.25 billion MIPS-years. (This sounds like a lot of computation, but you can see from my arguments above that this is in fact a rather conservative estimate of the security requirement for such a standard.)

How large a key-size is needed to withstand an attack of 1.25 billion MIPS-years? This depends, of course, on the cryptanalytic problem to be solved. In the case of your proposed DSA, the basic cryptanalytic problem is the "discrete logarithm problem": computing  $x$ , given  $g$ ,  $p$  and  $g^x \bmod p$ . Using the best-known algorithms for this problem, the number of operations required is approximately

$$L(p) = e^{\sqrt{\ln p \ln \ln p}} .$$

The state of the art in algorithms for the discrete logarithm problem is still

evolving, but the above formula certainly seems like a very conservative estimate of what will be possible in 2017, since it represents what is possible today. For example, with a 512-bit prime  $p$  (as in your proposal), we see that only

$$\begin{aligned} L(2^{512}) &= 6.7 \times 10^{19} \text{ operations} \\ &= 2.1 \text{ million MIPS-years} \end{aligned}$$

of computation are required to "break" a 512-bit problem. Thus, we see that your proposed DSA is over 500 times weaker than a conservative analysis suggests is required.

Another way of stating the above result is that the DSA, as proposed, has a maximum expected secure lifetime of approximately six years. (Since  $250,000 \times 1.4^{6.33}$  is greater than 2.1 million.)

Setting  $L(p)$  equal to 1.2 billion MIPS-years, and solving for  $p$ , we find that the DSA should be using keys of at least 640 bits, minimum.

This is, as noted, a conservative estimate. It doesn't plan for improvements in the state of the art of algorithms for solving the discrete logarithm problem, which can have a dramatic effect on the key size required. It has no margin built-in for faster-than-expected improvements in hardware, longer-than-expected use of the DSA, or richer-than-expected adversaries. The ability to harness for free "unused" processor cycles over large networks of workstations could also dramatically increase the computational ability of an adversary, thereby altering the equation further in his favor. For these reasons, and as a matter of sound conservative design, I feel that a substantial "margin of safety" should be built into the standard. Most importantly, certifying authorities should have generous key-sizes allowed. I would strongly recommend allowing key sizes of at least 1024 bits for certifying authorities, and at least 800 bits for users, in any digital signature standard. I feel that anything less is short-sighted and risky, possibly verging on the irresponsible. In cryptographic systems, responsible design is conservative design; generous allowance must be made for unforeseen developments.

For all the above reasons, I feel very strongly that your DSA proposal, with its proposed 512-bit keys, is not sufficiently secure to be acceptable as a national signature standard.

Sincerely,

Ronald L. Rivest, Professor of Computer Science, MIT, Cambridge, Mass. 02139

### Porn-Sabotage in Italian newspaper

*Enrico Musio* <ele9059@cdc835.cdc.polimi.it>

*Mon, 28 Oct 91 13:12:47 MET*

Two national newspapers (Corriere Della Sera and La Repubblica) reported on 25,26,27 October on a series of incidents occurred to a third Italian

newspaper,La Notte, circulated in Milan metropolitan area.

On Thursday 24 October someone (probably an insider) altered an advertisement for a coffee brand,exploiting the lack of acces control of the computer system used by the editorial staff to prepare the journal.

Each occurrence of the word 'coffee', including the headline, was changed to the four-letter (in Italian too.. :-) bad word commonly used to denote the female sexual organ.

The fact was discovered too late to block distribution of the first printing of the morning edition (35.000 copies).

The day after,the prankster stroke back,twice. He (or she) turned a definition in a crossword puzzle into an obscene phrase, and in the horoscope suggested to Capricorn-born : "explain as soon as possible a misunderstanding with a colleague:just put your hands on her \*\*\*\*" (politely: 'her buttocks'). The horoscope modify was caught in time by an emergency revision task-force,but the crossword wasn't.

The journalists have been denouncing the RISKy situation since last winter, and are ready to withdraw their signatures from articles if lasts the present situation in which everyone with minimal skills can modify everything,even the camera-ready files.

An internal inquiry was open and a denouncement versus unknown presented to law enforcers.

Enrico Musio, Politecnico di Milano , Italy ele9059@cdc835.cdc.polimi.it

---

### **re: MCI Friends & Family**

*Allan Meers - Sun Education/Professional Services <Allan.Meers@ebay.sun.com>  
Fri, 25 Oct 91 11:07:07 PDT*

Calling the 800-FRIENDS number lets you quickly build a list of all the listed "friends and family" of anyone currently on the service, and with the zip code, you can build an "ever-widening" circle of connections.

If I were a skip-tracer, tracking down a pastdue bill payer, OR trying to find an estranged spouse, or anyone who wishes not to be found, this could be an absolute boon. Even if you don't subscribe to the MCI service, people who call you do, and I only need to know of one of your family or friends phone numbers - and if they use MCI, and have your number listed, it becomes all but "public" information.

I would expect that any phone company like MCI, or the 800-FRIENDS number to access their database, would utilize CALLER-ID to track who is calling them. I am a fan of CALLER-ID, and believe it to be a valuable tool against this kind of possible abuse. If only they would use it for security instead of just phone marketing.

There are some other interesting risks when scanning the databases of your friends and family for occurrences of your phone number:

I actually felt insulted that my older brother had all of our 9 other brothers and sisters listed, BUT NOT ME ! I wonder why he didn't feel that I should be listed ?

A couple of the phone numbers listed were wrong, either because of a transposed digit, or because the phone number has changed. This means that you think you are getting a discount when you call your brother, but in fact, since the number is wrong, you are not. You might have been better off with another company that doesn't require a pre-planned list of numbers.

Not only do you have to have them on your list, but they also have to be an MCI customer for you to get the discount. I think you also have to be on their list for that discount. This means that you don't save if you are making calls to any companies or people unless they are pre-planned, and inserted on your F&F list. There may be a delay between the time you ask that they be listed, and the listing becomes effective.

I was listed on 6 different F&F databases. So far, MCI has called me 3 different times for 3 of those 6 F&F's. They tell you whether or not your listed F&F has accepted (they are on the "MEMBERS" list). If they are on the "NOMINEES" list, there is a notation for "Not called/accepted yet", or "Did Not Accept", which means you told the MCI salesman no.

1 of the entries for me is listed "Did Not Accept" (it must be they way they list "he said no thanks and hung up on me"). Even with that entry, I am still receiving other calls. I expect a call for EVERY person who lists me, because apparently they don't cross-reference F&F lists for your number to see if you have been contacted already. Either that, or they are hoping to wear me down.

There is a look up service were you can check your account for the inclusion of a specific number, rather than just relisting all of them. Every number I tried was marked "not in your calling circle", even tho they are listed on the big list. MCI must have serious problems with their database lookup scheme.

2 numbers listed on the members list were reported as "number not in the MCI plan" when I tried to look that number and zipcode up for their list. This is another occurrence which leads you to believe you are saving when you call them, but in reality, you are not. Both of those people were listed on other lists as "Did Not Accept", and I know that neither has chosen MCI as their plan. The people calling them are quite fooled however into thinking they are discount calls.

MCI has a very aggressive phone marketing strategy, and very much a part of their tactics, is to call you once a family member

has been signed-up and say "Don't you want them to save money?".  
If you don't sign up, you make your mom pay a lot more for calls.  
Of course, the hazards, pitfalls and misconceptions aren't well  
explained on the phone or in the literature.

The phone company can be helpful in translating a phone number  
into a geographical area, while the post office will help  
translate geo-info into zip-code info.

This service isn't for me - not with all the other flat-rate discount plans  
from other companies that don't require pre-planned, constantly updated,  
limited use, publicly available lists of your personal contacts.

---

### ✂ Do floor vibrations damage disks?

*Magnus Redin <redin@lysator.liu.se>*

*Mon, 28 Oct 1991 01:03:02 GMT*

Has anyone had experience with locating a computer hall on the same floor (slab  
of concrete) as a machine shop? Do the vibrations damage the disks?

Magnus Redin, Lysator Computer Club Magnus redin, Rydsv{gen 240C26,  
582 51 LINK|PING, SWEDEN Phone: Sweden (0)13 260046 (Answering machine)

---

### ✂ Re: Software migration at Johnson Space Center (Bouchard, [RISKS-12.48](#))

*"Doug Burke" <douglasburke@msavc.enet.dec.com>*

*Sun, 27 Oct 91 19:05:36 PST*

>2) Unisys A-Series (Burroughs) and 1100-Series (Univac/Sperry) ... go from  
>desktop processing to major mainframe class processing power with NO required  
>changes to the software...

As I said, I am not a salesman. However, it's necessary that the record be set  
straight. Being conservative, the VAX line spans more than 50 specific  
machines from Desktop, to Mainframe and SMP Mainframe Clusters, including  
server, Fault Tolerant, and high availability systems all using exactly the  
same operating system VAX/VMS. The range extends from roughly under .8 MIPS,  
to over 5000 MIPS, in increments of 2 to 3 MIPS. All code written on VAX/VMS  
is binary compatible across all of these lines with "NO required changes to the  
software". I have been lead to believe that this gives Digital Equipment the  
"largest RANGE" given the above criteria.

I must, unfortunately beg ignorance of the Unisys line. Making claims of  
"largest RANGE" though, can be highly subjective, and must be extensively  
qualified when dealing in the information processing environment. This is a  
risk that everyone working in the this field deals with on a daily basis.

Doug Burke, Senior Software Specialist, Digital Equipment (Malaysia),  
doug.burke@msa.mts.dec.com

---

## **✂ A New Twist on "Speed Controlled by Radar"**

*<acg@hermes.dlogics.com>*

*Mon, 28 Oct 1991 09:54:29 CST*

The current discussions regarding bridge warning signs that don't work and AT&T's problems with warning signals being ignored bring to mind a recent experience of mine. I'll leave the evaluation of RISKS to the readership.

There was until recently a rather bad intersection on Route 41 north of Chicago, where an expressway was interrupted by a traffic light at Clavey Rd. (This has finally been replaced by an overpass.) As this stop was very unexpected for northbound traffic speeding out of the city, the intersection was one of the deadliest in the state. Numerous crashes occurred when 3-D drivers (Drugged, Drowsy or Drunk) failed to notice the stoplight and plowed into stopped vehicles. Adding strobe lights to the red traffic lights gave too-little advance warning, and bump strips (like those at toll plazas) kept nearby residents awake at all hours.

As an additional remedy, radar transmitters were mounted behind signs on overpasses near the intersection. The idea was that they would trigger radar detectors in oncoming traffic and slow it down. I can attest from first-hand experience that they worked awfully well; my detector would go completely bonkers about two miles before the intersection, giving me plenty of warning to slow down.

So far, so good, but after a short time, the transmitters apparently failed (or were shut down; unfortunately I don't have the details). Nevertheless, the experiment raises some questions in my mind: How would anyone in an official capacity such as the State Police discover that the transmitters had suddenly failed and the hazard had escalated? (I rather doubt that they have their own radar detectors in the squad cars!) More to the point, how would they be able to enforce the speed limits or get coherent radar gun readings in an area flooded with bogus signals? I'm not taking a position on the 55 mph speed limit here (and I've had no difficulties with the local constabulary :-), but we know how difficult it is to fight a ticket imposed by radar gun. I wonder if the transmitted radar "flood" interfered with speed radar guns, and if so, how they knew where the limits of the range were. The basic idea of slowing a portion of the oncoming traffic with radar seems viable, but the attendant RISKS of error-detection (false indicated speeds and system failure) seem a bit unclear.

Andrew C. Green, Datalogics, Inc., 441 W. Huron, Chicago, IL 60610  
(312) 266-4431 UUCP: ..!uunet!dlogics!acg Internet: acg@dlogics.com

---

## **✂ Call for Papers ESORICS-92**

*Yves Deswarte <deswarte@laas.laas.fr>*

*Mon, 28 Oct 91 17:28:16 +0100*

ESORICS-92

CALL FOR PAPERS

## European Symposium on Research in Computer Security

Toulouse, France, November 23-25, 1992

Sponsored by AFCET

**AIMS AND TOPICS:** The aim of this symposium is to further the progress of research in computer security by bringing together researchers in this area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in areas related to computer science, information theory and artificial intelligence.

Papers are solicited in the following areas:

### Theoretical Foundations of Security

- security models, contribution of models for knowledge representation
- contribution of formal logic and information theory
- formal development techniques

### Secure Computer Systems

- operating system security, network security
- security management
- virus and worms
- contribution of artificial intelligence
- contribution of new architectures and new technologies

### Applications Requesting Security

- data bases, knowledge bases, transaction systems
- process control, real time
- distributed applications

### Cryptography

- applications
- validation of protocols
- authentication: protocols, key management, processes

### Security Verification and Evaluation

- formal methods
- measure and evaluation of risks
- measure and evaluation of security
- criteria

### Software Development Environments for Security

### Operation of Secure Systems

- management
- intrusion detection

This list is not exhaustive. Research papers, position papers and panel proposals will be welcomed.

**SUBMISSIONS:** Five copies of papers or panel proposals should be submitted to the program chair by April 3, 1992 at the following address:

Jean-Jacques Quisquater  
AFCET - ESORICS-92  
156, boulevard Pereire  
75017 Paris - France

The texts must be submitted in French or in English. Papers should be limited to 6000 words, full page figures being counted as 300 words. Each paper must include a short abstract and a list of keywords indicating subject classification. Papers will be refereed and the final choice will be made by the Program Committee. Notification of acceptance will be sent by June 15, 1992, and camera-ready copy will be due on September 1, 1992.

Panel proposals should include title, proposed chair, tentative panelists, a 2 or 3 paragraphs description of the subject, format of the presentation, and rationale for the panel.

For further information and/or copy of the advance program when available, send E-mail to:

deswarte@laas.fr

or write to:

AFCET, 156 bd Pereire, 75017 Paris, France.

**IMPORTANT DATES:**

Submission deadline: April 3, 1992

Acceptance notification: June 15, 1992

Camera-ready copy due: September 1, 1992

GENERAL CHAIR: Gerard Eizenberg (ONERA-CERT, France)

**PROGRAM COMMITTEE**

CHAIR: Jean-Jacques Quisquater (UCL, Belgium)

Bruno d'Ausbourg (ONERA-CERT, France)

Joachim Biskup (Universitat Hildesheim, Germany)

Peter Bottomley (RSRE, United Kingdom)

David Chaum (CWI, Netherlands)

Yvo Desmedt (University of Wisconsin-Milwaukee, USA)

Yves Deswarte (LAAS-CNRS & INRIA, France)

Gerard Eizenberg (ONERA-CERT, France)

Amos Fiat (University of Tel-Aviv, Israel)

Dieter Gollmann (University of London, United Kingdom)

Franz-Peter Heider (GEI, Germany)

Jeremy Jacob (Oxford University, United Kingdom)

Helmut Kurth (IABG, Germany)

Peter Landrock (Aarhus University, Denmark)

Jean-Claude Laprie (LAAS-CNRS, France)

Teresa Lunt (SRI, USA)

John McDermid (University of York, United Kingdom)

John McLean (NRL, USA)

Catherine Meadows (NRL, USA)

Jonathan Millen (MITRE, USA)

Emilio Montolivo (Fondazione Ugo Bordoni, Italy)

Alfredo de Santis (Universita di Salerno, Italy)

Einar Sneekenes (NDRE, Norway)  
Marie-Jeanne Toussaint (Universite de Liege, Belgium)  
Kioumars Yazdanian (ONERA-CERT, France)

ORGANISING COMMITTEE

CHAIR: Yves Deswarte (LAAS-CNRS & INRIA)  
Laurent Cabirol (SCSSI)  
Jean-Francois Cornet (CORESIA)  
Michel Dupuy (ENST)  
Marie-Therese Ippolito (LAAS-CNRS)  
Paul Richy (CNET)  
Pierre Rolin (ENSTA)  
Kioumars Yazdanian (ONERA-CERT)

==== 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 12: Issue 58

Tuesday 29 October 1991

## Contents

- [Would you put your rook and bishop out on knights like this?](#)  
[PGN](#)
- [Re: DSA/DSS -- Digital Signatures](#)  
[James B. Shearer](#)  
[Ron Rivest](#)
- [FDA-HIMA Conference on Regulation of Software](#)  
[Rob Horn](#)
- [UCI computing survives power outage \[almost\]](#)  
[Doug Krause](#)
- [Re: Swedish election results were delayed](#)  
[Lars-Henrik Eriksson](#)
- [Re: Licensing of Software Developers](#)  
[John Gilmore](#)
- [The risks of "convenient" technology](#)  
[Curtis Galloway](#)
- [Free Call-Back](#)  
[Lars-Henrik Eriksson](#)
- [The flip side of the 1-900 scam](#)  
[Andrew Koenig](#)
- [Info on RISKS \(comp.risks\)](#)

---

## ✉ **Would you put your rook and bishop out on knights like this?**

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Tue, 29 Oct 91 9:09:59 PST

Computer Solves Chess Argument

BALTIMORE (AP) [29Oct91]

A 25-year-old graduate student solved an ancient chess puzzle by taking a computer to places no computer has gone before. The double feat by Lewis Stiller, a computer scientist at Johns Hopkins University, not only settled an old chess conundrum. He opened the door for analysis once considered too complicated for even the fastest computers. [...] By performing one of the largest computer searches ever conducted, Stiller found a king, a rook and a

bishop can defeat a king and two knights in 223 moves, ending argument over whether the position is a draw. Stiller, who works in Hopkins' artificial intelligence lab, made the search by writing a new program that tapped the power of a massively parallel computer at the Los Alamos National Laboratories in New Mexico.

The computer is actually thousands of processors working side by side on parts of a program. Unlike most computers, the Los Alamos machine has 65,536 processors instead of one. [...] Stiller devised a way to avoid bogging down the computer with communications between the processors while it worked his 10,000-line program. The computer solved the chess problem in five hours after considering 100 billion moves by retrograde analysis working backward from a winning position.

The prod to push the computer came from Noam Elkies, a Harvard mathematics professor Stiller met on a computer bulletin board. The two were discussing computers and chess when Elkies suggested the six-piece endgame Stiller ultimately solved. Elkies said the solution goes beyond the gameboard. "This is an idea that can be used for a much greater generality of problems than just chess games," Elkies said in a recent interview. "The new thing he was able to figure out was some important ways to allow the parallel computer to work on the problem."

The program can solve a five-piece endgame in about a minute and a six-piece endgame in four to six hours, said Stiller, who said his chess aptitude has slipped since he took up computer science.

Kenneth Thompson of Bell Laboratories was the first to use retrograde analysis to solve chess endgames, the last portion of the game, proving a king and queen can defeat a king and two bishops. Thompson's program took weeks to solve a five-piece endgame using a much slower computer, Stiller said.

The Thompson analysis led the International Chess Federation to change its rules on what constitutes a draw. Before that, the federation said a draw was any game that couldn't be won in 50 moves after the last capture of a piece or move of a pawn. The federation now makes exceptions, Stiller said.

[There was a final comment from Stiller in the slightly longer version that I saw in the San Francisco Chronicle today, p.A7: ``The actual significance of this for full chess is minimal because the position is very rare. For the practicing chess player, I don't think it is going to have much effect."]

We already have parameterized openings, spanning many moves in sequence. Perhaps now we can get to macroized game endings; in the craze to package everything for TV, K,R,B against K,Kn,Kn can simply invoke Stiller and cut to the commercial. Of course, the 223 moves have to be impeccable, or else K,R,B might fall into a repeated-move draw play and K,Kn,Kn would ask for his quarterback (or halfback, or whatever).

This is wonderful example of the rapidly moving boundary of the computationally possible, perhaps leading nicely into the following on-going discussion on cryptographic complexity... PGN]

---

✉ **Re: DSA/DSS -- Digital Signatures (Rivest, [RISKS-12.57](#))**

<jbs@watson.ibm.com>

Mon, 28 Oct 91 21:16:02 EST

The letter by Rivest posted in [RISKS-12.57](#) contains at least one blatant error. Ron Rivest writes: "A convenient unit of computation is a ``MIPS-year''---the amount of computation performed by a one-MIPS processor running for a year. A MIPS-year thus corresponds to about 32 trillion basic operations. If we assume that a 100-MIPS processor lasts for about 10 years, we obtain an amortized cost estimate for today of \$100 per MIPS-year of computation."

The figure of \$100 was apparently derived by dividing \$1000 the assumed per processor cost by 10, the assumed lifetime in years. However the processors were assumed to be 100 mips. Hence the correct figure would be \$1 per mips-year of computation. However if in fact computation is getting cheaper by 40% per year computing equipment will lose 40% of its value per year for this reason alone (ignoring any physical deterioration). Therefore the straight-line 10 year depreciation assumption is totally inappropriate. One should instead write off at least 40% in the first year. This would give a cost of \$4 per mips-year. Many of the assumptions made throughout the computation are highly debatable as well.

James B. Shearer

---

## **✂ DSA/DSS -- Digital Signatures**

*Ron Rivest <rivest@theory.lcs.mit.edu>  
Tue, 29 Oct 91 12:57:04 EST*

How embarrassing! Shearer is correct in pointing out my oversight. I did forget to divide by 100 in estimating the cost per MIPS-year. With my approach, the cost should have been \$1 per MIPS-year. But I like his more refined suggestion on non-linear depreciation, and find his estimate of \$4 per MIPS-year to be reasonable.

Correcting this error, of course, only strengthens my argument and conclusions. The cost to an attacker will be 25 times smaller than my estimate. We now have as revised conclusions:

- An attacker in the year 2017 with \$25 million to spend should be able to mount an attack of 31.25 billion MIPS-years, not 1.25 billion MIPS-years.
- The security of the proposed DSS, with its 512-bit keys, is over 12,500 times too weak, not just over 500 times too weak.
- DSS should be attackable today for less than \$25 million. (Since buying 2.1 million MIPS-years will cost only \$8.2 million.)
- The required key size (setting  $L(p)$  equal to 31.25 billion MIPS-years), rises from 640 bits to 710 bits.

The importance of having larger keys should be even more apparent. While, as Shearer suggests, there are still debatable points about this analysis, I do not believe that the overall conclusions would change for a more refined analysis.

My apologies for the error and resulting confusion.

Sincerely, Ronald L. Rivest

---

## **FDA-HIMA Conference on Regulation of Software**

<HORN%athena@leia.polaroid.com>

Fri, 25 Oct 1991 16:38 EST

On 9 and 10 October 1991, the Health Industry Manufacturers Association (HIMA) and the Food and Drug Authority (FDA) had a joint conference to explain FDA regulation of software. The following is a summary of highlights from that conference. (If you are actually involved with potentially regulated software, contact the FDA for the complete rules and contact an expert. This area is as complex in its details as the tax laws.)

First, what does the FDA regulate?

- 1) Under the 1936 Act, any medical device, drug, or practice.
- 2) Under the 1990 Safe Medical Devices Act, authority to examine devices was expanded.

Software may be involved in any of four ways:

- 1) It may be a device
- 2) It may be used in the manufacture of a device or drug
- 3) It may be used in record keeping
- 4) It may be contracted or purchased from a third party for one of the above.

FDA approval involves two steps: approval to market and approval to sell.

Approval to market involves one of two things: 1) A PMA for new medical technologies (see an expert now). 2) A 510(k) for equivalent medical technologies (substitutes for some previously approved device).

For a 510(k) approval there are three categories of approval difficulty based upon the hazard to patients and others:

- 1) minor, little risk of injury either direct or indirect
- 2) moderate,
- 3) major, risk of death

An example of a minor is a urological machine comprised of a funnel, flask, scale, and computer for measuring urinary function. It is very hard to hurt anyone when this machine malfunctions. A misdiagnosis injury is also very unlikely because many other measurements and human interventions will take place before a decision is made. An example of major is the remote programmer for a pacemaker. Death is a likely direct result of a malfunction.

The FDA examination for a 510(k) is proportionate to the risk. For a minor risk item the FDA will probably accept a detailed development plan, and defensible development, configuration control, and validation methodologies. For a major risk item, they will examine all the validation results in detail and demand thorough hazard analysis. They will challenge many details to assure themselves by spot inspection that the validation is probably complete.

For more details ask the FDA for a copy of the 510(k) reviewers guidance. This is the document used by the 510(k) reviewer and is freely available to the public.

Then comes approval to sell. This is based upon a Good Manufacturing Practices (GMP) inspection. Again, the inspection detail will be a function of the risk to the patient and others.

For a minor risk item, they might not inspect at all. Most likely, they just verify by spot checks that the claims made in the 510(k) are being kept. For a major risk item, they may inspect a lot. If someone actually gets hurt, expect an army of inspectors swarming over everything.

For software there was little surprise that the inspectors verify all the claims in the 510(k). The surprise was in how ancillary manufacturing software and purchased software are treated. First, any software might be inspected. If its failure could lead to injury it is subject to inspection. This means that a spreadsheet program on a PC will be subject to inspection if it is used to compute a quality parameter. Second, there is no assumption of validity for off the shelf software.

For more details, the FDA provides copies of GMP practices regulations to anyone who asks.

In a recent GMP inspection a drug maker was hit with violation notices because an off-line PC was being used to run a statistical process control package as part of a process improvement effort. The SPC was not directly used to control manufacture or determine quality. Other equipment handled that. The problems listed were:

- 1) The PC was not under strict hardware maintenance schedule with change control and serial number tracking of components.
- 2) The specific PC hardware configuration was not validated.
- 3) The SPC program validation was inadequate (the drug manufacturer had run and documented test cases before placing it in use).
- 4) The PC was not regularly backed up
- 5) There were no documented procedures for disk space management.
- 6) There was not a documented procedure and records for software change and update validation.
- 7) There was not sufficient security and auditing to assure that the software was not changed during use.

The manufacturer was told to fix these problems. If they were not fixed, the factory would eventually be shut down.

This attention to software is new at the FDA. It went into effect this summer and more regulations take effect this fall.

The other area that is catching people by surprise is the extent of the definition of device and manufacture. Most recently, the makers of blood bank software were hit. They had not previously realized that the database software for tracking blood donations was a medical device and probably a class 3 device. Big time mistake. About a third of the blood bank software vendors have been closed, and their software recalled by the FDA. There is an open issue around hospital and laboratory information systems. These may also be medical devices depending upon how they are used.

As an example: a mainframe manufacturer M ran an advertisement claiming that since hospital X used M's machines, it could deliver superior care. By doing this, manufacturer M has made a medical efficacy claim and converted their mainframe into a medical device. In theory, they must now get a 510(k), GMP inspected, prove the safety of their mainframe, and demonstrate that it does in fact improve medical care. In practice, they get a phone call telling them ``Don't be fools. Stop running that ad. You don't realize what you are doing."'

The HIS and LIS vendors are at more risk. If a failure in an HIS or LIS software leads to incorrect recording of critical patient information that can then cause death, they may be class 3. It depends upon what other safeguards exist. If the usage label does not require other safeguards exist, class 3 may follow.

The FDA approach differs from that of MoD and others in that there is no FDA approved methodology. The FDA will not state that anything is guaranteed acceptable. Instead you are always subject to challenge. They claim that this allows them to accept new methodologies as they are proven. It also lets them reject anything and not expose them to the risk of making a decision. If anything goes wrong, its your fault and you (not the FDA) are liable.

Rob Horn   horn%hydra@polaroid.com

---

### ✂ UCI computing survives power outage [almost]

*Doug Krause <dkrause@hydra.acs.uci.edu>  
Sat, 26 Oct 91 02:06:09 -0700*

Re: Power outage downs New York Stock Exchange ([RISKS-12.55](#))  
> The NYSE was down between 10:21am and 10:45am on Tuesday 22Oct91 because of a  
> power outage that downed all of the computers (but not the lights!)

Yesterday (the 25th) we (UCI Academic Computing) had a power failure that took out our lights and AC but left the computers up. However, within 15 minutes the temperature in the machine room had shot up 10 degrees and we needed to bring all the systems down. So much fun.

Douglas Krause, University of California, Irvine   BITNET: DJKrause@uci.edu

---

### ✂ Re: Swedish election results were delayed (Minow, [RISKS-12.56](#))

*Lars-Henrik Eriksson <lhe@sics.se>  
Mon, 28 Oct 91 10:20:47 +0100*

Martin Minow <minow@ranger.enet.dec.com> writes about a computer miscalculation during the recent Swedish elections.

What is even more frightening about miscalculations is how people blindly trust computer calculations. As usual, during the evening after the elections,

Swedish TV were continuously presenting forecasts.

At one point, the results from one voting district from the city of Nacka, outside Stockholm, were shown. The distribution of votes between parties was completely weird, and the commentators went into great detail explaining how individual districts could have a distribution of votes that differed substantially from the national average. They also wondered what particular factors could have caused the voters of this district to vote the way they did.

At no point did they notice that the proportion of votes given to the different parties added up to about 140%.

Lars-Henrik Eriksson, Swedish Institute of Computer Science, Box 1263  
S-164 28 KISTA, SWEDEN +46 8 752 15 09

---

## **✉ Re: Licensing of Software Developers**

*John Gilmore <gnu@toad.com>  
Sun, 27 Oct 91 00:05:24 PDT*

David Parnas steps beyond advocacy to misrepresentation (in [RISKS-12.54](#)):

- > They assume that the body that issues the licenses is the government.
- > That is not the case for other engineers. In many jurisdictions there
- > is a professional body that is charged with this task. In Ontario it is
- > the APEO, Association of Professional Engineers of Ontario. In
- > Australia there is an "Institution of Engineers". Thus, it becomes the
- > job of professionals to set the standards for their own profession and
- > to enforce them.

He was doing fine until he came to `...and to enforce them'.

We already have plenty of organizations in the computer field who issue licenses to people after testing their competence. Universities that issue degrees are a good example. The Certified Data Processor exam is another. Professionals setting the standards for their own profession, just like he said.

What's different is that nobody is forced to get one. The licenses Mr. Parnas mentions to us are in fact *\*issued\** by private boards, but *\*enforced\** by the government. A law states that to practice that profession, you must get a license from the board; failure to do so results in civil or criminal penalties. The boards are `private' in the sense that the government does not contribute funds to them, but they hold the government's monopoly-creating power. He even mentions that this varies by `jurisdiction' (government control boundary).

We had to defeat such a proposed law in the New Jersey jurisdiction this year. It turned out to be easy, since the legislator who introduced the bill knew nothing about the industry, and was willing to be corrected by feedback from the people actually affected.

Each of us has opinions, and everyone holds at least one opinion that differs significantly from the common opinion on that topic. Though Mr. Parnas and the gentleman from Praxis differ from the mainstream on this issue, they don't deserve to be called 'crackpots'.

John Gilmore, Licensed Libertarian, Free Software and Crypto-Privacy Crackpot

---

### ✂ The risks of "convenient" technology

*Curtis Galloway <curtisg@sco.com>*

*Mon, 28 Oct 1991 21:53:45 PST*

Mark Bartelt <sysmark@orca.cita.utoronto.ca> writes about his experience with an ATM:

>I'm just lucky that I was only trying to make a deposit. What if it had been  
>an emergency situation, where I needed cash quickly? If an ATM is down, I can  
>generally find another one that works. But if this were my only account, and  
>all ATM access is denied, I'm out of luck.

Back in the "good old days" before ATMs, you were always out of luck outside normal banking hours! But this brings up an important point: when is it OK to give in to "convenient" technology?

For example, many people where I work keep their telephone number list on their computers. When the computer is down, they can't look at their phone list. (Of course, the thoughtful people print out their list occasionally.)

Relying on convenient technology is very tempting, and leads to a certain amount of risk. It's convenient to balance your checkbook with your home computer because you don't have to do it by hand. But if you don't do it by hand, then what do you do when your hard disk crashes? I'm oversimplifying, of course, but you get the point.

I long ago learned not to depend on ATMs always being able to give me money, but I do admit to still relying on some RISKY technology for the sake of convenience, even though it sometimes fails me.

Curtis Galloway, The Santa Cruz Operation, Inc. uunet!sco!curtisg

---

### ✂ Free Call-Back

*Lars-Henrik Eriksson <lhe@sics.se>*

*Mon, 28 Oct 91 10:07:26 +0100*

There are many risks involved with new computerised services on telephone networks. Recently a poster pointed out how you can use "900" for fraud. I had the following experience in using a Swedish phone booth earlier this year:

I was going to make a long distance call from a public phone booth. The number I called was busy for a long period of time. After being fed up with trying to

call again and again, I thought that if the payphone was connected to a computerised switch, it might have automatic callback from busy numbers. On getting the busy signal I dialed the code for automatic callback and waited.

After about five minutes the phone rang, I answered and was connected to the number I had dialed. The twist is that on my unsuccessful attempts to call, all coins were returned, since I received a busy signal. When the automatic callback took place, the payphone didn't require any coins, since \*it\* was being called! The effect was that I could make my call without having to pay anything.

I have heard rumours that Swedish Telecom has now disabled this service on payphones.

Lars-Henrik Eriksson, Swedish Institute of Computer Science, Box 1263  
S-164 28 KISTA, SWEDEN +46 8 752 15 09

---

### ✂ The flip side of the 1-900 scam

<ark@research.att.com>

Sat, 26 Oct 91 09:01:43 EDT

The building where I work deals with the 900 problem by prohibiting 900 calls from all phones in the building, period.

This fact was discovered by one of my colleagues when a commercial software package he was using in his work didn't behave the way he expected. It turns out that the vendor provides technical support via a 900 number so he couldn't call them.

He couldn't call them with his telephone credit card, either -- when they say no calls to 900 numbers, they mean it! He finally had to go home and call from there.

--Andrew Koenig



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 12: Issue 59**

**Tuesday 5 November 1991**

## Contents

- [New Computer Center for Soviet President](#)  
[anonymous](#)
- ["Computer rats on students who don't show up in class"](#)  
[Steve M. Barr?](#)
- [Bank tries to lose 14 billion pounds](#)  
[Nigel Cole](#)
- [Management Often Bungles Firing Process](#)  
[Jeff Helgesen](#)
- [Chaos Congress 91](#)  
[Klaus Brunnstein](#)
- [Japan's barriers against IT risks \(Tokyo conf.report\)](#)  
[Klaus Brunnstein](#)
- [DES is better than anyone would have guessed!](#)  
[John Sullivan](#)
- [DES Watch](#)  
[Richard Outerbridge](#)
- [Risks of "record" and "replay" terminal capabilities](#)  
[Bertrand Meyer](#)
- [Re: Licensing of Software Developers](#)  
[David Parnas](#)
- [Re: campaign against telco info services](#)  
[Dave Bakken](#)
- [Re: Mathematical and scientific foundations](#)  
[Leslie J. Somos](#)
- [Re: UCI computing survives power outage](#)  
[William Walker](#)
- [Info on RISKS \(comp.risks\)](#)



<[anonymous]>  
[lost]

Moscow (TASS, 31Oct91, by TASS special correspondent sergei zinchuk)

A new scientific and technical computer center `sistema' (the system) is now in operation, aiming to provide immediate and reliable information for the Soviet president's apparatus and communicate directly with various regions of the country, as well as with capitals of other states. The new computer networks will soon enable president Mikhail Gorbachev to contact leaders of other states not only by telephone but directly through the computer displays. Boris Tolstykh, former deputy chairman of the USSR council of ministers, who also headed the state committee for science and technology and the state committee for computing machinery and informatics, has been appointed chief of the `sistema' center. "Rechner und Peripherie Vertriebs GMBH" of Germany supplied the hardware for the center and the "Software AG" transnational company arranged the software. "Creation of the `sistema' center is a vivid example of international collaboration. So, the design and the control system of the center was worked out by Soviet specialists, the office fitting was done by an Italian company, the computers were provided by our company and the software - by `Software AG' company", Gerd Lutz, head of the hardware firm told TASS. "As a result of joint international efforts we have managed to create an ultramodern computer center which can compete in efficiency with any similar computer network in the world", Gerd Lutz pointed out.

---

### ✦ "Computer rats on students who don't show up in class"

<BARRSTEV@uncg.bitnet>  
Thu, 31 Oct 91 10:15 EST

This is from wire reports collected into a column in the Winston-Salem Journal, October 31, 1991.

"Computer rats on students who don't show up in class"

Skipping class and ignoring homework won't be as easy for students at John Muir Middle School in Burbank now that a computer is waiting to call their homes. The school has installed a 24-hour homework hot line that allows Mom and Dad to find out what homework is due and what activities are going on in class. The computerized telephone system also rats on students who miss class by calling their parents each night. "The great thing about this is that the computer will keep calling until it hears a live voice or an answering machine," principal Bill Kuzma says. "In the morning, a printout tells us who it contacted and who it didn't."

[It is indeed a "great thing" that the map is now equal to the territory. SMB]

---

### ✦ Bank tries to lose 14 billion pounds

Nigel Cole <100020.1170@compuserve.com>  
04 Nov 91 14:35:55 EST

I have just seen the following on CEEFAX (BBC TV's Teletext service):

BARCLAYS MAKES A NEAR MISS

Barclays bank is investigating how 14000 million pounds was almost mistakenly transferred to the National Bank of Greece.

A spokeswoman for Barclays said the mistake was spotted by a computer security system just before the transaction was due to go through.

Fourteen thousand million pounds is the equivalent of more than the entire Greek national debt.

((Nice to see computers catching an error instead of creating or compounding one, although the whole affair sounds like another case of "Computer Operator Error". Does anyone else know more details? - NHC))

---

### **✂ Management Often Bungles Firing Process (WSJ 10/14/91)**

*Jeff Helgesen <jmh@morgana.pubserv.com>  
Mon, 4 Nov 91 15:19:14 -0600*

>From the 14 October 1991 Wall Street Journal, "Firms Get Plenty of Practice at Layoffs, But They Often Bungle the Firing Process":

When reporters and other employees at the Record of Hackensack newspaper tried to log onto their desktop computers on a recent Wednesday morning, a puzzling thing happened. None of them could get into the system.

It had nothing to do with computer failure. Rather, it was the way workers learned which ones among them would be getting pink slips. Reporters were directed to an editor's office, where they either for an envelope containing a new password---meaning they still had a job---or a note to see a supervisor---meaning they didn't.

"It was really tense," says one staffer who survived the cut of 138 employees. "People felt really angry. And a lot of people felt betrayed, too."

The story goes on to describe firing methods and practices, and other horror stories regarding botched firings.

After all these years, still no improvement over the time-honored method of moving the employee's desk into the hallway... :-)

---

### **✂ Chaos Congress 91**

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de>  
1 Nov 91 10:36 +0100*

According to an invitation (participation in panel "Techno-Terrorism coming?"), annual (8th) Chaos Congress 91 will be held in Hamburg (-Eidelstedt, Buergerhaus) on Dec.27-29, 1991. Besides introductions into networking, survey

of networks, mailbox software, operating systems and application software (usually with several practical demonstrations), IT security will be one major focus, esp. sociological and legal aspects. Besides the 2nd topic (Techno-Terrorism, the development of which was strongly warned of by CCC chairman Frank Simon in a recent discussion), network technologies and possible applications of networks in environment protection (as started in last years) and social implications will be discussed. One discussion will be devoted to '10 years Chaos Computer Club'.

Klaus Brunnstein, University of Hamburg

---

### **✂ Japan's barriers against IT risks (Tokyo conf.report)**

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de>*

*30 Oct 91 18:00 +0100*

Conference Report: 'Information Security 91' (Tokyo, Oct.17-18,1991)

During this year's Informatization Week in Japan, an international conference was held in Tokyo on 'Information Security'. Invited experts from USA, Australia, United Kingdom, Germany and Japan discussed, in a plenary part (on Oct.17) and in 3 parallel streams (on Oct.18) several 'hot' topics in related areas. The conference was organized by Japanese Information Processing Development Center (JIPDEC) and Ministry for International Trade and Industries (MITI)'s Information Technology Processing Agency (IPA); attendance was well over 700.

During plenary day #1, introductory lectures were given by Solomon Buchsbaum, AT&T's senior vice president, on 'Information Security Strategy Towards 21st Century', in which he outlined deficiencies in contemporary digital communication systems by analysing some accidents (e.g. INTERNET worm); he described in some detail AT&T's approach to network security. According to him, the new version of Secure (System V) UNIX designed at B2 level is currently under NCSC B2-evaluation.

NCSC director Patrick Gallagher, in his contribution on 'Role of Public and Private Security Activities' introduced concepts of Orange Book and also discussed the European IT Security Evaluation Criteria (the new release of which, Version 1.2 was released by EEC in June 1991). In some background discussion, some experts said that Japan might well (after evaluating this conference and its results) look at their own Security Criteria to compete with multi-color US and EEC criteria (which both deserve scientific substance and development).

Justice Michael Kirby, Judge at the High Court of New South Wales, introduced into the actual work of OECD expert group on security of information systems, whose chairman he is. In his impressive lecture (38 pages in the conference proceedings), he discussed IT risks, demands for and impediments to security harmonization efforts, and the mission and state of the OECD group. His paper is surely worth wider recognition in the community of risk analysers and security experts.

The Japanese contribution was from Tadahiro Sekimoto, Chairman of (influential)

Japan Electronic Industry Development Association; to analyse his country's position, his (Japanese) paper is very worthwhile to be translated into English.

On day#2, three parallel sessions were focused on 'Security Policies' featuring Japan (Kaoru Nakamura/MITI), USA (Bill Calvin/NASA) and UK (Michael Jones/DTI) (session 1), 'Computer Viruses' (session 2, about 200 attendants) and 'Security Activities in Business Societies' (session 3), with contributions of Toshio Hiraguri (Fujitsu), William Whitehirst (IBM) and Alan Stanley (European Security Foundation).

In session 2 (the only one which the author could attend), Dr. Tojo of MITI's IPA reported on experiences of IPA's Virus Control Office, founded in October 1990. From the beginning, the office asked Japanese institutions \*to report any case on malicious software\*. Though probably not all incidents have been reported (esp. in universities), the \*detailed survey of 49 incidents\* shows essential differences to Western incidents. One major part is concerned with MACINTOSH virii, among which WDEF/WDEF A/WDEF B (9+4+1 cases) and nVir B (1 case). On Japanese IBM-compatible PCs, only a small subset of the worldwide virii have appeared: Stoned (8), Jerusalem (4), Joshi, Sunday and Yankee Doodle (each: 2), and 1701, AZUSA, Invader, Keypress, Vienna (each: 1), plus a simultaneous occurrence of Dark Avenger and Liberty. Most interesting, there is also a report about a mainframe virus (VM/SP on IBM 4381/R23) which is only described in Japanese (Dr. Tojo's report is very worthwhile to be translated in English/German..)

Dr. Tojo reported also about 6 natively Japanese virii on DOS-PCs and Sharp X68000 'Human OS'. Following their own naming scheme, he reported on virii DBf-1, DApM-2, DBo-3, DBh-4, DAn-5 and DSbm-6. In it's naming convention, IPA's Virus Control Office describes the system base (D: DOS, M: MACINTOSH, U:UNIX), infection (B=Boot, S=OS, A=application), and disease functions (F=FAT, O=OS, P=EXE/COM.., D=data, H=hangup, m=message, n=nothing). As additional information, virii are serially labeled with the number in the occurrence list. The naming scheme resembles Patricia Hoffman's classification, though significantly simpler; the appended sequence number is helpful when a unique office exists to which virii must be reported.

In the afternoon (after contributions of Fred Cohen and the author, see below), a major part of the panel discussion was devoted to the question why so few virus incidents have appeared, and why \*Japan\* is world-wide (among high developed countries) the \*country with lowest per-capita-density of virii\* (with no major native hacker attack reported). Among several reasons, the low PC-density (about 100,000 PCs only) as well as 'cultural' and 'language' barriers are worthwhile to analyse.

The \*language barrier\* is established by Japanese laws and regulations which require all foreign software to be adapted to Japanese standards and language. This requires all software to be adapted, and in this process, major 'anomalies' may vanish (probably, the high percentage on Mac virii comes from the fact that the exchange of Mac software is nearly as free as in Western countries).

The \*cultural barrier\* was described by some participant with the sentence: 'In Japanese culture, students would be ashamed to damage any organisation by writing a virus'. From Western experience (e.g. in discussion with hackers and

virus authors), this built-in ethics seems as the most reasonable Japanese barrier, while the 'language barrier' is often accused for the closure of Japanese markets against Western products. Consequently, political pressure may well damage this antivirii barrier, while the cultural barrier may remain strong for some time (slowly eroding, as some Japanese discutants admitted).

Fred Cohen's contribution consisted of two rather controversial parts. In his first part, he analysed - in an outstanding contribution - essential features in PCs and MSDOS which are basically responsible for virus proliferation. He described concepts of his (=ASP's) integrity product which (as this part of his lecture) deserves broader recognition; his suggestion of a 'safe snapshot' (established as virus-free) which is loaded at any boot time seems promising (VTC will test it against it's virus database) against all virii which do not (mis)use hardware features to protect (stealth) themselves.

Fred Cohen's second part will also be controversial in western conferences. He repeated arguments of his dissertation, recently published in Science (Sept/Oct-edition), that virus technology should be used for 'good purposes'. While his dissertation contained examples of compression and encryption, today's examples are a 'viral bill collector' and 'garbage collection'. Moreover, to get more examples, Fred has publicly devoted \$1,000 in a contest to the programmer of the best good virus (Science). Fred's argument is, that in adequate (evidently not contemporary) systems environments, technology of self-replicating programs may be used for good purposes. Starting from genetic principles ('liveware'), several models of garbage collectors, bill collectors may concur, on a birth-and-death-basis: the successful ones survive (if enough 'food' is available) and replicate, while the unsuccessful ones 'die'.

In the wake of his Science contribution, Gene Spafford gave an essential argument that replicative techniques should not be used in cases where more controllable techniques are available. All examples up-to-now can be solved (more controllably) by a good operating system. The author mentioned moreover, that in contemporary systems, \*virii steal the author's copyright as well as the user's quality guarantee\*. The argument is as follows: if a user buys a software product, he/she gets a (usually written) quality assurances limited to the tested product; as virii change the assured product, the quality assurance is no longer valid for an infected product. Similarly, the copyright holds only for the product as shipped; with any change of the product at the user's site, the copyright no longer holds. In the lively discussion, Fred was alone to defend his 'good virus' idea.

In his contribution 'Malicious Software: Trends and Counteraction', the author analysed essential paradigms inherent in von Neumann architectures (PCs, large systems and networks) as well as in contemporary systems analysis and software construction. He argued that known forms of malicious software (virii, worms, trojans) and future 'hybrids' (trojanized virii, virus-worms etc) are the consequence of inherent insecurity of contemporary concepts. In a live show, he demonstrated (with 28 virii, known since at least 5 months) the discrepancies in quality of selected antivirii (McAfee's V84 found 21 virii but misclassified 14 yielding in 25% success quota; Solomon's Version 5 properly classified 2, and Skulason's F-PROT 1.16 found 16). According to the author, contemporary antivirus techniques will experience more trouble when future stealth virii use hardware protection (not used by the operating systems) to undergo protection

mechanisms, where contemporary integrity checkers (checksum etc) will also fail. He suggested new architectural designs which combine von Neumann concepts with functional concepts not dissimilar to Japanese 5th Generation concepts (which were not discussed in this event).

While some part of the conference proceedings is in Japanese, the invited speaker's contributions are in English. The conference demonstrated Japan's interest to become a major player also in fields of Computer Security; in several areas (e.g. Classification of Computer Security), evident deficiencies (esp. ill-understood concepts in Europe's ITSEC) may be uncovered when Japan plays a major independent role. This may lead to new concepts and approaches and competitiveness.

Klaus Brunnstein, University of Hamburg (October 26, 1991)

---

### **✂ DES is better than anyone would have guessed!**

*<sullivan@geom.umn.edu>*

*Sat, 2 Nov 91 00:23:13 CST*

In the NYT "Week in Review" for 13 October, Gina Kolata writes about DES. The basic thrust of the article is that DES is a much better code than anyone would have guessed; nobody (outside the NSA, anyway) understands why it is better than any similar codes that have been tried. The recent Israeli attack on DES is only a "slight improvement over laboriously trying every key". Martin Hellman of Stanford is quoted as saying that special purpose hardware costing \$10million could break DES by brute force in two hours. [So in 20 years, if costs go down 40%/yr, your desktop workstation will do this easily.]

Shamir evidently says that DES is "the strongest possible code of its kind"; his method "devastates similar codes", while only denting DES. He doesn't believe DES has a trap-door for NSA.

Whitfield Diffie of Sun points out that a cryptosystem must last for many years: the British got an encrypted Soviet message in the 30's and continued for 30 years to try to decode it.

-John Sullivan

---

### **✂ DES Watch**

*Richard Outerbridge <71755.204@compuserve.com>*

*04 Nov 91 20:20:58 EST*

Apropos of the robustness of DSS, RISK readers might be interested by our guesstimation of the strength of DES during the next nine years. The title says it all- "DES Watch: An Examination of the Sufficiency of the Data Encryption Standard for Financial Institution Information Security in the 1990's", Gilles Garon and Richard Outerbridge, in CRYPTOLOGIA Volume XV Number 3 July 1991, pp. 177-193. The pun on "DEATH Watch" was intentional.

Highlights:

Time-to-Break	Investment			Cost-per-Period		
	90	95	2000	90	95	2000
One Year	\$129K	\$52K	\$10K	\$48K	\$19K	\$4K
One Month	\$1532K	\$600K	\$117K	\$45K	\$18K	\$4K
One Day	\$46622K	\$18265K	\$3580K	\$45K	\$18K	\$4K

If we adopt Dr. Rivest's metric of "\$25 million"-worth of resistance to attack, single-key DES will be obsolete for protecting transactions with a lifespan of under 12 hours by about 1995 or so. If single length DES keys are changed less frequently than once every couple of days, single-key DES is already exposed when used to protect more than \$48,000 worth of information.

Richard Outerbridge, Senior Security Analyst, CIBC

---

### ✂ Risks of "record" and "replay" terminal capabilities

*Bertrand Meyer @ Interactive Software Engineering Inc. <bertrand@eiffel.com>  
Sat, 2 Nov 91 17:35:03 PST*

Has this risk been documented before? Bertrand Meyer

From in a letter by "Paul J. Lourd, Greenwich, CT" to the magazine "Enterprise Systems Journal", October 1991:

Recently there was a situation in which several customers received products from my company they claimed were never ordered. [...] The [originating] clerk claimed he never entered them, but did say that his terminal was acting "wacky" that morning.

[...] The orders matched [others shipped] nine months ago to the same customers. [...]

After much head scratching, the staff realized that these particular "dumb" terminals (IBM 3192) had a keystroke record and play feature. Although no one believed it was possible, it turned out that this clerk had accidentally hit the record button which recorded some of his work and assigned it to a PF key. Nine month later, he managed to hit the play key while in just the right screen and it re-entered the orders!

The staff then checked the rest of the 3192 terminals and found that more than 75 percent had accidental keystrokes recorded and assigned to various PF keys. Naturally, the staff is in the process of rendering these key inoperable. [...]

---

### ✂ Re: Licensing of Software Developers ([RISKS-12.58](#))

*David Parnas <parnas@qusunt.eng.McMaster.CA>  
Wed, 30 Oct 91 16:29:04 EST*

John Gilmore, suggests that I have gone "beyond advocacy to misrepresentation".

Having read his contribution twice, I still can't figure out what was misrepresented. In the jurisdictions that I know, if a professional engineer is accused of having violated some of the rules of the profession, the decision about his/her right to continue practicing is made by the professional society. In that sense, the standards are enforced by the practicing professionals.

This is exactly analogous to the situation in Medicine. Government's decide that you must have a medical license to perform heart surgery. Doctor's decide who can have such a license. Doctor's consider themselves a self-enforcing profession, but the government does not allow them to determine their own "scope".

Nobody is forced to get a medical license either.

Although I don't recall anyone in this conversation being called a "crackpot", I was glad to read that Mr. Gilmore believes I that I don't deserve that classification. It has to be the nicest thing a self-avowed crackpot has said to me this year.

I repeat that we are discussing the wrong issue. I don't believe that we can afford to ignore the issue of qualifications for software professionals, but the question we should be debating is what those qualifications should be and who should be covered. It is not an all-or-nothing problem.

Prof. David Lorge Parnas, Comm.Res.Lab, Electrical and Computer Engineering Dept., McMaster University, Hamilton, ONT Canada L8S 4K1 416 525 9140 Ext. 7353

---

**✉ Re: campaign against telco info services (Seecof, [RISKS-12.56](#))**

*"Dave Bakken" <bakken@cs.arizona.edu>  
Wed, 30 Oct 91 15:18:23 MST*

In [RISKS-12.56](#) Mark Seecof of the Los Angeles Times used this forum to try to rally people to support HR 3515, in the name of privacy. I think that it would be very beneficial to hear exactly how he or others fear that the telcos providing information services could be a threat to privacy. (Must I note that the LA Times and the other groups he mentioned have a very big vested commercial interest in this? And yet they raised the bogeyman of "potential invasion of privacy" without being questioned.)

I myself look forward to the telcos providing information services (and TV shows, as the FCC just allowed this last week). This greatly increases the probability that we will get fiber optic phone lines in "the last mile" to our houses and small businesses, and is likely to accelerate the pace at which it comes. As long as the telcos are required to rent the lines to others on a fair basis, I can see nothing but good coming out of this, and a lot of good at that.

Dave Bakken, Dept. of Computer Science, U of Arizona, Tucson, AZ 85721; USA  
+1 602 621 4089

---

**✉ Re: Mathematical and scientific foundations (Petroski, [RISKS-12.51](#))**

*Leslie J. Somos <ah739@cleveland.freenet.edu>*

*Thu, 31 Oct 91 14:23:11 -0500*

My wife Kathy Bacon had an interesting experience in a class while getting her Computer Engineering B.S. at Case Western Reserve University: After one particular homework assignment, many of the students complained to the professor about how the problems were graded. The (engineering) students had ruled out certain of the solutions which were physically impossible (the problem was a word problem about a mechanical linkage). The professor said that the class he gave the problems to last year had no problem. He scratched his head some, and realized that last year he taught the course to mathematics students, who had solved the equations as-is, and not ruled out the answers which were negative numbers.

So, it's not really engineering versus mathematics, it's more of not doing reasonability checks on your results.

Leslie J. Somos

---

**✉ Re: UCI computing survives power outage [almost] (Krause, [RISKS-12.58](#))**

*"William Walker C60223 x4570" <WALKER@aedc-vax.af.mil>*

*31 Oct 91 11:05:00 CST*

This type of power outage is really not surprising considering how most (if not all) buildings receive their electricity from the power company. To reduce the size (and subsequently cost) of power feed lines and main breakers or fuses, as well as provide a more efficient distribution of power, AC electricity is provided to buildings in three phases (houses and small buildings often have only two phases). Each phase, or "leg," is separately protected by a fuse or breaker at the point it enters the building. Each circuit coming off of each leg is also separately protected by a fuse or breaker. Here's the RISK: often the sum of the ratings of the breakers for the circuits exceeds the rating of the breaker for that leg. So, it is possible to overload and trip the breaker for that leg without tripping any breakers for the individual circuits. The other legs will not normally be affected, unless the breakers for all legs are connected to trip at once. If one leg supplies computers and one supplies lights (and maybe AC), one can see how these scenarios are possible, but more likely:

The same can occur on a larger scale. OUTSIDE of the buildings, on the power poles, are line fuses for each leg of power. Sometimes several buildings (or several mains for one building) will be "downstream" of the line fuse. Then, if the line fuse is overloaded and blows, all mains served by that leg will go down. I have experienced this twice: once while at the University of Alabama in Tuscaloosa, and once while at Holly Farms Headquarters in Wilkesboro, North Carolina. The line fuse for one leg blew, knocking out power to computers but not lights (at U of A), or to the mainframe (thank goodness for UPSs) and some of the lights but not the PCs (at Holly Farms).

Bill Walker, OAO Corporation, Arnold Engineering Development Center, M.S. 120,

Arnold Air Force Base, TN 37389-9998 ( [WALKER@AEDC-VAX.AF.MIL](mailto:WALKER@AEDC-VAX.AF.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 12: Issue 60

Wednesday 6 November 1991

## Contents

- [Driver arrested in computer muddle: Data protection problem](#)  
[paj](#)
- [Computer Saboteur Pleads Guilty](#)  
[Rodney Hoffman](#)
- [Blaming the computer \(again\)](#)  
[Randal L. Schwartz](#)
- [YAHIR \(Yet another human interface risk\)](#)  
[Friedrich Knauss](#)
- [Certified Voting Program](#)  
[Brian A Wichmann](#)
- [Electronically controlled bus transmission](#)  
[Mark Secof](#)
- [V-22 Tiltrotor Roll Sensors and Triple Redundancy](#)  
[Mike Allard](#)
- [Re: FDA-HIMA Conference on Regulation of Software](#)  
[Frank Houston](#)
- [RISKS of propagating legendary RISKS](#)  
[Paul Karger](#)
- [Software safety, formal methods and standards](#)  
[Jonathan Bowen via Jim Horning](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***⚡* Driver arrested in computer muddle: Data protection problem.**

*paj* <[paj@gec-mrc.co.uk](mailto:paj@gec-mrc.co.uk)>  
6 Nov 1991 15:26:44-GMT

According to Computer Weekly, Oct 31 1991, a youth was mistakenly arrested after the DVLA (Driving & Vehicle Licensing Authority) computer in Swansea allowed two cars to be given the same registration plate. When the poor guy asked the DVLA for information on previous owners of his car, in an attempt to sort out the mess, the DVLA refused. The Data Protection Registrar has now backed the DVLA.

It seems a pity that legislation that is supposed to protect the innocent citizen from this sort of thing has in fact made life more difficult.

Paul.

[By coincidence, I had just sent off my January 1992 Inside Risks column, called What's In a Name, devoted to such problems... Here's one more to add to our rather large list of name- and ID- related horror stories! PGN]

---

### **✂ Computer Saboteur Pleads Guilty**

*Rodney Hoffman <Hoffman.El\_Segundo@Xerox.com>  
Wed, 6 Nov 1991 06:50:55 PST*

In [RISKS-11.95](#), PGN reported on "Programmer Accused of Plotting to Sabotage Missile Project." Here's the next installment:

Computer Saboteur Pleads Guilty: Michael John Lauffenburger, 31, a former General Dynamics computer programmer who planted a destructive 'logic bomb' in one of the San Diego defense contractor's mainframe computers, pleaded guilty to one count of attempted computer tampering. He faces up to one year in prison and a fine of \$100,000.

Federal prosecutors said Lauffenburger had hoped to increase his salary by creating a problem only he could solve: a program that was designed to destroy a database of Atlas Rocket components. He set the program to activate, then resigned, hoping, investigators say, that the company would rehire him as a highly paid consultant once it discovered the damage. But another General Dynamics programmer inadvertently ran across the program and alerted security, which disarmed the program.

[Source: Wire service report in the 'Los Angeles Times', 5 Nov. '91, p. D2]

---

### **✂ Blaming the computer (again)**

*Randal L. Schwartz <merlyn@iwarp.intel.com>  
Wed, 6 Nov 91 14:46:53 PST*

Background: Oregon recently passed a property tax limitation. Much gnashing of teeth was heard when property owners received their recent tax bills, in which property values had soared between 20% and 200%(!) in the last 18 months, leaving many owners with \*larger\* bills than in the previous cycle.

In today's Oregonian (Portland Oregon):

#####  
\_Oregon assessments go up, but this one is just ridiculous\_

Californians are used to hearing stories of Oregonians giving them a hard time. But the tax assessment of nearly \$100 million on one California couple's Josephine County farmland [eastern oregon] was only a computer error. Honest. [...]

[The county officials] are scrambling to send out new tax bills to the county's other 40,260 property owners to make up for the \$986,312 that was incorrectly billed to the Millers.

County officials discovered the error when Carol Miller called the county assessor Oct. 25 to complain about the taxes on a 38.8-acre parcel near Williams that she and her husband own. Because there was only a barn on the land, which was assessed as farmland, they should have received an \$8,850 assessment, instead of the \$97 million property valuation. Their tax bill should have been for just \$117 [...].

[Bill for someone's \$70K home will go from \$710 to \$760 to make up for the deficit from the bad math.]

"It has been absolute bedlam around here," said [the county deputy treasurer]. She said she had just about given up blaming the error on the computer. "So we are just sitting here taking the blame."

Rhodes [the county assessor] said that the erroneous tax bill can be blamed in part on [the recent legislation]. The tax limitation measure requires assessment notices to be sent with the tax bills. Had the assessment notices been sent out in the spring, as in previous years, the error would have been caught before tax rates were computed and bills sent out. It was a change "that created the crack through which the error fell through," Rhodes said.

County officials still are trying to figure out what exactly went wrong. As near as anyone can tell, it occurred when the assessor's office was updating farm assessments. A glitch of some kind occurred as the computer was figuring the Miller's property. "And it just kept on going until it ran out of digits," Rhodes said.

The error affected only the one property, so everything else appears to be functioning normally. Rhodes said he hopes to be able to update the 17-year-old [!] software so that the computer will scan tax roles for these kinds of anomalies.

#####

I find it amazing that they are using 17-year-old software. I also find it amusing that they had no cross check for "are we in the right ballpark for total county assessments", and that they believe that everything is correct now.

Just another homeowner in Oregon, Randal L. Schwartz, Stonehenge Consulting Services (503)777-0095

---

**✶ YAHIR (Yet another human interface risk)**

*Friedrich Knauss <megatek!fritzz@uunet.uu.net>  
Wed, 6 Nov 1991 00:41:01 GMT*

At our company (as with many) the computer center is separate from the engineering department. Administrative requests are sent to the support division to be processed. Recently, we needed to retrieve a file from a moderately recent backup tape. We sent in the request, and the retrieval was done as requested. As an undesired fringe benefit that entire neighborhood in the directory tree was restored as well, overwriting several days worth of work in the process. The cause for this: When support receives a request they print it out and process the request from hardcopy. The laser printer used for this

does not wrap lines (a not uncommon feature). As a result, the path printed out in the request was truncated at a point several directories short of the actual path, and the restore was done on the truncated tree overwriting everything below it. Although several different varieties of safeguards could have prevented this, none are in use. Other potential risks of this are left as an exercise to the reader.

---

## **✉ Certified Voting Program**

*Brian A Wichmann <baw@seg.npl.co.uk>*

*Mon, 4 Nov 91 15:38:12 GMT*

An example of Certified software for Elections

### Background

In July 1990, the Church of England changed the regulations concerning the method of undertaking elections to allow computer programs to be used. The Church of England uses the Single Transferable Vote method for most of its elections, and therefore the counting process is non-trivial.

The new regulations required that any software used by the Church was certified by the Electoral Reform Society (ERS) as adhering to the counting method specified.

The author was asked to advise ERS as to the suitability of a particular program for certification by them. The actual system consisted of several programs, but the main logic was undertaken by a program consisting of about 1,000 lines of standard Pascal. Since the Church wanted to use the program in October 1990, only about 36 man-hours could be devoted to the certification process *\*{This was an unofficial activity of the author}\*.*

### Certification

The process used to check the program was based upon the statements metric applied just to the main program. The reason for analysing just the main program was that errors elsewhere are likely to be immediately apparent, while the work needed to check the main logic is quite significant.

The main program was transferred from an IBM-PC to an Archimedes. This transfer was done for practical reasons but acted as a cross-check on the code. The program was then instrumented by hand to discover the statements executed. Special test data was then constructed to execute all the statements. All statements proved executable except two which would not be executable on either the Archimedes or IBM-PC. In fact, a program was already available to generate random test cases, so there was a potentially large source of data.

The specification of the computer program was to follow the same logic as the hand counting rules. Hence, in principle, it was easy to check the output from any specific test. However, for the larger tests, the amount of hand-checking is significant, so it was important to minimise the checking required. This was done by computing the minimum number of test cases which would ensure all the

(feasible) statements were executed. This left 13 test cases which were hand checked by the ERS expert --- the ideal 'oracle' in this case.

The results of this exercise was that one significant bug was found and about six minor ones. No fault has been found subsequently in the program (although a minor fault has been found in another program concerned with the data preparation).

The author therefore concludes that this is a cost-effective method of improving the quality of software (assuming that the original development did not include this same process).

Postscript

Two Diocese used the computer program to elect their representatives to the General Synod in 1990. This Synod will decide on the final stages of admitting women to the ministry.

The Church of England wish the program extended to include provisions for 'constraints'. However, it is clear that the general problem of including constraints is NP complete.

Brian Wichmann (baw@seg.npl.co.uk)

---

### **✂ Electronically controlled bus transmission**

*Mark Seecof <marks@capnet.latimes.com>*

*Tue, 5 Nov 91 11:36:07 -0800*

At a hearing of the safety board investigating the crash of a chartered bus carrying Girl Scouts (which killed several and injured the rest) the maker of the bus confirmed that its automatic transmission was designed to shift up when the engine was in danger of "over-revving" regardless of the gear range selected by the driver using the electronic controls.

Also, the bus maker explained that the transmission would not obey a control selection of a lower gear range if the engine were already running fast. This would moot any attempt by a driver to obtain greater compression braking after a partial or complete brake failure.

The California Highway Patrol investigation had concluded that the front brakes of the bus (which ran off a cliff while descending a steep mountain near Palm Springs because the driver allowed it to go too fast) were out of adjustment, that the rear brakes had overheated and failed, and that the automatic transmission had been in too high a gear for the engine to provide adequate compression braking for safety. The gear position of the automatic transmission was determined by examining the wreckage. It is not clear that the driver had selected the high gear the bus was in. The CHP has suggested that the crash need not have occurred had the bus been in the proper gear for the downward drive.

The driving instructor employed by the bus company testified that he was

unaware that the transmission would shift up even if low range had been selected, so he did not train the driver of the ill-fated bus to avoid this potential occurrence. The instructor was surprised to learn that the transmission was designed to disobey its control setting. The driver was killed in the crash, so it is not possible to question him about his operation of the bus.

I remember seeing something in RISKS about automatic transmissions on certain recently-built passenger cars. Certainly this situation reminds one of the A-320 control limits.

It would be entirely proper to sacrifice a bus engine, even the whole drive train, to save the lives of a busload of Girl Scouts. I think mechanisms which override the controls of a vehicle or other device to protect the machine from harm at the expense of its users are wicked.

Also, it's poor M-M interface design to have a control which doesn't work. Why have a "low range" setting on an automatic transmission if the thing will shift up regardless? And why change a very standard design (the availability of low range on automatic transmissions for safety purposes) without need or warning? If there's a lawsuit, I hope the bus maker loses.

Mark Seecof <marks@latimes.com>

---

## **V-22 Tiltrotor Roll Sensors and Triple Redundancy**

*Mike Allard <acd4!IEDV5!mja@uunet.UU.NET>*

*Mon, 4 Nov 91 14:44:06 EST*

The following is an excerpt from "V-22 Tiltrotor Test Flights Resume," from the November 1991 issue of "AOPA Pilot" magazine (used without permission; all spelling errors are mine):

"Aircraft number five crashed on June 11 during its first test flight at New Castle County Airport in Wilmington, Delaware. [...] The pilots were attempting to land when the V-22 became unstable in roll, and the left-hand engine struck the ground. The aircraft lifted, rolled left, and crashed on the runway, ending up on its back. The Navy halted further flights pending an investigation.

"The Navy probe, concluded in September, attributed the crash to faulty hardware connections in the V-22. Two roll-rate sensors, which provide roll-rate information to the flight control computer, were hooked up backward, according to the Navy. There are three such sensors, which provide a triple-redundant system; if one sensor sends an erroneous signal, it is 'voted out' by the other two. Because two of the three sensors were reverse-wired, the input from the sole sensor providing correct roll information was canceled out. The result: 'The aircraft went divergent in the lateral axis and impacted the ground.'

"Further investigation revealed that one out of three roll-rate sensors was reverse-wired in two other [V-22] Ospreys, but that snafu has been corrected."

An observation by a pilot and programmer here: "I guess fault tolerance only works if you wire up your sensors right."

Mike Allard, Applied Computing Devices, Inc. <uunet!acd4!mja>

---

## **✉ Re: FDA-HIMA Conference on Regulation of Software**

Frank Houston <houston@itd.nrl.navy.mil>

Tue, 5 Nov 91 15:21:37 EST

I read Mr. Horn's report on the HIMA/FDA Conference with interest. There are some misconceptions that need clearing up.

First, FDA regulation of software is not new. The HIMA conference was the latest and strongest public statement by FDA acknowledging that software is regulated when it is used in certain ways.

Some of the history needs to be cleared up. Mr. Horn writes:

<>First, what does the FDA regulate?

- <> 1) Under the 1936 Act, any medical device, drug, or practice.
- <> 2) Under the 1990 Safe Medical Devices Act, authority to examine devices was expanded.

This is sort of true, but incomplete. The Medical Devices Act of 1976 first gave FDA explicit authority and responsibility to regulate commerce in medical devices. Before 1976 the FDA's authority was implicit. FDA has the authority to regulate "manufacturing" practices, not medical practice. The 1990 act amended this authority in several ways, including expanded authority to inspect medical device manufacturing firms.

Mr. Horn goes on:

<>Software may be involved in any of four ways:

- <> 1) It may be a device
- <> 2) It may be used in the manufacture of a device or drug
- <> 3) It may be used in record keeping
- <> 4) It may be contracted or purchased from a third party for one of the above.

Regulated software must either be a medical device or "a component, part, or accessory" of a medical device. Of the remaining categories 2, and 3 are subject to audits based on the FDA Good Manufacturing Practice regulations to the extent they are substantially involved in controlling manufacturing processes and keeping records of design, manufacturing, and service. For software in the 4th category, FDA investigators look for evidence that the purchased or contracted software is safe and "fit for use." Medical device software may require stronger evidence of safety and fitness than manufacturing or recordkeeping software. The kind of evidence that FDA typically seeks consists of V&V plans, Safety Plans, and records that the firm has followed the plans.

Next comes a big misunderstanding:

<>FDA approval involves two steps: approval to market and approval to

<>sell. Approval to market involves one of two things:

<> 1) A PMA for new medical technologies (see an expert now).

<> 2) A 510(k) for equivalent medical technologies (substitutes for

<> some previously approved device).

<> . . .

<>Then comes approval to sell. This is based upon a Good

<>Manufacturing Practices (GMP) inspection. Again, the inspection

<>detail will be a function of the risk to the patient and others.

<>

<>For a minor risk item, they might not inspect at all. Most likely,

<>they just verify by spot checks that the claims made in the 510(k)

<>are being kept. For a major risk item, they may inspect a lot. If

<>someone actually gets hurt, expect an army of inspectors swarming

<>over everything.

It is more accurate to say that permission to market a medical device involves two processes, a premarket process of review and a process of periodic inspection and surveillance of the firm. Permission initially may be granted through an approval in the case of PMA, or it may be granted through a finding of "substantial equivalence to a previously marketed device") in the case of 510(k). PMA stands for Pre-Market Approval, and is the only device "approval" that FDA acknowledges officially. Once a firm has been granted permission to market it is subject to inspection by FDA investigators.

In theory, the rigor of an inspection does not depend on the level of risk associated with a device. In practice, it might.

More misunderstanding:

<>For a 510(k) approval there are three categories of approval

<>difficulty based upon the hazard to patients and others:

<> 1) minor, little risk of injury either direct or indirect

<> 2) moderate,

<> 3) major, risk of death

These categories are used to decide how closely to review an application to market a medical device. They have nothing to do with inspections by FDA field investigators. These are hazard categories and the list has been limited to three. They are not legislated categories. Those categories are: Class I, products for which no special controls or standards are needed; Class II, products which need special controls like standards; and Class III, products which require premarket approval. These classes do not represent a hierarchy of risk, although Class III devices are usually riskier than Class II which are usually riskier than Class I.

By all means:

<>For more details ask the FDA for a copy of the 510(k) reviewers

<>guidance. This is the document used by the 510(k) reviewer and is

<>freely available to the public.

Call the Division of Small Manufacturers Assistance, (301)443-6597.

The report goes on:

<>. . . there is no assumption of validity for off the shelf  
<>software.

Knowing the current state of affairs with off-the-shelf software, this is a rational choice for risk avoidance. However it places a burden on the company that wants or needs to use shrink-wrap applications. Firms that use shrink-wrap software should be forewarned to at least put the package through its paces, i.e. verify and validate their particular application, before turning it loose in quality control monitoring, record keeping, etc. You might still be written up, but you have a stronger rebuttal than if you did no planned testing. Mr. Horn repeated a horror story that one drug firm presented to illustrated the practices that can be written up as violations according to the letter of the GMP regulations.

<>For more details, the FDA provides copies of GMP practices  
<>regulations to anyone who asks.

Call the division of Small Manufacturers Assistance.

Next misunderstanding:

<>This attention to software is new at the FDA. It went into effect  
<>this summer and more regulations take effect this fall.

The attention to software is not new. The Therac incidents raised the consciousness of the agency. What Mr. Horn perceives as new is the fruition of several years of internal training and discussion.

<>The other area that is catching people by surprise is the extent of  
<>the definition of device and manufacture.

The legal definition of a medical device is in part: "... an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part or accessory which is . . . (2) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals ... (3) intended to affect the structure or any function of the body of man or other animals." Not a limiting definition is it? Note that the definition hinges on the way the product is used. If the product materially affects diagnosis, treatment, etc., when it is used as intended, then it is a medical device. As further examples demonstrate, claims made in labeling and advertising are considered evidence of intended use.

Manufacture includes such activities as repackaging for commercial distribution, that is buying a product and reselling under a different label. In such cases the repackager is held responsible for assuring the quality of the product, not the supplier.

<>Most recently, the makers of blood bank software were hit. They had

<>not previously realized that the database software for tracking blood <>donations was a medical device and probably a class 3 device.

The blood bank situation is unfortunate. Everybody loses, FDA, the firms in the business, and the public. I am not, however, aware of any plan to classify blood bank software in class 3. As I explained earlier, medical device classification is not tied directly to risk. You must read the law to appreciate the complexity of classification, but I do not think blood bank software, HIS software, or LIS software meets the legal criteria for anything higher than class 2.

Blood bank software is used for much more than tracking donations. Often blood bankers depend on the computer to maintain the integrity of test results for serious or fatal diseases that could be spread by infected blood. These results are reviewed as part of the decision to make blood units available for human use. Undetected errors will be fatal for the recipient of the improperly released blood, because there is seldom time for redundant testing before the blood is used. It is a tough call to decide which is worse, the risk that a patient might die because blood is not available or the risk that the patient will contract AIDS if he survives.

<>The FDA approach differs from that of MoD and others in that there <>is no FDA approved methodology. ... They claim that this allows <>them to accept new methodologies as they are proven. It also lets <>them reject anything and not expose them to the risk of making a <>decision.

Regrettably true. That is one reason to foster industry standards for acceptable methodologies. FDA can be influenced by the weight of evidence and expert opinion. If industry standards produce demonstrably better software, FDA will be hard-pressed to ignore them. Similarly, a substantial consensus of expert opinion is hard for FDA to ignore, for example, FDA has embraced the concept of V&V in its recommendations for software review.

<>If anything goes wrong, its your fault and you (not the FDA) <>are liable.

This is the case whether or not there are FDA approved development methodologies. Compliance with FDA regulations will not protect any firm from product liability suits. FDA regulations are completely compatible with good business; they are incompatible with practices where cutting corners may cause undue harm.

Frank Houston, Software Safety Champion, Food and Drug Administration Center for Devices and Radiological Health. All the usual disclaimers apply in that I am not contributing in an official FDA capacity. I just want the readers to know that this is a well-informed contribution.

---

**✶ RISKS of propagating legendary RISKS (Fulmer, [RISKS-12.52](#))**

*Paul Karger, 1 617 621 8994 <karger@osf.org>  
Tue, 05 Nov 91 18:11:13 -0500*

In [RISKS-12.52](#), there was a discussion about the market pushing out poorly-designed products as part of a discussion of licensing software engineers.

fulme-ce@lea.csc.ncsu.edu (Christopher E Fulmer) wrote:

>2. The market does tend to push out poorly-designed products. However, for  
>some products, it may not be desirable to wait for the market to decide. After  
>all, Audi's sales dropped after the problems with "Instant Acceleration" were  
>found by real people, not before.

While it is true that there can be a time-lag in pushing out poorly-designed products, the Audi "Instant Acceleration" problem that cost 50% of Audi's sales, turned out to be a result of driver error as Audi had claimed all along.

(It is true that one could criticize Audi on human factors related to the pedal placement, but that is very different from a criticism that the transmissions and/or engine computers were faulty. Since then, Audi and other manufacturers have placed interlocks onto automatic transmissions to prevent shifting into gear without having your foot on the brake pedal.)

This problem and the resolution that it was indeed driver error had been discussed in RISKS at great length several years ago. It is hard both for the readers and our moderator (who works very hard and does an admirable job in editing RISKS) to remember that this accusation was in fact disproven. It is very easy to criticize a manufacturer for producing an unsafe product without actually proving that the manufacturer was actually at fault. It is much harder to undo that damage if the product was in fact OK. Audi unjustifiably lost over 50% of its market share and has yet to fully recover in the US.

---

### **✂ Software safety, formal methods and standards [via Jim Horning]**

*Jonathan Bowen <bowen@prg.ox.ac.uk>  
6 Nov 91 12:29:45 GMT*

I am writing a review paper on software safety, formal methods and standards. In particular, I am looking at the recommendations for the use of formal methods in software safety standards (and draft standards). So far I have considered the (some draft) standards listed below. If anyone has any recommendations of others to consider, please send me details of how to obtain them (or the document itself if possible!).

I am also interested in general references in this area. I have quite a few already, but I may have missed some. If they are obscure and you can send me the paper itself, so much the better.

If there is enough interest, I will summarize the responses.

Jonathan Bowen, Oxford University Computing Laboratory, Programming Research Group, 11 Keble Road, Oxford OX1 3QD, England.

Tel: +44-865-272574 (direct) or 273840 (secretary)

FAX: +44-865-272582 (direct) or 273839 (general)

Email: Jonathan.Bowen@comlab.ox.ac.uk

ESA software engineering standards,  
European Space Agency, 8-10 rue Mario-Nikis, 75738 Paris Cedex, France,  
ESA PSS-05-0 Issue 2, February 1991.

Programmable Electronic Systems in Safety Related Applications:

1. An Introductory Guide,  
Health and Safety Executive,  
HMSO, Publications Centre, PO Box 276, London SW8 5DT, UK, 1987.

Programmable Electronic Systems in Safety Related Applications:

2. General Technical Guidelines,  
Health and Safety Executive,  
HMSO, Publications Centre, PO Box 276, London SW8 5DT, UK, 1987.

Software for computers in the application of  
industrial safety related systems,  
International Electrotechnical Commission,  
Technical Committee no. 65, 1989. (BS89/33006DC)

Functional safety of programmable electronic systems: Generic aspects,  
International Electrotechnical Commission,  
Technical Committee no. 65, 1989. (BS89/33005DC)

Standard for software safety plans,  
Preliminary - subject to revision,  
P1228, Software Safety Plans Working Group,  
Software Engineering Standards Subcommittee,  
IEEE Computer Society, USA, July 1991.

The Procurement of Safety Critical Software in Defence Equipment  
(Part 1: Requirements, Part 2: Guidance),  
Interim Defence Standard 00-55, Issue 1,  
Ministry of Defence, Directorate of Standardization,  
Kentigern House, 65 Brown Street, Glasgow G2 8EX, UK, 5 April 1991.

Hazard Analysis and Safety Classification of the Computer and  
Programmable Electronic System Elements of Defence Equipment,  
Interim Defence Standard 00-56, Issue 1,  
Ministry of Defence, Directorate of Standardization,  
Kentigern House, 65 Brown Street, Glasgow G2 8EX, UK, 5 April 1991.

Safety related software for railway signalling,  
BRB/LU Ltd/RIA technical specification no. 23,  
Consultative Document, Railway Industry Association,  
6 Buckingham Gate, London SW1E 6JP, UK, 1991.

Jonathan Bowen, <Jonathan.Bowen@comlab.ox.ac.uk>  
Oxford University Computing Laboratory.

[Message forwarded to RISKS by horning@Pa.dec.com (Jim Horning),  
who thinks RISKS readers could help here... 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 12: Issue 61**

**Thursday 7 November 1991**

## Contents

- [Cop Charged with Doctoring Computerized Citation Record](#)  
[PGN](#)
- [Legal status of digital signatures](#)  
[Steve Bellovin](#)
- [The dangers of telco competition](#)  
[Lauren Weinstein](#)
- [Oven temperature regulator problem](#)  
[Jane Beckman](#)
- [No Power backup on Electronic Fuel Injection](#)  
[Gareth Howell](#)
- [Another smart card risk](#)  
[34AEJ7D](#)
- [UK Phone charge card risk](#)  
[Graham Toal](#)
- [Risks of telephones with status displays](#)  
[Neil Strauss](#)
- [Don't bank on computer viruses!](#)  
[Gene Spafford](#)
- [NSF researchers required to undergo security checks?](#)  
[Nancy Leveson](#)
- [Re: Have you tested your machine lately?](#)  
[Matt Crawford](#)  
[Dave W. Hamaker](#)
- [Re: Blaming the computer \(again\)](#)  
[George Malits](#)  
[Paul J. Karafiol](#)
- [Re: A new twist on "Speed Controlled by Radar"](#)  
[Clive Dawson](#)
- [Re: Electronically controlled bus transmission](#)  
[Adam V. Reed](#)  
[Jamie Mason](#)
- [Info on RISKS \(comp.risks\)](#)

---

✉ **Cop Charged with Doctoring Computerized Citation Record**

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

Thu, 7 Nov 91 9:15:27 PST

Emily Fields, a San Francisco police officer, has been charged with evading payment and tampering with records after accumulating almost \$700 in traffic citations. Assigned to the PD's warrant section, she allegedly gained access to the police computer and cleared a warrant issued against her for nonpayment of tickets, changing the record to indicate she had been arrested and taken into custody. (She had previously defaulted on payment and failed to appear in court, which resulted in the warrant appearing in the computer database.) [San Francisco Chronicle, 5Nov91]

---

### **✂ Legal status of digital signatures**

<smb@ulysses.att.com>

Wed, 06 Nov 91 20:08:37 EST

I'm looking for information the legal status of documents authenticated by digital means, i.e., RSA, ElGamal, the recent proposal by NIST, etc. Do any countries have laws, regulations, or judicial precedents governing such matters? Are such records admissible as evidence in civil or criminal trials in these jurisdictions? Will the relevant government authorities, or non-government financial practices bodies (i.e., the FASB in the United States) accept digital signatures in contexts where a paper audit trail had been required? I'm thinking of things like employee time cards, payment vouchers, purchase orders, etc.

Please reply by mail. I'll be happy to compile a summary for any interested parties (and for the list as a whole, if demand so indicates, and the quality of the information received permits).

--Steve Bellovin smb@ulysses.att.com

---

### **✂ The dangers of telco competition**

Lauren Weinstein <lauren@vortex.com>

Tue, 5 Nov 91 19:25:29 PST

There are quite a number of reasons why various items now on the local telcos' agendas, especially those relating to the provision of information services or television programming, would ultimately be bad news for most consumers.

Fundamentally, the problems relate to there being, in practice, an extremely uneven "playing field" involving local telcos vs. any outside competition.

It can be expected that most enhanced services that telcos operate will be priced in such a way as to undercut competition, either in terms of pricing, or in terms of features that only the telco can provide, due specifically to the telco's unwillingness to provide equal access to their switches at "fair" prices.

Meanwhile, the telcos have the ability to jack up the price on those services for which there is no effective competition and for which most consumers have nowhere else to go. Exactly this is happening right now in California, with the two main telcos, PacBell and GTE, requesting massive increases in basic local service rates, theoretically in exchange for lower rates for certain types of toll calls. Unfortunately, any consumer or small business who has a number of lines and doesn't make enough of the "correct" type of toll calls loses out big time. While there is supposed to be a division between telco enhanced services and basic services in terms of funding and cost factors, in practice the two are usually so intertwined that its essentially impossible to control.

I mentioned the uneven playing field above. There's an obvious example of this right now. Look at the telco provided "voicemail" services in comparison to the similar services provided by outside firms. With outside firms, you have to call forward into the service, and if you're on a measured rate phone line (as most businesses are these days, usually by edict, and increasing numbers of residence subscribers as well) you have to pay for every call transferred to the voicemail vendor. When you want to check to see if you have messages, you have to make yet another call to check on the status of your voicemail box.

Now look at the telco systems, which are tightly integrated with their switches. The voicemail system is directly trunked to the various central offices. No forwarding, no call charges for each call. If messages are waiting, you get a "stutter" dialtone when you pick up the phone.

The outside vendors of voicemail services would very much like to get access to the switch on the same basis. But at this stage of the game, they can't. Eventually a complex set of FCC rules may supposedly allow for the access of outsiders to various network "elements" as individual units. However, it appears that the pricing of such elements will be quite predatory and in practice continue the telcos' pricing advantage as it relates to tightly coupled enhanced services. Other similar cases already exist. Various telco-sponsored information services for cellular phone users, accessible more easily (fewer digits) and more cheaply (even free!) than outside services, have already been announced.

Now the telcos want to do video (Cable TV) too! They're waving the promise of fiber-to-the-home in front of Congress, and waxing poetic about all sorts of glamorous future information services (most of which, by the way, sound much the same as services available now from outside vendors). Little (if any!) mention of pricing ever comes up in these discussions (the high rates for current ISDN implementations may be instructive here). Nor is it mentioned that, inevitably, the telcos will keep coming back to the local basic service ratepayers to help bail them out from any failed projects. You can also be sure that most telco information services will be oriented toward dense urban areas and well-heeled business customers.

The example of the French Minitel system comes up from time to time as a "successful" telco-related info service with many outside vendors. I don't believe that this example can be applied to the U.S. telecommunications market. The French government provided most of the Minitel terminals for "free", and even now, after all these years, the system requires large government subsidies to stay in operation. The government/private industry/telecommunications

structure there is fundamentally different from what we see in the U.S. environment, with government control and government funding/subsidies playing much more central roles than would be tolerated in this country.

This message can but give a taste of the issues involved; it's all a very complex matter. But boiled down to its essence, the problem is that in practice we cannot depend on the owners of the fundamental "pipelines" (the telcos) being able or willing to provide truly equal access, both in terms of pricing and features, to their competitors who need to use those same pipelines. This is especially critical since the telcos are in the enviable position of having that handy collection of basic ratepayers to fall back on, one way or another--theoretical provisions to prevent this notwithstanding.

--Lauren--

---

### **🔥 Oven temperature regulator problem**

*Jane Beckman <jane@stratus.swdc.stratus.com>  
Mon, 28 Oct 91 18:02:05 PST*

Seeing the recent discussion of furnace thermostats going haywire reminded me of a recent problem a friend had with her oven.

Her stove is one of these modern models with electronically regulated oven temperature control, digital readouts, etc. These things are great, until... She was baking some cookies, and when she took them out, she thought it was weird that they were overdone. The timing was right, but the oven temperature seemed to be way too high. She turned off the oven and didn't think a thing about it until she put a casserole in a couple days later. The casserole seemed to be cooking too fast, and the oven was like a blast furnace, and yet the stove told her everything was fine. So she decided to turn off the oven.

The oven would not turn off. For the next couple hours, she tried to turn off the oven, to no avail. The kitchen was getting pretty warm, by then. The final solution to this was to turn off the gas to the stove. She called the repairman, and when he came out and evaluated the problem, it turned out some vital piece of electronics had shorted out, and the cost of replacement was \$200, which was a sizable chunk of the price of the stove! She seriously discussed simply replacing the stove with a \$400 non-electronic stove, for fear of this happening again, but finally broke down and had it fixed. She has had other problems, since, with the temperature not being what the sensors think it is. It sounds like the entire sensor system may have had design problems, from the first. (Sorry, I don't remember the brand of stove.)

Jane Beckman [jane@swdc.stratus.com]

---

### **🔥 No Power backup on Electronic Fuel Injection**

*Gareth Howell <garethh@sadss.uucp>  
Thu, 03 Oct 91 04:57:15 BST*

This concerns the risk to the environment when the Electronic Control Unit (ECU) for the fuel injection doesn't have a protected power supply.

I used to own a Rover 800 (sold as a Sterling in the US). One of the models in the range (820E) has a 2litre single-point fuel injected engine. The configuration setup of the ECU (which controls the fuel-air mixture, and hence controls emissions) is held in volatile RAM, which is powered from the car's battery.

Unfortunately, if you disconnect the battery the RAM is cleared, and whilst you can still run the engine, it runs in a default state which can cause excess emissions. The detailed workshop manual contains a method of re-tuning the engine if the settings are lost, but it doesn't indicate that disconnecting the battery (which has to be done for many repair/service type operations) will cause the ECU settings to be wiped.

Here in the UK, we have just introduced emission checks on all cars as part of their annual safety check - I wonder how many 820E's will fail because either their owners or the garage didn't re-set the ECU settings?

73 Gareth

Note: As far as I know the other models in the range don't suffer from this problem.

Gareth Howell, Information Technology Services Agency, Department of Social Security, Lytham St Annes, England, FY8 1ZZ [garethh@sadss.uucp](mailto:garethh@sadss.uucp)  
[sadss!garethh@eros.uknet.ac.uk](mailto:sadss!garethh@eros.uknet.ac.uk) [garethh@cix.compulink.co.uk](mailto:garethh@cix.compulink.co.uk) +44 (253) 797096

---

### **Another smart card risk**

<34AEJ7D@cmuvvm.bitnet>

Mon, 04 Nov 91 11:36:47 EST

The Florida-based Advanced Promotion Technologies has developed a smart card, dubbed a "Vision Value Card" to accumulate details of buying patterns, etc. at various mega-markets. I believe the VVC is in use, or testing, in the Mormon-owned Safeway foodstore chain. The card also doubles as an electronic "trading stamp" by accumulating "bonus points" awarded for purchasing certain products. These points are redeemable for "gifts" from a catalog published by APT.

---

### **UK Phone charge card risk**

Graham Toal <[gtoal@gem.stack.unc.tue.nl](mailto:gtoal@gem.stack.unc.tue.nl)>

31 Oct 91 23:32:26 GMT

This may be old news to comp.risks or comp.dcom.telecom, but it was the first time it was drawn to \*my\* attention; Barry Fox has an article in this week's New Scientist (UK weekly) explaining that phone charge cards in the UK work by dialling 144 + card no + PIN + phone no; it seems that Hotel/business/etc call loggers (understandably) record this string of numbers as the number dialled.

He doesn't say that this \*has\* been used to fraudulently use someone's account, but I think that's a fair assumption. (There has been talk on uk.telecom of possible large-scale fraud going on recently)

Fox says that 'Telecomms Regulation Review' trade magazine had informed BT of this some time ago, but BT have done nothing to warn their customers. [I wonder what sort of warning would be appropriate?]

Graham

PS I'm posting to comp.risks for the risk aspect; to comp.dcom.telecom because I wonder how this problem was solved in the US who have had this technology much longer than us.

---

### **⚡ Risks of telephones with status displays**

*Neil Strauss <neil@ps.quotron.com>*

*Thu, 7 Nov 91 15:31:05 EST*

I recently used a telephone at a customer of ours to call my office voicemail. This phone had a LED display which echoed every button I pressed from the time the handset was raised until I hung up. This resulted in my voicemail password being prominently displayed to any passing individual.

The risks of my voicemail being compromised are relatively small, but the same type of compromise would have occurred if I had been using a telephone credit card.

I learned after completing the call that there is a button on the phone which will prevent button presses from echoing, but this button was not clearly labelled and could not be used by an uneducated user.

The most logical approach to a status display on a phone is to echo the phone number to prevent wrong numbers and then inhibit echoing after the call has been connected. I also wonder if a phone that displays my keystrokes may not also be recording them somewhere for accounting purposes.

---

### **⚡ Don't bank on computer viruses! [WWN strikes again!]**

*<spaf@cs.purdue.edu>*

*Mon, 04 Nov 91 20:34:19 EST*

We've heard all about the usual stealth computer viruses and "armored" viruses that are being written these days. It seems that in some places the writing of nasty viruses has become a national pastime. Some of these authors delight in finding new methods of damage and camouflage. The problem has mainly been for IBM PCs, and the most sophisticated virus-writing has been in Bulgaria and the USSR.

Now, however, we have a new and far worse problem from South America, according

to the November 12th issue of the "Weekly World News." [This is the "newspaper" you may find at supermarket checkout lines with the kind of headlines you don't see in the more mainstream media. Obviously, a conspiracy by the mainstream media. The November 12th issue is headlined with "Ohio Woman has a 3rd Eye -- in the back of her head!"]

On page 7, there is an article by one Sally O'Day, "special to the WWN," and entitled: "Demon Computer Kills 2 Workers!" It is subtitled "Exorcist called in after experts discover virus-bred evil spirit!"

The article goes on to explain how a computer system installed in a bank in Valparaiso, Chile is possessed by a demon. A consultant from the computer company that installed the system claims that it must be the result of a virus installing an evil demon that has caused:

- \* observers to see a hideous horned demon appear on the screen
- \* anyone who tries to turn off the machine to black out and fall to the floor
- \* Carmen de la Fuente to have a fatal heart attack within 2 minutes of sitting down at the terminal
- \* Maria Catalan to be found sitting at the terminal with her head in her lap [decapitated, I presume, rather than a contortionist]
- \* a computer expert to began babbling like a madman when he got within 10 feet of the terminal

This brings up many interesting questions:

- How long before commercial anti-virus vendors start advertising that their products work against this type of virus?
- Does the exorcism ritual end with extinguishing the candle, closing the book, and sounding the BEL?
- Could this actually be the result of using Ada rather than a virus?
- Do you know any computer experts who don't begin to babble when within 10 feet of a computer?
- Does normal business insurance cover an exorcism?
- Maybe it's a Unix system and this is the first time they've seen the sendmail daemon?
- Will Fred Cohen allow this to be entered in his virus-writing contest?

Or, it could be that Ms. O'Day has recently seen the movie "Evilspeak"? [If you have yet to see the movie, rush right out and rent it. Lay in a supply of beer and pizza, and invite the neighbors over. It is a classic wherein a nerdy Ken Howard (Ron's little brother -- the one who used to hang out with Gentle Ben) summons up the devil on an Apple II computer. He should have guessed something was amiss when he started getting Stardent-level graphics on his little Apple, and when it started demanding blood sacrifices. The credits include mention of the "stunt demons" and "Satan's Sows." Not to be missed.]

Hey, it must be true if they printed it, right? :-)

[It is astounding how they manage to recycle old stories. The basics of this appeared years ago in WWN, 3 March 1987 (see [RISKS-4.50](#), 23 February 1987,

---

**✂ NSF researchers required to undergo security checks?**

<leveson@cs.washington.edu>

Fri, 01 Nov 91 06:18:33 -0800

The Washington Post, on Tuesday 29 Oct. 1991, page A21, contains an article about the new NSF Presidential Faculty Fellows program (like PYI but more money). The article states:

Recipients of the Presidential Faculty Fellows awards will have to be formally approved by the White House, though Bromley said no one will be denied a grant for political reasons. They will also have to undergo an FBI background check.

Presidential approval is OK -- that is also part of the PYI program and is probably just a formality -- but why should an FBI background check be required to receive an NSF research award? Surprisingly, the author of the Post article did not mention the fact that this might be out of line (the article only expressed concern that the award was just a shell game that would actually reduce the total number of young scientists supported in the combined PYI and PFF programs). This seems like a very dangerous trend, and I am shocked that NSF would agree to go along with this.

nancy

[This item is marginally related to computer risks, but seemingly relevant to some of the related threads running through RISKS, such as privacy of computer scientists who might apply for PYIs? PGN]

---

**✂ Re: Have you tested your machine lately? (Roberts, [RISKS-12.54](#))**

"Matt Crawford" <matt@odjjob.uchicago.edu>

Wed, 30 Oct 91 16:04:16 CST

> All the software using floating point is broken -- in mysterious ways.

A few months back we had a problem with a VAX/8650 running VMS. approximately 9 out of 10 attempts to log in would fail as if the password were wrong. It sounds like the classic Trojan horse login program, but it was actually a bad floating point board. It took a few days to figure it out, but eventually some vax guru inside DEC gave field service the answer.

---

**✂ Re: Have you tested your machine lately? (Roberts, [RISKS-12.54](#))**

Dave W. Hamaker <dwh@eco.twg.com>

25 Oct 91 17:33:54 GMT

In [RISKS-12.54](#) Boyd Roberts writes about his tribulations with his DECstation 5000 when its FPU failed. A day of his time was consumed trying to figure out why strange things were happening, and the problem became evident only after he started trying hardware swaps. This necessitated rebooting and the self tests then incidentally revealed the true problem.

This reminds me of the time the FPU in a mainframe had a failure which took me only a few minutes to diagnose. I was responsible for taking care of the system software. It was reported to me that many DBMS users were getting incorrect results. I knew the software hadn't been changed recently and there were too many reports for me to suspect "user error." Hardware seemed the only other alternative. "But why isn't the whole system crashing?," I thought. "Maybe the operating system doesn't use floating point," and a few quick tests showed the results of floating point adds and subtracts always came out negative ( $1 + 1 = -2$ ). Sometimes one is fortunate enough to ask the right question first.

At another job, a colleague got the source code for a quick instruction set diagnostic from the computer vendor's service engineers and spliced it into the operating system's "idle" loop. When the machine wasn't doing anything else, it would be testing itself. As I recall, that this caught a hardware failure at least once. Perhaps this is something hardware vendors might do that would help with the kind of failure Boyd Roberts experienced.

Dave Hamaker

---

**✂ Re: Blaming the computer (again) (Schwartz, [RISKS-12.60](#))**

*George Malits <malits@sgtyork.sw.stratus.com>  
Thu, 7 Nov 91 09:33:02 EST*

Concerning the article on the \$1M tax bill. Deja Vu all over again. If you've ever read *\_The Elements of Programming Style\_* there is a very similar example. This was back in the days of punch cards and a data entry error shifted one of the fields by one column. The result was that the rightmost character in one field ended up in the leftmost column of the next field. This turned out to place a letter in what was supposed to be a numeric field. No matter, the software managed to "interpret" the letter into a digit. The result was that some poor guys Chevy was valued at several million dollars. The best part of the whole thing was the error was detected (by manual inspection and not by the software) and a new card punched but somehow the old card was not destroyed. The tax payer received 2 bills, one correct and one very wrong. In this case, the town could/would not print new tax bills at a higher rate so they were forced to cut the town budget to make up the deficit BTW: All of this is from memory so I apologize in advance for any errors in detail that might have crept in.

---

**✂ ORegon Misassessed property tax (Re: Schwartz, [RISKS-12.60](#))**

*<karafiol@husc.harvard.edu>  
Thu, 7 Nov 91 14:07:47 -0500*

>[a farm in rural Oregon] should have received an \$8,850 assessment,  
>instead of the \$97 million property valuation. Their tax bill should have  
>been for just \$117 [...].

whereas, according to the Oregonian, they were billed for \$986,312.

So, Schwartz notes,

>Bill for someone [else's] \$70K home will go from \$710 to \$760 to make up  
>for the deficit from the bad math.

There is another problem that came out in a similar case in Massachusetts last spring: the county may well have counted on their share of the incorrectly billed \$986,312. This indeed happened in the Mass. case, which led to a fiscal crisis: the county had by that time committed itself to spending money which it just wasn't going to get, (a) because it wasn't owed it, (b) because the possibilities for a small town getting a million-dollar loan to cover such a screwup are low, and (c) because there was no clear governmental agency willing or able to cover them.

Questions, comments, solutions? Note that it wasn't at all the county's fault: they got a printout from the state that said, "Your share of local property taxes is going to be so-and-so-much." And while we would like to say that the state owes them the money, realistically speaking, that would probably be an unacceptable solution.

== paul j karafiol

---

### **🔥 Re: A new twist on "Speed Controlled by Radar"**

*Clive Dawson <AI.CLIVE@MCC.COM>*

*Thu 31 Oct 91 07:54:33-CST*

A recent message from Andrew Green (acg@hermes.dlogics.com) described the use of unattended radar transmitters to cause vehicles to slow down by triggering their radar detectors, and raised the question of how failure of these transmitters could be detected.

About ten days ago while visiting Canada, I was driving from Toronto to Buffalo and noticed a similar system. During the approach to a particularly sharp turn along Queen Elizabeth [Free]Way, I observed the usual warning signs indicating that it would be a good idea to slow down. I slowed down slightly, but not down to the recommended speed. When the turn was imminent, I saw a large red sign directly ahead suddenly begin to flash "TOO FAST". My instant reaction as I immediately slowed down further was, "Wow, what an effective feedback device!"

I would suggest that adding a visual sign of this sort to the system in Chicago would not only serve to warn vehicles without radar detectors as well, but would also address the risk of error-detection, since a transmitter failure would be much more obvious.

What about other uses for unattended radar? I know of several residential neighborhoods that use huge(!) speed bumps (the kind would rip out your suspension at anything over 15 mph but are a pain at any speed) to enforce speed limits. I can imagine a system in which radar could raise physical devices which would make speeding noticeable (1-inch bumps), unpleasant (4-inch bumps), or impossible (parking-lot-style spikes?! ;-), thus allowing a smooth ride for vehicles within the speed limit.

One of the Risks which I find fascinating is the idea that once people are accustomed to having a system like this provide a warning about a speed-limit (or any other law or regulation), then failure of the system causes people to think they have temporary license to ignore the law, even in the face of all of the conventional warning signs, etc. The more general theme here is that any time we allow a computer to assume the role of a conscience, we must remember that a failure does not imply that people will automatically and immediately revert to a backup system, i.e. using their own consciences!

Clive Dawson, MCC, Austin, Texas

---

**✉ Re: Electronically controlled bus transmission (Secof, [RISKS-12.60](#))**

*Adam V Reed <avr@mtfmi.att.com>*

*Wed, 6 Nov 91 22:25:15 EST*

More on risks of accepting human-hostile design!

==> A car with misplaced pedals is just as faulty as one with misplaced gears.

[Audi...] Blink. Are the pedals any less a part of the car's acceleration control subsystem than is the transmission? Audi lost half it market share because its wanna-be-"engineers" placed the brake and accelerator pedals so close together, that drivers could not tell what they were stepping on. This, even though reliable standards for the placement of mechanical controls, including pedals, have been available since the early 1950s. As an engineer and a human, I find Audi's fate justified, market forces vindicated, and consequences salutary.

Adam\_V\_Reed@ATT.com

---

**✉ Re: Electronically controlled bus transmission (Secof, [RISKS-12.60](#))**

*Jamie Mason <jmason2@utcs.utoronto.ca>*

*Thu, 7 Nov 1991 04:23:30 -0500*

The problem here is the 'computer knows best' attitude. Far too many problems arise because of this. Not only does that automatic transmission make decisions that a competent human should be making (the choice of gear), but it also ignores an explicit override.

This is one of many reasons why I chose to drive manual transmission vehicles. When you have a stick physically linked to a gearbox, it is hard for the car to second-guess you.

Unfortunately, this is not the first time I have heard of automatic transmissions doing this. Many expensive cars have this feature, I believe the Benz will prevent you from putting the car in an 'inappropriate' gear. I'm not sure what it would do if you put it in "LO". I think the Tiptronic manual/auto transmission on the new Porsche is like this as well. (You would think that those who could afford a car like THAT would not put up with their car telling

them what to do!)

It's a bad day when critical systems have NO manual override. There should always be SOME way for the OPERATOR to have the final word. Unfortunately, some designers must not realize how critical the control systems of an automobile are. I hope the designers of "electronically controlled super-highways" keep this in mind.

The driver is smarter than a tachometer. Even if the passengers DID NOT MATTER, and the sole purpose of the rev-limiter was to protect the engine (from over-revving) the device FAILED at its task. Afterall, the engine WAS destroyed in the crash, wasn't it? :-)

Jamie ...



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 12: Issue 62**

**Tuesday 12 November 1991**

## Contents

- [Leaves cause railway signal failure](#)  
[Graeme Tozer](#)
- [Computer controlled train is unsafer](#)  
[Bob Devine](#)
- [More air scares and phone moans](#)  
[PGN](#)
- [RISKS of infrared car door locks](#)  
[Andrew Evans](#)
- [Summary of responses on UK phone card risks](#)  
[Graham Toal](#)
- [Re: Licensing of Software Developers](#)  
[Brinton Cooper](#)  
[David Parnas](#)
- [Searching a library database](#)  
[Matthew Merzbacher](#)
- [Audi Pedal Pushers](#)  
[Bob Ayers \[and others\]](#)
- [Religious bias in RISKS posts is counter-productive](#)  
[Bill Gray](#)
- [Re: Radar](#)  
[Eric Florack](#)
- [Security failure: recycled "unlisted" phone number](#)  
[Steven J. Edwards](#)
- [You can help build the National Public Network.](#)  
[Gerard Van der Leun](#)
- [Call for Papers: 5th Annual Computer Virus & Security Conference](#)  
[Jack Holleran](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Leaves cause railway signal failure**

*Graeme Tozer* <[graeme@inmos.com](mailto:graeme@inmos.com)>

*Tue, 12 Nov 91 13:32:02 GMT*

The following story was reported in "Computer Weekly", November 7th.

AUTUMN LEAVES FOX BR'S SIGNAL SYSTEM, by Tony Collins.

Autumn leaves have taken British Rail's latest computerised signalling system by surprise. BR'S Integrated Electronic Control Centre (ICC), based on three parallel systems, is designed as a fail-safe answer to the older electromechanical processes. Installed at Liverpool Street, Newcastle, York and Leamington Spa the IECC is supposed to tell signals staff exactly where trains are located by displaying positions on a visual display unit. But BR discovered this week that the system is only fail-safe when tracks are free of Autumn leaves. It found that leaves under wheels cause trains to 'disappear' from computer circuits. The leaves form an insulating paste, preventing the wheels making contact with sensors which tell systems the train's position.

On Monday hundreds of passengers were stranded at stations as services were canceled or delayed as BR struggled to identify the location of trains. A BR spokesman said the problem was being overcome by using older, heavier trains whose wheels make better contact with the signalling sensors. He stressed that the problem of Autumn leaves would in no way affect BR's plans to expand its use of IECC systems.

Graeme Tozer, iq Software Group, INMOS Ltd., 1000, Aztec West, Almondsbury, Bristol BS12 4SQ, UK. +44 454 616616 graeme@inmos.co.uk ...!ukc!inmos!graeme

[Leaves something to be desired? NO WAY. But if you tried to count how many there were, you would probably take leaves of your census. PGN]

---

### **✂ Computer controlled train is unsafer**

*Bob Devine 12-Nov-1991 1302 <devine@cookie.enet.dec.com>  
Tue, 12 Nov 91 12:17:22 PST*

From "The Denver Post" comes a story of a train crash caused by the elimination of a safety device for a modern locomotive engine.

The root cause of the crash was that the engineer fell and hit his head causing him to lose consciousness momentarily. Meanwhile the 4 engines started rolling down a slight hill. None of the engines were running but because of their weight (380,000 pounds each) and the distance they rolled (about 25 miles), the engines went as fast as 75 mph. They finally stopped when they hit a parked train.

The computer risk in this is (quote from Post):

Years ago, locomotives had a "dead man's control" to stop a train if the engineer released tension on the throttle. Now rail engines use sophisticated electrical devices to determine if something is wrong with the engineer [the NTSB guy] said. In this case, they did not apply because there was no engineer aboard.

The article did not say what the seemingly omniscient "sophisticated electrical

devices" are nor does it say if the locomotive engineers have to be running to generate electricity for those devices...

Bob Devine

---

### **✂ More air scares and phone moans**

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

*Sun, 10 Nov 91 17:48:10 PST*

An AP item from 10 Nov 91 adds a few more air and phone problems to our burgeoning archives. Here are a few excerpts:

The Federal Aviation Administration, in a report to a House subcommittee, said that from August 1990 to August 1991 there were 114 "major telecommunications outages" across the country that led to flight delays and generated safety concerns.

On May 4, four of the FAA's 20 major air traffic control centers shut down for five hours and 22 minutes. The cause: "Fiber cable cut by farmer burying dead cow. Lost 27 circuits. Massive operational impact."

A year ago, the Kansas City, Mo., air traffic center lost communications for four hours and 16 minutes. The cause: "Beaver chewed fiber cable."

Other causes include lightning strikes, misplaced backhoe buckets, blown fuses and computer problems.

Most recently, two technicians in an AT&T long distance station in suburban Boston put switching components on a table with other, unmarked components, then put the wrong parts back into the machine. That led to a three-hour loss of long distance service and flight delays at Logan International Airport.

On Sept. 17, AT&T technicians in New York attending a seminar on warning systems failed to respond to an activated alarm for six hours. The resulting power failure blocked nearly 5 million domestic and international calls and crippled air travel throughout the Northeast. Some 1,174 flights were canceled or delayed and 85,000 passengers including Al Sikes [FCC Chairman] and Ervin Duggan [panel member] were inconvenienced. [See [RISKS-12.36](#), 38, 43...]

[I guess that got their attention! An example of Sikes-seeing?  
Of course, crossing the Kansas City tale with Graeme Tozer's fall rail saga above, we get "Leave it to Beaver's high-fiber diet."  
<Yes, you're right. It is getting late again.> PGN]

---

### **✂ RISKS of infrared car door locks**

*Andrew Evans <andrew@airs.com>*

*12 Nov 91 19:18:20 GMT*

In the current issue of "Car and Driver" is an article about the new Mercedes-Benz 400 SE. One of the features mentioned was its infrared remote locking/unlocking system, in which the transmitter on the key and the receiver in the door would recode themselves each time they were used to prevent unauthorized entry.

This leads me to wonder: could you use one of those programmable universal

infrared remote controls to learn the pulse sequence of an infrared key, and use the programmed remote to unlock the car? Anyone have both a car and a remote to test this?

[NEW POLICY ON SUCH TOPICS: PLEASE RESPOND TO THE ORIGINAL CONTRIBUTOR AND HOPE THAT HE OR SHE DISTILLS THE RELEVANT RESPONSES SUFFICIENTLY THAT THEY ARE INTERESTING, RELEVANT, etc. TO RISKS READERS. RESPONSES ONLY TO RISKS WILL BE IGNORED BY ME. THANKS. THE MANAGEMENT. PGN]

---

### ✂ Summary of responses on UK phone card risks

Graham Toal <gtoal@gem.stack.unc.tue.nl>

11 Nov 91 22:11:13 GMT

I posted recently of the risks of UK calling cards - the PIN is dialed as an extension of the number, and therefore can be logged on call-loggers, as used in hotels, businesses, local government offices etc.

I wondered how this had been solved in the US, as I hadn't heard of the the problem before and would have expected the US to hit it first.

The answer is that the US thought about it in advance! :-) [typical BT] The US system effectively succeeds in placing a call \*before\* dialing the PIN, therefore the PIN goes through as data and not part of the number. BT could perhaps consider switching to such a system. However I \*think\* the US system would mean that pulse-dialing phones would be unusable. The UK system certainly works on pulse-dial phones.

Thanks for all the replies.                      Graham

---

### ✂ Re: Licensing of Software Developers ([RISKS-12.58](#))

Brinton Cooper <abc@BRL.MIL>

Sun, 10 Nov 91 23:39:21 EST

David Parnas writes

- > I don't believe that we can
- > afford to ignore the issue of qualifications for software professionals, but
- > the question we should be debating is what those qualifications should be and
- > who should be covered. It is not an all-or-nothing problem.

Earlier in the same contribution, he wrote:

- > This is exactly analogous to the situation in Medicine. Government's decide
- > that you must have a medical license to perform heart surgery. Doctor's decide
- > who can have such a license. Doctor's consider themselves a self-enforcing
- > profession, but the government does not allow them to determine their own
- > "scope".

This indicates a principal difficulty with licensing software professionals.

In medicine, law, and engineering, the applicant for license has already been through a program of instruction and clinical practice that has been accredited by a nationally-recognized professional society. Applicant must provide some evidence of experience and pass some sort of formal examination. Thus, the licensing process has (at least) three components: formal and recognized education, practice, and formal examination. In the main, I believe it works well in all three professions. At least it sets lower bounds to competence with a high degree of reliability.

On the other hand, some of our finest software professionals have skipped or prematurely terminated the "formal" part of training in accredited (or otherwise) institutions. Thus, a licensing authority would have to review their cases solely on the basis of (claimed) experience and a formal examination. There seem to be too many points of competence that are missed under these conditions.

Anticipating the next argument, I am well aware that we would be lots poorer without the notable works of a few university drop-outs and at least one who never even finished high school! I dare say that medicine, law, and engineering, in their respective infancies, produced similar genius-level practitioners. But today, these are no longer allowed. I fear that licensing of software professionals would deny us the talents of similar visionaries.

Are we ready for this? ACM, et al., have been accrediting CS departments for only a few years. Academics continue to debate whether CS belongs in the school of engineering or of arts & sciences in the university. Perhaps it is appropriate that we begin this discussion now and carry it on for a very long time.

\_Brint

---

### **✦ Re: Licensing of Software Developers ([RISKS-12.58](#))**

*David Parnas <parnas@qusunt.eng.McMaster.CA>  
Mon, 11 Nov 91 13:58:05 EST*

We certainly are ready. The engineering societies already have mechanisms for handling people who do not have accredited degrees. I believe that the only error was made 25 years ago when people treated "computer science" as a science rather than as an engineering speciality.

Dave

---

### **✦ Searching a library database**

*Matthew Merzbacher <matthew@lynn.CS.UCLA.EDU>  
Tue, 12 Nov 91 01:21:48 GMT*

Orion, UCLA's online library database, has a reasonable user interface, but sometimes it's just too smart. Orion's title matching algorithm is to take the user-provided phrase, remove punctuation, compress blanks, do some other routine stuff, and then check the online index. Thus, if you asked for works by J.P. Morgan, you'd also get works entered under J P Morgan (without the

periods).

The problem is, that Orion also does its transformations on keywords and titles. Pity the poor user who wanted to find all the books with "C++" as a keyword or title word. Orion dutifully transforms the request and finds all books with "C" as a keyword or title word.

And, according to user services, there's not a darned thing that can be done about it. There's no bypassing that particular "feature" of Orion.

Matthew Merzbacher UUCP: ...!{uunet|rutgers|ucbvax}!cs.ucla.edu!matthew

---

**✂ Audi Pedal Pushers (Re: Seecof, [RISKS-12.60](#), Reed, [RISKS-12.61](#))**

*Bob Ayers <ayers@Pa.dec.com>*

*Fri, 8 Nov 91 11:41:46 -0800*

I suggest that you filter out references, especially incorrect ones, to the supposed Audi problem of a couple of years ago.

[RISKS-12.61](#) repeats the claim that the pedals of the Audi were especially close together and easy to confuse. In fact, they were, as I recall, in the 2nd quartile of closeness, and Audi's were *\*not\** the most popular car to suffer 'sudden acceleration' incidents.

[Good idea. We had extended discussions in [RISKS-4.17](#) and 7.25 on the Audi. [RISKS-8.87](#) discussed the pedal puddle. More in [RISKS-9.01](#).

The Aud-acious bogosity of Audi pedal propinquity was also noted by trt@cs.duke.edu (Thomas R. Truscott) and hsu@eng.umd.edu (David Hsu), along with other comments somewhat peripheral to the original discussion. On the other foot, Norman Yarvin <yarvin-norman@CS.YALE.EDU> notes the desirability of pedal propinquity for heel-and-toe shifting. And chaz\_heritage.wgc1@rx.xerox.com suggests that perhaps

"... American customers simply lack the skill necessary to drive a sophisticated car like an Audi successfully? The American driving tests are notoriously lax; few Americans can drive a manual-transmission car; and Americans are far more prone than Europeans to being so grossly overweight that they have difficulty getting into, let alone driving safely, an average-size car. American cars are in general badly designed, usually by marketing suits who don't `wanna-be' engineers at all, and with the intention of pandering to ill-informed fashion (e.g., front-wheel drive for limos) rather than producing anything worth having; they are excessively large and heavy, and their handling (I speak from experience) is utterly diabolical, barely safe in a straight line."

[Excerpt from a message that was probably not relevant anyway, but it might make a few folks think... Remember, many of the risks are in THE PEOPLE AS WELL AS IN THE TECHNOLOGY... Sorry if I have truncated any other worthy opinions... PGN]

---

**✂ Religious bias in RISKS is counter-productive (34AEJ7D, [RISKS-12.61](#))**

<gray@s5000.rsvl.unisys.com>

Fri, 8 Nov 91 15:30:16 CST

I quote from your masthead:

"The RISKS Forum is moderated. Contributions should be relevant, sound, in good taste, objective, coherent, concise, and nonrepetitious."

^^^^^^^^^^^^ ^^^^^^^^^^^^^

Now I quote from a recent post received here on 8 November 1991:

Date: Mon, 04 Nov 91 11:36:47 EST

From: 34AEJ7D@cmuvm.bitnet

Subject: Another smart card risk

... I believe the VVC is in use, or testing, in the Mormon-owned Safeway foodstore chain.

^^^^^^^^^^^^^^^^

First, I see an assertion that a particular church owns a food store chain. No attribution for this claim is given, not surprising since it is false. I took an entire 60 seconds to call the Piper Jaffray & Hopwood stock brokerage office in Minneapolis and learn that Safeway Stores is publicly traded, had a 52-wk high of 21 5/8, a 52-wk low of 11 1/4, and closed off a half point at 18 1/4.

Even if the church in question did own the stores, how is that relevant to the story--except as a feeble attempt to smear a church with the stain of profiteering? That datum, even had it been true, contributed nothing to anyone's appreciation of any RISK.

Yellow journalism like this coming from a biased reporter is unsurprising. For it to slip past a credible editor is most disappointing.

I call upon you to retract that allegation and avoid similar jabs at religious groups in the future.

Bill

[Bill, Sorry. I should have yanked that one. But I do wish contributors would exercise a little more self-discipline. Remember that on-line newsgroups are a wonderful opportunity for maturity to emerge on the part of the discussants. However, the expectations that your moderator can catch EVERYTHING is unreal. On the other hand, I really should have caught that one. Thanks for the reminder. PGN]

---

**✂ Re: Radar**

<Eric\_Florack.Wbst311@xerox.com>

Mon, 11 Nov 1991 12:44:36 PST

I've noted with some degree of wry humor, all the glowing reports (pun intended) about the good that radar can do. Clive Dawson, for example:

<>What about other uses for unattended radar? I know of several residential neighborhoods that use huge(!) speed bumps (the kind would rip out your suspension at anything over 15 mph but are a pain at any speed) to enforce speed limits. I can imagine a system in which radar could raise physical devices which would make speeding noticeable (1-inch bumps), unpleasant (4-inch bumps), or impossible (parking-lot-style spikes?! ;-), thus allowing a smooth ride for vehicles within the speed limit.<<

Consider, however: Simply running through a radar trap exposes the driver and passengers to more X-band radiation than OSHA law allows.

Consider: Cops in one state (I forget which) refuse now to use the radar `guns' after being diagnosed as having cancer as a direct result of using the devices.

Seems perhaps another way to achieve the goals is in order.

I can't allow the foregoing to go out without adding that I've always thought speed radar had far less to do with public safety than with making money for the state.

---

### **✂ Security failure: recycled "unlisted" phone number**

*Steven J. Edwards <sjed@xylos.ma30.bull.com>  
Fri, 8 Nov 91 14:49:58 EST*

Security failure: recycled "unlisted" phone number (Steven Edwards)

Four months ago I obtained an unlisted telephone number by New England Telephone as part of the service for a new residence. I was told at the time that this number had not seen recent use and was not assigned to anyone else, nor was it present in the NET telephone directories or from NET directory assistance (555-1212). There was a fairly hefty tariff associated with installation (about US\$50, just for a software entry; all hardware was in place). There was also a cost of about US\$25 for a service request for getting an unpublished and unlisted number, along with a monthly tariff of about US\$4 for the same. These expenses were justified at the time by an NET service representative as being necessary for "the high level of service traditionally supplied by New England Telephone".

The number was to be used mostly for automated computer telecommunications, so I had no desire for unwanted incoming voice calls. After noting some problems with the computer connection over the first three months' usage, I installed a voice answering machine and recorder on the line. I set the outgoing tape to answer with the complete telephone number dialed so wrong number dialers would realize their mistake. Much to my surprise, I would come home after work and find a number of calls for people I did not know from people I did not know. Furthermore, a number of these calls surprisingly contained rather intimate details of people's business and private lives. The callers obviously thought they were dealing the correct number because of the outgoing message.

I had been unable to track the origin of these calls until yesterday

evening, as most of the callers thought that the party they were trying to call knew their return phone number. Finally, one caller did leave her return number (she was not at her regular number, I suppose). I contacted her and was able to get the correct spelling of the name of whom she thought she called. I was also told that she had gotten the number from NET directory assistance.

A quick check of the new 1991-1992 Nynex White Pages phone book for my area found my "unlisted" number listed on page 164 under another person's name! Another entry with the same last name, but different first name, was located. Furthermore, a call to directory assistance proved that their computer was still supplying this false information. It took a nearly thirty minute long conversation with three different people at NET directory assistance to convince them that they were giving out false information. Because of my knowledge of the first names referenced in messages left on my recorder (along with other information inadvertently recorded), I correctly guessed that this was a husband and wife living at different addresses and they had recently moved into a single residence. I called the other (correct) number and confirmed that this was all a result of a big screw-up by NET. I also took the opportunity to relate several of the topics referenced in the supposed confidential calls. The intended recipients were quite surprised, to say the least. Fortunately for them, I am not a crook; however, if it had been a crook that had their old phone number, the opportunities for fraud may have been too tempting to resist.

First moral of the story: if you ask for an unlisted number, don't assume that you'll get one that was not very recently in use by another party.

Second moral of the story: if you change residences, make sure that your old listing is deleted by the directory provider and is correctly handled by directory assistance.

Third moral of the story: never leave personal or otherwise confidential information on a recording answering machine unless you are absolutely certain that only the intended receiver will replay such recordings.

Steven J. Edwards, Bull HN Information Systems Inc., 300 Concord Road  
Billerica, MA 01821 (508) 294-3484

---

** You can help build the National Public Network. Here's how.**

*Gerard Van der Leun <van@eff.org>  
Tue, 12 Nov 1991 21:24:58 -0500*

THE NATIONAL PUBLIC NETWORK BEGINS NOW. YOU CAN HELP BUILD IT.

Telecommunications in the United States is at a crossroads. With the Regional Bell Operating Companies now free to provide content, the shape of the information networking is about to be irrevocably altered. But will that network be the open, accessible, affordable network that the American public needs? You can help decide this question.

The Electronic Frontier Foundation recently presented a plan to Congress

calling for the immediate deployment of a national network based on existing ISDN technology, accessible to anyone with a telephone connection, and priced like local voice service. We believe deployment of such a platform will spur the development of innovative new information services, and maximize freedom, competitiveness, and civil liberties throughout the nation.

The EFF is testifying before Congress and the FCC; making presentations to public utility commissions from Massachusetts to California; and meeting with representatives from telephone companies, publishers, consumer advocates, and other stakeholders in the telecommunications policy debate.

The EFF believes that participants on the Internet, as pioneers on the electronic frontier, need to have their voices heard at this critical moment.

To automatically receive a description of the platform and details, send mail to [archive-server@eff.org](mailto:archive-server@eff.org), with the following line:

send documents open-platform-overview

or send mail to [eff@eff.org](mailto:eff@eff.org).

---

## **Call for Papers - Fifth Annual Computer Virus & Security Conference**

*Jack Holleran <[Holleran@DOCKMASTER.NCSC.MIL](mailto:Holleran@DOCKMASTER.NCSC.MIL)>*

*Mon, 11 Nov 91 13:46 EST*

Dates: March 11-13, 1992

Place: Marriott Marquis and Summit Hotel, New York City

### TOPICS of Interest:

- \* Prevention, Detection, and Recovery from Viruses and other Unauthorized Usage
- \* Case studies of mainframe, PC and/or network security
- \* Access control, accountability, audit, data recovery
- \* Surveys or demonstrations of products & techniques
- \* Particulars of LAN, UNIX, cryptology, military use
- \* Computer crime, law, data liability, related contexts
- \* US/International sharing of Research & Techniques

### PAPER Submission requirements:

A submission may take the format of *\*EITHER\** a long abstract (3-5 double spaced pages) *\*OR\** a draft final paper. Final papers will usually be 6-20 pages in length. Four copies of the submission should be sent via regular Government Postal Service to the follow address:

Program Chairman  
Computer VIRUS & SECURITY Conference  
NYU, DPMA Fin. Ind. Ch.  
609 West 114th Street  
New York, New York 10025

The submission should be received by December 16, 1991.

Please include a small photo and introductory biography not exceeding 50 words. Successful submitters or co-authors are expected to present in person. Presenters receive the Proceedings.

**PAPER FORMAT:**

Typed double spaced, with last name/page# below bottom line (may be handwritten), brief (to 200 words) abstract following four centered heading lines: TITLE (Caps); Name; Position Affiliation; Telephone, City/State/Zip/Country, Electronic mail address (optional).

**NOTIFICATION:**

Written (and where practicable) telephoned conformation will be initiated by Monday, January 27, 1992, to facilitate low cost travel. Those needing earlier confirmation should submit papers sooner and attach a note to this effect. You may be asked to perform specific revisions to be accepted. Nobody can guarantee you a place without an acceptable paper.

**CONFERENCE:** There are five tracks. Don't hesitate to submit a presentation given elsewhere to a more specialized audience. Most of our attendees will find it new, interesting, and necessary.

**SPONSOR:** DPMA Financial Industries Chapter in cooperation with ACM-SICSAC & IEEE-CS & ICCP



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 12: Issue 63

Weds 14 November 1991

## Contents

- [Copy of Letter to NIST in response to proposed DSS](#)  
[Martin Hellman](#)
- [Antivirus software vendor creates viruses](#)  
[Richard Kulawiec](#)
- [I DEMAND AN APOLOGY FOR THIS LIBEL!](#)  
[W. K. Gorman](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Copy of Letter to NIST in response to proposed DSS

*Martin Hellman <hellman@isl.stanford.edu>*  
*Wed, 13 Nov 91 12:24:11 PST*

Martin E. Hellman  
Professor of Electrical Engineering  
Stanford University  
Stanford, CA 94305-4055  
(415) 723-4002 (tel) 723-8473 (fax)  
November 12, 1991

Mr. James H. Burrows, Director  
Computer Systems Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899

Dear Mr. Burrows:

I am responding to your request for comments on the "Proposed Digital Signature Standard," published in the Federal Register on August 30, 1991. My detailed comments are attached on the following pages, but I can summarize by saying that I am deeply concerned by faults in the technical specifications of the proposed DSS and by its development process.

NIST has lost considerable credibility with the non-military cryptographic

research community and, unless the revision process of DSS is carried out in a much more rapid and open fashion, NIST is likely to become totally ineffective in the setting of cryptographic standards. That would be a grave loss to both NIST and the nation, so I hope change is possible.

I look forward to seeing your response to these concerns.

Sincerely,  
Martin E. Hellman  
Professor of Electrical Engineering

cc: Congressman Tom Campbell  
Senator Alan Cranston  
Senator John Danforth  
Congressman John Dingell  
Senator Patrick Leahy  
Congresswoman Constance Morella  
Senator John Seymour  
Congressman Tim Valentine

-----

1. DSS DOES NOT INCLUDE KEY EXCHANGE. Public-key cryptography provides two advantages over conventional cryptography:

Key Exchange: the ability for users to communicate privately without fear of being overheard, and without using couriers, registered mail, or similar means for prearrangement of a secret key.

Digital Signatures: the ability to sign messages which are easily checked by anyone, yet which cannot be forged or modified, even by the intended recipient.

The DSS addresses only the second of these two needs. Until a key exchange standard is developed, users who follow the standard will be at a severe disadvantage in terms of the privacy of their communications. It would have been a simple matter for NIST to include a key exchange standard with the DSS, either by adopting the RSA system [1] for both operations or by specifying the Diffie-Hellman key exchange system [2] as the key exchange standard to be used with the current DSS. (The Diffie-Hellman system is the natural key exchange choice if the proposed DSS is used for digital signatures. The DSS is derived from the Diffie-Hellman system.) Because of its early publication (1976), the Diffie-Hellman system possesses a high degree of confidence as to its security level as discussed under #4 below.

2. THE KEY SIZE IS TOO SHORT. The proposed DSS is restricted to a 512 bit modulus or key size. It is generally accepted in the cryptographic research community that this is too short for a system such as DSS, which is based on discrete logarithms and which requires a long life. To quote from a recent paper by LaMacchia and Odlyzko [3] written prior to the announcement of DSS "even 512-bit primes [key size] appear to offer only marginal security." This is such a well established viewpoint that further explanation seems

unnecessary. While there should be lower limits on the key size to ensure a reasonable level of security, there is no reason for an upper limit. If, in spite of this argument, NIST keeps an upper limit, it should be increased to at least 1024 bits.

The proposed DSS also limits the "subkey" size 160 bits, a value that is again too short. [4] Using the ideas in my paper with Pohlig [5], it is possible to recover a user's secret key  $x$  from his public key  $y$  in  $2^{80}$  operations by using  $2^{80}$  words of memory. (Any other breakdown can be used so long as the time memory product is  $2^{160}$ , for example  $2^{100}$  operations and  $2^{60}$  words of memory.) While such a computation is currently infeasible, it is closer to possibility than seems comfortable considering probable advances in technology and improvements in algorithms. The particular cryptanalytic problem involved in breaking the DSS has not been well studied (see #4 below), making such improvements highly probable. As with the 512-bit modulus, the subkey length should not have an upper bound. Or, if NIST insists on keeping an upper bound, it needs to be at least double, and preferably, quadruple the current 160-bit value.

3. NIST DOES NOT PROVIDE ADEQUATE WARNING ON THE DANGER OF USING DSS AS A COMMON MODULUS SYSTEM. While common modulus systems have an advantage in speed of key generation, they allow a successful attack on one user's secret key to be extended to all users of the common modulus. Using a common modulus is analogous to having all personnel within an organization use combination locks with ten digit combinations, but with the first nine digits being common to all users. This simplifies setting the combination of a lock, but allows an opponent to amortize the cost of an attack on one lock over the large number of locks that are then easily picked.

While DSS need not be used in common modulus mode and there are some applications where that mode is desirable, clear warnings are needed about reduced security in common modulus mode. The proposed DSS says that the modulus "can be common to a group of users" without any mention of the attendant danger.

Use of a common modulus would be of less concern if the key and subkey sizes of DSS were increased as suggested in #2 above.

4. DSS IS BASED ON A SYSTEM WHICH HAS HAD LIMITED TIME FOR APPRAISAL. Cryptography is still more an art than a science. For most systems, including all digital signature systems, proofs of security are currently impossible. Rather, we rely on concerted attacks by "friendly opponents" intent on fame, rather than thievery, if they are successful in breaking the system. We become more confident of the security of a system as it is subjected to widespread public scrutiny for long periods of time.

The DSS is based on Schnorr's variant [6] (published 1990) of the ElGamal signature scheme [7] (published 1985). There has thus been little time to gain confidence in Schnorr's variation. ElGamal's system, while older, is still only half the age of its primary competition as a digital signature standard, the RSA system [8] (published 1978).

Unless Schnorr's scheme possesses some major advantage compared to RSA, it is strange that Schnorr's scheme was selected as the standard. I am aware of no such major advantage of Schnorr over RSA. The only advantage I see is that Schnorr's signatures are somewhat shorter (320 bits versus 512 bits for a comparable security RSA using today's best known algorithms). On the other hand, in addition to possessing a higher confidence level as regards its security, RSA has a major advantage over Schnorr: Using RSA would automatically have provided for public key exchange, a critical part of the public-key standard that NIST has not yet developed (see #1 above).

5. NIST HAS IGNORED THE DANGER OF PROBABLE IMPROVEMENTS IN CRYPTANALYTIC ALGORITHMS. Cryptanalyzing the DSS is a special case of computing a discrete logarithm. The history of this problem, as well as the closely related problem of factoring, shows a slow but steady improvement. It was only about fifteen years ago that the subexponential nature of the problem was realized. Prior to that time, estimates of the effort required to break DSS with a 128-bit key would have been beyond the realm of reasonability, while today, even a 256-bit key would be insecure.

Improvements over the last fifteen years in finding discrete logarithms have effectively cut key sizes by a factor of four. Should that happen again over the next fifteen years, the DSS would be totally insecure. For similar reasons, I have always advocated at least a factor of two, and preferably a factor of four, as a safety margin. The proposed DSS imprudently has little or no safety margin.

The danger is increased because of recent advances. Until two years ago, all subexponential algorithms for discrete logarithms and for factoring took time of the form  $\exp[k \ln(n)^{1/2} (\ln \ln(n))^{1/2}]$  with  $k=1$  as the best value. Recently, number field sieves have been proposed that solve both problems in time  $\exp[k \ln^{1/3}(n) (\ln \ln(n))^{2/3}]$  with  $k$  approximately equal to 2. While the higher value of  $k$  makes the new algorithm no better for 512-bit keys ( $1E20$  operations versus  $7E19$  operations for the earlier algorithms), it is probable that the value of  $k$  will be reduced as attention becomes focussed on number field sieves.

Over the last fifteen years, algorithms requiring  $\exp[k \text{SQRT}(\ln(n) \ln \ln(n))]$  operations have been improved from  $k=2$  to  $k=1$ . It would be prudent to assume similar advances in number field sieves, in which case breaking the DSS would become trivial, requiring only  $1.0E10$  operations, a computation that can be done on a personal computer.

6. NIST HAS MISSTATED PATENT LICENSING REQUIREMENTS. Raymond G. Kammer, Deputy Director of NIST, has stated that "the digital signature standard is expected to be available on a royalty-free basis in the public interest world-wide." [8] Yet at least two privately owned US patents cover the DSS (#4,200,770 and #4,218,582).

I understand that Schnorr is claiming that his patent (#4,995,082) is also needed to practice the DSS. If Schnorr's claim holds, then the DSS has a patent disadvantage compared to either RSA or ElGamal/Diffie-Hellman since the United

States Government has the right to use the latter systems on a royalty-free basis, but I doubt that it has rights to Schnorr's work. (Clarification from NIST would be appreciated.)

7. NIST HAS CONFUSED THE ISSUE OF SPEED COMPARISONS. In his above referenced statement, Mr. Kammer, also stated that

... the digital signature technique [DSS] provides for a less computational-intensive signing function than verification function. This matches up well with anticipated Federal uses of the standard. The signing function is expected to be performed in a relatively computationally modest environment such as with smart cards. The verification process, however, is expected to be implemented in a computationally rich environment such as on mainframe systems or super-minicomputers.

Under the environment specified by Mr. Kammer, the DSS would have an advantage over RSA, the primary competing technique. However, as a universal standard, the DSS will often be used in complementary environments where signing is done in a computationally-intensive environment and verification in a computationally modest environment. A good example is the use of digital signatures generated by a bank and checked by a customer on his or her home computer. This environment would favor "small exponent" RSA systems which allow verification to be performed with approximately one percent of the total signing effort of DSS (including precomputation).

Rather than claim an advantage for DSS or RSA in a particular environment, I believe that the best standard is the one which is usable in the greatest number of environments envisioned for its use. That approach leads to the most widely applicable standard. On that basis, ElGamal or Schnorr's signature scheme is approximately equal to RSA. Hence, none of the competing systems should be deemed to have a speed advantage over the others.

8. THE ADOPTION PROCESS APPEARS TO HAVE BEEN CONDUCTED IN SECRET. Although listed last, this is the most important change since a more open adoption process would have avoided most of the above shortcomings in DSS.

I am not aware of any attempts on NIST's part to involve researchers in academia and industry. (If there were such attempts, I hope NIST will make these a matter of public record.) Rather, NIST appears to have worked in secret with only NSA providing advice. This is dangerous because much of NSA's legally mandated mission involves foreign espionage which would be hampered by secure public encryption. As with any organization or individual, NSA is likely to put greater emphasis on its concerns than would a neutral third party.

There is an unavoidable tradeoff in that providing a high level of communications security to American business and citizens also makes this protection available to our foreign adversaries. NIST's actions give strong indications of favoring protection of NSA's espionage mission at the expense of American business and individual privacy. While an impartial working group might conclude that such a policy was in the nation's best interests, relying solely on NSA for advice is unlikely to produce an optimal tradeoff for the

nation as a whole.

1. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, pp 120-126, 1978.
2. W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. IT-22, pp 472-492, 1976.
3. B. A. LaMacchia and A. M. Odlyzko, "Computation of Discrete Logarithms in Prime Fields," Design, Codes, and Cryptography, vol. 1, pp 47-62, 1991.
4. I am indebted to Prof. Leonard Adleman of USC for pointing this out.
5. S. C. Pohlig and M. E. Hellman, An Improved Algorithm for Computing Logarithms Over GF(p) and Its Cryptographic Significance, IEEE Transactions on Information Theory, vol. IT-24, pp 106-110, 1978.
6. C. P. Schnorr, "Efficient identification and signatures for smart cards," Advances in Cryptology: Proceedings of Crypto '89, (Giles Brassard editor), Lecture Notes in Computer Science 435, New York: Springer-Verlag, pp. 239-251.
7. Taher ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. IT-31, pp 469-472, 1985.
8. June 27, 1991 statement before the Subcommittee on Technology and Competitiveness of the Committee on Science, Space and Technology of the House of Representatives.

[This letter duplicates some of the material in Ron Rivest's letter to NIST which was included in [RISKS-12.57](#) and the correction in [RISKS-12.58](#). However, there is some new knowledge here regarding subkey size, patent rights, etc. It also serves as a reminder that the OFFICIAL DEADLINE for responses to NIST is basically before Thanksgiving (90 days from 30 August) for comments that will be officially recorded and acknowledged. I was told that as of recently NIST had received ONLY TWO RESPONSES, and they were both POSITIVE. You are encouraged to write NIST if you have an opinion on DSS. PGN]

---

### **✶ Antivirus software vendor creates viruses**

*Richard Kulawiec <rsk@gynko.circ.upenn.edu>  
Wed, 13 Nov 91 09:54:22 EST*

[Page 59 of the November 1991 "Sun Observer", in the "New Products" section]

Vfind locates viruses on Unix, Mac, DOS systems.  
Sun-3, Sparcstations (Software)

Cybersoft has released its first Unix product, Vfind.

Vfind is a scanner that executes directly on the Unix system and helps detect viruses on Unix computers which have problems with malicious computer programs related to viruses.

Although many people do not believe that computer viruses are a direct problem to Unix systems, CyberSoft has developed, under quarantine, a Unix virus in an effort to help the company anticipate the types of viruses that may appear in the future, Pete Radatti, a compure representative, said.

Unix computers also can act as carriers for MS-DOS and Apple Macintosh viruses creating the Typhoid Mary syndrome. DOS and Mac systems connected to the same LAN as Unix computers can be reinfected continuously by the Unix systems where the viruses are undetected.

---end excerpt--

While Unix-based viruses have been developed before (Tom Duff of Bell Labs engineered a virus that propagates via executable binaries; numerous authors have demonstrated simple viruses that propagate via shell scripts) I found this report curious for two reasons:

1. The tactic of developing variations of hostile organisms in an attempt to better understand them (and thus more effectively eradicate them) is well-known in the biological and medical research communities. However, normal research practice includes a great deal of peer review, especially with respect to the quarantine procedures. The idea, of course, is to ensure that organisms more hostile than those found in the environment do not escape; the peer review process provides some measure of assurance to the public that reasonable precautions have been taken in this regard. Should a similar practice be adopted for those researchers creating and studying computer viruses and worms?

2. I find it curious that such an anti-virus product has been developed for the Unix market, where security problems due to viruses are much rarer than security problems due to poor password selection, incorrect permission modes on files, sendmail bugs, setuid programs, etc. One of the many risks that crossed my mind was that users coming from the PC/Mac worlds might be tempted to spend \$7500 (cost of the package described above) and then conclude that their systems are reasonably secure -- even though the security area they've dealt with is not one of the prime areas of concern for those working with Unix. (In fact, I would recommend instead that Unix admins spend \$30 or so on either of the excellent Unix security books by Curry (Addison-Wesley) or Garfinkel/Spafford (O'Reilly), and avail themselves of some of the freely available software, such as John F. Haugh II's "shadow", Alec Muffett's "crack", or Dan Klein's "cops".)

Rich Kulawiec rsk@gynko.circ.upenn.edu Cardiothoracic Imaging Research Center

---

**✂ I DEMAND AN APOLOGY FOR THIS LIBEL!**

"W. K. Gorman" <34AEJ7D@cmuvm.bitnet>  
Fri, 8 Nov 91 15:30:16 CST

[This is a copy of letter to: <gray@s5000.rsvl.uisys.com> from W.K. Gorman.]

Sir:

In your UNSIGNED post in [RISKS-12.62](#) you utter and publish a number of spurious, gratuitous libels against myself with publicly presented, false and malicious accusations of "lying", "bias", "yellow journalism", and "smear" tactics on my part.

You also libel the Safeway food store chain itself with your unsubstantiated, scattergun insinuations of "profiteering" on their part.

You libel The Church of Jesus Christ of Latter Day Saints (Mormon) by inferring that some irregularity attaches, or might attach, to their legitimate ownership of a business, whether in whole, in part or as a controlling interest.

You compound your libel by accusing me of lying, seeking to justify your tactics with the irrelevant assertion that Safeway is "publicly traded", together with a fragment of their price history.

You in no way indicate that you are privy to any list of shareholders, nor do you seek to justify your libel with facts in any form. Instead, you deliberately gloss over the fact that any business corporation may be publicly traded, yet the aggregate of all shares available for public trading may nonetheless constitute a minority, (that is, a NON-controlling) interest in that business. Since you claim to have called a stockbroker to obtain information, in the absence of evidence to the contrary I must presume that your failure to point out this fact was deliberate.

You have taken my purely informational post, which contained no pejorative or derogatory information whatsoever, and transformed it into a vehicle from which to launch a libelous electronic vendetta against me.

Having done all this, you have then presumed to make our moderator (PGN) accomplice to your actions by publicly "chiding" him for not censoring this post in accordance with your notions, then managing to convince him to let your vicious personal attack slip through unedited.

It was obviously your intent to commit libel against me by the manner in which you sent this post. It was unsigned. It was not sent privately as a criticism to myself, but was deliberately and maliciously uttered and published in a public forum in what seems only capable of interpretation as a preconceived, premeditated attempt at libel directed against me.

Now quite simply, you have managed to demonstrate nothing beyond your ability to generate needless flames on an already crowded network. Your claims and allegations against me are false and libelous in their entirety.

To put in bluntly:

I DEMAND A PUBLIC APOLOGY AND RETRACTION, SINCE YOU CHOSE TO MAKE THIS LIBEL A PUBLIC AFFAIR IN THE FIRST PLACE!

Signed: W. K. Gorman <34AEJ7D@CMUVM.BITNET>

[Here is part of WKG's justification TO ME as to why I should permit this strangely escalating sequence to continue:

"Having published my original note, which contained NO pejorative or derogatory information whatsoever, you then specifically chose to publish the libelous comments \*deliberately directed against me, personally\* by <gray@s5000.rsvl.unisys.com>. You cannot be an on-again, off-again moderator. If, as you now claim to think, my initial posting was unacceptable then so was the one from <gray@s5000.rsvl.unisys.com>." ...  
W.K. Gorman

YES. They are both unacceptable \*per se\*, but having let the first one through, it somehow seems necessary to let the response through. Clearly there are great risks in publishing such discourses. Anyway, I already stated in [RISKS-12.62](#) that I am sorry that I did not yank "Mormon-owned", which would have avoided the whole mess. By allowing this message through it may escalate still further. That is one of the risks of imMODERATION. But WKG's message seems to be justified -- even if it is itself possibly a defensive overreaction -- under the circumstances.

I need to note that I had absolutely no intention of libelling WKG.  
I hesitate to add that WKG's original note was also UNSIGNED. I wish all of you -- and especially BITNET folks -- would at least sign your EMail! 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 12: Issue 64**

**Friday 15 November 1991**

## Contents

- [MCI's Response for RISKS](#)  
[Sally McCaffrey](#)
- [Computer-assisted trading](#)  
[Brendan Kehoe](#)
- [Risks of truncation in the stock market](#)  
[Frank G Kienast](#)
- [gray vs gorman](#)  
[Fred Gilham](#)
- [ACM SIGSOFT'91: SOFTWARE FOR CRITICAL SYSTEMS](#)  
[Peter G. Neumann](#)
- [5th Refinement Workshop: Theory and Practice of Formal Software Development](#)  
[Cliff B Jones](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **MCI's Response for RISKS**

SALLY McCAFFREY <0004568823@mcimail.com>  
Thu, 14 Nov 91 22:20 GMT

MCI Telecommunications Corporation  
Consumer Relations  
Consumer Markets  
1200 South Hayes Street  
Arlington, Virginia 22202  
(703) 425-6000

November 13, 1991

In response to the piece posted by Brian R. Krause on your [inter]national bulletin board, RISKS Forum, titled "MCI Friends & Family & anyone else with a touch-tone phone" on October 23, 1991, MCI wishes to post the following information.

MCI is aware and sensitive to privacy concerns of its Friends & Family

customers.

Additionally, MCI is aware of the isolated incident where its Friends & Family voice response unit (VRU) Update Line was abused. MCI has made -- effective November 7 -- the access more private by altering the VRU access procedures.

In order to acquire information about a Friends & Family Calling Circle, customers have two options depending on the information they want.

Option 1: Enter the last three digits of your MCI account number to receive the status of all Calling Circle members.

Option 2: Enter an individual Circle member's 10-digit phone number to learn the status of that individual.

We hope this explanation addresses any concerns that may have arisen as a result of the "RISKS" posting.

Karen Heyison, Manager, Consumer Relations

---

### **computer-assisted trading**

*Brendan Kehoe <brendan@cs.widener.edu>  
Sat, 16 Nov 1991 12:49:28 -0500*

Yesterday's sudden fall in the stock market brought to light a serious Achilles heel in the way our country's economy is growing. As panic hit more and more traders, the faint clatter of computer keyboards added to the fray -- virtual stocks were being virtually sold at an amazing pace.

It was less of a concern in the 1989 crash, but now we should be even more aware of the effect computer-assisted trading can have on the market. Inside of ten minutes, millions of shares can be unloaded very quietly.

The securities industry can only grow faster in the coming years; if it doesn't build some cushions to avoid massive "anonymous" selling, it may be in for an even more serious down-turn.

Brendan Kehoe, Sun Network Manager, Widener University, Chester, PA

---

### **Risks of truncation in the stock market**

*Frank G Kienast <well!fgk@well.sf.ca.us>  
14 Nov 91 01:50:26 GMT*

In their stock statistics sections, Prodigy has a 14-character maximum length for the company name. Apparently, they just chop off any remaining characters. This morning, I was surprised to see the following stock among the ten listed under yesterdays "NYSE Biggest Percent Gainers":

STOCK	LAST	CHANGE	PCT CHG
-------	------	--------	---------

ELECTRONIC ASS 2 3/8 + 1/4 11.76

(I think this is supposed to be Electronic Associates, ticker EA).

Well: well!fgk@ucbvax.Berkeley.EDU CIS: 73327,3073 V-mail: 804-980-3733

---

**✉ gray vs. gorman (RISKS-12.61-63)**

*Fred Gilham <gilham@csl.sri.com>*

*Fri, 15 Nov 91 06:39:40 -0800*

I've completely lost track of what's going on with the gray vs. gorman "discussion". I hope you'll put something in the next Risks saying that further communications on the issue will be conducted through the lawyers of the parties involved or something to that effect, something that leaves RISKS out of it!

P.S. I'm sure this is an example of the risk of computer communication -- most people would post things they wouldn't say to another person standing next to them.

---

**✉ gray vs. gorman (RISKS-12.61-63)**

*Peter G. Neumann <neumann@CSL.SRI.COM>*

*Sat, 16 Nov 91 14:14:26 PDT*

I greatly appreciated all the supporting mail I received on this topic. I try very hard to keep RISKS consistent with the self-imposed standards of being OBJECTIVE, INTERESTING, PROVOCATIVE, THOUGHTFUL, in GOOD TASTE, and, above all, INFORMATIVE. I certainly learned something from both antagonists, and about them. Whether or not that was RISKS-RELEVANT or not, I believe that once something unfortunate has slipped through, it becomes necessary to set the record straight. But in keeping with the current efforts to raise the standards (again) in the continuing epicyclicity of RISKS, there are likely to be fewer mundanities for a while. Thanks again to all of you for your continuing contributions, including those that do NOT get included. Sorry, I cannot respond to everything. So, if you think I missed a GOOD ONE, PLEASE poke me; I probably did miss it, especially if the Subject: line was nonspecific. PGN]

---

**✉ ACM SIGSOFT'91: SOFTWARE FOR CRITICAL SYSTEMS**

*Peter G. Neumann <neumann@CSL.SRI.COM>*

*Sat, 16 Nov 91 14:12:16 PDT*

[I will have very limited net access for the next few weeks, and would like to post one more reminder for SIGSOFT '91 before it happens. Registration is coming along very nicely, and hotel space is starting to fill up, so those of you wishing to register might want to do so soon. Please contact

Judith Burgess for further details:

Registration and Coordination: Judith Burgess, SRI International  
burgess@csl.sri.com phone: (415) 859-5924, FAX (415) 859-2844  
Thanks. PGN]

4-6 December 1991  
Fairmont Hotel, New Orleans

WEDNESDAY, 4 DECEMBER 1991

Welcome and Introduction: 8:45am - 9:00

Mark Moriconi, SIGSOFT '91 Chair (SRI International)  
Peter G. Neumann, Program Co-chair (SRI International)

Session 1: 9:00 - 10:15, Carl Landwehr, Chair

Formal Verification of Algorithms for Critical Systems  
John Rushby (SRI International), Friedrich von Henke (University of Ulm)

State-Based Model Checking of Event-Driven System Requirements  
Joanne M. Atlee and John Gannon (University of Maryland)

Open Discussion

Session 2: 10:45 - 12:30, Dines Bjørner, Chair

Rigorous Development Using RAISE  
Bent Dandanell (CRI, Birkerød, Denmark)

Specifying and Verifying Requirements of Real-Time Systems  
K.M. Hansen, A.P. Ravn, and Hans Rischel (Tech. University of Denmark)

A Systematic Kernel Development  
J.F. Sjøgaard-Andersen, C.O. Rump and H.H. Lovengreen (Tech. Univ. Denmark)

Open Discussion

Session 3: 2:00 - 3:45, John Rushby, Chair

The Infeasibility of Experimental Quantification of Life-Critical  
Software Reliability  
Ricky Butler and George Finelli (NASA Langley Research Center)

PANEL: The Limits of Probabilistic Risk Assessment

Bev Littlewood (City University, London)  
David Parnas (McMaster University)  
Martyn Thomas (Praxis, Ltd)  
Ricky Butler (NASA Langley Research Center)  
John Musa (AT&T Bell Labs, Whippany, NJ)

The Butler/Finelli paper argues that ultra-high reliability cannot be validated directly from testing, nor can it be demonstrated by appeals to software fault-tolerance. What progress might we reasonably expect

to make toward numerical risk assessment of life-critical software?

Session 4: 4:15 - 5:30, Martyn Thomas, Chair

PANEL: The Confused World of Standards for Critical Software

Martyn Thomas (Praxis, Ltd)  
Peter Neumann (SRI International)  
Mike DeWalt (FAA)

This session will explain and assess current government regulation such as British MoD DEFence STANdard 00-55/56 and various security criteria (e.g., U.S. TCSEC, European ITSEC, Canadian CTCPEC). What role should such standards play? What should be mandated?

THURSDAY, 5 DECEMBER 1991

Session 5: 9:00am - 10:30

Comparing Fault Detecting Ability of Testing Methods  
P.G. Frankl (Polytechnic University), E.J. Weyuker (NYU Courant Institute)

An Exception Handling Model For Parallel Programming and its Verification  
Valerie Issarny (IRISA/INRIA)

Open Discussion

Session 6: 11:00 - 12:30

INVITED TALK: Human Error in Design  
Henry Petroski (Duke University)  
Author of the widely-acclaimed books "To Engineer is Human: The Role of Failure in Successful Design" and "Pencil"

Session 7: 2:00 - 3:30, Victoria Stavridou, Chair

A Real-Time Transition Model for Analyzing Behavioral Compatibility of Telecommunications Services  
E.J. Cameron and Y-J Lin (Bellcore)

Programming and Verifying Critical Systems by Means of the Synchronous Data-Flow Language LUSTRE  
C. Ratel (Merlin-Gerin), N. Halbwachs and P. Raymond (IMAG/LGI)

Open Discussion

Session 8: 3:45 - 5:30, Mark Moriconi, Chair

Invited Presentations on Practical Experiences:

Validation of Critical Flight Controls  
Jim McWha (Chief Engineer in charge of 777 Flight Controls, Boeing)

Reliable Software for the 4 ESS Switch  
Michael Meyers (AT&T Bell Labs)

A Case Study of the THERAC-25 Accidents  
Nancy Leveson (U.C. Irvine)

Session 9: 8:00pm - 9:30pm, Evening Poster Session

FRIDAY, 6 DECEMBER 1991

Session 10: 8:30am - 10:30, Hermann Kopetz, Chair

Stepwise Design of Real-Time Systems  
Reino Kurki-Suonio (University of Technology, Tampere)

On Satisfying Timing Constraints in Hard-Real-Time Systems  
Jia Xu (York University) and David Parnas (McMaster University)

Automated Analysis of Bounded Response Time for Two NASA Expert Systems  
C-K Wang, R-H Wang, D-C Tsou, J.C. Browne, and A.K. Mok (University of Texas, Austin)

Open Discussion

Session 11: 11:00 - 12:30

PANEL: Future Directions, Nancy Leveson, Chair

Adjournment at 12:30

=====

AIR TRANSPORTATION. Delta Airlines is offering 40% off RT Coach fares within the U.S., 35% Canada, 5% off already discounted fares. Call 1-800-221-1212, ask for Special Meeting Network, refer to file ref no. V18006. Valid for travel from Nov. 30 to Dec. 10. 7-day advance purchase required.

=====

ADVANCE REGISTRATION FORM

SIGSOFT '91 -- Software for Critical Systems  
Fairmont Hotel, New Orleans, Dec. 4 -- 6, 1991

Name \_\_\_\_\_

Affiliation \_\_\_\_\_

Address \_\_\_\_\_

City, State and Zip \_\_\_\_\_

Phone (and FAX) \_\_\_\_\_

Email address \_\_\_\_\_

ACM or SIGSOFT Membership No. \_\_\_\_\_

Registration Fees

Category

-----

ACM or SIGSOFT Member \$330  
Non-Member \$380  
Full-time Student \$230

To pay by credit card, circle one: AMEX VISA MC

Name on card \_\_\_\_\_

Card number \_\_\_\_\_ Exp. date \_\_\_\_\_

Signature \_\_\_\_\_

Make checks payable to SIGSOFT '91 in U.S. dollars. Fees include 3 continental breakfasts, 2 lunches, and the Proceedings.

Dietary requests: Vegetarian \_\_\_\_\_ Kosher \_\_\_\_\_

SEND THIS FORM WITH FULL PAYMENT TO:

Judith Burgess / EL266, SRI International, 333 Ravenswood Ave.,  
Menlo Park, CA 94025, USA

For further information, contact Judith Burgess,  
telephone: (415) 859-5924, FAX (415) 859-2844, EMail burgess@csl.sri.com

NOTE: REGISTRATION BY EMAIL OR FAX IS ALSO PERMITTED (ONLY WITH CREDIT CARD).

=====

FAIRMONT HOTEL RESERVATION FORM  
SIGSOFT '91 -- Software for Critical Systems  
New Orleans, Dec. 4 -- 6, 1991

Name \_\_\_\_\_

Affiliation \_\_\_\_\_

Address \_\_\_\_\_

City, State and Zip \_\_\_\_\_

Phone (and FAX) \_\_\_\_\_

Date/Time of Arrival \_\_\_\_\_

Date/Time of Departure \_\_\_\_\_

Room Rates (subject to taxes):

Circle one: Single \$99 Double/Twin \$119

RESERVATIONS: 1-800-527-4727 or 1-504-529-7111

To guarantee your reservation by credit card:

Circle one: AMEX MC Visa Carte Blanche Diners Club

Name on card \_\_\_\_\_

Card number \_\_\_\_\_ Exp. date \_\_\_\_\_

Signature \_\_\_\_\_

These rates apply from Nov. 29 through Dec. 8, subject to availability.

Reservations should be received 30 days in advance to ensure availability, but later reservations will be accepted as possible. A deposit for the first night must accompany your reservation to guarantee it for arrival after 6:00pm. Cancellations must be made 24 hours in advance.

SEND THIS FORM TO:

The Fairmont Hotel, University Place, New Orleans, LA 70140, USA

=====

General Chair: Mark Moriconi, SRI International

Program Co-Chairs: Peter Neumann, SRI International

Nancy Leveson, Univ. of California, Irvine

Travel Arrangements: Johnette Hassell, Tulane University

Registration and Coordination: Judith Burgess, SRI International

burgess@csl.sri.com phone: (415) 859-5924, FAX (415) 859-2844

Program Committee:

David Barstow (Schlumberger)

Dines Bjorner (Technical University of Denmark)

Marie-Claude Gaudel (Universite de Paris - Sud)

Jim Horning (DEC Systems Research Center, Palo Alto)

Bill Howden (University of California, San Diego)

Hermann Kopetz (Technical University of Vienna)

Carl Landwehr (Naval Research Laboratory)

Bev Littlewood (City University, London)

Leon Osterweil (University of California, Irvine)

David Parnas (McMaster University, Canada)

Fred Schneider (Cornell University)

Vicky Stavridou (University of London)

Martyn Thomas (Praxis, Inc.)

Walter Tichy (University of Karlsruhe)

Elaine Weyuker (NYU Courant Institute)

---

**✂ 5th Refinement Wkshp: Theory and Practice of Formal Software Developmnt**

*Cliff B Jones <cliff@computer-science.manchester.ac.uk>*

*Fri, 15 Nov 91 16:35:15 GMT*

BCS FACS

Fifth Refinement Workshop

Theory and Practice of Formal Software Development

8 - 10th January 1992

LONDON, UK

Sponsored by Lloyd's Register, Program Validation Ltd and the DTI

The workshop theme is Refinement: the systematic decomposition of formal specifications into designs which are functionally correct or implement important properties such as safety or information security.

VENUE: Lloyd's Register of Shipping, 71, Fenchurch Street, London EC3

INVITED SPEAKERS: Roger Jones ICL  
 Prof. Robin Milner FRS University of Edinburgh  
 Dr Jose Oliveira University of Minho  
 Dr Jim Woodcock University of Oxford

Registration fees include lunches, intermission refreshments, workshop handouts, full Proceedings published by Springer-Verlag (to be dispatched after the workshop), and a social evening event.

Accommodation costs are not included in the registration fee, but rooms can be booked in student accommodation at the City University which is a short Underground ride or a two mile walk from the Workshop venue. The cost of accommodation and breakfast at the City University is 17 pounds inclusive of VAT.

A limited number of assisted places are available at 60 pounds for bona fide research students. To apply for this please use the registration form and do not enclose the fee yet.

A 10 pound premium is charged for registration not accompanied by a fee, except for those initially applying for an assisted place.

A Tools Exhibition will be held. Potential exhibitors please contact the Publicity Officer.

ORGANISING and TECHNICAL COMMITTEE: Prof. Bernard Carre (Chairman), Prof. Cliff Jones (Translation(Technical Programme)), Roger Shaw (Local Arrangements), Paul Smith (Publicity), Dr. John Cooke, Tim Denvir, Jeremy Jacob.

CHAIRMAN: Prof Bernard Carre	PUBLICITY: Paul Smith
Program Validation Limited	Secure Information Systems Ltd
26 Queen's Terrace	Sentinel House
Southampton	Harvest Crescent
SO1 1BQ	Ancells Park
Tel: +44 (0)703 330001	Fleet
Fax: +44 (0)703 230805	Hampshire
	GU13 8UZ
	Tel: +44 (0)252 811818
	Fax: +44 (0)252 811435

=====

BCS FACS  
 Fifth Refinement Workshop  
 Theory and Practice of Formal Software Development  
 8 - 10th January 1992  
 LONDON, UK

Sponsored by Lloyd's Register, Program Validation Ltd and the DTI

REGISTRATION FORM:

RETURN TO: Roger Shaw  
 Performance Technology

Lloyds Register  
Lloyd's Register House  
29 Wellesley Road  
Croydon  
CRO 2AJ  
Tel: +44 (0)81 681 4848  
Fax: +44 (0)81 681  
Email: tcsrscs@aie.lreg.co.uk

Name: .....

Address: .....

Registration Fee: Enclosed / Please Invoice / Assisted place requested\*

Encircle applicable figure:

	FACS Members	Speakers	Others
Fee Enclosed	125 pounds	125 pounds	140 pounds
Please Invoice	135 pounds	135 pounds	150 pounds

These prices include VAT. Cheques should be made payable to BCS FACS.

Special dietary requirements .....

Tick if accommodation at City University is required: .....

If so circle required dates: 7 8 9 January 1992

(unless otherwise specified, one single room will be reserved)

Tick if you would like a list of local hotels: .....

Any other information you think you will need:.....





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 12: Issue 65

Tuesday 26 November 1991

## Contents

- [Phone outages expected to be tied to typing mistake](#)  
[Rudy Bazelmans/Jim Horning](#)
- [Weather Service Circuit Failure](#)  
[PGN](#)
- [Problems with nuclear plant safety computer in the UK](#)  
[Peter Ilieve](#)
- [Results of Train Accident Investigations](#)  
[Jymmi C. Tseng](#)
- [Bank misdeposits money](#)  
[David Shepherd](#)
- [Mass. Governor wants to sell list of drivers licenses \[Yes and No\]](#)  
[Kent Quirk](#)
- [CPSR FOIAs U.S. Secret Service](#)  
[Craig Neidorf](#)
- [The Trojan Horse named 'AIDS'](#)  
[PGN](#)
- [Banning of autodialers?](#)  
[John Sullivan](#)
- [A new risk for computer folks? -- computers and termination policy](#)  
[Mark Bartelt](#)
- [E911 system brought to it's knees by a prank](#)  
[Glenn S. Tenney](#)
- [Study on Computer Addiction](#)  
[Chris](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Phone outages expected to be tied to typing mistake**

*Jim Horning* <[horning@Pa.dec.com](mailto:horning@Pa.dec.com)>

*Tue, 26 Nov 91 11:00:51 PST*

[Originally forwarded by Rudy Bazelmans to Alan Martin to Bill McKeeman]

DSC Communications - Phone outages expected to be tied to typing mistake

The Wall Street Journal, 25Nov91, p.B4.

A final report that may be presented to the Federal Communications Commission this week is expected to conclude that a mistyped character in software from DSC Communications Corp. resulted in several local-telephone service outages last summer. The report, compiled by Bell Communications Research Corp., also will show that the software didn't cause the failures alone. Faulty data, failure of computer clocks and other triggers led to a chain of events that caused the outages, according to the Dallas Morning News, which said it obtained a copy of the report. The newspaper said the report will conclude that none of the "trigger" events were caused by computer hackers. The disclosure echoes testimony before Congress last July, in which DSC officials admitted that three bits of information in a huge computer program were incorrect, omitting computational procedures that would have stopped DSC's signaling system from becoming congested with messages. A spokesman for DSC, which makes the signal transfer point that carries signals to set up a call, but not the call itself, confirmed that a "6" in a line of computer code should actually have been a "D." That one error caused the equipment and software to fail under an avalanche of computer-generated messages. The error was in an April software modification for the signal transfer point systems. The spokesman said the company won't distribute final copies of the report until Bellcore, as the research consortium of the Baby Bells is known, presents a copy to the FCC and a congressional telecommunications committee, possibly this week.

[For background, see Ed Andrews' earlier NY Times article excerpted in [RISKS-12.05](#), 11 July 1991.]

---

### ✦ Weather Service Circuit Failure

"Peter G. Neumann" <neumann@csl.sri.com>  
 Mon, 25 Nov 91 12:04:57 PST

WASHINGTON (AP, 23 Nov 91)

A National Weather Service circuit that serves as the source of routine weather information for most of the nation's newspapers and broadcast stations was knocked out for 12 hours on Friday. Urgent weather information flood or storm warnings and watches remained available to most outlets because that information is carried on a separate circuit relayed by The Associated Press. But the 9:04 a.m. EDT outage of the weather bureau's Public Products Service meant that routine forecasts were nonexistent for many media outlets until the wire was restored at about 9 p.m. [...]

The AP was able to restore routine weather service to many of its members before the PPS problem was solved because of a temporary arrangement with the Contel Federal Systems Division of GTE, which has a contract from the Weather Service. [...] Weather Service spokesman Bud Litton declared the "problem was due to a major foulup by Bell Atlantic."

---

### ✦ Problems with nuclear plant safety computer in the UK

Peter Ilieve <peter@memex.co.uk>

*Mon, 25 Nov 91 10:47:47 GMT*

Here is a story that appeared on the front page of the Independent on Sunday, a UK 'quality' paper, on 1991 Nov 24.

Sellafield safety computer fails

by Tom Wilkie and Susan Watts

Britain's nuclear watchdog has launched a full-scale investigation into the safety of computer software at nuclear installations, following an incident at the Sellafield reprocessing plant in which computer error caused radiation safety doors to be opened accidentally.

The investigation, by the Nuclear Installations Inspectorate (NII), could affect the computer-controlled safety system that Nuclear Electric wants to install at the new Sizewell B pressurised water reactor under construction in Suffolk.

Sizewell B will be the first nuclear power station in the UK to rely heavily on computers, rather than people, in its primary protection system. Nuclear Electric argued that they would be safer.

The £240 million Sellafield plant, opened in February by Michael Heseltine, Secretary of State for the Environment, was expected to help British Nuclear Fuels (BNFL) to return waste to its country of origin. The plant encases high-level waste in glass blocks for transport and storage, using a process that is known as vitrification.

In mid-September, a "bug" in the computer program that controlled the plant caused radiation protection doors to open prematurely while highly radioactive material was still inside one chamber. Nobody was exposed to radiation and the plant has since been shut down, but the incident has rung alarm bells within the nuclear inspectorate.

The inspectorate originally judged the computer software that controls safety as acceptable --- partly because it consisted of only a limited amount of computer code. However, the computer program was later amended with what is known as a software "patch". It is this patch that is thought to have caused the doors to open too soon.

BNFL did not believe that the amendment had any safety significance. The inspectorate is investigating not only the computer technology itself, but also BNFL's bureaucratic procedures.

Under British regulations, the safety-related functions of a nuclear power station must be completely separate from its normal control systems. Nuclear Electric wants to have a computer-based system for both the control and the safety functions at the new Sizewell pressurised water reactor. However, the safety-related computer program has grown so complicated that the distinction between the software which controls the reactor and that which protects it has become blurred. It is also almost impossible to check that the software would react as it should if the reactor were to behave in a dangerous way.

The protection software is thought to have reached its current size because it incorporates extra features which, although desirable, have complicated its structure. Observers doubt that Nuclear Electric will be able to convince the inspectorate that the software will function as designed.

The integrity of the software is the last technical issue on the safety of Sizewell still to be sorted out, according to the NII. The inspectorate feels the performance of the software, like the safety of the steel pressure vessel, cannot be demonstrated on the basis of previous operating experience.

A BNFL spokesman said the company had completed an internal inquiry in the last few days but had yet to send results to the nuclear inspectorate. It does not expect the plant to reopen before mid-December.

---

A short description of the organisations involved for non-UK folk: British Nuclear Fuels Limited (BNFL): A company, but all its shares are owned by the government, either directly or indirectly via other companies like Nuclear Electric. BNFL provides fuel manufacturing and reprocessing for both civil and military programs. Its main plant is at Sellafield but it has plutonium production reactors at Chapelcross in Scotland and an enrichment plant at Capenhurst.

Nuclear Electric: A company, but wholly owned by the government. During the privatisation of the electricity generation and distribution industry in the UK it became clear that the nuclear part was unsaleable, so the government kept it. Nuclear Electric owns all the nuclear power stations in England and Wales. There is a similar company, Scottish Nuclear, for the stations in Scotland.

Nuclear Installations Inspectorate (NII): The UK nuclear regulatory body. No nuclear plant can operate without a licence from it. It is part of the Health and Safety Executive, which is the statutory body for most health, safety and pollution matters in the UK.

Peter Ilieve peter@memex.co.uk

[Also noted by John.Fitzgerald@newcastle.ac.uk (John Fitzgerald)]

---

## **✂ Results of Train Accident Investigations**

*Jymmi C. Tseng <u431573@imux200.mgt.ncu.edu.tw>  
Wed, 27 Nov 91 03:38:30 +0800*

Abridged from China Times Nov. 23, 1991.

RESULTS OF TRAIN ACCIDENT INVESTIGATIONS INDICATE DRIVER'S NEGLIGENCE OF TRAFFIC SIGNALS DIRECT CAUSE OF ACCIDENT.

ACCORDING TO THE TRANSPORTATION SAFETY COMMITTEE OF THE RAILROAD AGENCY, FAILURE OF AUTOMATIC WARNING AND BRAKES NOT CITED AS MAJOR CAUSE.

The transportation safety committee of the railroad agency announced the results of its investigations into the Nov. 15th accident, when "Freedom" express

train 1006 rammed into the side of another incoming express train, and caused 30 deaths and 100 plus injuries.

The fact that the "Freedom" express train had knowledge before starting from station that its safety systems were not working and yet allowed to carry passengers was not cited as a direct cause.

After collecting onsite evidence, eyewitness reports, and five meetings, the traffic signals were determined to be normal, because 5 previous trains reported no problems with the signals.

```

B Freedom 1066    C
===<#####>=====
# (65 km/h)      /
# A              /
#####>=====
Oncoming Express Train
    
```

The oncoming express train was supposed to travel on the secondary route A because of its lower priority. But the "Freedom" express 1006 was travelling at 86km/h at point C and it was one minute early and interpreted the "slow down" signal at C as an "go ahead". In the meantime, the oncoming express train had only time to reach A when the "Freedom" express rammed into its side at point B with a speed of 65 km/h, emergency brakes applied only 70 minutes before collision.

If the driver had followed the signal at C, there would have been no accident.

The paper cited that all accidents are caused by many individual incidents, which unfortunately coincided at the same time, not the direct cause of any singular event. If we look closely, we will see:

- 1) If "Freedom" 1066 had reduced speed according to the signals, there would have been no collision.
- 2) If the warning system had been working, the system would have warned the driver to reduce speed.
- 3) If the automatic braking mechanism had been working, emergency brakes would have been applied automatically and there might not have been so serious.

The results of the investigations are therefore not convincing enough. Obviously, the current railroad procedures are at fault because trains with faulty safety mechanism which are not "readily fixable" to carry passengers, on the condition that drivers are given notice of their condition.

The reporter made an comparison to a public bus, it would be analogous to telling the driver of a public bus without brakes to drive with only the hand brakes, and extreme caution.

If operational procedures which have proved wrong and yet neglected is definitely a management problem. The negligence of the committee to address the overall problem, but only to emphasize the direct cause is a sacrifice of public safety and human lives.

Jymmi C. Tseng, National Central University, Taiwan, R.O.C.

---

### **✂ Bank misdeposits money**

*David Shepherd <des@inmos.com>*

*Mon, 18 Nov 91 10:34:18 GMT*

An item in the personal finance section of The Times (London) on Saturday told how someone had paid in a sizeable check into their account and then been surprised when a few days later the bank started bouncing checks. When he investigated he found that the check had not been credited to his account. The bank fairly quickly admitted that there had been a mistake but said they could not credit the money to him until they found where it had gone. When they explained the situation a few days later they said that a the clerk processing the check had dropped the last digit of his account number, the computer had decided that he had not typed a leading zero and this matched another account number at that branch!

david shepherd: des@inmos.co.uk or des@inmos.com tel: 0454-616616 x 379  
inmos ltd, 1000 aztec west, almondsbury, bristol, bs12 4sq

---

### **✂ Mass. Governor wants to sell list of drivers licenses**

*<lotus!"CRD!Kent\_Quirk@LOTUS"@uunet.UU.NET>*

*Wed, 20 Nov 91 14:50:34 EST*

WBUR-FM reported this morning (11/20/91) that Massachusetts Governor William Weld has targeted for change some 140 laws and regulations that he says cause difficulties to those trying to do business in Massachusetts. One of his planned remedies is to sell the list of people holding a Massachusetts driver's license. The list contains approximately four million names, addresses and in most cases, Social Security numbers. This is because Massachusetts uses the Social Security number as a license number, except when specifically requested not to.

It would require an act of the state legislature to make this possible; they may find it attractive because selling the list could earn some \$5 Million at a time when state budgets are VERY tight.

[SEE NEXT ITEM. PGN]

---

### **✂ Mass. Governor NO LONGER wants to sell list of drivers licenses**

*<lotus!"CRD!Kent\_Quirk@LOTUS"@uunet.UU.NET>*

*Thu, 21 Nov 91 11:21:05 EST*

Boston Globe, Nov 21 1991:

One day after unveiling the proposal, [Massachusetts] Governor Weld yesterday scrapped plans to sell computer access to Registry of Motor Vehicles records to

private companies, saying he was swayed by concerns it could violate motorists' privacy. "As someone who is always working to keep government out of our personal lives...I do not want to make state government an accomplice in the dissemination of personal information about law-abiding citizens," Weld said.

(Funny -- the day before yesterday he said something along the lines of "If people don't want their social security numbers included, they can just apply for a license without one.")

..

The records are already publicly available, but only by requesting a cumbersome manual search by Registry clerks, which is costly. Weld aides estimated the state could make \$5 Million a year by allowing firms to buy direct online computer access. However, civil libertarians...expressed concern that the move would make it far easier for companies to obtain sensitive information, such as Social Security numbers, which are used as drivers' license numbers, unless people request otherwise. They also feared that it would become easier to obtain information about people's ages and the cars they own [which could be used] to target marketing campaigns.

I was worried that the legislature would find this proposal attractive because of the added revenue, but apparently people are waking up to privacy risks. This reminds me of the Lotus Marketplace snafu.

---

### **✶ CPSR FOIAs U.S. Secret Service**

*Craig Neidorf <knight@eff.org>*

*Fri, 22 Nov 1991 17:08:47 -0500*

I just received this from CPSR so I am passing it on to RISKS:

The Secret Service's response to Computer Professionals for Social Responsibility's (CPSR) Freedom of Information Act (FOIA) request has raised new questions about the scope and conduct of the agency's "computer crime" investigations. The documents disclosed to CPSR reveal that the Secret Service monitored communications sent across the Internet. The materials released through the FOIA include copies of many electronic newsletters, digests, and Usenet groups including "comp.org.eff.talk," "comp.sys.att," "Computer Underground Digest" (alt.cud.cu-digest)," "Effector Online," "Legion of Doom Technical Journals," "Phrack Newsletter," and "Telecom Digest (comp.dcom.telecom)". Currently, there is no clear policy for the monitoring of network communications by law enforcement agents. A 1982 internal FBI memorandum indicated that the Bureau would consider monitoring on a case by case basis. That document was released as a result of a separate CPSR lawsuit against the FBI.

Additionally, we have found papers that show Bell Labs in New Jersey passed copies of Telecom Digest to the Secret Service.

The material (approximately 2500 pages) also suggests that the Secret Service's seizure of computer bulletin boards and other systems may have violated the Electronic Communications Privacy Act of 1986 and

the Privacy Protection Act of 1980.

Two sets of logs from a computer bulletin board in Virginia show that the Secret Service obtained messages in the Spring of 1989 by use of the system administrator's account. It is unclear how the Secret Service obtained system administrator access. It is possible that the Secret Service accessed this system without authorization. The more likely explanation is that the agency obtained the cooperation of the system administrator. Another possibility is that this may have been a bulletin board set up by the Secret Service for a sting operation. Such a bulletin board was established for an undercover investigation involving pedophiles.

The documents we received also include references to the video taping of SummerCon, a computer hackers conference that took place in St. Louis in 1988. The Secret Service employed an informant to attend the conference and placed hidden cameras to tape the participants. The documents also show that the Secret Service established a computer database to keep track of suspected computer hackers. This database contains records of names, aliases, addresses, phone numbers, known associates, a list of activities, and various articles associated with each individual.

CPSR is continuing its efforts to obtain government documentation concerning computer crime investigations conducted by the Secret Service. These efforts include the litigation of several FOIA lawsuits and attempts to locate individuals targeted by federal agencies in the course of such investigations.

For additional information, contact:

dsobel@washofc.cpsr.org (David Sobel)

---

### **🚩 The Trojan Horse named 'AIDS' ([RISKS-9.55](#), 65)**

*"Peter G. Neumann" <neumann@csl.sri.com>  
Mon, 25 Nov 91 11:06:31 PST*

A recent AP item from London (U.K. May Drop Computer Lawsuit) noted that prosecutors had requested that the case against Joseph W. Popp had be dropped. for lack of evidence. Popp, 39, of Willowick, near Cleveland, Ohio, a former consultant with the World Health Organization, had been arrested in the U.S. in February 1991, extradited to Britain, and charged with blackmail and distortion. The warrant alleged that Popp distributed around 20,000 computer diskettes from London in December 1989 containing information on AIDS for use by hospitals and medical researchers.

According to the U.S. attorney's office in Cleveland, Ohio, when the diskettes were inserted into personal computers by unsuspecting recipients, they found themselves unable to retrieve any data at all from their machines. At the end of the program, the diskettes asked the computer user for a leasing fee of \$378, then printed an invoice with a Panama address where money was to be sent, federal prosecutors said.

Computer operators were told on the invoice that the rogue program they had inserted into their machines would stop them from working until the money was paid, when they would receive a "de-contamination" diskette.

Popp's lawyers have maintained that a clear warning of the consequences of using the diskettes was included in the packaging and that he had committed no crime.

---

### **✂ Banning of autodialers?**

*<sullivan@geom.umn.edu>*

*Sat, 23 Nov 1991 14:56:26 -0600*

Congress is considering a bill outlawing autodialers. Edmund Andrews reports in the Oct 30 New York Times that 20,000 such machines are working in the US, each making 1000 calls every day. The machines usually are programmed to go through an entire exchange, calling each number and speaking at whoever or whatever answers. It might urge the listener to dial a 1-900 number, or try to record the names of interested parties.

Supposedly, small businesses make the most use of these devices; large companies can hire live operators to man central phone banks. It's not clear to me why such services can't be contracted out to smaller local businesses. Some states have already banned the use of these devices, and now Congress is likely to ban them for interstate use. One salesman who uses an autodialer illegally was interviewed, and says he uses a false name in the solicitation until he trusts a potential customer.

Autodialers seem to get the most negative publicity when they run through all extensions at some business, perhaps leaving voice mail or typing up pagers. To me, this is less worrisome than the calls to residential customers. There was no mention of the definition of an autodialer, though it seems that devices which automatically call computers would not be covered under the law.

-John Sullivan

---

### **✂ a new risk for computer folks? -- computers and termination policy**

*Mark Bartelt <sysmark@orca.cita.utoronto.ca>*

*Mon, 18 Nov 91 13:16:23 EST*

Last week, 81 (of 120) support staff positions at the University of Toronto's Faculty of Medicine were eliminated; 79 staff members were summarily dismissed, and two vacant positions will not be filled.

Most of the victims were dismissed with less than a day's notice, and some with far less than that. The university acknowledged that the dismissals violate the university's policies for layoffs and firings. An article in The Varsity (the UofT student newspaper) contained the following:

Michael Finlayson, vice-president of Human Resources, admitted that the university did not follow the staff

policy on consultation, but said giving notice would have caused security problems.

"The problem in leaving them in their old jobs was the computers. If you release people and then give them access to the university's computer system, you worry about security."

This raises some interesting questions. The administration's concerns about security may not be totally frivolous (but then again, they may be). But even if the concerns are justified, and if those concerns can be used as a basis for an employer to ignore its own policies, then -- given that as time goes on, and increasingly large percentage of all staff will be using computers in some capacity -- what's the point of having such a policy at all?

Mark Bartelt, Canadian Institute for Theoretical Astrophysics 416/978-5619

---

### **✂ E911 system brought to it's knees by a prank**

*Glenn S. Tenney <well!tenney@fernwood.UUCP>  
Sat, 23 Nov 91 00:55:09 pst*

The San Jose Mercury News reported that the San Mateo 911 system was brought to it's knees because of a prank. Were you wondering when some phone phreak or system cracker would do this...

It seems that a disc jockey at KSOL decided to play a recent MC Hammer record over and over and over... as a prank. Listeners were concerned that something had happened to the personnel at the station, so they called 911 (as well as the police department business line). It seems that a few hundred calls in forty five minutes or an hour was enough to jam up the system. There was no report in the newspaper of any deaths or injuries to the overloaded system.

The DJ didn't want to stop playing the record (claiming first amendment rights), but did insert an announcement to not call the police.

So, it seems that a low tech "assault" on a 911 center could be quite effective. The system in question provides E911 for a few communities in the San Francisco Bay Area. This is the same center that went down following the Loma Prieta earthquake a couple of years ago. At that time, they lost power and switched over to the emergency generator only to find that just starting a generator once a month wasn't enough -- the generator conked out in about an hour!

Glenn S. Tenney

---

### **✂ Study on Computer Addiction**

*CSRI Distribution Manager <distrib@turing.toronto.edu>  
Fri, 22 Nov 1991 15:16:10 -0500*

A group of researchers at the Ontario Institute for Studies in Education are currently conducting research on person/computer interaction to address the issue of computer addiction. We would dearly love to here about people's experiences in this matter and would be willing to post the results to risks.

We are most interested in hearing from people who at some time have felt that they were spending more time (especially recreational time) at the computer than they really thought they should.

Please feel free to contact me directly at: [distrib@turing.toronto.edu](mailto:distrib@turing.toronto.edu)

Thanks very much. Chris



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 12: Issue 66

Tuesday 26 November 1991

## Contents

- [Pentagon computers vulnerable](#)  
[PGN](#)
- [Risks of hardcoded hexadecimal instead of symbolic constants?](#)  
[Tom Blinn](#)
- [Re: Leaves cause railway signal failure](#)  
[Geraint Jones](#)
- [Re: Termination](#)  
[David Lamb](#)  
[anonymous](#)
- [Proposed Antivirus Certification](#)  
[Klaus Brunnstein](#)
- [Call for Papers: IFIP World Congress'92/Vulnerability](#)  
[Klaus Brunnstein](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **pentagon computers vulnerable**

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>  
Mon, 25 Nov 91 12:03:44 PST

Pentagon Computers Vulnerable  
DELFT, Netherlands (AP, 21 Nov 91)

A leading Dutch computer security expert Friday said any computer whiz around the world "who is a bit clever" can break into a Pentagon computer and cover his tracks. Prof. Bob Herschberg, who teaches hacking at the Delft University of Technology, said the teen-age hackers who allegedly penetrated U.S. military computers during the Gulf War most likely represent only the tip of the iceberg of such intrusions. And he questioned a U.S. congressional investigation's finding that the hackers that penetrated the Pentagon systems were Dutch. "Anyone who is a bit clever can do it using detours such that their number is untraceable," said Herschberg. "They could have been from anywhere in the world including the United States itself." Camouflaging a hacker's trail is so easy via interlinked global computer networks that an adept hacker would have to be "naive" not to escape detection, Herschberg said.

U.S. congressional investigators told a Senate subcommittee this week that a group of Dutch teen-age hackers broke into U.S. military computers at 34 sites over about a one-year period ending last May. The information the hackers retrieved was described as crucial, but not secret.

Herschberg acknowledged that there have been instances of Dutch computer operators breaking into American computer mainframes. But he called the allegations of Dutch break-ins in this case "fishy," suggesting it was an attempt to use the Dutch as a scapegoat since hacking has not been outlawed here. Herschberg suggested that American investigators may be trying to cover up what may be a far more serious problem. "Why else would they make all this fuss?" he said.

Herschberg, a professor of computer science at this nation's top engineering school, teaches his students hacking techniques as part of a course on computer security. He regularly assigns students to break into corporate computer systems, with prior authorization, to identify security gaps. "It's a good practical exercise," he said.

Initial reports surfaced last April that Dutch hackers had broken into U.S. defense systems computers via a worldwide computer research retrieval system. In the wake of those disclosures, an official at Utrecht University, who was told by students of the intrusion, defended it as a legitimate learning exercise and said it was up to the U.S. military to take precautions.

---

## DNA Dog Tags

*Wed, 20 Nov 91 22:39:01 GMT*

Army May Issue "DNA Dog Tags" (Federal Computer Week, 19 Nov 91)

In a world without computers this would be a nice use of biotechnology to unambiguously identify casualties in the event of disfiguring injury. In a world with databases and computers it represents a tremendous potential threat to personal privacy.

Background:

Although all humans share a common set of genes, if you look closely there are many small variations (polymorphisms) in our genes. As a result, we are each unique. By taking a sample of DNA and analyzing a set of sites likely to be polymorphic, it is possible to "finger print" an individual and determine with very good reliability if another sample of DNA did or did not come from the same person. These polymorphisms can also be used to infer familial relationships (you inherit half of each of your parent polymorphisms), and to map and trace genetic disease genes like cystic fibrosis, and sickle cell anemia.

When you have given a sample of your DNA, you have no control over how it will be analyzed. It could be used to define a set of polymorphic markers which are other anonymous (unlinked to any genes of known function). The same sample could also be used to see if you have or carry genetic diseases. If the military builds a database of soldier's genotypes, there is nothing to prevent them from including medically important markers as well as identification information. On the contrary, there is every reason to expect that they would

want to include as much medical information as possible because many medical conditions do impact your ability to function as a soldier.

The risks:

Genetic privacy - Would you be forced to provide your military genotype data when you applied for health insurance after discharge? Would the local police have the right to search the military genotype database every time a DNA sample (spot of blood, hair follicle etc.) was found at a crime scene. How are you going to protect innocent soldiers against computer errors in that kind of a search?

It affects people other than the soldier - because your relatives share your genes, if you find out that you carry a genetic disease, everyone in your family faces the questions of whether they also carry the gene, should they be tested, should they screen their children etc.

Inferred paternity - for about 5% of births the father of record is not the biological father. As a database of genotypes grew, cases would inevitably arise where the genotype data demonstrated that the bibliographic information being provided was wrong. How would the military handle this?

We all carry genetic diseases - there is a concept called "genetic load" which is the number of heterozygous genes (differences in the copies of a gene inherited from your mother and father) where one of the copies would be lethal if you got it from both your mother and father. An average human carries about 6 such genes. This is why incest is such a universal taboo; if close relatives father a child there is greatly increased risk of getting two copies of such a lethal or nearly lethal gene. As medical science progresses and we enumerate more and more such genes, the insurance companies will have the "justification" to demand anyone's genotype as a precondition for health insurance. Would insurance companies or the military have the right to screen and veto prospective marriage partners?

The ethical implications of genotype databases are complex and potentially threatening. It would be a terrible mistake to proceed blindly into this area without considering the numerous implications.

David States

National Center for Biotechnology Information / National Library of Medicine

---

### **✂ Risks of hardcoded hexadecimal instead of symbolic constants?**

*"Dr. Tom @MKO, CMG S/W Mktg, DTN 264-4865" <blinn@dr.enet.dec.com>  
Wed, 27 Nov 91 11:52:26 PST*

Re: "Phone outages expected to be tied to typing mistake" (from The Wall Street Journal, 25Nov91, p.B4) in [RISKS-12.65](#) (Tuesday 26 November 1991):

When you put together 'DSC officials admitted that three bits of information in a huge computer program were incorrect' with 'a "6" in a line of computer code should actually have been a "D"', you reach the inevitable conclusion that someone was coding in hexadecimal, unless the difference between a "6"

and "D" in some symbolic names just happened, coincidentally, to result in a binary difference of three bits.

It seems highly likely that the use of suitably named symbolic constants in place of cryptic hexadecimal constants would reduce the likelihood of such errors. Of course, many modern languages still make it easy to encode data using hexadecimal constants, not that using decimal or binary or octal would likely have avoided this error.

Dr. Thomas P. Blinn, Digital Equipment Corp.

Digital Drive -- MKO2-2/F10, Merrimack, New Hampshire 03054 (603) 884-4865

---

**✂ Re: Leaves cause railway signal failure ([RISKS-12.62](#))**

*Geraint Jones <Geraint.Jones@prg.oxford.ac.uk>*

*Wed, 13 Nov 91 14:58:59 GMT*

British Rail's problem with wet fallen leaves and electronic train detection is not caused by the lightness of the new Networker trains (and so is not fixed by the /weight/ of older heavier trains).

The problem with the newer units is that they use disc brakes. That means that the running surfaces of the wheels only ever touch the rails and the insulating paste of crushed leaf builds up on the /wheels/. The problem is therefore not cured by running track-clearing vehicles. The (clever) fix employed is to attach a single clutch-braked vehicle to each of the new trains (in many cases, this would be a heavier clutch-braked multiple unit, but just a carriage will do). That car has clean wheels, makes good electrical contact with the rails and so makes the train visible.

Modifications to clean the running surfaces of the wheels will probably be the longer-term fix.

It is a classic systems problem: who would have thought that changing from external clutch brakes to better-protected disc brakes would undermine the signalling system?

---

**✂ Re: Termination (Bartelt, [RISKS-12.65](#))**

*David Lamb <dalamb@umiacs.umd.edu>*

*27 Nov 91 23:27:07 GMT*

I don't see that the "computer system" makes things significantly different. I've known of companies whose method of laying someone off was essentially a Friday pink slip saying "Hand in your badge now, here's the contents of your desk in this box, don't come back Monday, and here's K ( $\geq 2$ ) weeks' pay in lieu of notice" - which in some jurisdictions at least is considered to satisfy statutory requirements about due notice. Computer security concerns might make such practices more widespread - but if you're going to get paid anyway, why is it important to be allowed to continue to have access to the company's property? I suppose you might have personal files on the company computers, which complicates things a bit.

[The COMPUTER-RELATED RISK from the company's viewpoint is that ANY access whatever could lead to retributational acts. On one hand, assuming an employee is reliable and responsible, there might be a lot of benefits to allowing computer accounts to be cleaned up by the individual in question. On the other hand, "friendly termination" may be oxymoronic in many situations... PGN]

---

### ✂ Re: Termination (Bartelt, [RISKS-12.65](#))

<[anonymous]>

Wed, 27 Nov 91 12:22:53 XST

A certain medium-sized software vendor recently went through the second set of layoffs in six months. How did people find out that they were laid off? They came into work Wednesday morning, and found all of the machines shut off. So, they waited, and talked to each other, and talked in the halls, until managers came by and picked people off one by one. Their accounts had been disabled the night before, you see, and management didn't want people finding out by not being able to log in. (I never said this company was intelligent.)

For the previous set of layoffs, the dial-in modems were shut down for a day or so, because some of the system administrators were fired.

Is there a RISK in all of this? I'm not sure. The firings (excuse me, "layoffs") were not done in a friendly manner, as near as I can find out. Since there were indications a couple of weeks in advance (some of the people I knew were positive they would be going before they were told to leave), the precautions were pretty useless in my opinion -- and the treatment of the employees in question did not seem designed to incur goodwill.

---

### ✂ Proposed Antivirus Certification

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de>

22 Nov 91 14:49 +0100

Computer-Anti-MalWare Certification. A Proposal

Vesselin Bontchev  
Dr. Klaus Brunnstein  
Morton Swimmer  
Faculty for Informatics, Virus Test Center,  
University of Hamburg  
Submitted to: NCSA Antivirus Conference  
Washington D.C, November 25-26, 1991

Abstract: To assure and enhance the quality of antiviral products, academic, user and industry organisations (e.g., EICAR, NCSA) should initiate a process of cooperation and standardization to lead to a process in which a "certification" service is offered by a volunteer cooperative of interested parties and organisations (here described as Anti-MalWare Certification

Institutions, AMCI). It is hoped that this certificate may become an accepted, respected and expected indicator of quality and function for software and hardware. Evaluation shall be based on published methodology and a collection of malware (short for: malicious software) both known to exist or to be feasible.

The tasks of AMCIs are described. Virus Test Center at the University of Hamburg is undertaking a pilot project to evaluate and describe the capabilities of existing antiviral products. Future research will try to advance the development and understanding of the methodology of antiviral products, including detection, prevention, repair of damages as well as side-effects.

#### 1) Foreword:

As problems of malicious software (malware) continue and spread worldwide and at fast pace (presently more than 10 per week in IBM-compatible PCs), enterprises, institutions and organisations find themselves more and more in danger to become a victim of a "computer accidents". Users must ever more rely on the quality of anti-malware measures whose producers depend on actual knowledge of new threats. With growing numbers and new virus methods, the "anti/viral gap" (understood as the time gap between detection of a new virus and the availability of an antiviral product recognising it) inevitably will also grow (as long, as inherently secure and safe architectures are not available).

To improve the likelihood of success and reduce the potential for damage, we identify two possible efforts that deserve our increased attention:

- \* secured and fast distribution of new malware knowledge to all parties with interest in anti-virus production,
- \* evaluation and description of the capabilities of available anti-malware products by "credible" (and possibly "authoritative") individuals or organisations.

Concerns have been raised, which we intend to give due considerations:

- (1) making (dangerous) knowledge about viral methods available only to trusted parties (both in regard to secure communications as in judging the intentions and likely actions of the intended recipient);
- (2) ensuring that decisions restricting the flow of knowledge of details of malware do not result in undesirable side-effects.

Speedy and effective improvement of anti-malware products and the benefit of free-market competition is recognized as directly influenced by decisions as to what information is made available.

#### 2) Mission of "Anti-Malware Certification":

- To develop a process of "Anti-Malware Certification", several independent institutions or individuals shall be asked (and suitably funded) to perform regular tests and

evaluations of anti-malware products or updates.

- To inaugurate and assist in such a development, user or industry organisations with knowledge on malware problems and anti-malware software (e.g., NCSA/USA or EICAR/Europe) may charge institutions or individuals with assessed knowledge to perform specific assessments to assure the quality of anti-malware products.
- Institutions charged with "Anti-Malware Certification" should not have commercial interests in production or distribution of anti-malware measures.
- The test basis shall be a collection of known malware based upon precise knowledge about any essential detail, the contents of which must be suitably published. To minimize the dangers of such a collection, state-of-the-art security and safety measures shall be applied.
- Each submitted anti-virus is tested for its detection, elimination or prevention capacity against the malware databank under a published methodology. The test for detection shall indicate, in a form understandable to users, correct, false and missing diagnosis.
- To guarantee the quality of the test methods applied and of the secure malware collection, "Anti-Malware Certification Institutions" will discuss their methods in critical scientific discourse. Where feasible and possible without undue bureaucratization, they may also seek some form of certification by legally established institutions (e.g., NIST/USA, German Information Security Agency).
- Generally, test results (protocol, remarks) shall be published as some sort of "Anti-Malware User Report"; the organisations supporting the certification institutions may publish statistical surveys. Only in cases of individual tests asked for by an anti-malware producer, results are confidential unless published by the submitter.
- As independent individuals and academic institutions cannot develop and maintain such quality assurance mechanisms (including hardware, software, personnel and management), some adequate method of funding must be established. One suggestion is that "Anti-Malware Certification Institutions" may charge a fee to cover personal, managerial and machine costs; other suggestions may adapt established consumer report and product test procedures. The adequacy of the financial arrangements shall be controlled by public discussion with users, academia and industry (possibly via related organisations).

### 3) Initialisation of the Anti-Malware Certification Process:

Based on the current work of Computer Anti-Virus Research Organisation (CARO), a collection of annotated trojans and viruses in IBM- and compatible PCs has been established at the Virus Test Center, University of Hamburg. A test

methodology is being developed and currently tested, to run antiviral products against the databank and to diagnose which malware (virus, trojan) is correctly or incorrectly recognized.

The collection's content will be published periodically (Index of Established Malware (IBM-PCs); next edition: December 1991). The test methodology (in the first phase, with a multiplicity of files infected with known file viruses) will be published when validated with some experience.

A first draft of this document has been initially discussed with the European Institute for Computer Antivirus Research (EICAR) at its meeting of chairpersons, on November 18, 1991 in Hamburg. Following suggestions from this meeting, Virus Test Center will perform experimental tests and evaluations of available anti-malware software and report on the results in spring 1992. After the EICAR meeting, the document had been refined; the authors wish especially to thank Werner Uhrig (Austin/Texas, major contributor to Macintosh antiviral activities) for his highly constructive contributions which helped to refine this paper.

The authors submit this document to the user and academic public, and to interested organisations. Especially, this paper is submitted to National Computer Security Association (NCSA/USA) at its first Antivirus Developers Conference, November 25-26, 1991 in Washington D.C. for discussion. Moreover, legal aspects of the proposed quality assurance procedure shall also be discussed with adequate institutions (e.g., NIST/USA, German Information Security Agency).

#### 4) Future developments:

Next scientific steps will undertake to assess also the reliability of eradication (esp. in multiple attacks) as well as preventive methods such as checksumming and integrity tools. Present experiences with shortcomings of antiviral software prove that there is a lack of knowledge in basic methods to assess such eradication or prevention of anti-viral methods. To certify also deletion and prevention methods, basic research will be needed.

---

### **✉ Call for Papers: IFIP World Congress'92/Vulnerability**

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de>  
22 Nov 91 17:11 +0100*

Call for Papers  
12th World Computer Congress  
IFIP Congress 92: From Research to Practice  
Madrid/Spain: September 7-11, 1992

especially for the Congress Stream:  
Diminishing the Vulnerability of Information Society

#### Overview of the Congress:

This IFIP Congress is composed of topical and interrelated conferences each organized by a separate subcommittee of the International Program Committee.

Five parallel streams                      Stream Committee chairman

-----  
Software Development and Maintenance      A.N.Habermann,Pittsburgh  
Algorithms and Efficient Computation      Jan van Leeuwen,Utrecht  
From Architectures to Chips                  Gerald L.Reijns,Delft  
Informatics and Education                  Peter Bollerslev, Copenhagen  
Diminishing the Vulnerability of  
the Information Society                  Klaus Brunnstein,Hamburg

Two subconferences:                      Subconference Committee chairman

-----  
Expanding the Power of the Personal Computer Friedrich Vogt,Hamburg  
Enhancing the Intelligence  
in Information Systems                  Gordon Davis,Minneapolis

The Congress will also include one day workshops, tutorials and an exhibition.  
IFIP Congress 92 papers will be published in the conference proceedings  
(Elsevier's "Transactions in Informatics" series).

International Program Committee:

Chair: Wilfried Brauer,                  Technical University, Munich, Germany  
ViceChair: Carlos Delgado Kloos Universidad Politecnica de Madrid,Spain  
PastChair: Herve Gallaire                  gsi, Paris, France

Organizing Committee:

Chair: Rosa Alonso                  Alcatel Standard Electrica, Madrid, Spain  
ViceChair: Jaume Argila                  Spain  
ViceChair: Jose Ignacio Boixo                  Spain  
ViceChair: Fernando Saez Vacas Universidad Politecnica de Madrid,Spain

Special Call for Papers

Stream: Diminishing the Vulnerability of Information Society

With worldwide use of Information Technology (IT), new opportunities arise but, likewise, new risks emerge through growing dependence on that same technology. This means all users become more vulnerable to attacks on and misuse of IT. New types of computer based crime have been reported while the efficient operation of both public and private enterprises has become susceptible to malfunction, deliberate or accidental, in the information technology itself.

New concerns have arisen and older ones have been enhanced. Such concerns include both human and civil rights, privacy and freedom of the individual, leisure and education, the roles and design of work, quality and reliability of the technology, etc. The very existence and competitiveness of enterprises has become, in many cases, totally dependent upon the efficiency and reliability of IT. Moreover, the problem of complexity in contemporary system design may mean that some systems are uncontrollable by their users and even unfamiliar to systems experts. At the same time, the overall quality and reliability of the technology plays an important role in system selection and design.

The Stream "Diminishing the Vulnerability of Information Society" will attempt to assess the degree of vulnerability to IT that has developed since the first discussions in the early 1980s. Moreover, this stream aims at identifying the ways and means by which this vulnerability may be reduced and how emerging problems may be solved in advance by anticipatory action.

Specific areas of interest which may be addresses in submitted papers include:

- Opportunities and risks in the adoption of Information Technology, particular at International levels, with special emphasis on developments in Latin America
- Social Vulnerability and major Risks
- Legal Aspects: Reducing Vulnerability through the Law
- Enhancing IT to meet demands for Reliability and Security, with particular emphasis on Personal Computers and Local Area Networks
- Hardware and software systems for identification and authentication of users and attached systems
- Reliability and security in Personal Computers and Local Area Networks (LANs)
- Computer Supported Work: Impact of Vulnerability of IT on groups and organisation in an enterprise
- Human centered strategies to cope with Vulnerability: the role of participation, education, and task design
- The Electronic Cottage: Delivering Information and Communication Technologies at Home: For Better or Worse?
- Women, Computers and Work
- Computer Ethics and Professional Responsibility.

Moreover, short presentations (posters) describing ongoing research projects are suggested esp. for the following topics (or others related to the topic):

- The Electronic Cottage
- Vulnerability of and through AI Systems
- Enhancing the Security and Safety of IT, with special focus on Electronic Data Interchange (EDI) and Electronic Funds Transfer Systems (EFTS)

Invited speakers in the stream:

Professor Harold Highland	New York/USA
Professor Lance Hoffman	Washington/USA
Professor Herbert Kubicek	Bremen/Germany
Professor Bryan Niblett	Abington/England

Panel sessions on:

Informatics and development  
Identification and authentication of users and systems  
The Electronic Cottage: How will daily life be affected  
Human, Man, Woman  
Ethics of Computing: Information Technology and professional responsibility

Stream Program Committee:

Klaus Brunnstein (chair)                      University of Hamburg  
William Caelli    Queensland University of Technology, Brisbane  
Robert R.Moeller                                Sears & Roebuck, Chicago  
Jose Pino    University of Chile, Santiago de Chile  
Fernando Saez-Vacas                          Polytechnic University, Madrid

Information for Authors:

Six (6) copies of a full paper in English (no longer than 4500 words or 12 double-spaced pages, including figures, with 150 word abstract, full title, name and affiliation of author(s) as well as postal and electronic mail addresses, and telephone and fax numbers) should be submitted not later than 10 January 1992 to the Stream's chairman:

Professor Klaus Brunnstein  
Faculty for Informatics  
University of Hamburg  
Vogt-Koelln-Str.30  
2000 Hamburg 54  
Germany  
email: Brunnstein@rz.informatik.uni-hamburg.dbp.de

All papers will be reviewed by at least three, and relevance, originality and clarity will be considered. Accepted papers will be published in full in the Conference Proceedings.

How to Submit a Poster: Three (3) copies of a one page abstract for a 10 minute presentation should be sent to the appropriate subcommittee chairman so as to arrive by April 15, 1992. The poster proposal will be judged for relevance and clarity. Acceptance/rejection will be notified by May 15, 1992. The final version of the abstract has to be sent to the organizing committee for inclusion into the poster brochure so as to arrive by June 20, 1992.

Key Dates:

January 10,1992: Deadline for submission of papers  
March 9,1992: Notification of acceptance/rejection of papers  
April 15,1992: Deadline for submission of posters  
April 24,1992: Camera ready paper at Program Committee  
May 15,1992: Notification of acceptance/rejection of posters  
June 20,1992: Camera ready poster at Organizing Committee  
September 7-11,1992: World Computer Congress, Madrid

For more details, please contact:

FESI (Federacion Espanola de Sociedades de Informatica)  
IFIP Congress '92  
Hortaleza 104  
E-28004 Madrid, Spain  
Fax: (+34-1) 2431003  
E-mail: fesi@dit.upm.es



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 12: Issue 67**

**Monday 2 December 1991**

## Contents

- [Computer Delays costs Hospital over \pounds 300,000](#)  
[Paul Leyland](#)
- [A RISK of dishonestly using a visible password](#)  
[Paul Leyland](#)
- [Sprint Voice Calling Card uses SS#](#)  
[Lauren Weinstein](#)
- [Bright AT&T billing sys?](#)  
[Thomson Kuhn](#)
- [`Contractor queries data security'](#)  
[Matthew Farwell](#)
- [Proposed traffic congestion charging system, Cambridge UK](#)  
[Hugo Tyson](#)
- [Mailing lists - a right royal mistake](#)  
[Dave Horsfall](#)
- [Re: Leaves, trains, and computers](#)  
[Peter Mellor](#)
- [Re: Proposed Antivirus Certification](#)  
[David A. Honig](#)
- [Re: Employee Termination](#)  
[anonymous](#)  
[Bill Murray](#)
- [Re: Pentagon computers vulnerable](#)  
[Brinton Cooper](#)
- [Re: Risks of hardcoded hex instead of symbolic constants?](#)  
[Bob Frankston](#)  
[Bennet Yee](#)  
[Graham Toal](#)  
[Brandon S. Allbery](#)  
[Paul S. Miner](#)
- [Info on RISKS \(comp.risks\)](#)

---

• **Computer Delays costs Hospital over \pounds 300,000**

*Paul Leyland* <[pcl@oxford.ac.uk](mailto:pcl@oxford.ac.uk)>

*Tue, 26 Nov 91 17:57:26 GMT*

*\_The Health Service Journal\_, 12 September, 1991.*

Nottingham splashes out \pounds 300,000 to bridge HISS gap

Nottingham City Hospital has been forced to spend more than \pounds 300,000 on a stopgap computer system because of delays to its wide-ranging hospital information support system (HISS).

The hospital is one of the pilot sites selected by the Department of Health to test the ISS concept, which involves computerising almost every aspect of hospital operation at a cost of millions of pounds. But clinical directors at the hospital have said that they cannot wait until the HISS is fully installed, according to HISS project manager Andy Norman.

The hospital is spending the cash on a case-mix system from ACT Medisys, which will collect and sift data from existing systems for costing, audit and other purposes. Installation of the case-mix software and hardware has already started. In contrast the HISS, which is being part-funded by the DoH, is unlikely to be fully installed for two or three years.

Even by NHS [National Health Service -- pcl] standards the purchase of the HISS for Nottingham has been protracted. Nottingham's HISS will require a substantial amount of programming work, unlike previous HISS projects which were largely based around existing packages, often already in use in the US. The project will be based around a detailed abstract description of how the NHS operates known as the common basic specification.

The contract was supposed to have been awarded at the end of last year. Mr Norman said last week that the contract would be awarded by the end of October. IBM has recently quit chasing the contract, saying that the two-year bidding process had wasted too many resources.

---

### **✂ A RISK of dishonestly using a visible password**

*Paul Leyland <pcl@oxford.ac.uk>*

*Tue, 26 Nov 91 17:44:27 GMT*

*\_The Health Service Journal\_, 12 September 1991.*

A 21-year-old supplies clerk with Berkshire County Council has been jailed for two years after stealing \pounds 120,000, using the council's computers. A senior manager had left the password to the payments system by the computer screen.

[Yet another example of password insecurity. There is no record of what sanctions, if any, were taken against the manager -- pcl]

---

### **✂ Sprint Voice Calling Card uses SS#**

*Lauren Weinstein <lauren@vortex.com>*

Thu, 28 Nov 91 12:22:19 PST

Just a quick note to mention that Sprint is apparently using customers' SSNs as the main portion of their experimental voice-activated calling card system. While Sprint claims this isn't a problem, since the system is only supposed to respond to the callers' own voice (I suppose time will tell how well this system really works!), the problems of people overhearing your SS#, and then using it for other non-calling-card purposes, are obvious.

I don't know at this time if Sprint plans to continue using SSNs after their system passes beyond the experimental stage, but it wouldn't surprise me, given their lack of concern over customer privacy in the past. By the way, I'm still arguing with them about their system that allows anyone to interrogate account balances using nothing but the 10 digit telephone number--no passcodes, no controls, and no way for customers to "opt-out" of the system. I'll report back if anything changes in this area...

--Lauren--

---

### **✂ Bright AT&T billing sys?**

Thomson Kuhn <70007.5444@compuserve.com>

01 Dec 91 14:49:06 EST

Recently I opened my phone bill and found it to be five times its normal size (in both dollars and pages!). Looking over the 50+ pages of charges and remembering a recent `_60_Minutes_` program, it became clear to me that someone had gotten hold of my AT&T calling card number and passed it to friends and relatives all over the American Hemisphere. The best part of the experience was a note from the AT&T billing system which followed nine pages of charges to (and from) places I have never been or called:

"\*After analyzing your AT&T long distance calls on this bill, we find you could have saved money with the AT&T Reach Out America Plan with the AT&T calling card discount for your direct-dialed out-of-state calls..."

Thomson Kuhn, American College of Physicians 70007.5444@@compuserve.com

---

### **✂ 'Contractor queries data security'**

Matthew Farwell <dylan@ibmpcug.co.uk>

29 Nov 91 02:36:14 GMT (Fri)

Computer Weekly, 28Nov91

A complaint to the data protection registrar has raised the issue of whether address lists compiled by contract staff agencies which then go bust can be sold to other companies.

Computer contractor Ian Dallison has complained after the employment Department told him that a regulation stating that only agencies can only pass on information when finding a person a job does not apply if an agency goes bust.

Dallison first wrote to the data protection registrar's office and to the Employment Department in the summer after being contacted by two agencies and a timeshare company which had bought the address list of a bankrupt agency from the liquidator.

The Employment Department's Employment Agency Licensing Office has only just come back with its negative reply - and Dallison is now pursuing the matter with assistant data protection registrar John Lamidey. Lamidey says this issue arises in the insurance business when a small broker goes out of business and another firm takes up its clients.

But in Dallison's case the relationship between the individuals and the new owners is different.

"The Data Protection Act says you have to tell people what you intend to do with the personal information when you collect it - but you can't predict that you'll go out of business and the list will be sold," Lampidey says. "This circumstance probably wasn't thought up when the Act was drawn up"

One point raised by Lampidey is that a Liquidator takes control of a company and in effect becomes the owner of the data and therefore legally responsible for it. He is considering where this leaves the liquidator in cases like Dallison's.

Dylan.                    dylan@ibmpcug.co.uk || ...!uunet!uknet!ibmpcug!dylan

---

## ✂ Proposed traffic congestion charging system, Cambridge UK

*Hugo Tyson <hugo@harlqn.co.uk>  
Fri, 29 Nov 91 16:43:49 GMT*

This is from memory of what I've read in the local papers and an article on the BBC2 motoring programme "Top Gear". I live in Cambridge so I do have an interest in preventing this lunacy. Objective from now on....

CAMBRIDGE, England:

This ancient university city suffers from bad traffic congestion during most of the day, and a risky solution has been proposed. All cars (vehicles?) registered within 15 or 20 miles of the city will be fitted with a box, connected to the speedometer (presumably) and the ignition system, which has a slot in it for a phonocard-like card. The box is enabled and disabled by microwave transmitters on the 7 roads in and out of the city. While the box is enabled, so the proposal goes, if you travel less than some small distance in a certain time (I think it was the order of 300 metres in 30 seconds) you are deemed to be, and be causing, congestion, and the your special card, which is in the slot in the box on the dashboard, will have its credits debited. If the card runs out, you allowed a short way into debt on the card, and then the engine cuts out (whether this is until you are no longer "congested" or not is unclear). You can get your card "recharged", or buy a new card (?) at machines on street corners, post offices and the like, by handing over money. Visitors will be directed by signs to one of a number of ticket machines where a

"day-pass" can be bought for a fixed fee.

The idea is that this charging will cause people not to travel at times of congestion to avoid paying the charges needed to keep their vehicles going at these times, thus reducing the congestion.

This is how it is different from other "road pricing" schemes - it only charges if you travel in, and thus cause, congestion.

There are many risks here - I present some in no particular order:

- \* if the system is expensive enough to be a deterrent to travelling during congested periods people will disconnect the box - it can't be hard. If it is cheap enough that they won't do this, it won't be a deterrent, and will thus only be a small income source.
- \* companies with offices in the city may have to pay the charges to attract employees - thus the deterrant value disappears.
- \* people in traffic jams will stop the engine for 30 seconds until there is a large gap in front then speed down it and stop the engine again to avoid the charge, unless the system detects this, leading to more congestion behind these people.
- \* visitors to the city pay a fixed fee - there is no deterrent for them, and unless there are many spot checks no reason to buy the pass at all.
- \* immobilised vehicles will cause more congestion, unless a rapid removal service exists - and how does that get through?
- \* what if the box breaks? And what if I break it? This is very difficult to police. The implications for my car for example are complex too, as it is owned by a company 200 miles away and leased to my employer. Maybe I will count as a visitor, but as I live in the city I'd not enjoy having to pay a daily visitors' fee.
- \* microwave transmitters on routes in and out of the city. Most of these are two-lane roads, one in either direction. Can transmitters be made directional enough to only get cars in the one lane - or travelling in one direction? Or will the box simply toggle its state on exposure to the signal? This is very unsafe, suppose it doesn't turn off and your engine then cuts in London where you can't recharge your card? Will Cambridge City pay your parking/other fines and costs?
- \* car repairs - often require the car to sit in my drive or in a garage with the engine running, not moving. The system would charge me for this.
- \* speedometer cable failure is not uncommon on older cars. It is illegal to drive a car like this, because the total mileage clock isn't incrementing (and you can't tell your speed). But the box would think you're always stationary and charge you on top of any other trouble you get on the way directly to the car spares shop for a new cable. ;-)
- \* all the other risks associated with cards that contain money, and adding a system capable of cutting the engine to a car.

Only some of these are computer or sensor failure risks - the others are system design risks. But the more special cases you put in to handle these other risks the more complex and failure prone the computer in the box becomes. For example: (conjecture) box only stays "on" for one hour regardless of whether it sees a turn-off signal, plus turn-on repeaters around the city interior fixes the non-turn-off problem. Maybe. And so on.

More conjecture:

The only way I can see to make this safe (safer) is to supply a pass-card or key to everyone as well, which allows you to progress for free, but if you are caught using it \_on the city streets\_ you get fined. This would require spot checks to police it, and it must not be trivial to change the card in the slot, but the slot and the display on the box must be visible through the window.

Reality:

Politically active friends do not believe that this will be implemented, for various reasons, one being that it would annoy too many voters. I believe the same. However it is worrying that such a dangerous system is being seriously studied, when straightforward tollbooths with time dependent charges would do the same job IMHO.

Hugo Tyson, Harlequin Limited, Barrington Hall, Barrington, Cambridge, CB2 5RG  
England; Tel. (UK) 0223 872522 (International) +44 223 872522

---

### ✉ Mailing lists - a right royal mistake

*Dave Horsfall <dave@ips.oz.au>*

*Tue, 3 Dec 1991 10:23:53 +1100*

Taken from "Column 8" in the "Sydney Morning Herald", 2nd Dec 91:

``Queen Elizabeth II Research Institute for Mothers and Infants is a section of the University of Sydney's Faculty of Medicine. In the best traditions of a computer mailing list gone berserk, it received an invitation the other day to join the New York Academy of Sciences. It began: "Dear Queen Elizabeth, It is my pleasure, indeed, to extend to you this invitation to membership...""

---

### ✉ Re: Leaves, trains, and computers

*p mellor <pm@cs.city.ac.uk>*

*Thu, 14 Nov 91 11:33:05 GMT*

Further to the item by Graeme Tozer in [RISKS-12.62](#), the official explanation of why leaves delay trains, contained in the leaflet recently distributed by Network Southeast to its commuters, is that the effect is mechanical. Wheels slip on the rails, or lock during braking, causing overheating due to friction resulting in cracking, or wearing flat spots on the circumference. Damaged wheels need to be replaced or repaired, hence available rolling stock is depleted, hence delays.

No mention of computers. This is odd, because I cannot remember such disruption being caused by leaves in any previous year.

Snow is a different matter, particularly the "wrong kind" of snow - the fine powdery stuff that gets into brake units. Perhaps we have the "wrong kind" of leaves this year! :-)

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 JANET p.mellor@uk.ac.city

---

**✂ Re: Proposed Antivirus Certification (Brunnstein, [RISKS-12.66](#))**

"David A. Honig" <honig@broadway.ICS.UCI.EDU>  
Fri, 29 Nov 91 22:53:25 -0800

A few comments on Dr. Brunnstein et al.'s proposal to create a bureaucracy to manage antiviral certification:

Some aspects of the proposal are beneficial, e.g., creation of an organization that evaluates antiviral products. "Consumer reports" -style journals are useful as long as they are accurate. They make the marketplace more efficient by reducing the cost of obtaining information.

But much of the proposal is stifling. For instance, the creation of a "certification" that one is a "trusted party" creates what the military calls a "security clearance". A result will be conferences with closed-doors. Should we licence owners of tech manuals too?

The concern that "(2) ensuring that decisions restricting the flow of knowledge of details of malware do not result in undesirable side-effects." is mentioned but not discussed at length. Indeed, some people believe that "security through secrecy" is fundamentally flawed. Yet many aspects of the proposal have precisely that problem.

In sum, the creation of a software testing house specializing in anti-malware is a good research topic and a useful idea; the creation of an academic/industrial "trustworthy" clearance is a dangerous one. Instead of secrecy, we should have dissemination of both caveats and solutions to security problems.

David Honig

---

**✂ Re: Employee Termination ([RISKS-12.65,66](#))**

<[anonymous]>  
Sat, 30 Nov 1991 13:19:22 -0500

[Previous poster describes firing practices implemented to prevent computer sabotage by people that were just fired.]

This also shows that the management is not very confident in their backups. Then again, does the fact that my site has very reliable backs make it easier to fire me?

---

**✂ Re: Computer-related Risk of Employee Termination ([RISKS-12.66](#))**

<WHMurray@DOCKMASTER.NCSC.MIL>

*Thu, 28 Nov 91 22:49 EST*

As I advise my clients, terminations should be timely and complete. What constitutes timely and complete is a function of the nature of the termination, the role of the employee, the residual relationship, and the culture of the institution.

If the termination is hostile, timely means immediate and complete means that all privileges, and tokens of privilege be collected or revoked immediately. This includes keys, identification, signature cards, and logon IDs. This often means that separation pay is given in lieu of notice.

In the case of mass layoffs, a presumption of some hostility [must exist. ???]

Sometimes, even in the case of voluntary termination, for example when the employee gives notice of her intent to leave, the sensitivity of the role may be such that timely means immediate and pay in lieu of notice is indicated. For example, some organizations do not want people who have given notice to continue in management roles. Personally, I would not want those who have given notice to continue to function as operators, system or security administrators, or system or application programmers.

On the other hand, senior employees with significant reputations to protect may be considered safe. It is not uncommon to provide such employees with office privileges to facilitate finding a new job.

Likewise, those employees to whom large sums of money are payable over time are usually safe. Retirees are not likely to put their retirements at risk by taking a parting shot. Many organizations give permanent credentials to their retirees. Most will provide offices to retired long-tenure founders or even CEOs.

Finally the culture of the institution may influence what constitutes timely. Some institutions or industries, as a matter of practice, do not offer long tenure employment; there employees do not expect it. The only question about termination is when, not if. These organizations enjoy a reputation of "friendly" terminations and often maintain mutually beneficial relations with their "alumni" for decades. Here again, timely means less than immediate.

All but the most amicable separations involve some risk. Computers may aggravate this risk to the extent that they empower individuals, blur the lines between what belongs to the institution and that which belongs to the individual, mask the consequences of the user's actions from him, are so attractive that the individual is reluctant to be separated from them, or makes us dependent upon the special knowledge of one or two individuals.

The first risk is the one that concerns most management. With a few key-strokes, the terminated employee might be able to wipe out or erase a great deal of information very quickly. Likewise he might be able to create a trap door that would make it impossible to exclude him. Management lacks confidence in the effectiveness of the controls that it has over the behavior of the system.

The risk of the exercise of power by the separated individual may be aggravated by the tendency of the computer to distance the user from the consequences of his acts. For example, an employee whose personal controls might not permit him to set fire to the files might easily be able to erase them.

I still have a diskette marked "VM Files" that contains data that I down-loaded from "my" VM system on the occasion of my retirement from IBM. This diskette contains a copy of my personal telephone directory, as well as copies of several papers that I wrote while a user of that system. I am satisfied that I have sufficient rights in that data, and that after I left, they were simply erased by the system managers. Of course I honored my employment agreement that required that I not disclose any IBM Confidential data for one year after my retirement. Nonetheless, my own separation illustrates many of the conflicts that might arise between the rights of the institution and those of the individual.

I also remember that one of the most difficult things for me to part with upon my retirement was access to that system and the network that I accessed through it. It has taken me years to replace it. I continued to use it for almost a month after my termination until my account was finally revoked. I can easily sympathize with the anxiety of a suddenly terminated employee who can no longer access "his" system and "his" data. I can also sympathize with the concern of management that a terminated employee might steal their data.

Finally, many institutions are dependent upon the special knowledge of a few individuals, mostly programmers, whose untimely separation might deprive the organization of knowledge that they require to properly manage their systems. Many managers would feel prevented from immediately separating such people who gave notice of their intent to leave.

Conversely, the risk of termination can be reduced by computer controls that involve multiple people in sensitive duties, clarify the division of rights between the institution and the individual, make the effects of computer operations explicit, or which reduce the dependence of the institution on the special knowledge of individuals by encapsulating that special knowledge within the system.

It should be noted that when management errs on the safe side in terminations they tend to embarrass both the separated employees and themselves; they may look both paranoid and insensitive. On the other hand, if they err in the direction of risk and something goes wrong, they will appear to be imprudent. Few managers will always, or even ever, walk this difficult line to the satisfaction of everyone.

When few employees used computers in the course of their jobs, those employees could be treated differently on separation than others. When all employees use computers, the capability for orderly separation will require that we control computers in a more appropriate manner in the normal course of events.

William Hugh Murray, Executive Consultant, Information System Security  
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840 203 966 4769

## **✂ Re: Pentagon computers vulnerable ([RISKS-12.66](#))**

*Brinton Cooper <abc@BRL.MIL>*

*Mon, 2 Dec 91 10:21:40 EST*

... The report cited recent "penetrations" of "U.S. military computers" at "the Pentagon" during the Gulf War. I heard this report, originally, on NPR and continue to have questions:

1. Were the computers really at "the Pentagon?"
2. If not, where were they?
3. Was classified information compromised?
4. If not, what sort of information was compromised?

The press might consider the computer from which this note is posted as a "Pentagon" computer because it is owned and operated by the US Army. My data files might be reported by a naive reporter as containing "military" information. In fact, they contain information on information theory, algebraic coding theory, decoding, and associated bibliographies.

Apart from the slightly sensational aspects of reporting "breaking into Pentagon computers," the article talks about how hackers can cover their tracks, appearing to have been anywhere in the world other than where they actually were at the time of hacking. Such discussions could be cited as evidence that tracing of the access path to Internet computers should be performed. This, in turn, could easily lead to exactly the same arguments seen here and in other forums (fora?) about telephone privacy vis a vis Calling Number ID. Is history about to repeat itself (again)?

\_Brint

---

## **✂ Re: Risks of hardcoded hexadecimal instead of symbolic constants?**

*<frankston!Bob\_Frankston@world.std.com>*

*30 Nov 1991 09:52 -0400*

Ultimately there is data somewhere deep in the bowels of a system. A 6 vs D could easily have been a data error in a table. Or it could have been in the definition of a symbolic constant. Giving a value a name doesn't make it correct and might even obscure errors. Even worse, errors in error paths are very difficult to check when they only show up in system-wide interactions in a very big system. It is amazing how well systems work despite serious errors until a particular set of conditions arise.

I'm sympathetic to approaches to minimize errors such as using closed loop systems, redundancy etc but I'm afraid of people making the assumption that perfection is achievable. The challenge is to make the systems resilient though not perfect. In something like the SS7 collapse the question is not whether we can discover the bugs beforehand, but that the system is so complicated that there weren't the firewalls to limit the collapse.

The two issues are related. If we expect failure then we should design firewalls independent of the complex failure recovery modes of the system. Of

course, this too is ideal since both the system design and the firewall design might suffer from the same systemic assumptions.

One product design I did involved dialup communications with two levels of protocols. I made the assumption that the recovery approach for any nontrivial error was to hangup the phone. Partially these was because I didn't want to spend limited RAM and programming resources. But also because I didn't see the point of using complicated algorithms when a simpler approach would work.

Since I don't know anything more about the SS7 collapse than the "6" vs "d" (more likely than "D" (a good example of how newspapers can mislead with the most innocuous of changes)), none of this might apply.

---

**✉ Re: Risks of hardcoded hexadecimal...? ([RISKS-12.66](#))**

*<Bennet\_Yee@PLAY.MACH.CS.CMU.EDU>  
Thu, 28 Nov 91 03:01:10 EST*

I fail to see how such symbolic constants can be defined other than in terms of a hexadecimal (or binary or ...) constant or other symbolic constant(s). You still have to have constants somewhere, even if it's only zero and the successor function. :-)

In any case, the typographic error could just as well have been in the definition of the symbolic constant. Symbolic names may well help, but are no panacea.

It's not really fair to be jumping to conclusions about the style of DSC software.

---

**✉ Re: Risks of hardcoded hexadecimal...? ([RISKS-12.66](#))**

*Graham Toal <gtoal@gem.stack.urc.tue.nl>  
1 Dec 91 02:25:56 GMT*

I would \*love\* to see the actual line of code. Is there any chance of getting it out of them? I don't see how someone could accidentally type D for 6 or vice-versa - too far apart. I wonder if somehow or other this code was scanned in - or (HHOS) typed in by a 'coder' like in the old days from a 'coding sheet'? :-)

Just using symbolic constants to hide your typing mistakes in another file isn't much of an improvement by the way. NASA-style red/black tiger teams might help a little, but I'm not sure what else would. From what I've heard of the state of the formal methods art, things haven't improved much since when I was a student in the seventies...

---

**✉ Re: Risks of hardcoded hexadecimal ... ([RISKS-12.66](#))**

Brandon S. Allbery KF8NH <allbery@ncoast.org>  
Sun, 1 Dec 91 10:33:31 -0500

I've had at least one bug creep into a program despite such care: I was careful to use symbolic constants even if I only used the constant once... then proceeded to insert a typo into the declaration of the constant.

Don't make unwarranted assumptions. That's a RISK in itself.

Brandon S. Allbery, KF8NH [44.70.4.88] allbery@NCoast.ORG

---

**✂ Re: Risks of hardcoded hexadecimal ... ([RISKS-12.66](#))**

Paul S. Miner <psm@air16.larc.nasa.gov>  
Mon, 2 Dec 91 09:50:42 -0500

Actually the conclusion that the data was HEX is not inevitable; the difference between the binary representations of ``d'' and ``6'' in ASCII is three bits (just as the difference between a ``6'' and ``d'' in HEX is three bits). Thus, the comments about the use of ``cryptic hexadecimal constants'' are not necessarily relevant to this problem.

Paul S. Miner, 1 Gregg Road / Mail Stop 130, NASA Langley Research Center  
Hampton, Virginia 23665-5225



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 12: Issue 68**

**Friday 13 December 1991**

## Contents

- [Hubble Trouble: Space Telescope shuts itself down](#)  
[Henry Cox](#)
- [Postal worker leaves automated stamper in test configuration](#)  
[Palmer Davis](#)  
[Joe Brownlee](#)
- [2 Safeway preferred customers, to go!](#)  
[Bear Giles](#)
- [Hospital computer solicits the dead](#)  
[Adam Gaffin](#)
- [Computer records track killer](#)  
[Robert Jenkins](#)
- [Train crash in UK - is it human error?](#)  
[Olivier M.J. Crepin-Leblond](#)
- [TRW lawsuit settled with FTC, 19 states](#)  
[Phil R. Karn](#)
- [National Fingerprint Database specs](#)  
[Clifford Johnson](#)
- [Bill on computer usage about to become law in Ireland](#)  
[Mark Humphrys](#)
- [The description is right, only the language is wrong](#)  
[Dan Franklin](#)
- [Poll tax incompetence](#)  
[Robin Fairbairns](#)
- [Truth in Antiviral Advertising](#)  
[Russell Aminzade](#)
- [Re: Pentagon computers vulnerable](#)  
[Steve Bellovin](#)
- [Post-structuralism and Technology](#)  
[Phil Agre](#)
- [Chaos Congress 91 Program](#)  
[Klaus Brunnstein](#)
- [Info on RISKS \(comp.risks\)](#)

---

✎ **Hubble Trouble: Space Telescope shuts itself down**

Henry Cox <cox@cadence.com>

Wed, 11 Dec 91 08:26:42 EST

[A short blurb from the Boston Globe, 11 Dec. 1991]

Washington - The Hubble Space Telescope has shut itself down temporarily because of a computer programming error that rotated its communications antenna into a technical no-parking zone. The Hubble went into a "soft safe mode," shutting down some but not all its systems and halting scientific work on Monday. It is programmed to take this kind of action whenever necessary to protect itself from harm. In this case, it was at the hands of what officials called a "fluke" buried undiscovered in its millions of lines of computer code.

[PGN provides the following additional excerpt from an AP item:]

The trouble was in the system that swivels to keep the Hubble's antenna pointed to an overhead relay satellite, as the telescope orbits the Earth. On Monday, the onboard computer issued a command that exceeded the software limits on the speed of antenna movement and the system went into an emergency "safe mode" to protect itself from harm. "These things are going to happen over 15 years," Weiler said, calling the incident "a non-problem." The Hubble's planned lifetime is 15 years.

---

### ✂ Postal worker leaves automated stamper in test configuration

Palmer Davis <davis@usenet.INS.CWRU.Edu>

Tue, 10 Dec 91 00:33:56 -0500

According to a report by WEWS-TV, a repair technician at a U.S. Postal Service facility in Columbus, OH, when repairing a machine used to automatically stamp messages on cancelled letters, reconfigured the machine to display a test message that he had learned from his instructor during training, but forgot to reset the machine to print the correct message after he completed his repairs. So now, instead of "MERRY CHRISTMAS" or "HOLIDAY GREETINGS", thousands of letters in circulation bear the message "YOU BITCH".

[Also noted by Mowgli Assor <mowgli@cis.ohio-state.edu>:

only envelopes 5 1/4-inches tall or taller were affected, but Johnson said postal officials estimated that more than 12,000 were printed and only a handful were caught before they were loaded onto trucks for delivery. The office handled about 5 million pieces of mail Saturday ...]

---

### ✂ Postal worker leaves automated stamper in test configuration

Joe Brownlee <jbr@cblph.att.com>

11 Dec 1991 8:17 EST

This rings a bell with me, because I have seen a few cases where this type of message was used in test versions of software. For example, a young programmer

I worked with placed a message in a program instructing the user to press a certain key to "bomb off", which would produce a dump of the program's current state so that he could examine it. The message made it out the door and into a customer's hands. They were less than amused. In another case, an obscene message was displayed when the use entered an illegal value at a prompt. That software was almost sent out the door, but was caught at the last minute and removed.

I suppose the moral is don't enter anything in the system you wouldn't want a customer to see.

---

## ✂ 2 Safeway preferred customers, to go!

*Bear Giles <bear@tiger.cs.colorado.edu>*

*Wed, 4 Dec 1991 20:16:52 -0700*

>From \_Westword\_, an alternative Denver weekly (12/4/91):

Safeway may be turning its "preferred customer" program into a "proffered customer" deal. According to the \_Wall Street Journal\_, grocery stores in Chicago, Dallas, Los Angeles and Denver are part of a Citicorp program that uses checkout scanners to record shoppers' buying habits. You may have thought that preferred customer card was just a way to get some free Jimmy Dean sausage and a friendly monthly letter from Safeway's Bob Green -- but it also links your name and mailing address to your shopping list. Once you've presented your card, your personal purchases are no longer so personal.

Citicorp originally planned to sell data on shoppers' purchasing patterns to grocery marketers. But for the last month, the \_Journal\_ says, that information has been for sale to all comers. It's handily divided into eight categories, including "weight-conscious consumers" (511,227 names of people caught buying lo-cal treats) and "fancy food buyers" (refrigerated pasta is enough to brand you fair game for marketers of travel magazines).

And just where does the fried-pork-rind-and-Cheese-Whiz contingent fit in?

[Imagine the fun a health insurance company could have with this information:

```
if (subscriber) {
  if (high-fat-foods && !fiber) {
    colon-cancer++;
    rates++; }
  if (cigarettes) {
    lung-cancer++;
    rates++; }
  if (condoms) {
    sexually-active++;
    rates++; }
  if (KY-Jelly) {
    test-for-aids++;
    rates *= large-number }}
```

(Of course, they would never purchase the records from my health club for "physically-active++; rates--").

The fact that Citicorp offers this information for Safeway customers certainly implies the same type of information is available on your Citicorp-issued credit cards.

Aha! A new, high-interest category: unfaithful spouses! (Check for flowers or hotel rooms within 50 miles of home charged to credit cards). Sure to be read by divorce lawyers across America!

Bear Giles bear@fsl.noaa.gov ]

---

### **✂ Hospital computer solicits the dead**

*Adam Gaffin <well!adamg@fernwood.UUCP>*

*Wed, 11 Dec 91 07:29:13 pst*

Middlesex News, Framingham, Mass., 12/11/91, page 1

Framingham Union letter solicits from dead - again

By Adam Gaffin  
NEWS STAFF WRITER

FRAMINGHAM - The letter expresses the hope that Matthew Jong's recent stay in Framingham Union Hospital went well and asks him to consider making as large a donation as possible. The only problem is that Matthew Jong was pronounced dead in the hospital emergency room on Oct. 5 after a car accident on Rte. 9 in Natick.

"This solicitation was the final straw," says his mother, Gail, a Wellesley resident. She has been fighting with the hospital for two months over the way she was told Matthew was dead - a phone call from the emergency-room doctor, rather than a visit from a Natick or Wellesley police officer.

At least one other deceased Framingham Union patient has received a similar letter since September, when the hospital said it had fixed a computer glitch that resulted in a number of dead people being sent fund-raising letters. At the time, Ross Mauro, the hospital director of marketing, said he had been assured this "will not, cannot happen again," by the hospital's data processing department and the firm hired to send out the letters to former patients. "Your gift will be an investment in the future health of your family and your community," the letter, signed by medical-staff President Joseph Baron concludes. "It could help save the life of someone you love."

"This family has suffered enough and we wish they never had gotten the letter," said hospital spokeswoman Ruth Stark. She said the mix-up occurred partly because of the way the emergency-room physician who attended Jong filled out a form on his case.

A standardized form is required for every patient who enters the hospital, and care-givers are supposed to mark a box on the form with a one-letter code indicating the patient's status.

In Jong's case, the doctor wrote "deceased - sent to morgue" in longhand across the form, rather than putting an "E" - for "expired" - in this box, Stark said. The form ultimately wound up in a data-processing office, where

workers type patient information into a hospital computer. A clerk did not notice the box was empty on Jong's form, and did not read the doctor's comments, and so entered his data into the computer, she said.

The computer is supposed to delete the records of anybody who is deceased, a prisoner or a Medicaid patient before the data is shipped to the mailing company, Stark said. "It's not a foolproof system," despite efforts to reduce such incidents..." She said hospital personnel have been reminded to fill out the box to prevent such mishaps. But she added that the computer program that does the deleting is currently set up to assume that a blank disposition box means the patient went home and that officials are looking at ways to change that. "We are intending to insure that this doesn't happen in the future," she said. [...]

---

### **✂ Computer records track killer**

*Robert Jenkins <rjenkins@cix.compulink.co.uk>  
Sun, 8 Dec 91 20:05 GMT*

According to a report in the Guardian newspaper (London), of 6 Dec 91, a recent murder case was solved by police partly through a computer disproving a suspect's alibi.

John Tanner murdered his student girlfriend and hid her body underneath the floorboards of her house. Initially, the police treated him as a witness rather than a suspect, but his story began to fall apart. He told the police that he and the girl had taken a bus ride together to the train station at a time when she was already dead. The Guardian reports:

"The company that runs the local bus service keeps computerised records of its tickets. Only one person got on the bus and bought a ticket to the station at the time Mr Tanner claimed."

A RISK, I suppose, of trying to get away with murder. But also another example of low-level, invisible, surveillance that computers introduce into our lives.

Jolyon Jenkins (rjenkins@cix.compulink.co.uk)

---

### **✂ Train crash in UK - is it human error?**

*"Olivier M.J. Crepin-Leblond" <UMEEB37@vaxa.cc.ic.ac.uk>  
Sun, 8 Dec 91 19:55 BST*

From Oracle Teletext Service (ITV, UK), 8 Dec 1991:

"Urgent checks are going-on following the Severn Tunnel rail crash on backup equipment installed after earlier technical problems with the signals. Sixteen people are still in hospital after the crash between an Intercity and a two-carriage Sprinter on Saturday. BR [British Rail] is looking at whether there was 'further failure of equipment' or whether human error was involved. The express had slowed to 20mph after a proceed-with-caution signal and was hit by the Sprinter from behind - so what signal, if any, did the Sprinter get?"

[`Intercity' and `Sprinter' are two types of train. The crash which happened on Saturday morning injured close to 100 people.]

Olivier M.J. Crepin-Leblond, Imperial College London, UK.

---

**✂ TRW lawsuit settled with FTC, 19 states [see [RISKS-12.05](#)]**

*Phil R. Karn <karn@thumper.bellcore.com>*

*Tue, 10 Dec 91 14:04:11 EST*

Excerpted from an article by EVAN RAMSTAD, AP Business Writer, 10Dec91:

DALLAS (AP) \_ TRW Inc. has settled a lawsuit with 19 states and the Federal Trade Commission, which accused the company's credit reporting unit of violating consumer privacy and making reporting errors that harmed the credit ratings of thousands of consumers. The settlement requires Cleveland-based TRW to make sweeping changes in its credit reporting business, including providing reports to consumers who ask within four days. [...]

The settlement comes against a background of growing consumer anger over the enormous power of credit reporting companies, which keep financial dossiers on tens of millions of Americans. [...]

The lawsuit cited cases where different consumers' reports were mixed together and said such inaccuracies are hard to correct. The states and FTC charged old information reappeared in consumers' files and that consumer disputes were not adequately investigated. [...]

The settlement requires TRW to improve its procedures so that files of consumers are not mixed up and to prevent old information from reappearing in consumers' files.

TRW also agreed to establish a toll-free number for consumer inquiries, investigate information disputed by consumers and check public records if necessary to verify information.

The company also agreed to notify consumers of their rights to dispute information and to tell them, upon request, about other companies to whom the credit reports have been sold.

TRW also agreed to disclose to consumers their individual credit scores, starting Dec. 31, 1992.

The company will have to keep records of its compliance and pay the states \$300,000 to cover legal costs, according to the settlement.

[PGN saw a Washington Post article on 11Dec91, page F1, by Albert B. Crenshaw, who noted that as part of the settlement TRW said it would

- \* Adopt procedures to prevent data mixups
- \* Review within 30 days any disputed information, and delete any that cannot be confirmed within 30 days
- \* Delete any disputed information when the consumer presents relevant documentation
- \* Implement procedures to prevent reappearance of seriously derogatory information that has been deleted following a complaint. ]

## **✂ National Fingerprint Database specs**

*"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>*

*Thu, 12 Dec 91 11:34:38 PST*

>From Gov't Computer News, Dec. 9, 1991:

### **FBI SHOPS FOR A SPEEDY FINGERPRINT SYSTEM**

... The FBI wants IAFIS [Integrated Automated Fingerprint Identification System] to complete urgent fingerprint matches in under 15 minutes. It expects a three second response to searches for name and description against its Criminal Master Database. Now the fingerprint and information searches can take two weeks... The system is slated to start running in Clarksburg, W.Va., in late 1994 ...

IAFIS will give law enforcement agencies throughout the country a way to check fingerprints electronically, through the FBI's National Crime Information Center (NCIC) network... AFIS will perform a search of the agency's national fingerprint database. The system will provide a list of the most likely candidates, or a message reporting that none were found... The FBI wants a system that has a 95% accuracy rate for 10-print searches. For crime scene prints, "the correct candidate shall be listed in the top-ranked position 50% of the time, and in the top 20 positions 65% of the time"... To keep the system secure, the FBI will not make technical details public.

---

## **✂ Bill on computer usage about to become law in Ireland**

*Mark Humphrys <C133-012@IRLEARN.UCD.IE>*

*Wed, 11 Dec 91 01:46:11 GMT*

The Criminal Damage Bill, 1990, is about to be passed into law in Ireland, containing what appears to be an extremely broad definition of 'unauthorised' use of computers. Section 5 reads as follows:

(1) A person who without lawful excuse operates a computer ... within the State with intent to access any data kept either within or outside the State ... shall, whether or not he accesses any data, be guilty of an offence ...

(2) Subsection (1) applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person.

Section 6 states that "lawful excuse" applies: "...if at the time ...he believed that the person... whom he believed to be entitled to consent to or authorise the ... accessing of the [data] in question had consented, or would have consented to or authorised it if he or they had known of .. the accessing and its circumstances, [or] if he is himself the person entitled to consent to or authorise accessing of the data concerned"

This Bill has been passed by the Dail (roughly equivalent to the House of

Representatives) and is on its 2nd stage in the Senate (roughly equivalent to the US Senate) on Thur 12th Dec.

I would appreciate any comments on what this Bill implies, and examples of legislation in other jurisdictions. The wording would appear to me to be extremely dangerous and ill-conceived.

This is NOT a hypothetical case. I have contacts in the Labour Party ( the 3rd largest party here ) who want to propose amendments to this Bill, and they have asked me for advice. There is every chance that they will succeed, if they can propose an intelligent alternative.

The last chance to amend it will be late Dec / early Jan. Then it will become law.

Mark Humphrys, Dublin, Republic of Ireland

---

### **✂ The description is right, only the language is wrong**

*<dan@BBN.COM>*

*Mon, 09 Dec 91 11:53:18 -0500*

The Boston Globe "TV Week" movie listings had an unusual description for one movie this past week:

*\_New York, New York\_ (1977) Robert De Niro, Liza Minelli.  
Après la deuxième guerre mondiale, une chanteuse aide un saxophoniste à joindre un orchestre fameux de jazz. (120m.)*

The rest of the listings were in English, as they normally are. The Globe had this to say (Saturday, December 7, 1991):

*A spokeswoman for Tribune Media Services, which supplies the movie listings to newspapers in the United States, Canada, and the Caribbean, tells us someone selected the wrong description of the film from the company's data base and included it in the listings sent to the Globe. Some television stations carry English-language films dubbed in French, she notes. The English description reads: "A singer and a saxophonist team up and break up in the postwar big-band era. Directed by Martin Scorsese."*

It is hard to believe that this error would have occurred, and not been caught, before the age of computers. The RISK here is that as the chain of events handled purely by computers lengthens, it becomes possible for relatively major errors to occur unnoticed, because no one is looking closely at the output at any stage.

Dan Franklin

P.S. A non-RISK is that those of us who can understand a little French can be amused at how different the two descriptions are...

---

### **✂ Poll tax incompetence**

*Robin Fairbairns <robin.fairbairns@isl.co.uk>  
Thu, 05 Dec 1991 09:14:47 +0100*

I've now simmered down, but I was in a state of seething fury yesterday from the behaviour of our local Poll Tax office.

Earlier this year, I split up from my wife, and moved house. Still within the city, but they gave me a new tax account number: I thought it pretty daft then. Three months ago I changed the method of payment; in October, they recognised this and sent me a letter saying that the first payment would be requested from my bank on 26th November. On the 2nd December I received a tax demand; when I finally got through to the payments office, they agreed that it was silly, and should be dealt with by the direct debit. Almost immediately, they rang me back and said there was no direct debit mandate on my account. If I'd really given them one, would I please call my bank and ask them to send a copy of their half of the mandate? Yesterday, I called them again: I had with me a copy of their letter about the mandate. They were adamant; finally we came to the joint realisation that there were 3 accounts involved - the one at my old address, my present one, and the one that had the mandate. The payment people had no record on any account they could look at of my mandate. Through to the registration people: ah yes, they said, we had a problem with the accounts of the previous occupants of your house, so we deleted all accounts with that address. Sorry, we seem not to have transferred your mandate when we created a new account for you.

The risk? Incompetent use of computers causes raised blood pressure!

Robin Fairbairns, Senior Consultant, postmaster and general dogsbody  
Laser-Scan Ltd., Science Park, Milton Rd., Cambridge CB4 4FY, UK

---

### **✂ Truth in Antiviral Advertising**

*"Russell Aminzade: Trinity College of VT" <AMINZADE@uvmvax.bitnet>  
Mon, 9 Dec 1991 07:17 EST*

An advertisement has been running in major computer professional magazines that I find both obnoxious and dangerous. I've seen it in several places, but I'm looking at the inside back cover of the December 2, 1991 PC WEEK (Vol 8. #48). It's an ad for Central Point Software's "Central Point Anti-Virus."

The ad has an illustration of nine computer screens. Eight of them appear to show illustrations of the results of these virii, but to anyone familiar with one or more of them they are obviously "artists interpretations."

Though I haven't encountered every virus "shown," it appears that all of these screens embellish the actual results of the virus, not only making the results of infection look scarier, but giving some expensive publicity to the authors of the Stoned Virus, Friday the 13th Virus, Datacrime Virus, Aircop, Ping Pong, and Falling Letters.

The RISK here, of course, is that giving free publicity to virus authors will

encourage them (and others) to new heights of "creativity". I'm angry in part because I have been victimized by computer virii. I think I've got at least some understanding of the mind of a computer vandal, and the only motivation I could see for releasing a virus would be a desire to see your program widely publicized and your programming "skill" demonstrated. This ad takes it one step further, prominently identifying and enhancing (in garish color) the on-screen look of the virus.

I would feel the same way if I was a park system manager, and a company that sold cleaning agents highlighted the work of a graffiti artist who was well-known in my town. If they also hired professional artists to improve the quality of this punk's graffiti, and ran photographs showing statues and benches allegedly painted by him or her, I'd be raging mad.

Central Point makes some pretty good software. I've purchased some of it (not this product, though). I angered that they seem willing to stoop this low to sell their product. I also wonder how long it will be before some company is willing to stoop low enough to unleash some nasty code from which their product can protect users.

---

### **✂ Re: Pentagon computers vulnerable**

*<smb@ulysses.att.com>*

*Mon, 02 Dec 91 19:55:12 EST*

I certainly can't speak about all of the break-ins. But I was part of a team that monitored many such attempts -- and these were very definitely traced back to the Netherlands. For more details, see Bill Cheswick's paper at the forthcoming Usenix conference.

As for the notion that it's up to the U.S. military to take precautions -- nonsense! What ever happened to ethics? Is it not sufficient that it's their computer -- for almost any value of ``their" -- and they don't want you there? I note that Herschberg's students have prior permission to conduct their break-ins. That's fine -- I not only have no problem with that, I conduct such authorized break-ins myself as part of my job. Again, though, note that I'm acting with prior permission.

--Steve Bellovin

---

### **✂ Post-structuralism and Technology**

*Phil Agre <pagre@weber.ucsd.edu>*

*Mon, 2 Dec 91 17:20:07 pst*

John Bowers (University of Manchester) and I were talking a couple months ago about various interesting people who have been studying technological issues using new-fangled methods from philosophy, literary criticism, and sociology. One recurring theme is the influence of "post-structuralists" like Derrida, Foucault, Lacan, and Deleuze [\*]. We realized, though, that these folks are all scattered among disciplines and countries, so that a lot of them don't yet know each other. So we've started up a network discussion group for such

people and their sympathizers. Its main purpose is to get everyone introduced and exchanging papers, though perhaps some interesting discussion will start up as well. Its address is [postech@weber.ucsd.edu](mailto:postech@weber.ucsd.edu). Anyone who wants to be included can send a note to [postech-request@weber.ucsd.edu](mailto:postech-request@weber.ucsd.edu). (Make sure to include a network address that's accessible from the Internet: [me@here.bitnet](mailto:me@here.bitnet), [uucpnode!me@gateway.somewhere.edu](mailto:uucpnode!me@gateway.somewhere.edu), [me@machine.here.ac.uk](mailto:me@machine.here.ac.uk), [me@ibm.com](mailto:me@ibm.com), or whatever.) We'll collect addresses for a month or so; then we'll invite everyone to describe their work and see what happens.

Phil Agre, UCSD

[\*] The relevance to Risks is that a number of these people tend to take a dim view of technology as a system of social practices, and have novel things to say about why we should care. Foucault in particular has defined an interesting broad sense of "technology" that includes both the physical machinery and the kinds of cultivated selves that together, he argues, make up the deep workings of power. These ideas have led to some challenging new work, such as Valerie Walkerdine's book "The Mastery of Reason" (Routledge, 1988), which uses ideas from Foucault and Lacan in a genuinely deep way to explain how children learn to use mathematical language.

---

### **✂ Chaos Congress 91 Program**

*Klaus Brunnstein <[brunnstein@rz.informatik.uni-hamburg.dbp.de](mailto:brunnstein@rz.informatik.uni-hamburg.dbp.de)>  
12 Dec 91 16:08 +0100*

I just receiving the program of Chaos Congress 1991 (over 300 lines, in German), the following is a condensed survey/translation:

8th Chaos Communication Congress:

"Hitchhiking through the Networks - The European Hacker Party"

-----  
Friday, Dec.27 (12:00) to Sunday, Dec.29 (16:00), 1991  
Eidelstedter Buergerhaus, Hamburg-Eidelstedt (54), Elbgaustr.12

Fee: CCC members 20 DM; non-members: 30 DM; press: 50 DM;  
commercial participants: 150 DM.

Program:

Fri 27 11:00 press conference  
12:00 Opening session, welcome  
12:30 Informatics and Ethics  
12:30 Corn Flake Whistles and new methods (workshop)  
12:30 Journalists and new media  
  
14:30 Liability in cases of program faults and viruses  
(Freiherr von Gravenreuth, lawyer)  
  
16:30 Data protection - theory and practice  
16:30 DTP  
16:30 Btx DocuSystem (Btx=minitel)  
  
17:30 Feminin computer handling (only female participants!)

19:00 Questions of nomenclature and definitions

Sat 28 10:00 ComLink and APC (regional networks for social communication and environment protection)

10:00 Waffle (UUCP on MS-DOS)

10:00 Mercury/Hermes (UUCP on Atari ST)

10:00 AmigaUUCP (UUCP on Amiga)

12:00 Individual Network (IN) for private communication)

12:00 Zerberos

12:00 Unix

14:00 Mailboxes and telecommunication as seen from German PTT  
Dr. Ruetter, German Telecom

14:00 TeX

14:00 MUD - Cyberspace (Multi User Dungeons)

16:00 Net services (email, news, IRC, FTP, Telnet, remote login,  
Talk ...)

16:00 Workshop Mailboxes and legal status

16:00 Voice Mail and PID

18:30 Citizen Networks, example Gay-Net

18:30 Stupidity in Networks (#3)

18:30 Workshop Net services

Sun 29 11:00 Computer Viruses - State of the Art: Morton Swimmer (VTC)

11:00 Citizen Packet Radio

11:00 Hack center: net demonstrations (INTERNET)

13:00 10 years CCC

13:00 Workshop on Viruses - questions and discussion (M.Swimmer)

13:00 RISC - CISC comparison

15:00 Closing session

16:00 Party

If you wish to receive the full German program, including details on location (telephone/fax number..), how to arrive and get rooms etc, please contact me.  
Klaus Brunnstein, University of Hamburg (Dec.12,1991 at 4:00 pm German time)



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 12: Issue 69

Monday 16 December 1991

## Contents

- [800 telephone outage due to software upgrade](#)  
[PGN](#)
- [Stock-listings typo: The possibilities are scary.](#)  
[James Parry](#)
- [More on Lauda crash and computers](#)  
[Nancy Leveson](#)
- ["Questioning Technology" in WHOLE EARTH REVIEW](#)  
[Rodney Hoffman](#)
- [Privacy of Email](#)  
[James Ting Lui](#)
- [More on E911 and representation](#)  
[Bob Frankston](#)
- [Re: Computer records track killer](#)  
[Brinton Cooper](#)
- [Re: The description is right, only the language is wrong](#)  
[Scott E. Preece](#)
- [The EFF Pioneer Awards](#)  
[Gerard Van der Leun](#)
- [Info on RISKS \(comp.risks\)](#)

---

### 800 telephone outage due to software upgrade

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

Sat, 14 Dec 91 12:24:37 PST

AT&T Restores '800' Service

BASKING RIDGE, N.J. (AP, Friday the 13th, December 1991)

Thousands of toll-free "800-number" calls were blocked throughout the East on Friday night, American Telephone & Telegraph said. The outage struck at 7:20 p.m. as technicians loaded new software into computers in Alabama, Georgia and New York, said Andrew Myers, an AT&T spokesman. The software identifies and transfers 800 calls, he said. Several thousand calls from New England to the South were affected.

The company restored service around 9 p.m., when it switched back to old

software. AT&T plans to use the old software until it can find and fix problems with the new. "Obviously we don't like it when a single call doesn't get through, but I wouldn't consider this a serious problem," Myers said.

---

### ✂ **Stock-listings typo: The possibilities are scary.**

*James 'Kibo' Parry <kibo@world.std.com>*

*Sat, 14 Dec 91 18:27:17 -0500*

This is a quote from a message I just received (sent Sat, 14 Dec 91)

> investor's daily has what i hope is a typo in it today  
> ibm is listed at 0-1/16, down 88-1/2

Now, the question is, what happens if a typo gets into the electronic stock quotations that are monitored by trading programs? Someone's computer sees IBM losing most of its value, dumps it all ASAP...

kibo@world.std.com James Parry, 271 Dartmouth St. #3D, Boston MA 02116  
(617) 262-3922 Independent graphic designer and typeface designer.

---

### ✂ **More on Lauda crash and computers**

*<leveson@cs.washington.edu>*

*Sun, 15 Dec 91 07:03:26 -0800*

>From the Seattle Post-Intelligences, Saturday December 14:

"Boeing Hush-up Charged" by Bill Richards

A former Boeing computer expert said yesterday that the company ordered him to play down his discovery of a software flaw in a critical control unit that could have triggered last May's fatal crash of a Lauda Air Boeing 767. Darrell Smith, a computer software engineer employed as a troubleshooter by Boeing in 1989 and 1990, said in an interview with the P-I that he warned the company last year of problems with software that runs the "proximity switch electronics unit" (PSEU) on Boeing's 747 and 767 jetliners.

The device allows the plane's computerized parts to electronically converse. Smith said he told Boeing officials the software could trigger a rogue signal that would cause the plane's computer-driven systems to malfunction. But Smith said Boeing officials in charge of the troubleshooting program told him they "didn't want to get anybody excited" and ordered him to omit any mention of potential system-wide problems resulting from the flawed software from his formal report. Instead, he was told to report just on the PSEU's internal problems, he said. "They said this is a non-critical system and I couldn't use terms like `crash' or `catastrophic' in the report because they didn't want people to get excited," he said.

Boeing spokesman Chris Villiers said yesterday the company hasn't had time to study all of Smith's allegations. Villiers said Boeing doesn't believe the PSEU was responsible for the Lauda Air crash. Smith's concerns about the unit's software on the 747 has been "addressed and resolved," Villiers said.

Smith, who has 13 years experience as a computer engineer, resigned in June 1990 after turning in what he called a "diluted" report with no mention of the potential ramifications from the software flaws. Boeing awarded him its Certificate of Outstanding Performance just before he quit. Smith, ..., said he told Boeing officials the software contained an "architectural flaw" that could lead the unit to send a random signal to other electronic systems within a jetliner, providing them with false information. So poorly designed was the PSEU software, he said, that he recommended that it be completely redesigned.

One of the electronic subsystems linked to the PSEU is the auto-restow, which is supposed to automatically retract a jet's backup ground braking system, the thrust reverser, if it accidentally starts to deploy in flight. [old news about the cause of the accident omitted].

While Villiers said that the PSEU can electronically converse with the auto-restow system on the 767, he said it could only order the system to retract the thrust reversers, not deploy them. Villiers said Boeing tested the software system in the 767 and found no evidence that the PSEU unit was putting out false messages to other systems. [Wishy washy statement by FAA omitted]

But Smith said that because the software's false messages are random, it is almost impossible to determine in a laboratory setting if the PSEU software isn't working. "It all depends on what is going on with the airplane at the time," Smith said. "There's no way to repeat the exact conditions that would cause the messages to be sent. It can cause the system to crash, or get false information, or just go crazy." For example, Smith said, the control unit could notify the rest of the electronic subsystems that the plane's landing gear was down while the plane was still in flight. That would cause the auto-restow to switch to a ground-speed mode check, Smith said. The system would then "see that the aircraft was going too fast, and kick in the reverse thrusters -- while the aircraft was really in flight."

[more old news about cause of crash and repetition of above deleted]

Smith said that Boeing passed on the report to Eldec Corp. of Lynnwood, which wrote the software for the company, and the findings were independently verified by other Boeing computer experts. The report says Eldec's software violated seven of Boeing's own software specification.. "This problem ... is a very real and serious impediment to the correct operation of the PSEU," it concludes. Thomas Brown, Eldec's president and COO, said yesterday that the company was not aware of Smith's report. Brown said that while Eldec produced the software for PSEU units on both the 747-400 and 767, he does not know whether software could trigger the auto-restow or activate the thrust reverser system on either jet. "We are not in a position to answer that question," Brown said. "We don't know all the uses of our signals. Only Boeing can answer that."

[P.S. This story was followed by a story that Lauda had just ordered four Boeing 777 jetliners and was the seventh airline to do so. It now has 86 firm orders for the 777.]

---

## "Questioning Technology" in WHOLE EARTH REVIEW

*Rodney Hoffman <Hoffman.El\_Segundo@Xerox.com>*

*Sat, 14 Dec 1991 16:06:44 PST*

The Winter 1991 issue of WHOLE EARTH REVIEW is a special focus issue on "Questioning Technology". I haven't yet read it, but it certainly contains some provocative feature articles (summaries are from the magazine):

Excerpt from the 1991 book "In the Absence of the Sacred: The Failure of Technology and the Survival of the Indian Nations" by Jerry Mander. Our unquestioning faith in technology's ability to solve problems has led us to the "greatest environmental crisis since the dawn of human life."

"Artifact/Ideas and Political Culture" by political theorist and author Langdon Winner. Political ideas embedded in our technological tools often conflict with our stated ideals. "No innovation without representation" is the first of three steps toward technological democracy.

"Assessing the Impacts of Technology" by Linda Garcia, a project director and senior analyst at the Office of Technology Assessment. Describes the approach and political pressures of OTA's work.

"Renegotiating Science's Contract" by Howard Levine, philosopher and former director of the National Science Foundation's Public Understanding of Science Program. We need greater public participation in the formation of scientific and technical decisions.

"Reclaiming Our Technological Future" by Patricia Glass Schuman, president of the American Library Association and of Neal-Schuman Publishers. Debunks current myths of a paperless future.

"Privacy and Technology" by MIT sociologist Gary T. Marx. Examines data-gathering techniques and offers tips on protecting your privacy.

Additional pieces:

"NASA Goes to Ground" by Wendy Alter and James Logan

"Designer As Savior, Designer As Slave" by J. Baldwin

"Beauty and the Junkyard" by Ivan Illich

"Technology's Backside" by Marshall P. Smith

"Figure and Ground: Information Technology and the Economic Marginalization of Women" by Elin Whitney-Smith

"Why Multi-Media Publishing is a Crock" by Tim Oren

"The Vision Vine" by Earl Vickers

"Genes, Genius, and Genocide" by Jason Clay

---

## Privacy of Email

*James Ting Lui <jl3p+@andrew.cmu.edu>*

*Thu, 12 Dec 1991 16:19:54 -0500 (EST)*

The following is an article that appeared in one of this week's Pittsburgh Post-Gazettes. I was originally going to paraphrase the article, but I think that the entire article is relevant. So here it is:

Is 'E mail' private on firm's computer? (by Glenn Rifkin, New York Times)

When Alana Shoars arrived for work at Epson America Inc. one morning in January 1990, she discovered her supervisor reading and printing out electronic mail messages between other employees. As electronic mail administrator, Shoars was appalled. When she had trained employees to use the computerized system, Shoars told them their mail was private. Now a company manager was violating that trust. When she questioned the practice, Shoars said, she was told to mind her own business. A day later, she was fired for insubordination. She has since filed a \$1 million wrongful termination suit.

A spokesman for Epson America, which is based in Torrance, CA, refused to discuss Shoars's account of the monitoring episode and insisted that her dismissal had nothing to do with her questioning of the electronic mail practice. He denied that Epson America, the United States marketing arm of a Japanese company, had a policy of monitoring electronic mail.

The Shoars case has brought attention not only to issues of technology and employee privacy, but also to broader questions of ethics among computer professionals. By taking a public stand, Shoars has become a visible exception in a profession that tends to ignore or avoid ethical issues, according to academicians and consultants who monitor the field. Although Shoars has found a new job as electronic mail administrator at Warner Brothers in Burbank, CA, she still bristles about Epson: "You don't read other people's mail just as you don't listen to their phone conversations. Right is right and wrong is wrong."

Michael Simmons, chief information officer at the Bank of Boston, disagrees totally. "If the corporation owns the equipment and pays for the network, that asset belongs to the company, and it has a right to look and see if people are using it for purposes other than running the business," he said. At a previous job, for example, Simmons discovered that one employee was using the computer system to handicap horse races and another was running his Amway business on his computer. Both were fired immediately. "The guy handicapping horses was using 600 megabytes of memory," Simmons said.

Federal Express, American Airlines, Pacific Bell and United Parcel Service all have electronic-mail systems that automatically inform employees that the company reserves the right to monitor messages. But many companies have yet to formulate clear policies. "It's highly irresponsible for an employer not to have a policy," said Mitchell Kapor, former chairman of Lotus Development Corp., who left the company five years ago.

Some believe, however, that even if there is advance notice, the monitoring of electronic mail or searching through personal files is flat out wrong. One who takes that position is Eugene Spafford, a computer science professor at Purdue University. He said: "Even if a company does post notice, is that something it should do? The legal question may be answered, but is it ethical? The company may say it is, employees say it isn't, and there's a conflict."

Though they oversee the electronic mail networks, computer professionals have generally removed themselves from such debates. Simmons said that if ethics were the topic of a meeting of information systems experts, "it would be a very short meeting."

Technologists approach the information resource in a distinctive way, said

Detmar Straub, assistant professor of management information services at the University of Minnesota. "They say 'If the system can do it, let's do it,' rather than 'should the system do it?'" Straub said. "I've talked to systems managers who say they wouldn't hire a programmer who couldn't break into any system." But as computers and networks extend their reach into global business, such attitudes may no longer suffice.

"Information systems people should be held to a higher level of ethics than the general population, just as doctors and lawyers are," said Donn B. Parker, a senior management consultant at SRI International in Menlo Park, CA.

---

### **More on E911 and representation**

*<frankston!Bob\_Frankston@world.std.com>*

*12 Dec 1991 13:44 -0400*

My cousin, who lives in Wurstboro NY told me that her address was changed from a more rural form to one that is suitable for the 911 database. Just a reminder that the representation problem works both ways, we can change the representation to conform to the data or we can change the data to conform to the representation. The latter, in fact, is what happens when the a medical diagnosis must conform to the data coding.

Another comment on telecom and 911 is that 911 doesn't work universally for the same reason that I cannot simply tell my son to always dial my 800 number or my pager number to reach me. The problem is the design flaw in the phone system that requires I not only know my destination phone number, but also the particular rules of the phone (and PBX or hotel) I happen to be using. Maybe some of this will get fixed in ISDN, but for now, I'd like to start a campaign to get a standard for dialing that is location-independent.

Ideally, we'd replace "9" on a PBX with "\*\*\*" to mean a local call. Alternatively, we'd establish a new access code such as "\*\*\*" that would always place one into universal dialing mode that would allow dialing of 1-xxx. And since "1" is the North American access code, it would allow uniform dialing of any international number. (Yes, it would be very easy to accidentally dial the codes for other countries -- a solvable problem).

The key here is that if we want to take advantage of telecommunications technology we mustn't accept historic accidents like "9" to exit a PBX and the inability to use area codes on many local calls, but must tame the technology. More to the point, if we can renumber our houses in the interest of safety then we should be willing to complete the process and make the phone simple to use -- especially for those who are panicked or simply not ready to deal with arcania. (I also want check digits on phone numbers but that is a separate issue).

Maybe we can use the laws protecting the handicapped to argue that the phone system is not sufficiently accessible in its present form.

[In Wurstboro, The Wurst is Yet to Come.  
Neither a wurstboroer nor a wurstlender be.

Unless you are an Auslaender. 'Aus bayou?  
You never sausage nonsense before? At SIGSOFT '91  
in New Orleans, there were lots of sausages. And maybe  
even the wurst computer-related pun you ever heard? PGN]

---

**✂ Re: Computer records track killer (Jenkins, [RISKS-12.68](#))**

*Brinton Cooper <abc@BRL.MIL>  
Sun, 15 Dec 91 20:41:14 EST*

Robert Jenkins reports on one John Tanner who  
"murdered his student girlfriend and hid her body underneath the  
floorboards of her house..." and how "...his story began to fall apart"  
when, "He told the police that he and the girl had taken a bus ride  
together to the train station at a time when she was already dead." A  
computer check of the company's records showed, "Only one person got on  
the bus and bought a ticket to the station at the time Mr Tanner claimed."

Mr Jenkins calls this "... another example of low-level, invisible,  
surveillance that computers introduce into our lives..." as though it were  
something objectionable, generally to be avoided.

Mr Jenkins missed the point. The computerized records were used in a way that  
would pass strict Constitutional test in the USA, yet contributed (I assume) to  
the arrest and conviction of a murderer. In fact, the \*identity\* of the  
passengers was not recorded. You might say that Mr Tanner was convicted as  
much by mathematics as by computerization. Then, perhaps this would be  
"...another example of low-level, invisible, surveillance that mathematics  
introduces into our lives."

\_Brint

---

**✂ Re: ... only the language is wrong (Franklin, [RISKS-12.58](#))**

*Scott E. Preece <preece@urbana.mcd.mot.com>  
Sat, 14 Dec 91 23:00:08 -0600*

| It is hard to believe that this error would have occurred, and not been  
| caught, before the age of computers. The RISK here is that as the chain  
| of events handled purely by computers lengthens, it becomes possible for  
| relatively major errors to occur unnoticed, because no one is looking  
| closely at the output at any stage.

The observation is clearly correct, but the claim in the first sentence is  
simply incorrect. Such errors can and do happen all the time at every  
newspaper in the world. Proofreaders are, as they say, human and to err is, as  
we used to admit before we took to blaming computers for everything, human. I  
haven't seen any French in my local paper's classified, but I have seen blocks  
of Latin (a classical layout mockup tool), ads set in totally pided type, ads  
run upside down and, occasionally, backwards, ads run in the wrong section,  
etc., etc.

scott preece, motorola/mcg urbana design center 1101 e. university, urbana, il  
61801 uucp: uunet!uiucucx!udc!preece 217-384-8589

---

## **✶ The EFF Pioneer Awards**

*Gerard Van der Leun <van@eff.org>*

*Fri, 13 Dec 1991 17:02:52 -0500*

### THE ELECTRONIC FRONTIER FOUNDATION'S FIRST ANNUAL PIONEER AWARDS CALL FOR NOMINATIONS

(Attention: Please feel free to repost to all systems worldwide.)

In every field of human endeavor, there are those dedicated to expanding knowledge, freedom, efficiency and utility. Along the electronic frontier, this is especially true. To recognize this, the Electronic Frontier Foundation has established the Pioneer Awards. The first annual Pioneer Awards will be given at the Second Annual Computers, Freedom, and Privacy Conference in Washington, D.C. in March of 1992.

All valid nominations will be reviewed by a panel of outside judges chosen for their knowledge of computer-based communications and the technical, legal, and social issues involved in networking.

There are no specific categories for the Pioneer Awards, but the following guidelines apply:

- 1) The nominees must have made a substantial contribution to the health, growth, accessibility, or freedom of computer-based communications.
- 2) The contribution may be technical, social, economic or cultural.
- 3) Nominations may be of individuals, systems, or organizations in the private or public sectors.
- 4) Nominations are open to all, and you may nominate more than one recipient. You may nominate yourself or your organization.
- 5) All nominations, to be valid, must contain your reasons, however brief, on why you are nominating the individual or organization, along with a means of contacting the nominee, and your own contact number. No anonymous nominations will be allowed.
- 5) Every person or organization, with the single exception of EFF staff members, are eligible for Pioneer Awards.

You may nominate as many as you wish, but please use one form per nomination. You may return the forms to us via email at:

pioneer@eff.org.

You may mail them to us at:

Pioneer Awards, EFF,  
155 Second Street  
Cambridge MA 02141.

You may FAX them to us at:

(617) 864-0866.

Just tell us the name of the nominee, the phone number or email address at which the nominee can be reached, and, most important, why you feel the nominee deserves the award. You can attach supporting documentation.

Please include your own name, address, and phone number.

We're looking for the Pioneers of the Electronic Frontier that have made and are making a difference. Thanks for helping us find them,

The Electronic Frontier Foundation

-----EFF Pioneer Awards Nomination Form-----

Please return to the Electronic Frontier Foundation via email to:

[pioneer@eff.org](mailto:pioneer@eff.org)

or via surface mail to EFF 155 Second Street, Cambridge, MA 02141 USA;

or via FAX to USA (617)864-0866.

Nominee:

Title:

Company/Organization:

Contact number or email address:

Reason for nomination:

Your name and contact number:

Extra documentation attached:

-----EFF Pioneer Awards Nomination Form-----

[USE WHATEVER SPACE YOU NEED; BLANKS AND UNDERSCORES DELETED BY 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 12: Issue 70

Wednesday 18 December 1991

## Contents

- [Life, Death, and Faxes -- Convicted forger released by bogus fax](#)  
[PGN](#)
- [BT ordered to pay damages for keyboard injuries](#)  
[Olivier M.J. Crepin-Leblond](#)
- [Re: Privacy of Email](#)  
[Eric Florack](#)
- [Re: More on E911 and representation](#)  
[Erling Kristiansen](#)
- [Software safety, formal methods and standards](#)  
[Jonathan Bowen](#)
- [2nd Conf on Computers, Freedom, and Privacy](#)  
[Lance J. Hoffman](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✂ Life, Death, and Faxes -- Convicted forger released by bogus fax**

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>  
Wed, 18 Dec 91 12:06:13 PST

Jean Paul Barrett, a convict serving 33 years for forgery and fraud in the Pima County jail in Tuscon, Arizona, was released on 13Dec91 after receipt of a forged fax ordering his release. It appears that a copy of a legitimate release order was altered to bear HIS name. Apparently no one noticed that the faxed document lacked an originating phone number or that there was no "formal" cover sheet. The "error" was discovered when Barrett failed to show up for a court hearing.

The jail releases about 60 people each day, and faxes have become standard procedure. Sheriff's Sergeant Rick Kastigar said "procedures are being changed so the error will not occur again." [Abstracted by PGN from "Fraudulent Fax Gets Forger Freed", an item in the San Francisco Chronicle, 18Dec91, p.A3]

The RISKS annals contain earlier cases of people getting out of jail by altering the prison computer system database (LA County) or nearly succeeding

in doing so (Santa Clara). Authentication sufficient to automagically detect bogus messages (EMail, Fax, voice mail, etc.) has been discussed here in the past, and might have been useful here. But probably not... PGN

---

### ✂ BT ordered to pay damages for keyboard injuries

"Olivier M.J. Crepin-Leblond" <UMEEB37@vaxa.cc.ic.ac.uk>  
Mon, 16 Dec 91 22:46 BST

Oracle Teletext service (ITV, UK), 16-Dec-1991, has just reported that two former keyboard operators have been awarded 6000 pounds Sterling damages (approx. \$10000) against British Telecom for pain caused by their work. It appears that the two operators suffered repetitive strain injury (RSI) because of unsuitable chairs. Judge John Byrt, sitting at a court in London's Guildhall, said that BT was not negligent by making them work too hard. " Union officials said the ruling was a breakthrough in making employers take responsibility for serious injuries caused by high-speed work on computers. "

Olivier M.J. Crepin-Leblond, Elec. Eng. Dept., Imperial College London, UK.

---

### ✂ Re: Privacy of Email (Lui, [RISKS-12.69](#))

<Eric\_Florack.Wbst311@xerox.com>  
Tue, 17 Dec 1991 07:28:21 PST

<>A spokesman for Epson America, which is based in Torrance, CA, refused to discuss Shoars's account of the monitoring episode and insisted that her dismissal had nothing to do with her questioning of the electronic mail practice. He denied that Epson America, the United States marketing arm of a Japanese company, had a policy of monitoring electronic mail.<<

Allow me to suggest that there may be some merit in this statement. I would further suggest that there was far more to Epson v Shoars than we have been led to think. Some stories I've seen circulating suggest that Shoars was far from what you would call the ideal worker, in terms of what she produced. At this point, Epson was searching for a way to eliminate her. Here, their problems began. HAVe any of you who happen to be supervisors, attempted to fire a non-productive worker who was among the people supposedly trampled on by society? I'm talking about EEO laws, of course.

(Before you get bent outta shape, I don't object to the concept of equality, certainly... just the way the idiots in Washington have decided to provide it.)

The Shoars case is one where the real issues were being masked by supposed abuses of electronic mail, IMHO. It is perhaps this reason, that causes many to think that it's not the landmark case that Shoars, as well as certain groups, would have you think.

Another point... one that nobody seems to get... is her old super still working for the company?

My old school-mate, Gene Spafford and I disagree on this one, I'm afraid. As Mike Simmons says:

"If the corporation owns the equipment and pays for the network, that asset belongs to the company, and it has a right to look and see if people are using it for purposes other than running the business,"

I would think restraint could be used on the part of the employer... and is in most cases.... (FOr example, if my employer didn't, you'd not be reading this).

However, I would point out that with so much work today being done on company computers... so much of the work day focused on that one item... that watching Email is one of the few tools left to the employer to monitor the employee. Sit accross an office from someone on their terminal. Can you tell if they're doing cost estimates, if if they're laying odds on the ponies, or perhaps playing D&D?

As someone recently said: If a train station is where a train stops, what is a work station?

Opinions are my own, of course, and may or may not agree with official policy... but give me time....

---

### **✉ Re: More on E911 and representation ([RISKS 12.69](#))**

*"E. Kristiansen - WMS" <EKRESTIA@estec.bitnet>  
Wed, 18 Dec 91 09:04:11 CET*

In the Dutch telephone numbering plan, all area codes starting with 06 were unused until a few years ago, presumably "reserved for future use". When this empty can was finally opened, it quickly turned into a can of worms. Within the 06 prefix today, you find:

- toll free services
- services carrying a surcharge, such as party lines (10 callers randomly put in "teleconference"), sex lines, etc.
- PTT special services such as Information, Fault reporting, Time, Weather
- Private and public companies and institutions wanting a nation-wide number

And, since mid 1991, the notion-wide emergency number 06-11!

The first digit following the 06 does provide some classification, for example, 06-0 and 06-4 are toll free numbers. But this is not consistent. 06-11 is toll free, as you might assume, but the number as such is not in the 06-0 or 06-4 number group. The significance of the third digit is not widely publicized, so it is not obvious what the charge for a certain number will be, unless you study the subject rather carefully.

And now the computer RISK:

Many companies have programmes their PABXs to disallow calling 06 numbers because most of these have little or no relevance to the company, and many carry rather heavy surcharges. In so doing, calling the 06-11 emergency number is also blocked!

Some companies start to realize the problem, and do something about it. But, to my opinion, the real problem is a bad numbering plan. An emergency number should really stand out from "common" numbers, and not be grouped together with surcharge numbers.

Finally, I totally agree with Bob Frankston that more standardization is called for in numbering. I travel quite a lot to several countries, and often have difficulty remembering the international prefix when calling out from a particular country.

Erling Kristiansen - ESTEC, Noordwijk, The Netherlands

---

## **Software safety, formal methods and standards**

*<Jonathan.Bowen@prg.oxford.ac.uk>*

*Wed, 4 Dec 91 16:54:37 GMT*

I am sending you an edited version of the messages I received back from my request in this area. I have posted this to the comp.software-eng and comp.specification newsgroups. It is probably too long for comp.risks, but perhaps it would be worth including a pointer to these two newsgroups.

Jonathan Bowen, PRG, Oxford.

[Yes, it is much too long -- it does not even fit in one issue. It includes responses from the following:

"Ben L. Di Vito" <bld@gov.nasa.larc.air16>  
steph@edu.uci.ics.rennes  
bryan@edu.Stanford.asterix (Douglas L. Bryan)  
ramu@com.mot.corp.cadsun  
kuhn@swe.ncsl.nist.gov (Rick Kuhn)  
Steve Emmerson <steve@edu.ucar.unidata>  
Nancy Leveson <nancy@murphy.ICS.UCI.EDU> (2)  
Al Stavely <al@edu.nmt.jupiter>  
Chris.Holt@newcastle.ac.uk (Chris Holt)  
John Rushby <RUSHBY@com.sri.csl>  
David Parnas <parnas@ca.mcmaster.eng.qusunt>  
Charles R. Martin" <martinc@edu.unc.cs>  
Debra Sparkman <Debra\_Sparkman.ADD@gov.llnl.ocf.lccmail>  
Jim Pyra <jpyra@ca.ns.nstn.fox>  
heiner <heiner@uucp.b21> [unido!b21!heiner]  
JZ01 <JZ01%SWT.DECNET@net.the.relay>

It can be FTPed from the CRVAX RISKS: DIRECTORY as RISKS-12.BOWEN.  
REMEMBER THE COLON IN "CD RISKS:" ; IT IS VITAL... PGN]

---

## **2nd Conf on Computers, Freedom, and Privacy**

*Lance J. Hoffman <hoffman@seas.gwu.edu>*

*Mon, 9 Dec 91 14:28:09 EST*

First Announcement of

THE SECOND CONFERENCE ON COMPUTERS, FREEDOM, AND PRIVACY  
L'Enfant Plaza Hotel, Washington DC March 18-20, 1992

(A longer, complete, electronic version of this announcement is available by sending a request with any title and any message to [cfp2-info@eff.org](mailto:cfp2-info@eff.org).)

(The printed announcement (brochure) is available -- see end of this notice.)

The rush of computers into our workplaces, homes, and institutions is drastically altering how we work and live, how we buy and sell, and with whom we communicate. Computers are obliterating traditional political and organizational boundaries, making time zones irrelevant, and bridging diverse cultures. They are fundamentally changing our culture, values, laws, traditions, and identities.

The turmoil of the changes calls into question many old assumptions about privacy, freedom of speech, search and seizure, access to personal and governmental information, professional responsibilities, ethics, criminality, law enforcement, and more. The only way to sort out these issues and arrive at a consensus for action is to acknowledge that we don't know the answers -- and then, with reason and good will, to find the answers through discussion and education. That's why the Conference on Computers, Freedom, and Privacy was founded in 1991.

The Computers, Freedom, and Privacy Conference is unique. It has no "agenda for change". It seeks only to bring together people from all the major communities and interest groups that have a stake in the new world being shaped by information technology, so that they may share their ideas, ideals, concerns and experiences.

At the first conference, hundreds of people from the fields of law, computer science, law enforcement, business, public policy, government, education, research, marketing, information providing, advocacy and a host of others met for several days. It was the first time such a diverse group had ever assembled, and the exchange of ideas and points of view was electric.

The conference is "single-track" -- all participants attend all the sessions. A morning of tutorials at the beginning of the conference will help participants get up to speed in specific "hot" areas. The conference sessions themselves take up timely and, at times, thorny issues. Each session aims for a balance of perspectives in order to assist diverse groups appreciate the views of others. A brief examination of the long list of sponsoring and supporting organizations will reveal that this respect for diverse outlooks is built into the conference from the ground up.

The question is no longer whether information technologies will change our world. They are, now. The real question is how we, as citizens and professionals, will respond to and manage that change. Those at the Second Conference on Computers, Freedom, and Privacy will lead the way.

Sponsors: Association for Computing Machinery, Special Interest Groups on Computers and Society, Communications, Security, Audit, and Control

Host: Department of Electrical Engineering and Computer Science



### Making Information Law and Policy

Jane Bortnick, Congressional Research Service, Library of Congress

Information policy is made (or not made) by a bewildering array of government officials and agencies. This tutorial gives a road map through this maze of laws, regulations, practices, etc.

### Getting on the Net

Mitchell Kapor, Electronic Frontier Foundation

Practical issues of access to the Internet for the nontechnical end-user, including basic services (email, USENET, ftp), PC and Mac-based network applications, and net-speak.

### Communications and Network Evolution

Sergio Heker, JVNCNet

The underlying technical infrastructure for the Internet, for persons not deeply immersed in the technology. Possible future technologies and projects, and what privacy and freedom problems they may bring.

### Private Sector Privacy

Jeff Smith, Georgetown University

An introduction to laws, rules, and practices regarding personal information gathered and stored by private organizations such as direct marketers, hospitals, etc.

Group B: 10:30 a.m.

### Constitutional Law for Nonlawyers

Harvey Silverglate, Silverglate & Good

An overview of Constitutional law with special emphasis on the First, Fourth, and Fifth Amendments and the application of their principles in the information age.

### Computer Crime

Don G. Ingraham, Alameda County District Attorney's Office

Investigation, search, seizure, and evidence requirements for pursuing computer crime. For computer users, owners, sysops, and investigators and attorneys unfamiliar with computer crime practices.

### Modern Telecommunications: Life after Humpty Dumpty

Richard S. Wolff, Bellcore

Roles and relationships of the key players in telecommunications, developments in communications technology, and new services. Signaling System 7, ISDN, and advanced intelligent network features.

### International Privacy Developments

David Flaherty, University of Western Ontario

Privacy-related developments within the European community, OECD, and the United Nations, and how they affect the United States. Comparison of privacy regulations here and abroad.

#### CONFERENCE PROGRAM

1:00-2:00 p.m. KEYNOTE ADDRESS:

Al Neuharth, Chairman, The Freedom Forum and Founder, USA Today  
"Freedom in Cyberspace: New Wine in Old Flasks?"

The differing legal and regulatory constraints on publishers of newspapers, owners of television stations, and the telephone service providers imply that some dogfights will occur and some tough decisions will have to be made to balance privacy and freedom in the coming decade, since the old wine of 1970's-era regulation will not fit into the new flasks of 21st Century. Mr. Neuharth, a self-proclaimed S.O.B., will give us a peek at his vision of what the future holds.

2:30 pm - 4 pm Who logs on?

- \* Chair: Robert Lucky, AT&T Bell Laboratories
- \* Panel: Linda Garcia, Office of Technology Assessment
- \* Alfred Koeppe, New Jersey Bell
- \* Brian Kahin, Harvard University

4:30 pm - 6 pm Ethics, Morality, and Criminality

- \* Chair: J. Michael Gibbons, Federal Bureau of Investigation
- \* Panel: Scott Charney, U. S. Dept. of Justice
- \* James Settle, Federal Bureau of Investigation
- \* Mike Godwin, Electronic Frontier Foundation
- \* Emory Hackman, Esq. (former president, Capital Area Sysops Association)
- \* Don Delaney, New York State Police

6:00 pm - 7:30 pm RECEPTION

9:00 pm BIRDS OF A FEATHER SESSIONS

THURSDAY, MARCH 19, 1992

9:00 am - 10:30 am For Sale: Government Information

- \* Chair: George Trubow, John Marshall Law School
- \* Panel: Dwight Morris, Los Angeles Times Washington Bureau
- \* Ken Allen, Information Industry Association
- \* Patricia Glass Schuman, American Library Association
- \* Evan Hendricks, Privacy Times
- \* Fred Weingarten, Computing Research Association
- \* Franklin S. Reeder, Office of Management and Budget
- \* Costas Torreagas, Public Technology, Inc.
- \* Robert R. Belair, Kirkpatrick and Lockhart

10:45 am - 12:15 pm Free Speech and the Public Telephone Network

- \* Chair: Jerry Berman, ACLU Information Technology Project
- \* Panel: Henry Geller, The Markle Foundation

- \* Eli Noam, Columbia University
- \* John Podesta, Podesta Associates

12:15 pm - 1:45 pm Luncheon with Address: Bruce Sterling  
"Speaking for the Unspeakable"

Mr. Sterling will gamely attempt to publicly present the points of view of certain elements of the "computer community" who are not represented at CFP-2. He will speak up for those who, in his words, are too "venal, violent, treacherous, power-mad, suspicious or meanspirited to receive (or accept) an invitation to attend.

2:00 pm - 3:30 pm Who's in Your Genes?

- \* Chair: Phil Reilly, Shriver Center for Mental Retardation
- \* Panel: John Hicks, FBI Laboratory
- \* Tom Marr, Cold Spring Harbor Laboratory
- \* Paul Mendelsohn, Neurofibromatosis, Inc.
- \* Peter Neufeld, Esq.
- \* Madison Powers, Kennedy Center for Ethics, Georgetown University

3:45 pm - 5:15 pm Private Collection of Personal Information

- \* Chair: Ron Plessner, Piper and Marbury
- \* Panel: Janlori Goldman, Privacy and Technology Project, ACLU
- \* John Baker, Equifax
- \* James D. McQuaid, Metromail
- \* James Rule, SUNY-Stony Brook
- \* Mary Culnan, Georgetown University
- \* P. Michael Neugent, Citicorp

5:15 pm - 6:45 pm EFF Awards Reception

9:00 pm Birds of a Feather Sessions

FRIDAY, MARCH 20, 1992

9:00 am - 10:30 am Privacy and intellectual freedom in the digital library

- \* Chair: Marc Rotenberg, Computer Professionals for Social Responsibility
- \* Panel: Robert A. Walton, CLSI, Inc.
- \* Gordon M. Conable, Monroe (MI) County Library System
- \* Jean Armour Polly, Liverpool (NY) Public Library

10:45 am - 12:15 pm Computers in the Workplace: Elysium or Panopticon?

- \* Chair: Alan F. Westin, Columbia University
- \* Panel: Gary Marx, MIT
- \* Mark DiBernardo, National Association of Manufacturers
- \* Kristina Zahorik, Subcommittee on Employment and Productivity, U. S. Senate Labor Committee

12:15 pm - 1:30 pm Lunch (on your own)

1:30 pm - 3:00 pm Who Holds the Keys?

- \* Chair: Dorothy Denning
- \* Panel: Jim Bidzos, RSA Data Security
- \* David Bellin, Pratt Institute

- \* John Gilmore, Cygnus Support
- \* Whitfield Diffie, SunSoft, Inc.

3:00 pm - 4:15 pm Public Policy for the 21st Century  
Co-chairs: Peter J. Denning, George Mason University  
Lance J. Hoffman, George Washington University

## GENERAL INFORMATION

### Registration

Please register for the conference by returning the Conference Registration Form (below) along with the appropriate payment -- check, Visa, or Mastercard. Registration fee includes conference materials, Thursday luncheon, and receptions. The registration is \$295 for ACM members and \$350 for nonmembers, \$65 for full-time students. Tutorials, \$95 (\$35 students).

### Premium for Early Registration

While they last, a limited number of premiums are available to early registrants on a first-come, first-served basis. Early registrants will receive by mail a voucher which they can exchange at the conference for one of a number of premiums. These include:

Videotapes of CFP-1 sessions  
Audiotapes of CFP-1 sessions  
Proceedings of CFP-1  
Computers Under Attack: Intruders, Worms, and Viruses  
by Peter Denning, editor  
Rogue Programs: Viruses, Worms, and Trojan Horses  
by Lance Hoffman, editor  
"Citizen Rights and Access to Electronic Information"  
by Dennis Reynolds, editor  
The Cuckoo's Egg by Cliff Stoll  
The Difference Engine by Bruce Sterling and William Gibson  
Confessions of an S.O.B. by Al Neuharth  
Cyberpunk by Katie Hafner and John Markoff

**CONSIDER REGISTERING BY FAXING THE REGISTRATION FORM BELOW OR TELEPHONING IF YOU ARE INTERESTED IN ONE OF THESE PREMIUMS. THEY WON'T LAST LONG!**

### Registration Scholarships

Full-time students and others wishing to apply for one of a limited number of registration scholarships should send a request to the address listed in the complete announcement, copies of which are available as described elsewhere in this shorter electronic notice.

### Hotel Accomodations

The 1992 Computers, Freedom, and Privacy Conference will be held at the

Loew's L'Enfant Plaza Hotel, Washington, DC. One of the finest hotels in the city, it is just ten minutes from Washington National Airport, five minutes from Capitol Hill. The world-renowned Smithsonian Institution Museums are located within a few blocks.

To qualify for the conference rate of \$105 single or \$110 double, call the hotel reservation line (below) and identify yourself as a CFP-2 participant. To ensure a room at the L'Enfant Plaza, reservations should be made by February 10, 1992. After this date, rooms will be released to the public. Hotel reservations: (800) 243-1166; (202) 484-1000 (local).

Transportation

As a participant in CFP-2, you are eligible for discounted rates as follows: 40% off unrestricted coach fares and 5% off the lowest available fares on specified carriers (all rules and restrictions apply). To receive the best rate available call GW Travel (below) and make your reservations early. Seats may be limited. Please mention that you are attending the CFP-2 Conference. (Code C-6) GW Travel: (800) 222-1223; (301) 897-8001 (local).

Accreditation

The Second Conference on Computers, Freedom, and Privacy has been approved by The George Washington University Medical Center for Category One Continuing Medical Education Units.

Refund Policy

Refund requests received in writing by February 28, 1992 will be honored. A \$50 cancellation fee will apply. No refunds will be made after this date; however, you may send a substitute in your place.

REGISTRATION FORM

YOU CAN NOT REGISTER BY ELECTRONIC MAIL. YOU MAY REGISTER BY MAIL, BY FAX, OR BY PHONE. YOU CAN PRINT THIS REGISTRATION FORM OUT, FILL IT IN, AND MAIL OR FAX IT. OR YOU CAN REQUEST A PRINTED BROCHURE FROM THE "BY MAIL" ADDRESS BELOW, WHICH WILL HAVE A PRINTED ONE-PAGE REGISTRATION FORM IN IT. YOU CAN ALSO OBTAIN THIS PRINTED BROCHURE BY ELECTRONICALLY MAILING A SHORT REQUEST WITH YOUR NAME AND (POSTAL) MAIL ADDRESS TO cfp2@seas.gwu.edu.

\* \* \* \* \* REGISTRATION FORM \* \* \* \* \*

By mail: Conferences & Institutes, The George Washington University, 2003 G St. N.W., Washington, D. C. 20052

By fax (24 hrs., with credit card): Send registration form to (202) 994-7048

By phone (with credit card): (202) 994-7238 (9 a.m. to 5 p.m., EST)

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Affiliation: \_\_\_\_\_

Mailing address: \_\_\_\_\_

City \_\_\_\_\_ State \_\_\_\_\_ Zip \_\_\_\_\_

Country (if not USA): \_\_\_\_\_  
Telephone: \_\_\_\_\_  
FAX number: \_\_\_\_\_  
E-Mail address: \_\_\_\_\_

PRIVACY NOTE: This information will not be sold, rented, loaned, exchanged, or used for any purpose other than official CFP-2 activities. A roster will be distributed to attendees. Please indicate your preference:

\_\_\_\_ Print all information above      \_\_\_\_ Print name only  
\_\_\_\_ Print only name, affiliation, city, state, zip      \_\_\_\_ Omit all above information

REGISTRATION FEES:

Conference fee (check one) \_\_\_\_ ACM member (\$295) \_\_\_\_ Non-member (\$350)  
[includes conference materials, Thursday luncheon, and receptions]

\_\_\_\_ Student (full-time/valid ID): \_\_\_\_ \$65 (no lunch) \_\_\_\_ \$30 (lunch)

Tutorial fee      \_\_\_\_ Tutorial (half-day, 1 or 2 sessions, \$95)  
(Pick 2, 75 min. each)      \_\_\_\_ Student (half-day, 1 or 2 sessions, \$35)

Group A 9:00 a.m.

- \_\_\_\_ T(1) Making Information Law and Policy
- \_\_\_\_ T(2) Getting on the Net
- \_\_\_\_ T(3) Communications and Network Evolution
- \_\_\_\_ T(4) Private Sector Privacy

Group B 10:30 a.m.

- \_\_\_\_ T(5) Constitutional Law for Non-lawyers
- \_\_\_\_ T(6) Computer Crime
- \_\_\_\_ T(7) Modern Telecommunications
- \_\_\_\_ T(8) International Privacy Developments

Please check method of payment:      Amount enclosed: \$ \_\_\_\_\_

\_\_\_\_ Visa      \_\_\_\_ MasterCard      \_\_\_\_ Check (payable to  
The George Washington University)

Credit card number: \_\_\_\_\_

Expiration date: \_\_\_\_\_

Name on card: \_\_\_\_\_

Signature: \_\_\_\_\_

For Continuing Medical Education accreditation, give state and medical #:

\* \* \* \* END OF FORM \* \* \* \* \*

The complete announcement will be mailed to you in printed form via the postal service if you request one by telephone, fax, electronic mail, or regular mail from

CFP - 2  
Office of Conferences and Institutes  
The George Washington University  
2003 G St. NW  
Washington DC 20052

phone (202) 994-7238  
fax (202) 994-7048  
email cfp2@seas.gwu.edu

\* \* \* \* \* END OF ANNOUNCEMENT \* \* \* \* \*

Professor Lance J. Hoffman, Department of Electrical Engineering and  
Computer Science, The George Washington University, Washington, D. C. 20052  
(202) 994-4955 fax: (202) 994-0227 hoffman@seas.gwu.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 12: Issue 71

Weds 24 December 1991

## Contents

- [Illegal sales of confidential data](#)  
[Fernando Pereira](#)
- [The London Stock Exchange "Taurus" System](#)  
[Brian Randell](#)
- [Computer Database of Former E. German State Police \(Stasi\)](#)  
[Sanford Sherizen](#)
- [Remember, computer data is far from sacred.](#)  
[Dean Pentcheff](#)
- [Outgoing fax numbers and Mercury PIN security](#)  
[Nick Rothwell via Werner Uhrig](#)
- [Info on RISKS \(comp.risks\)](#)

---

### illegal sales of confidential data

*Fernando Pereira <pereira@mbeya.research.att.com>  
Thu, 19 Dec 91 13:54:02 EST*

Associated Press writer Joseph Neff reports from Newark, NJ on 18 Dec 91 that eighteen private investigators and Social Security Administration employees in nine states were charged Wednesday with buying and selling confidential data from SSA and FBI computers. The information included earnings histories and criminal records. The private investigators, many advertising in legal journals, sold the information to companies. If convicted on all counts, the defendants face maximum sentences of 20 to 150 years and multimillion dollar fines.

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)

[Also noted by Mark Seecof <marks@capnet.latimes.com> and Rodney Hoffman <Hoffman.El\_Segundo@Xerox.com>. PGN]



## The London Stock Exchange "Taurus" System

<Brian.Randell@newcastle.ac.uk>

Sat, 21 Dec 91 12:44:17 GMT

The following text constitutes most of the text of an article in yesterday's Financial Times, and is reprinted without permission. (The remaining text is not relevant to RISKS.)

Taurus poised to clear final hurdles

By Richard Walters in London

The UK government appeared yesterday to have overcome legal obstacles to the introduction of Taurus, the London Stock exchange's much delayed computer settlement system. After more of a year of effort by the Department of Trade and Industry lawyers, formal regulations were laid before parliament which would create the legal framework necessary for Taurus. At the same time a safeguard for personal shareholders, which had been built into the Taurus system at the request of ministers has been dropped.

Investors would have had to quote confidential 13-digit personal authorisation codes before being able to deal in their shares. This requirement has now been judged too cumbersome for the small amount of extra security it would have bought. Instead shareholders will be able to tell the registrars who maintain their shareholders only to transfer their shares after they receive written instructions. This extra level of security will be available only to investors who specifically request it.

The legal changes tabled yesterday are needed because share certificates and transfer forms, currently required by law to give evidence of title and enable a change of title to take place, will cease to be produced under the new, paperless system of share ownership and dealing. ...

Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, UK  
PHONE = +44 91 222 7923 FAX = +44 91 222 8232

---

## **Computer Database of Former E. German State Police (Stasi)**

Sanford Sherizen <0003965782@mcimail.com>

Mon, 23 Dec 91 16:18 GMT

An unverified report indicates that a German private detective agency that was thought to be operated by former Stasi members bought a computer database containing the names and salaries of 97,058 members of the Stasi in 1989. The detective agency then pressed charges against the computer specialist who sold them the information. The charges are not indicated, although they may be under the strict (West) German privacy laws. If so, Stasi support for privacy is new. In addition to their prying into the lives of (East) German citizens, the Stasi had agents actively hacking into West German systems, including Berlin's drivers license agency.

Sanford Sherizen, Data Security Systems, Inc., Natick, MASS

---

**Remember, computer data is far from sacred.**

*Dean Pentcheff <dean2@garnet.berkeley.edu>*

*Sat, 21 Dec 91 02:07:18 -0800*

The following "news" message greeted us today (Dec. 21, 1991) here at UC Berkeley. It is curious that the message is dated two days into the future...

U N I X N E W S  
Items ordered most current first.

23 Dec 91 <> Important Information about Computer Systems Court Order <<

We were recently required by order of the Alameda County Superior Court to search files on Garnet and Violet that may contain a particular individual's name within the file. We are complying with that court order.

We think it is important to alert you that files on the shared systems, or even on personal workstations or microcomputers, are subject to search, and even seizure, by court order.

Curtis Hardyck, Vice Provost

[Dean Pentcheff, Department of Integrative Biology, University of California, Berkeley CA 94720 Work Phone: (415) 643-9048]

---

**Outgoing fax numbers and Mercury PIN security**

*Nick Rothwell <nick@dcs.edinburgh.ac.uk>*

*Tue, 17 Dec 1991 10:11:08 +0000*

Perhaps I should explain the subject line... Mercury offer an alternative long-distance telephone network which is available to ordinary users who have the standard British Telecom connections, and which offers improved itemized billing, lower costs, etc. etc. This is implemented by issuing Mercury users with a long personal identification number which represents their account, and which is known only by the user (very much like bank card PIN's, only much longer). Mercury calls are made from standard British Telecom phones by dialing a special prefix followed by the secret Mercury PIN and then the "real" phone number.

See the problem yet? I can't send TelePort faxes this way because the \*destination\* fax number is printed on the cover page. This includes my Mercury PIN which would be compromised by any fax I sent using it. This is a serious drawback.

Possible solutions: (i) suppression of printout of destination fax number on cover sheet (yes, I could use an empty cover sheet, but I want to send faxes from applications like text editors which don't let me paste graphics). Better

option: (ii) provision in the TelePort/Fax software for a "secret prefix" which is dialed for all numbers but not reported on the cover sheet, or a pair of numbers ("reported" and "dialed") for each fax address. (It's possible I'm missing something here in the way long distance codes are specified in the address book - in this case each long distance code would be around 20 digits - might this do what I want?)

Is there no system in the US that works in a similar way to Mercury? Just curious whether anyone in the US is going to come across the same problem.

Nick.



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 12: Issue 72

Tuesday 31 December 1991

## Contents

- [Airbus Fuel monitoring; tanks shown full when they were not](#)  
[John Van Voorhis](#)
- [Recent Novell Software Contains a Hidden Virus](#)  
[John Markoff](#)
- [Has anybody ever been spoofed on the wide network?](#)  
[George Michaelson](#)
- [Re: Whole Earth Review Questions Technology](#)  
[Tom White](#)
- [The Whole Earth is greater than the sum of its parts \(Re: Jerry Mander\)](#)  
[PGN](#)

---

### ✉ Airbus Fuel monitoring; tanks shown full when they were not

*John Van Voorhis <[john@chsun1.spc.uchicago.edu](mailto:john@chsun1.spc.uchicago.edu)>  
Fri, 27 Dec 1991 15:53:18 GMT*

A few weeks ago I flew on an A320 for the first time. Overall the flight was fine; however, we were delayed at the gate while the ground crew tried to fuel the plane. It seems that the computer that ran the the fuel pump onboard the aircraft would not pump in any more fuel, even though the tanks were not full. I do not know how they managed to do it, but eventually they did load on enough fuel to get us from Chicago to Phoenix. Does anyone know how this system works? What happens if the flight or ground crews are careless and just let the computers tell them what is going on? It did not make me feel very safe.

John Van Voorhis, Chapin Hall Center, 1155 E 60th St Chicago, IL 60637  
(312) 753-5983 [john@chsun1.spc.uchicago.edu](mailto:john@chsun1.spc.uchicago.edu)

---

### ✉ Recent Novell Software Contains a Hidden Virus

*"John Markoff" <[markoff@nyt.com](mailto:markoff@nyt.com)>  
Mon, 30 Dec 91 13:16:29 PST*

By JOHN MARKOFF (from the New York Times, 20 Dec 1991)

The nation's largest supplier of office-network software for personal computers has sent a letter to approximately 3,800 customers warning that it inadvertently allowed a software virus to invade copies of a disk shipped earlier this month.

The letter, sent on Wednesday to customers of Novell Inc., a Provo, Utah, software publisher, said the diskette, which was mailed on Dec. 11, had been accidentally infected with a virus known by computer experts as "Stoned 111."

A company official said yesterday that Novell had received a number of reports from customers that the virus had invaded their systems, although there had been no reports of damage.

But a California-based computer virus expert said that the potential for damage was significant and that the virus on the Novell diskette frequently disabled computers that it infected.

#### 'Massive Potential Liabilities'

"If this was to get into an organization and spread to 1,500 to 2,000 machines, you are looking at millions of dollars of cleanup costs," said John McAfee, president of McAfee & Associates, a Santa Clara, Calif. antivirus consulting firm. "It doesn't matter that only a few are infected," he said. "You can't tell. You have to take the network down and there are massive potential liabilities."

Mr. McAfee said he had received several dozen calls from Novell users, some of whom were outraged.

The Novell incident is the second such case this month. On Dec. 6, Konami Inc., a software game manufacturer based in Buffalo Grove, 111. wrote customers that disks of its Spacewrecked game had also become infected with an earlier version of the Stoned virus. The company said in the letter that it had identified the virus before a large volume of disks had been shipped to dealers.

#### Source of Virus Unknown

Novell officials said that after the company began getting calls earlier this week, they traced the source of the infection to a particular part of their manufacturing process. But the officials said they had not been able to determine how the virus had infected their software initially.

Novell's customers include some of nation's largest corporations. The software, called Netware, controls office networks ranging from just two or three machines to a thousand systems.

"Viruses are a challenge for the marketplace," said John Edwards, director of marketing for Netware systems at Novell. "But we'll keep up our vigilance. He said the virus had attacked a disk that contained a help encyclopedia that the company had distributed to its customers.

#### Servers Said to Be Unaffected

Computer viruses are small programs that are passed from computer to

computer by secretly attaching themselves to data files that are then copied either by diskette or via a computer network. The programs can be written to perform malicious tasks after infecting a new computer, or do no more than copy themselves from machine to machine.

In its letter to customers the company said that the Stoned 111 virus would not spread over computer networks to infect the file servers that are the foundation of networks. File servers are special computers with large disks that store and distribute data to a network of desktop computers.

The Stoned 111 virus works by attaching itself to a special area on a floppy diskette and then copying itself into the computer's memory to infect other diskettes.

But Mr. McAfee said the program also copied itself to the hard disk of a computer where it could occasionally disable a system. In this case it is possible to lose data if the virus writes information over the area where a special directory is stored.

Mr. McAfee said that the Stoned 111 virus had first been reported in Europe just three months ago. The new virus is representative of a class of programs known as "stealth" viruses, because they mask their location and are difficult to identify. Mr. McAfee speculated that this was why the program had escaped detection by the company.

#### Steps Toward Detection

Novell has been moving toward adding new technology to its software to make it more difficult for viruses to invade it, Mr. Edwards said. Recently, the company licensed special digital-signature software that makes it difficult for viruses to spread undetected. Novell plans to add this new technology to the next major release of its software, due out at the end of 1992.

In the past, courts have generally not held companies liable for damages in cases where a third party is responsible, said Susan Nycum, a Palo Alto, Calif., lawyer who is an expert on computer issues. "If they have been prudent it wouldn't be fair to hold them liable," she said. "But ultimately it may be a question for a jury."

[Also noted by Werner Uhrig <werner@rascal.ics.utexas.edu>]

---

#### **✂ Has anybody ever been spoofed on the wide network?**

*George Michaelson <G.Michaelson@cc.uq.oz.au>  
Fri, 20 Dec 91 11:16:44 +1100*

In a mailing list for some X.400 s/w development, the 'trustedness' of callers into mail has been raised. There certainly seems to be a feeling that SMTP, in not performing any 'application-level' checks like a password, or some of the 3rd party verification thingies like kerberos is left only with reverse-address lookup to verify who and where the sender system really is.

X.400 provides for a password exchange between the communicating systems,

and also includes a 'turn around' mechanism that permits an inbound caller to switch to being fed outbound queued material. SMTP provides an analogous 'TURN' command, but few of the current implementations support it. Thus X.400 developers are choosing to see this 'two way alternate' mode as a potential security hole, and thus do not implement it.

I don't disagree that a potential hole does exist, but I am interested if anybody in the wider community, especially the Internet and members of PTT provided communities over X.25, is aware of EVER having been hit in this way operationally, by somebody 'spoofing' another machines address and thus forging (in some sense) who they are. I say operationally since many of us at one time or another may have deliberately set a machine to forge somebody elses IP or X.25 address, eg during an extended downtime to provide coverage.

X.25 switches are certainly capable of changing both sender and recipient addresses in processing packets

IP routers can also do this sort of thing.

I do not believe that the 'wider community' has ever yet been hit by an attack where a PTT provided service like X.25, let alone a distributed and self-administered network like the Internet, permitted the sender to mis-represent their network address. end-user identity, doubtless has been compromised countless times. machine-address or network address, I am not so sure has been abused in the wider network.

The holes are pretty obvious. On campus, nobody can really be trusted. Off campus the best you know is the major network-number must be being routed validly, and hence you know a general 'pool' of addresses the real machine could be from.

In X.25, subaddressing can provide similar levels of networking, so you can really only know who is sending the packets to a resolution that matches the PTT billing policy!

I also believe the security risk is identical inbound and outbound: classically people discussing this issue seem to assume 'you' opening a call to 'them' is more trustworthy. I deny this, and say both are equally risky.

I would love to see a general discussion of this, perhaps headers in news need to be re-worked to a more appropriate newsgroup. However I would also like to try and find out if on an operational network, providing a service like e-mail using SMTP and related protocols, if ANYBODY has been knowingly compromised in this way.

I will collate any replies e-mailed to me direct, respecting any request for privacy. Simply being told such an attack HAS taken place will be sufficient if you don't want to go into details.

George Michaelson, The Prentice Centre, University of Queensland  
QLD Australia 4072 +61 7 365 4079

---

## ✂ Whole Earth Review Questions Technology

Tom White <well!tomwhite@apple.com>

Fri, 27 Dec 91 21:17:17 pst

Thanks for the invitation to let readers in the RISKS Forum learn about the unique gathering of writers that Whole Earth Review has brought together to question technology.

Avid online readers can access selected articles from Mead, Dialog and BRS.

WHOLE EARTH REVIEW to Readers:  
Question Technology (while we still have the chance)

Sausalito, CA -- The Winter 1991 issue of WHOLE EARTH REVIEW, the "Access to Tools" quarterly supplement to the WHOLE EARTH CATALOG, questions the political, economic, social and physical effects technology has on our lives. WHOLE EARTH REVIEW also questions its fundamental assumption that providing access to tools is a good and noble enterprise.

Is technological innovation invariably beneficial? Do we control new technologies or do they control us? Will books and libraries become obsolete? These are some of the questions that authors in this special issue attempt to answer. Editor-in-Chief Howard Rheingold writes in the introduction: "Perhaps our readers will be inspired to create new tools for thinking about tools."

Among the authors showcased are Jerry Mander, whose book "In the Absence of the Sacred" is excerpted at length in the lead article; Howard Levine, former director of the National Science Foundation's Public Understanding of Science Program; Langdon Winner, a political theorist and author; Patricia Glass Schuman, president of the American Library Association and of Neal-Schuman Publishers; Linda Garcia, a project director and senior analyst at the Office of Technology Assessment; Gary T. Marx; Ivan Illich; Amory and Hunter Lovins of the Rocky Mountain Institute.

For the past two decades WHOLE EARTH REVIEW has provided its readers "access to tools" -- practical information about technologies ranging from manual post-hole diggers to virtual-computer systems. Subscription price is \$27 for four issues, add \$6 foreign. No advertising accepted.

Copyright 1991, POINT. Permission granted to redistribute freely.  
Whole Earth Review, PO Box 38, Sausalito, CA 94966

CONTACT: Tom White (415) 332-1716: E-mail:tomwhite@well.sf.ca.us

---

## ✂ The Whole Earth is greater than the sum of its parts (Re: Jerry Mander)

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

Mon, 30 Dec 91 13:16:29 PST

Long ago I read an earlier counter-culture book by Jerry Mander, Four Arguments

for the Elimination of Television (Wm Morrow, NY 1978). In PGN's book chapter "Psychosocial Implications of Computer Software 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), I included and discussed the following quote from that Mander book, which in retrospect seems highly relevant to RISKS:

Human beings no longer trust personal observation, even of the self-evident, until it is confirmed by scientific or technological institutions; human beings have lost insight into natural processes that are now exceedingly difficult to observe.

I also summarized Mander's enumeration of eight conditions for the flowering of autocracy and the degeneration of human individuality (loc.cit.), which also seem relevant here...

By the way, HAPPY NEW YEAR to all RISKS READERS. I presume that in the coming year we will see lots more of the same stuff that has concerned RISKS for the past 6.5 years! PGN



Search RISKS using [swish-e](#)

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